Здесь выложен "Систематизированный авторский материал (можно сказать книга) по теории и практике строительства сетей" с сайта http://nag.ru/, склеенный в одну длинную "портянку".

мыло выложившего: nagbook@yandex.ru **Высказаться в гостевой**

ОРИГИНАЛ книги на сайте автора, разбитый на 130 страниц

Телефоны уже вышли из строя,
но, как ни странно, он все еще имел связь
с Юджином благодаря компьютерной сети...
(c) Дэвид Брин.

в Интернет через Ethernet

От соединения двух компьютеров до сети микрорайона

Часть 1.

Теоретические вопросы строительства инфраструктуры Ethernet-провайдера.

    - Сеть небольшой фирмы (40-60 рабочих мест).
    - Особенности практической реализации сети.
- **Глава 6. Домашние (территориальные) сети**.
    - Дилемма 10/100.
    - Основные понятия.
    - Магистральная кабельная система.
    - Выбор топологии в реальных условиях.
    - Абонентская система здания.
- **Глава 7. Электрическая среда передачи данных**.
    - Сети на основе коаксиального кабеля.
    - Витая пара (Twisted Pair).
    - Витая пара (соотношение сигнал и шум)
    - Типы и использование электрических разъемов.
    - Измерение параметров среды передачи.
- **Глава 8. Оптическая среда передачи данных**.
    - Физические параметры оптических волокон.
    - Одномодовые и многомодовые оптические волокна.
    - Разновидности оптоволоконных кабелей.
    - Виды и типы разъемов.
    - Конструкционные элементы (шкафы и муфты).
- **Глава 9. Сетевые протоколы**.
    - Модели коммуникации.
    - Физический уровень.
    - Присоединение к физической среде (PMA).
    - Коммутируемый Ethernet.
    - Канальный уровень.
    - Сетевой уровень.
    - Межсетевой протокол управляющих сообщений (ICMP).
- **Глава 10. Активные устройства**.
    - Повторители и концентраторы.
    - Мосты.
    - Маршрутизаторы.
    - Коммутаторы (Свитчи).
    - Технические параметры коммутаторов.
    - Коммутаторы 3-го уровня.
    - Приоритезация в Ethernet. Продолжение пишется.

Часть 2.

ПРАВОСВЯЗИЕ опыт практической юриспруденции в отрасли "связь" отдельно взятой страны.

- **Глава 1. Введение в правосвязие**.
    - Законы, субъекты и объекты права.
    - Правовые акты.
    - Материальное и процессуальное право.
    - Участники правоотношений: лица.
    - Государственная власть.
    - Государственное принуждение и ответственность субъектов права.
    - Мифология переходного периода.
- **Глава 2. Операторы и государство**.
    - Легализация: выживание или развитие.
    - Лицензирование.

    - Приемка в эксплуатацию объектов связи.
    - Административная и уголовная ответственность в отрасли.
- **Глава 3. Операторы и подрядчики или правила бега по минному полю**.
    - Сертификация: мифы и право.
    - Основы в проектирование сетей.
    - Строительство сетей связи.
    - Немного о метрологии.
    - Свобода и надзор (кто и как нас проверяет).
- **Операторы и пользователи**.
    - Абоненты и клиенты
    - Расчеты, тарифы и карточки
    - Авторское право и контент
    - Агенты и коммерческие представители
- **Практикум (примеры договоров и другие сугубо практические вопросы)**.
    - Договор межсетевого взаимодействия.
    - Абонентский договор.
    - Агентский договор.
    - Аренда оборудования.
    - Аренда помещений для узлов и сетей связи.
- **Заключение**.

Часть 3.

Практические моменты создания и эксплуатации Ethernet-сетей в провайдинге.

- **Глава 1. Прокладки "воздушек"**.
    - ротяжка кабеля через несколько домов.
    - Протяжка кабеля через оживленную улицу. Подготовка.
    - Протяжка кабеля через оживленную улицу. Дорога.
    - Борьба с деревьями.
    - Использование существующих воздушных коммуникаций.
    - Протяжки кабеля по столбам освещения и стенам домов.
    - Крепление и подвес кабеля.
    - Работа с П-296.
    - Отдельные полезные советы.
    - Требования муниципалитетов.
    - Сотрудничество с коммунальными службами.
- **Глава 2. Размещение активного оборудования и кабелей внутри зданий**.
    - Пожаробезопасность внутридомовых узлов.
    - Место размещения узлов.
    - Способы защиты оборудования.
    - Конструкции ящиков.
    - Кабельные линии внутри дома.
- **Глава 3. Работа с оптоволокном**.
    - Три дилеммы.
    - Клеевое соединение. Подготовка.
    - Клеевое соединение. Приклейка и полировка.
    - Сварка, установка муфт.
    - Прочие технологии монтажа оптических разъемов.
- **Глава 4. Электропитание и заземление.**.
    - Термины по "ПУЭ".
    - Заземление (зануление).
    - Молниезащита кабелей.

Глава 1. Обзор сетей передачи данных

Использование сетей, построенных с использованием Ethernet, в провайдинге еще нельзя назвать привычным. Для глубокого понимания роли этой технологии на рынке нужно хорошо представлять путь развития и современное состояние оборудования, используемого в магистральных сетях передачи данных.

Вполне возможно, с ними придется конкурировать. Или использовать, модифицировать под свои нужды, заменять на что-то более современное. Для этого, как минимум, нужно разговаривать на одном языке со связистами. При этом никак не обойтись без знания основных понятий.

Глава 1

История магистральных сетей передачи данных

К сетям передачи данных можно подойти издалека. Тем более, путь прогресса прямым назвать сложно - барабаны и сигнальные костры используются в джунглях до наших дней. Старые технологии соседствуют с новыми. О чем говорить, если даже закон о связи, принятый 16 февраля 1995 года, сегодня выглядит весьма архаичным - для телекоммуникаций это уже практически юрский период (в крайнем случае меловой). А ведь это главный документ, реально регламентирующий деятельность Российских операторов связи (и провайдеров в их числе).

Определение, под которое подпадают в свете действующего законодательства компьютерные сети, используемые для провайдинга, звучит так: "сети электросвязи - технологические системы, обеспечивающие один или несколько видов передач: телефонную, телеграфную, факсимильную передачу данных и других видов документальных сообщений, включая обмен информацией межу ЭВМ, телевизионное, звуковое и иные виды радио- и проводного вещания".

Даже из этого определения видно, что ситуацию, в которую молниеносное развитие технологий за последние десять лет завело связь, простой назвать никак нельзя. Попробую привести аналогию из смежной отрасли. Представьте задачу организации совместной работы отдела, половина которого использует ПЭВМ класса "Нейрон" (клон PC XT Советского производства), а другая недорогие Pentium-III. Плюс немного оргтехники от всех промежуточных этапов развития.

Справедливости ради надо сказать, что это вызывает сложности не только у интернет-провайдеров. Операторы телефонной связи зачастую попадают в еще более тяжелую ситуацию - на них, в дополнение ко всему прочему, давит огромный груз существующих сетей, и полный объем устаревшей законодательной базы. Если разобраться, то система сигнализации ОКС-7 стоит к 2ВСК (челнок) не ближе, чем современные персоналки к компьютерам начала 90-х годов.

В любом случае, для того, что бы выбирать оптимальный путь развития сетей, желательно хотя бы в общих чертах знать, какие технологии использовались в глобальных сетях передачи данных ранее и какие используются сейчас. Это даст возможность сравнивать варианты, понимать возможности, недостатки, и преимущества различных вариантов.

Попробуем посмотреть, в какую глубину десятилетий тянутся коммуникации, использующие цифровые технологии.

Глава 1

Плезиохронная иерархия цифровых потоков E1

Первый цифровой поток установила в 1957 г. компания Bell System. В дальнейшем технология была стандартизована, и теперь известна как T1. Сделано это было для удовлетворения все возрастающих потребностей операторов связи. Местная телефония на родине технологии, в США, на тот момент была сравнительно хорошо развита. Изменений на клиентской сети, состоящей из медных пар, не предвиделось (и не произошло до сих пор). Поэтому основные усилия операторов сосредоточились на

построении магистральных (транспортных) сетей и их эффективного использования для передачи голоса. Естественно, о передаче данных в те времена даже не шло и речи.

Разработанные системы использовали принцип импульсно-кодовой модуляции и методы мультиплексирования (суммирования) с временным разделением каналов (Time Division Multiplexing, сокращенно TDM) для передачи нескольких голосовых каналов, иначе называемых тайм-слотами, в одном потоке данных.

В США, Канаде и Японии за основу был принят поток T1, который со скоростью 1,536 кбит/с передавал 24 тайм-слота, а в Европе (и немного позже в Советском Союзе) - поток E1, имеющий скорость 2,048кбит/с, и позволяющий передавать 30 каналов передачи данных со скоростью 64 кбит/с, плюс канал сигнализации (16 тайм слот) и синхронизации (нулевой тайм-слот). Это без преувеличения казалось вершиной прогресса.

Дальнейшее развитие привело к появлению ещё ряда стандартизированных потоков E2 - E3 - E4 - E5 скоростями передачи данных соответственно 8448 - 34368 - 139264 - 564992 кбит/с. Они получили название плезиохронной цифровой иерархии - PDH (Plesiochronous Digital Hierarchy), которая до сих пор часто используется как для телефонии, так и для передачи данных. Более современные технологии практически полностью вытеснили PDH с оптических коммуникаций, но на устаревших медных кабелях ее позиции до сих пор непоколебимы.

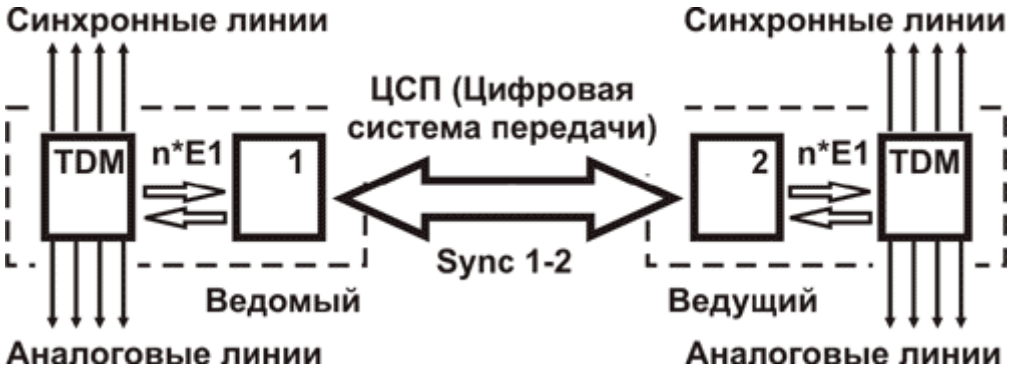

Рис. 1.1. Структура сети PDH.

В каждом устройстве есть свой тактовый генератор, который работает с небольшими отличиями от других. В паре приемопередатчиков ведущий узел задает свою синхронизацию (Sync 1-2), а ведомый подстраивается под него. Единая синхронизация для большой сети отсутствует. Поэтому плезиохронная в данном случае означает "почти" синхронная. Это удобно для строительства отдельных каналов, но вызывает лишние сложности при создании глобальных сетей.

Глава 1

Синхронная цифровая иерархия SDH

По мере объединения сетей различных операторов связи остро встает проблема глобальной синхронизации узлов. Плюс к этому, усложнение топологии вызвало трудности при извлечении из потока составляющих каналов. Технические особенности независимой синхронизации разных узлов (наличие выравнивающих бит) делали это

невозможным. То есть, чтобы извлечь из потока E4 поток E1, необходимо демультиплексировать E4 на четыре E3, затем один из E3 на четыре E2, и только после этого получить нужный E1.

Такой метод существенно увеличивал сложность (особенно высокоскоростных систем), усложнял эксплуатацию и повышал стоимость. В этой ситуации удачным решением стала разработанная в 80-х годах синхронная оптическая сеть SONET, и синхронная цифровая иерархия SDH, которые часто рассматриваются как единая технология SONET/SDH.

Преобразование и передача данных в этой системе достаточно сложны, и механизм выходит далеко за рамки этой книги. Нужно отметить лишь несколько моментов. В качестве минимальной "транспортной" единицы используется контейнер, размер полезной нагрузки которого составляет 1890 байтов, а служебной части - 540 байтов.

Для безболезненного внедрения на рынок эта технология должна была быть совместимой с имеющимся оборудованием и потоками PDH. Это условие было соблюдено, и сегодня SDH составляют основу подавляющего большинства транспортных сетей во всем мире.

Упрощенно, их можно рассматривать как некоторое количество каналов T1/E1, объединенных (мультиплексированных) в один Sonet/SDH канал. При этом какая либо связь между потоками, или их изменение, не предусматривается (если не считать появившихся позже и сравнительно малораспространенных кросс-коннекторов).

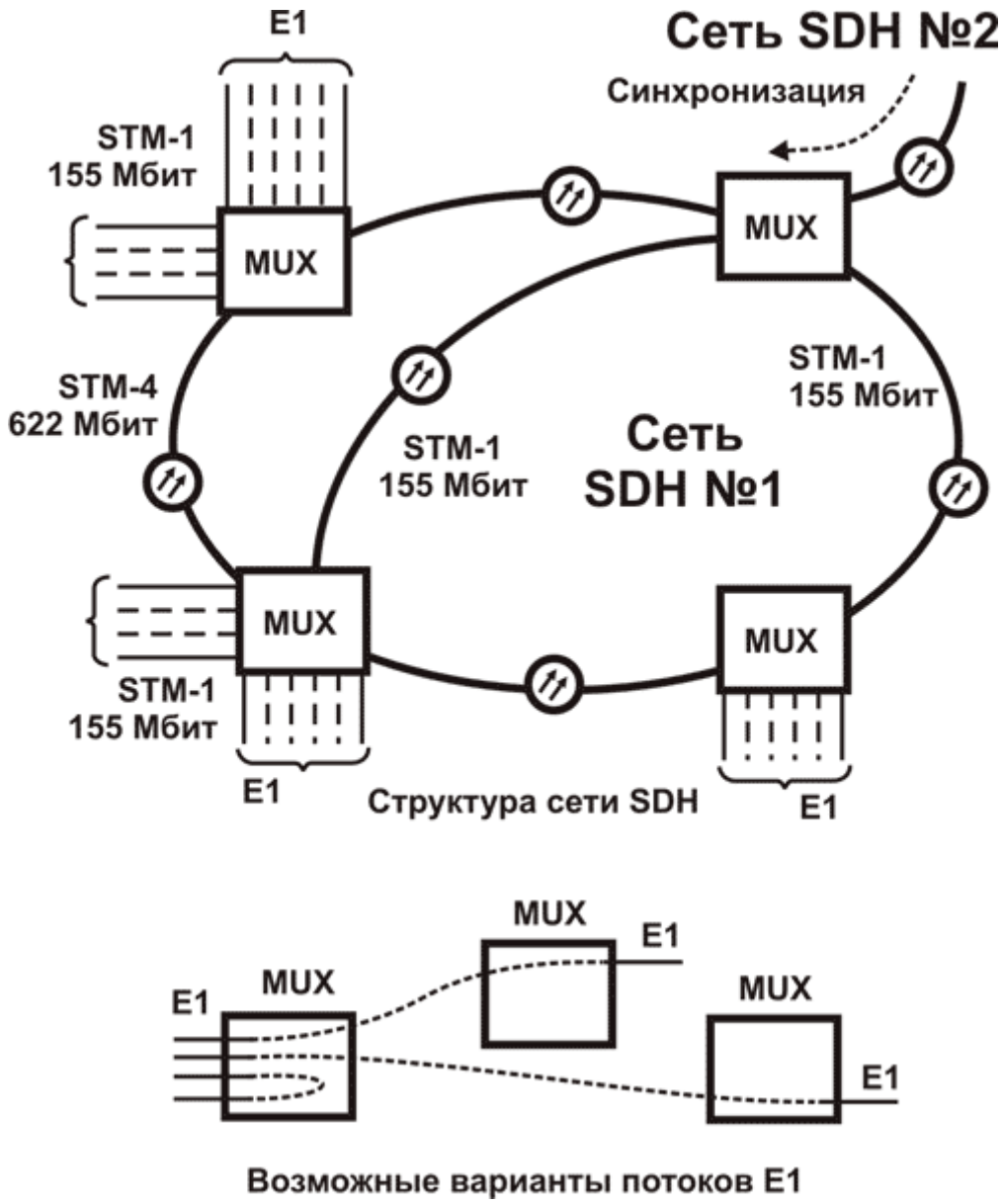

Рис. 1.2. Структура транспортной сети Sonet/SDH и схема возможных вариантов прохождения потоков E1.

Можно видеть, что такая схема создавалась строго под нужды телефонии. Действительно, мультиплексоры (MUX) обычно устанавливаются на АТС, где потоки E1 (собранные с других мультиплексоров) переводятся в медные аналоговые линии. Оптимизация пропускной способности сети (иначе говоря, межстанционных соединений) достигается подбором соотношения количества абонентских линий и используемых потоков. Способ не слишком экономичный, зато простой и понятный.

Так как скорости в сети используются вполне приличные (уровень STM-1 - 155 Мегабит, STM-4 - 622 Мегабита, STM-16 - 2,4 Гигабита), то даже использование низкоскоростных кодеков и подавления пауз не получило особого распространения.

Но для передачи данных статическая структура точка-точка, мягко говоря, не слишком удобна. Плюс принципиально не решенный вопрос последней мили: Наверно поэтому SDH очень редко используется для передачи данных напрямую. Это стало задачей протоколов, использующих SDH в качестве магистрального транспорта.

Глава 1

Коммутация пакетов на примере Frame Relay

Первой технологией, соединяющей глобальные и локальные сети, была X.25, которая сегодня постепенно отмирает. Более прогрессивными стали появившиеся в 1984 году сети Frame Relay. При их использовании данные разделяются на кадры (фреймы) разной длины передающим устройством, причем каждый кадр содержит заголовок с адресом получателя. После передачи они собираются на приемном конце. Максимальная скорость передачи данных в ранних версиях составляла 2 Мбита. Позже у некоторых вендоров появились варианты, поддерживающие скорости до 44,725 Мбит/с, но широкого распространения, в связи с появлением ATM, они не успели получить.

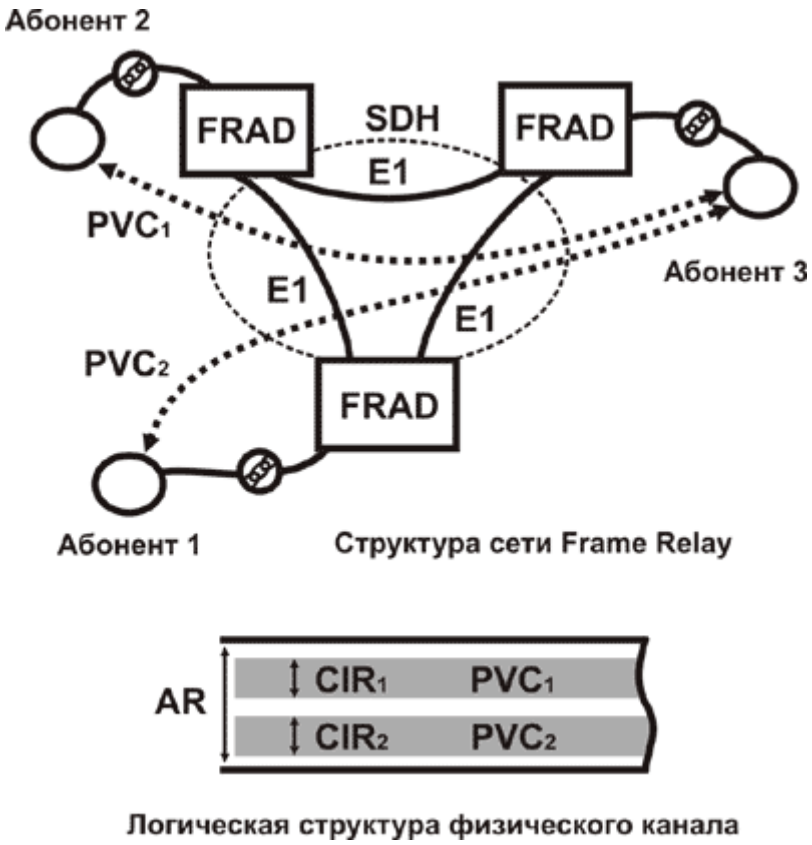

Рис. 1.3. Схема сети Frame Relay

Для каждого типа трафика может задаваться свой виртуальный канал (PVC), и соответственно может быть организована своя топология соединений. Скорость регулируется параметрами CIR (минимальная информационная скорость) и AR (скорость физического канала). Для соединения узлов Frame Relay обычно используется сеть SDH, а для организации каналов менее чем E1 - мультиплексоры TDM. На практике скорости более 128 кбит используются редко - более быстрое оборудование для соединения на "последней миле" появилось совсем недавно и успело устареть до своего широкого внедрения.

К достоинствам технологии можно отнести высокий уровень защиты данных, что в совокупности с прозрачность FR для протоколов более высокого уровня снискало ему популярность в кругах распределенных банковских и корпоративных сетей.

Глава 1

Универсальная технология ATM

Примерно на этом же этапе (разработана в 1974 году, стандартизована в 1984), возникла технология цифровой сети интегрального обслуживания - ISDN (Integrated Service Digital Network), которая обеспечивает передачу данных по медным проводам со скоростью до 144 Кбит/с.

В отличие от Frame Relay, ISDN была изначально ориентирована на два типа передачи - голоса и данных. Достигалось это благодаря развитым средствам приоритезации трафика. Но из-за низких скоростей передачи ISDN (обычно 64кбит/с), быстро возникла идея новой широкополосной технологии, названной ATM (Asynchronous Transfer Mode, или режим асинхронной передачи), которая принципиально может применяться на различных скоростях (от 1,5 Мбит/с до 40 Гбит/с). К большим ее достоинствам можно отнести возможность относительно простого "наложения" на существующие сети SDH.

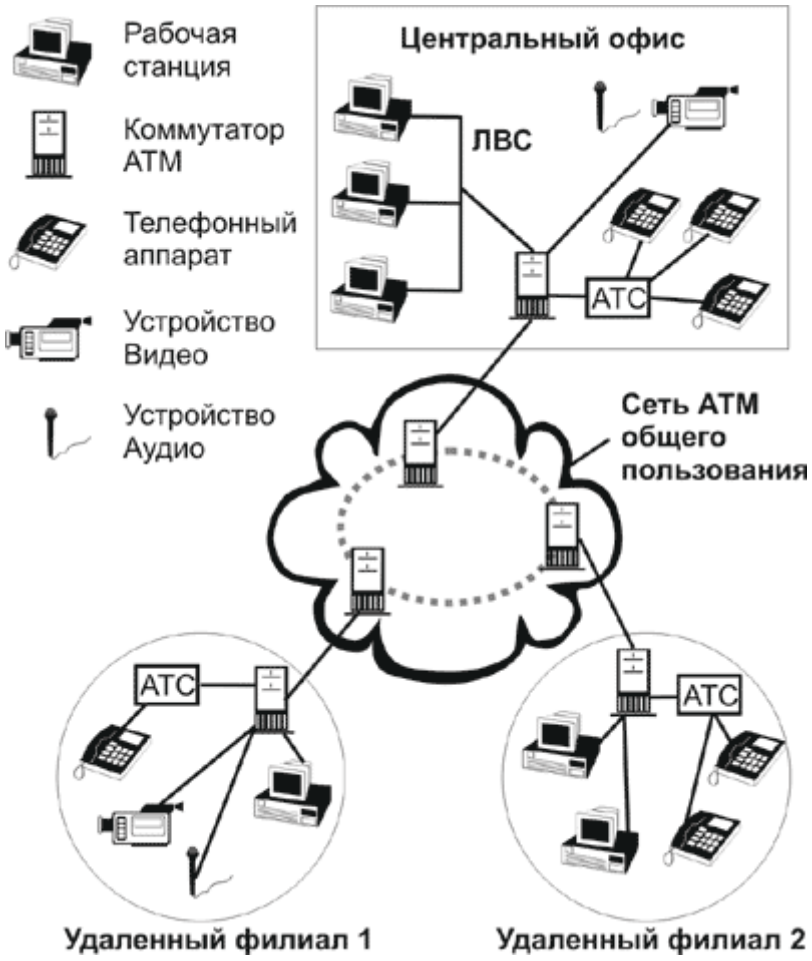

Рис. 1.4. Схема сети ATM

Этот момент можно по праву назвать поворотным в истории коммуникаций. Уже успела сформироваться исторически узкая специализация транспортных сетей. Для каждого вида связи существовала, по, меньшей мере, одна сеть, которая передает информацию этой службы. Имелось большое количество выделенных структур, каждая из которых

требовала собственного этапа разработки, производства и дорогостоящего технического обслуживания. Хуже того, свободные ресурсы одной сети не могли быть использованы другой - и это при очень дорогих физических каналах.

ATM изначально разрабатывалась как универсальная и "академически правильная" технология, не зависящая от типа передаваемого трафика. Её могут использовать все существующие службы, так как ATM определяет протоколы на уровнях выше физического.

При условии, что все виды информации транспортируются одним методом, возможно проектирование, создание, управление и обслуживание одной сети. Это сокращает затраты и делает её (в теории) наиболее экономичной транспортной сетью электросвязи на сегодняшний день.

Несмотря на такой перечень достоинств, путь ATM не был легок. Как любое универсальное средство, эта технология уступала другим во многих частных случаях. Оборотная сторона универсальности, избыточная сложность, влекла удорожание, и часто выливалась в большое количество неполадок не только на этапе внедрения, но и на начальных стадиях эксплуатации.

Поэтому в сферу локальных сетей ATM проникнуть не смогла, и была вытеснена Ethernet в телекоммуникацию. Там, при отсутствии реальной альтернативы, именно ATM в настоящий момент принято рассматривать как основную технологию при построении транспортных сетей. Более дешевый и простой Ethernet только начинает теснить ее с занимаемых позиций. Но об этом пойдет речь в следующих главах.

Если в общем оценить состояние отрасли связи в настоящий момент, то это Sonet/SDH, который используют в качестве транспорта ATM и Frame Relay. Последние, в свою очередь, связывают локальные сети конечных пользователей ресурсов сети передачи данных.

Глава 1

Основные методы коммутации

Для обобщения материала рассмотрим объяснение физической сущности описанных выше методов переноса информации. Основные режимы переноса информации, используемые в сетях связи, следующие:

- коммутация каналов,
- многоскоростная коммутация каналов,
- быстрая коммутация каналов,
- быстрая коммутация пакетов,
- коммутация пакетов или кадров.

Передача голоса в телефонии - классический пример канала. Если объединить несколько каналов в один поток, то появится необходимость управлять, или коммутировать отдельные каналы. Делается это для транспортировки данных в аналоговых сетях телефонной связи (и узкополосных цифровых сетях) на основе временного разделения

потока (например, E1). Причем для передачи информации по каждому каналу используется один или несколько фиксированных временных интервалов (тайм-слотов).

Данный метод, по сути, лишен гибкости, так как продолжительность временного интервала (количество тайм-слотов) однозначно определяет скорость передачи. Передаются в канале данные, или нет - место в потоке занято постоянно. Поэтому, коммутация каналов не лучший способ использовать магистральные сети.

Метод многоскоростной коммутации каналов был разработан для устранения недостатков предыдущего решения. В этом случае использовалось несколько каналов с различными временными интервалами и, следовательно, скоростями передачи. Однако недостатки оставались - при занятости низкоскоростного канала ни одно низкоскоростное соединение не могло быть установлено, даже при наличии не занятых более высокоскоростных каналов.

Технология быстрой коммутацией каналов, основана на тех же методах временного разделения, но соединение устанавливается только тогда, когда требуется передача данных. Хорошей иллюстрацией будет пример телефонного разговора. При коммутации и многоскоростной коммутации каналов будет установлено одно соединение на всю длительность разговора, а при быстрой коммутации будет установлено множество последовательных соединений, каждое из которых служит для передачи конкретного фрагмента речи.

Эффективность использования канала в последнем случае достаточно высокая, но минусы метода то же велики. Уже нет гарантированной задержки, так важной для передачи голоса. Да и сложность (а значит, и стоимость) программно-аппаратного комплекса увеличивается в разы. Все это приводит к тому, что на практике используется в основном простая коммутация каналов с синхронной иерархией Sonet/SDH.

Для передачи данных между компьютерными сетями, а с появлением коммутаторов и внутри локальных сетей, используются методы коммутации пакетов или кадров. И кадр, и пакет в общем случае могут иметь разную длину, и выделяются из общего массива информации только благодаря специальным последовательностям символов (флагам, заголовкам).

Классическим примером коммутации кадров является протокол Frame Relay (ретрансляция кадров). При передаче информация разных пользователей или служб передается по одному потоку (каналу), а коммутаторы выполняют функции определения маршрута данных и создания и хранения очередей пакетов/кадров при перегрузке транспортной системы.

Популярный в настоящее время "классический" Ethernet построен еще проще. Механизмы работы с очередями не предусмотрены, а вместо определения полного маршрута "заранее" используется более простая маршрутизация каждого пакета данных, причем только на пограничных узлах. Внутри сети пакеты передаются всем пользователям.

Но если рассматривать проблему с точки зрения метода переноса информации Frame Relay и Ethernet близки. И обладают общим существенным недостатком - не могут гарантировать постоянной скорости.

Тут надо сделать существенное дополнение. Современный Frame Relay имеет развитые механизмы управления скоростью, позволяющие обойти этот недостаток. То же самое

можно сказать и про коммутируемый Ethernet - новое оборудование вполне надежно использует механизмы очередей, приоритизации трафика, и другие атрибуты транспортных сетей.

Примером метода быстрой коммутации пакетов является ATM. Для достижения временной прозрачности применен метод, при котором информация всех типов сначала разбивается на пакеты малой фиксированной длины (53 байта, из них - 5 байт заголовок), называемые ячейками. Которые затем мультиплексируются в едином цифровом тракте. При этом ячейки, в зависимости от принадлежности к типу службы, могут иметь разный приоритет.

Если подходить строго, то ATM нельзя назвать методом быстрой коммутации пакетов. Ячейка хоть и мала, но имеет вполне конечную длину, и даже один байт информации вызовет передачу всего пакета. По той же причине, нельзя сказать, что в полной мере обеспечивается гарантированная постоянная скорость. Разумеется, при реальном использовании смело можно не обращать внимания на сделанные допущения. Но для понимания сути процессов желательно про них помнить.

Материал по основам сетей передачи данных, на мой взгляд, достаточно сложен для восприятия. Но, не определившись с основами, трудно будет составить целостное понимание места и роли той или иной технологии в современном мире телекоммуникаций.

Перед переходом к следующему "тяжелому" блоку попробуем немного расслабиться, и отвлечься от технических деталей.

Глава 1

Немного о сети сетей

Вспомним о том, что уже более трех десятков лет так сильно подстегивает развитие технологий передачи данных. Ведь именно Интернет дает львиную долю той самой информации, которая передаются по сетям электросвязи. И именно ему они обязаны головокружительным ростом. Поэтому, их нельзя разделять ни в технических, ни в бизнес-рассчетах - как нельзя разделять две стороны одной медали.

Предыстория Интернет начинается с 1966 года, когда Ларри Робертс пришел в DARPA с идеей распределенной (не имеющей центрального компьютера) сети - ARPAnet (Advanced Research Projects Agency Network). В 1968 начали работать совместно четыре станции, в 1969 принят первый RFC (Request for Comment) "Программное обеспечение узла" Steve Crocker.

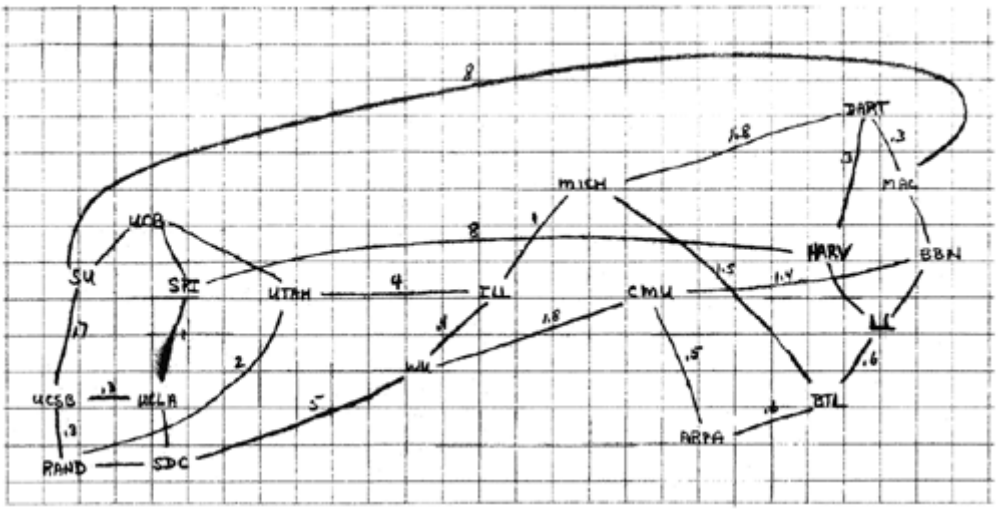

Рис. 1.5. Схема ARPAnet конца 60-х годов.

В 1972 произошел "выход в свет" - международная конференция с демонстрацией сети из 40 машин. 1982 - оформление протоколов ARPA в знакомое сегодня всем семейство TCP/IP.

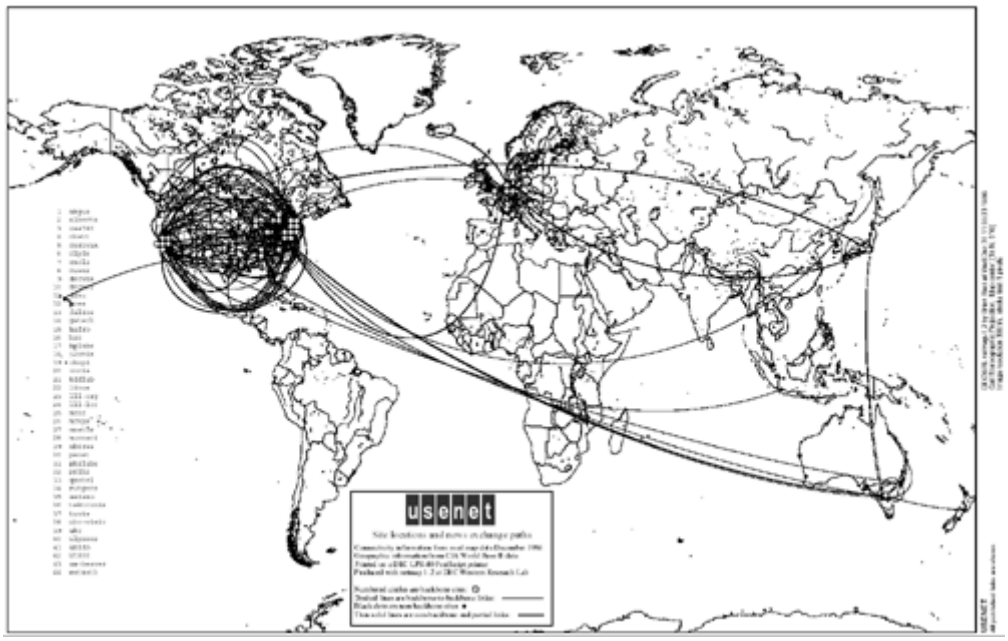

Рис. 1.6. Схема ARPAnet 1982 года.

Но реальным рождением этого восьмого чуда света можно считать объединение шести крупных IP-сетей США в единую научную сеть NSFNET в 1986 году. Свою основополагающую роль NSFNET сохраняла до 1996 года, после чего сменила свою роль на менее значимую.

Всемирная паутина - World Wide Web (WWW) появилась много позже, в 1992 году. Точно известен автор - Тим Бернерс-Ли из Европейского центра ядерных исследований (CERN), расположенного в Женеве, Швейцария. Мало кому известная, появившаяся за счет энтузиазма, технология обеспечила лавинообразный рост Интернет, и тот океан информации, который мы видим сейчас. Рубежом можно считать 1993 год, когда

количество подключенных серверов перевалило за миллион. После этого пропали последние сомнения в перспективах сети сетей.

Менее десятилетия спустя, сложно отделаться от мысли, что Интернет представляет из себя что-то большое, цельное. Существующее помимо воли отдельных людей. С философской точки зрения это, пожалуй, соответствует действительности. Но в техническом плане все по другому. Даже присоединяя свой компьютер при помощи модема к узлу интернет сервис провайдера, вы делаете его полноправным участником всемирной сети. Который может (в теории) пользоваться такими же правами, как и любой другой узел.

Ведь Интернет представляет собой не более, чем сеть связанных друг с другом компьютерных систем и различных компьютерных служб. Иначе говоря, является совокупностью различных компонентов. Таких, например, как электронная почта, телеконференции, WWW или FTP.

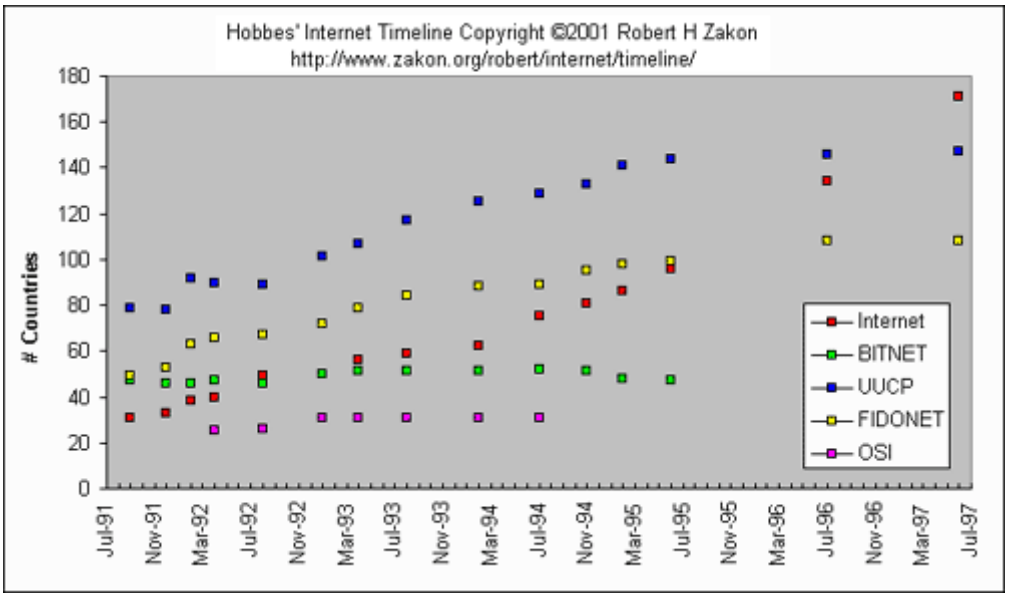

Рис. 1.7. Количество узлов разных типов сетей. Только в 1997 году Internet стала самой большой сетью.

Видимость единства Интернет создается единой системой адресации и доменных имен, которые назначаются специальной организацией под названием IANA. Для этого существует продуманная иерархическая схема, которая гарантирует уникальность каждого имени. В следующих главах, посвященных маршрутизации, этот вопрос будет рассмотрен более подробно.

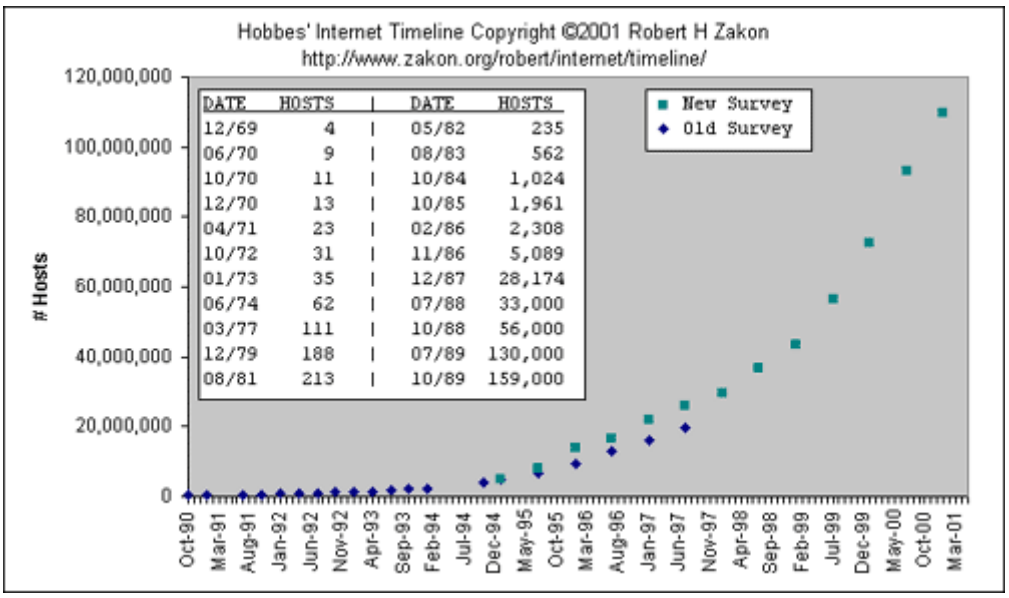

Рис. 1.8. Количество хостов Интернет.

В данном контексте надо лишь особо отметить, что Интернет далеко не единственная глобальная сеть, которая существует в мире. Она лишь самая крупная из многих.

История интернет в России

Обратимся к истории Интернет в России (или Советском Союзе). Отсчитывают ее с 1982, когда Курчатовский институт начал разрабатывать unix-подобную операционную систему. К 1986 году появилась сеть из трех узлов Демос - КИАЭ - СП Диалог. Там же в начале 1990 года состоялся первый сеанс связи с зарубежными сетями Интернет (Хельсинки). И уже к осени 90-го сложилось ядро UUCP'шной сети СССР. Узлы общались друг с другом по dial-up (скорость 1200/2400), то есть выделенных линий не было. Но это не помешало уже в сентябре зарегистрировать домен .SU.

В феврале 1991 был запущен первый в России междугородний канал связи на протоколе TCP/IP. Работал он по модему между Москвой и Барнаулом на скорости 9600 бод. А к середине этого же года в Советском Союзе уже существовала коммерческая сеть Релком, первоначально организованная Демосом. Вообще говоря, история достаточно запутанная, и имеется несколько вариантов развития событий. Но, в рамках данной книги, это не слишком важно.

Постепенно новая технология вошла в моду, а движение от сетей "академического" назначения к коммерческой передаче данных стало массовым. Назвать его быстрым и согласованным нельзя (разумеется, по меркам Интернета). Известны и громкие скандалы, и успехи. Но общим было то, что развитие шло скорее за счет энтузиазма и веры в будущее, чем реальных доходов.

Некоторое изменение ситуации стало заметно только в 1994 году. Быстро начало расти количество пользователей. 7 апреля зарегистрирован домен .RU, зеверивший официально существование Интернета в России. А в начале ноября начал выходить первый в Рунете гипертекстовый журнал т.е. заработал протокол http.

Далее "писаная" история сетей плавно превратилась в историю контента - видимой стороны передачи данных. Романтика кончилась - началась будничная инженерная

работа. В фокус общественного интереса вышли совсем другие персонажи. Это понятно, и, скорее всего, правильно. Проекты, решения, согласования, нормы, правила: Все то, что сопровождает современный провайдинг, мало кому интересно.

Подобное развитие событий (разумеется, в значительно меньшем масштабе) ждет и домашние (кампусные, территориальные, районные) сети. Экзотичность решений, новизна, поиск места на рынке еще не стали историей. Но они уже позади. Начинается серьезная инженерная работа.

Ethernet is a trademark of Xerox,
Intel and Digital Equipment Corp.

Глава 2. Технологии локальных сетей.

Перейдем от технологий построения транспортных коммуникаций к локальным сетям. Различия большие даже на первый взгляд. Изначально они были продиктованы разной физической основой среды передачи (организации канала). Проблема совместимости с телефонной инфраструктурой отсутствовала, с полосой пропускания кабелей (в основном коаксиальных) то же проблем не возникало. Ограничения в основном накладывала скорость работы элементной базы конечного оборудования.

Думаю, не надо рассказывать о скорости прогресса последнего десятилетия в полупроводниковой индустрии. Сетевое оборудование постигла судьба всей отрасли. Лавинообразный рост производства, большие скорости и минимальные цены. В 1995 году, который считается переломным для Интернет, было продано около 50 миллионов новых портов Ethernet. Неплохой задел для доминирования на рынке, которое за следующие 5 лет стало подавляющим.

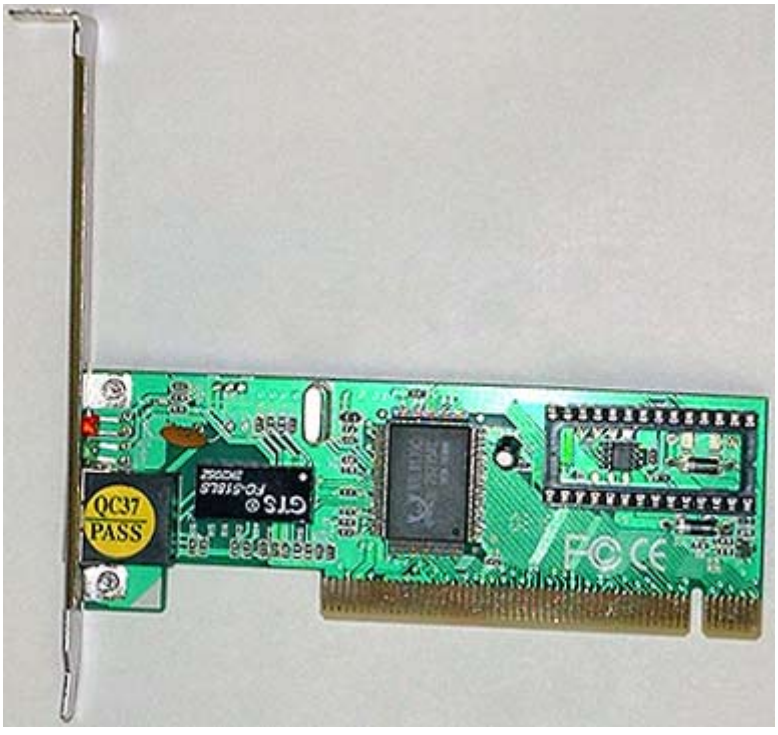

Рис. 2.1. Сетевой адаптер 10/100 стоимостью $6. Истинный победитель в гонке технологий.

Для специализированного телекоммуникационного оборудования такой уровень цен недоступен. Сложность устройства при этом не играет особой роли - вопрос скорее в количестве. Сейчас это кажется вполне естественным, но еще 10 лет назад безусловное господство Ethernet было далеко не очевидным (например, в промышленных сетях до сих пор нет явного лидера).

Однако, только в сравнении с другими способами построения сетей, можно показать преимущества (или недостатки) сегодняшнего лидера.

Глава 2

Физические принципы, в соответствии с которыми функционирует оборудование, не слишком сложны. По методу получения доступа к среде передачи, их можно разделить на два класса - детерминированные и недетерминированные.

При детерминированных методах доступа передающая среда распределяется между узлами с помощью специального механизма управления, гарантирующего передачу данных узла в течение некоторого интервала времени.

Наиболее распространенными (но далеко не единственными) детерминированными методами доступа являются метод опроса и метод передачи права. Метод опроса мало применим в локальных сетях, но широко используется в промышленности для управления технологическими процессами.

Метод передачи права, наоборот, удобен для передачи данных между компьютерами. Принцип работы состоит в передаче по сети с кольцевой логической топологией служебного сообщения - маркера.

Получение устройством маркера предоставляет ему право на доступ к разделяемому ресурсу. Выбор у рабочей станции в этом случае ограничен лишь двумя вариантами. В любом случае она должна отправить маркер следующему по очереди устройству. Причем сделать это после доставки данных адресату (при их наличии), или сразу (при отсутствии информации, нуждающейся в передаче). На время прохождения данных маркер в сети отсутствует, остальные станции не имеют возможности передачи и коллизии невозможны в принципе. Для обработки возможных ошибок, в результате которых маркер может быть утерян, существует механизм его регенерации.

Недетерминированные - случайные методы доступа. Предусматривают конкуренцию всех узлов сети за право передачи. Возможны одновременные попытки передачи со стороны нескольких узлов, в результате чего возникают коллизии.

Наиболее распространенным методом такого типа является CSMA/CD (carrier-sense multiple access/collision detection) - множественный доступ с контролем несущей / обнаружением коллизий. Перед началом передачи данных устройство "прослушивает" сеть, чтобы убедиться, что никто больше ее не использует. Если среда передачи в данный момент кем-то используется, адаптер задерживает передачу, если же нет, то начинает передавать.

В том случае, когда два адаптера, обнаружив свободную линию, начинают передачу одновременно, происходит коллизия. При ее обнаружении обе передачи прерываются, и

устройства повторяют передачу спустя некоторое случайное время (естественно, предварительно опять "прослушав" канал на предмет занятости). Для получения информации устройство должно принимать все пакеты в сети, чтобы определить, не оно ли является адресатом.

Глава 2

История и развитие Ethernet

Начать рассмотрение с какой-либо другой технологии означает не учитывать реальное значение, которое Ethernet играет в мире локальных сетей. Волею ли сложившихся обстоятельств, или технических преимуществ, но конкуренции он на сегодня не имеет, занимая около 95% рынка.

Днем рождения Ethernet считается 22 мая 1973 г. Именно тогда Роберт Меткалф (Robert Metcalfe) и Дэвид Боггс (David Boggs) опубликовали описание экспериментальной сети, построенной ими в Исследовательском центре Xerox. Базировалась она на толстом коаксиальном кабеле и обеспечивала скорость передачи данных 2,94 Мбит/с. Новая технология получила имя Ethernet (эфирная сеть), в честь радиосети Гавайского университета ALOHA, в которой был использован схожий механизм разделения среды передачи (радиоэфира).

К концу 70-х годов под Ethernet была подведена солидная теоретическая база. А в феврале 1980 года фирма Xerox, совместно с DEC и Intel, представила разработку IEEE, которая спустя 3 года утвердила ее в качестве стандарта 802.3.

Метод получения доступа к среде передачи данных у Ethernet недетерминированный - множественный доступ с контролем несущей и обнаружением коллизий (CSMA/CD). Говоря проще, устройства разделяют среду передачи хаотично, случайным образом. При этом алгоритм может приводить к далеко не равноправному разрешению соперничества станций за доступ к среде. Что, в свою очередь, может породить длительные задержки доступа, особенно в условиях перегрузки. В экстремальных случаях скорость передачи может упасть до нуля.

Рис. 2.2. Схема "классического Ethernet"

Из-за такого неупорядоченного подхода долгое время считалось (и считается до сих пор), что Ethernet не обеспечивает качественной передачи данных. Предсказывалось его вытеснение сначала маркерным Tokeng Ring, потом ATM: Но реалии оказались прямо противоположными.

Во многом это произошло благодаря большим изменениям, которые претерпел Ethernet за время своего 20-ти летнего пути. Тот "гигабит" в полном дуплексе, который мы видим сейчас уже в сетях начального уровня, очень мало похож на родоначальника семейства 10base5. В то же время, после введения 10base-T совместимость сохраняется как на уровне взаимодействия устройств, так и на уровне кабельной инфраструктуры (!).

Развитие от простого к сложному, рост вместе с потребностями пользователей - вот вероятный ключ невероятного успеха технологии. Судите сами:

- Март 1981 - фирмой 3com представлен Ethernet-трансивер.
- Сентябрь 1982 - первый сетевой адаптер для персонального компьютера.
- 1983 - появление спецификации IEEE 802.3, определена шинная топология сети 10base5 (толстый Ethernet) и 10base2 (тонкий Ethernet). Скорость передачи 10 Мбит/сек. Определено предельное расстояние между точками одного сегмента - 2,5 км.
- 1985 - выпущена вторая версия спецификации IEEE 802.3 (Ethernet II), в которой были внесены небольшие изменения в структуру заголовка пакета. Сформирована жесткая идентификация Ethernet устройств (MAC - адреса). Был создан список адресов, в котором любой производитель может зарегистрировать уникальный диапазон (сейчас это стоит всего $1250).

- Сентябрь 1990 - IEEE утверждает технологию 10baseT (витая пара) с физической топологией звезда и концентраторами (hub). Логическая топология CSMA/CD не изменилась. В основу стандарта легли разработки SynOptics Communications под общим названием LattisNet.
- 1990 - фирма "Kalpana" (впоследствии быстро купленная вместе с разработанным коммутатором CPW16 начинающим гигантом "Cisco") предлагает технологию коммутации, основанную на отказе от использования разделяемых линий связи между всеми узлами сегмента.
- 1992 - начало применения коммутаторов (swich). Используя адресную информацию, содержащуюся в пакете (MAC адрес), коммутатор организует независимые виртуальные каналы между парами узлов. Коммутация фактически незаметно для пользователя преобразует недетерминированную модель Ethernet (с конкурентной борьбой за полосу пропускания), в систему с адресной передачей данных.
- 1993 - спецификации IEEE 802.3x, появляется полный дуплекс и контроль соединения для 10baseT, спецификация IEEE 802.1p добавляет групповую адресацию и 8-ми уровневую систему приоритетов. Предложен Fast Ethernet:
- В июне 1995 введен Fast Ethernet стандарт IEEE 802.3u (100BaseT).

На этом историю можно закончить - Ethernet принял вполне современные очертания. Развитие технологии на этом, конечно, не остановилось. Но об этом речь пойдет немного позже.

Глава 2

Незаслуженно забытый ARCnet

Attached Resourse Computing Network (ARCnet) - сетевая архитектура, разработанная компанией Datapoint в середине 70-х годов. В качестве стандарта IEEE ARCnet принят не был, но частично соответствует IEEE 802.4 как сеть с передачей маркера (логическое кольцо). Пакет данных может иметь любой размер в пределах от 1 до 507 байт.

Из всех локальных сетей Arcnet обладает самыми широкими возможностями в области топологий. Кольцо, общая шина, звезда, дерево может быть использованы в одной сети. Плюс к этому можно использовать весьма протяженные сегменты (до нескольких километров). Такие же широкие возможности имеются и по использованию среды передачи - годится коаксиальный, оптоволоконный кабель, витая пара.

Доминировать на рынке этому недорогому стандарту помешало малое быстродействие - всего-то 2,5 Мбит/с. И когда в начале 90-х Datapoint разработала ArcNet PLUS со скоростью передачи до 20 Мбит/с, время было уже упущено. Fast Ethernet не оставил ArcNet ни малейшего шанса на широкое применение.

Тем не менее, в пользу большого (но так и не реализованного) потенциала этой технологии можно сказать, что в некоторых отраслях (обычно АСУТП) сети живут до сих пор. Детерминированный доступ, возможности автоконфигурирования, согласования скорости обмена в диапазоне от 120 Килобит/с до 10 Мбит/с, в сложных условиях реального производства бывают просто незаменимы.

Кроме этого, Arcnet обеспечивает необходимую для систем управления возможность точно определять максимальное время доступа к любому устройству в сети при любой

нагрузке по простой формуле: T = (TDP + TOBoNb)oND, где TDP и TOB -времена передачи пакета данных и одного байта, зависящие от выбранной скорости передачи, Nb - количество байтов данных, ND - количество устройств в сети.

Глава 2

Token Ring. Классический пример передачи маркера.

Еще одна технология, берущая свое начало в 70-х годах. Разработка голубого гиганта IBM, основа стандарта IEEE 802.5, она имела больше шансов на успех, чем многие другие.

Token Ring является классической сетью с передачей маркера. Логическая топология (и физическая в первых версиях сети) - кольцо. Более современные модификации построены на витой паре по топологии "звезда", и с некоторыми оговорками, совместимы с Ethernet.

Изначальная скорость передачи, описанная в IEEE 802.5, составляет 4 Мбит/с, однако существует более поздняя реализация на 16 Мбит/с. Из-за более упорядоченного (детерминированного) метода доступа к среде, Token Ring на ранних этапах развития часто продвигался как более качественная замена Ethernet.

Несмотря на существование схемы приоритетного доступа (который назначался каждой станции в отдельности), обеспечить постоянный темп передачи битов (Constant Bit Rate, CBR) не удавалось по весьма простой причине. Приложений, которые могут использовать преимущества этих схем, тогда не существовало. Да и в настоящее время их не стало больше.

Без этого можно было только гарантировать, что производительность снизится для всех станций сети в равной мере. Для победы в конкурентной борьбе этого не могло сыграть решающую роль, и сейчас найти реально работающую сеть Token Ring практически невозможно.

Глава 2

FDDI - первая локальная сеть на оптоволокне

Технология Fiber Distributed Data Interface (FDDI) была разработана в 1980 году комитетом ANSI. Это была первая компьютерная сеть, использовавшая в качестве среды передачи только оптоволоконный кабель. Причиной разработки была недостаточная в то время скорость (не более 10 Мбит/с) и надежность (отсутствие схем резервирования) локальных сетей. Так же, это была первая (и не слишком удачная) попытка вывести сети передачи данных на "транспортный" уровень, составив конкуренцию SDH.

Стандарт FDDI оговаривает передачу данных по двойному кольцу оптоволоконного кабеля со скоростью 100 Мбит/с, что позволяет получить надежный (зарезервированный)

и быстрый канал. Расстояния вполне глобальные - до 100 км по периметру. Логически работа сети была построена на передачи маркера.

Дополнительно предусматривалась развитая схема приоритезации трафика. Сначала рабочие станции разделялись на два вида - синхронные (имеющие постоянную полосу пропускания), и асинхронные. Последние, в свою очередь, распределяли среду передачи с помощью восьмиуровневой системы приоритетов.

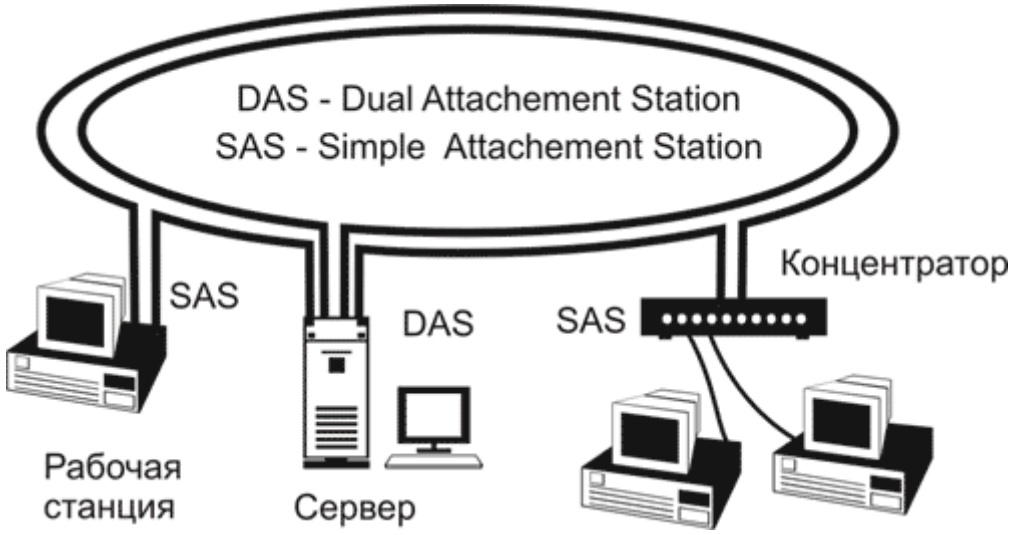

Рис. 2.3. Кольцо FDDI

Несовместимость с сетями SDH не позволила FDDI занять сколь-нибудь значимую нишу в области транспортных сетей. Сегодня эта технология практически вытеснена ATM. С другой стороны, высокая стоимость не оставила шансов в борьбе с Ethernet в локальной нище. Не помогли стандарту и попытки прейти на более дешевый медный кабель. Технология CDDI, основанная на принципах FDDI, но с применением в качестве среды передачи витой пары, популярностью не пользовалась, и сохранилась только в учебниках.

Глава 2

Разработка AT&T и HP - 100VG-AnyLAN

Как и FDDI, эту технологию можно отнести ко второму поколению локальных сетей. Создавалась она в начале 90-х, совместными усилиями компаний AT&T и HP, как альтернатива технологии Fast Ethernet. Летом 1995 года он практически одновременно со своим конкурентом получила статус стандарта IEEE 802.12. И имела неплохой шанс на победу благодаря своей универсальности, детерминированности и более полной, чем Ethernet, совместимости с существующими кабельными сетями (витая пара Категории 3).

Схема квартетного кодирования Quartet Coding, использующая избыточный код 5B/6B, позволяла использовать 4-х парную витую пару Категории 3, которая была тогда распространена едва ли не более, чем современная 5 категория. Переходный период, по сути, не затронул Россию, в которой из-за более позднего начала строительства сети были повсеместно проложены уже с использованием 5 категории.

Кроме использования старой проводки, каждый концентратор 100VG-AnyLAN может быть настроен на поддержку кадров 802.3 (Ethernet), либо кадров 802.5 (Token Ring). Метод доступа к среде "Demand Priority" определяет простую двухуровневую систему приоритетов (высокий для мультимедийных приложений, и низкий для всех остальных).

Надо сказать, это была серьезнейшая заявка на успех. Подвела высокая стоимость, обусловленная большей сложностью и, в немалой мере, закрытостью технологии от тиражирования сторонними производителями. К этому прибавилось уже знакомое по Token Ring отсутствие реальных приложений, использующих преимущества системы приоритетов. В результате 100base-T удалось надолго и безвозвратно захватить лидерство в отрасли.

А новаторские технические идеи немного позже нашли применение сначала в 100BaseT2 (IEEE 802.3y), а затем и "гигабитном" Ethernet 1000base-T.

Глава 2

Сети параллельных миров

Кроме локальных сетей персональных компьютеров архитектуры PC существует несколько параллельных систем передачи данных. Их развитие шло (и идет до сих пор) по своим правилам, только отдаленно пересекаясь с массовым Ethernet.

"Яблочные сети" - Apple Talk, Local Talk

Apple Talk - стек протоколов, предложенный компанией Apple в начале 80-х годов. Изначально протоколы Apple Talk применялись для работы с сетевым оборудованием, объединяемым названием Local Talk (адаптеры, встроенные в компьютеры Apple).

Топология сети строилась как общая шина или дерево, максимальная длина 300 метров, скорость передачи 230,4 Кбит/с. Среда передачи - экранированная витая пара. Сегмент Local Talk мог объединять до 32 узлов.

Малая пропускная способность быстро вызвала необходимость разработки адаптеров для сетевых сред с большей пропускной способностью - Ether Talk, Token Talk и FDDI Talk для сетей стандарта Ethernet, Token Ring и FDDI соответственно. Т.е. Apple Talk пошел путем универсальности на канальном уровне, и может подстраиваться под любую физическую реализацию сети.

Как и большинство других изделий компании Apple, эти сети живут внутри "яблочного" мира, и практически не пересекаются с PC.

UltraNet - сеть для суперкомпьютеров

Ещё одним практически неизвестным в России видом сетей стала UltraNet. Она активно использовалась для работы с вычислительными системами класса суперкомпьютеров и мейнфреймами, но в настоящее время активно вытесняется Gigabit Ethernet.

UltraNet использует топологию "звезда", и способна обеспечить скорость обмена информацией между устройствами до 1 Гбит/с. Отличается весьма сложной физической

реализацией и очень высокими, под стать суперкомпьютерам, ценами. Для управления сетью UltraNet используются компьютеры PC, которые подключаются к центральному концентратору. Дополнительно в ее состав могут входить мосты и роутеры для соединения с сетями, построенными по технологиям Ethernet или Token Ring.

В качестве среды передачи могут использоваться коаксиальный кабель и оптоволокно (на расстояния до 30 километров).

Промышленные и специализированные сети

Надо отметить, что сети передачи данных используются не только для связи между компьютерами или телефонии. Есть еще довольно большая ниша промышленных и специализированных устройств. Например, сравнительно популярна технология CANBUS, созданная для замены одной общей шиной толстых и дорогих жгутов проводов в автомобилях.

Здесь нет большого выбора физических соединений, ограничена длина сегмента, небольшая, до 1 Мбит/с, скорость передачи. Но это удачное сочетание необходимых для малой и средней автоматизации показателей качества и низкого ценового уровня реализаций.

К подобным системам можно так же отнести ModBus, PROFIBUS, FieldBus.

Сегодня интересы разработчиков CAN-контроллеров постепенно смещаются в сторону домашней автоматизации.

Глава 2

ATM как универсальная технология передачи данных

Описание стандарта ATM не зря помещено в конец списка. Это, пожалуй, одна из последних, но безуспешных попыток дать бой Ethernet на его поле. Пути этих технологий находятся в полной противоположности по истории создания, ходу внедрения и идеологии. Если Ethernet поднимался "снизу вверх, от частного к общему", увеличивал скорость и качество, идя за потребностью пользователей, то ATM развивался совсем по-другому.

В середине 80-х годов американский национальный институт стандартов (ANSI) и Международный консультативный комитет по телефонии и телеграфии (CCITT, МККТТ) начинали разработку стандартов ATM (Asynchronous Transfer Mode - Асинхронный Режим Передачи) как набора рекомендаций для сети B-ISDN (Broadband Integrated Services Digital Network).

Только в 1991 усилия академической науки увенчались созданием ATM-Форума, который до сих пор определяет развитие технологии. Первым же крупным проектом, сделанным с ее использованием в 1994 году, стала магистраль известной сети NSFNET (до этого использовавшей канал T3).

Если говорить в общем, то суть ATM очень проста - нужно смешать все виды трафика (голос, видео, данные), уплотнить, и передать по одному каналу связи. Как уже отмечалось выше, достигается это не путем каких-либо технических прорывов, а скорее многочисленными компромиссами. В чем-то это похоже на способ решения дифференциальных уравнений. Непрерывные данные разбиваются на интервалы, которые достаточно малы, и с которыми можно проводить операции по коммутации.

Естественно, такой подход сильно усложнил и без того непростую задачу разработчиков и производителей реального оборудования, и недопустимо для рынка задержал сроки внедрения.

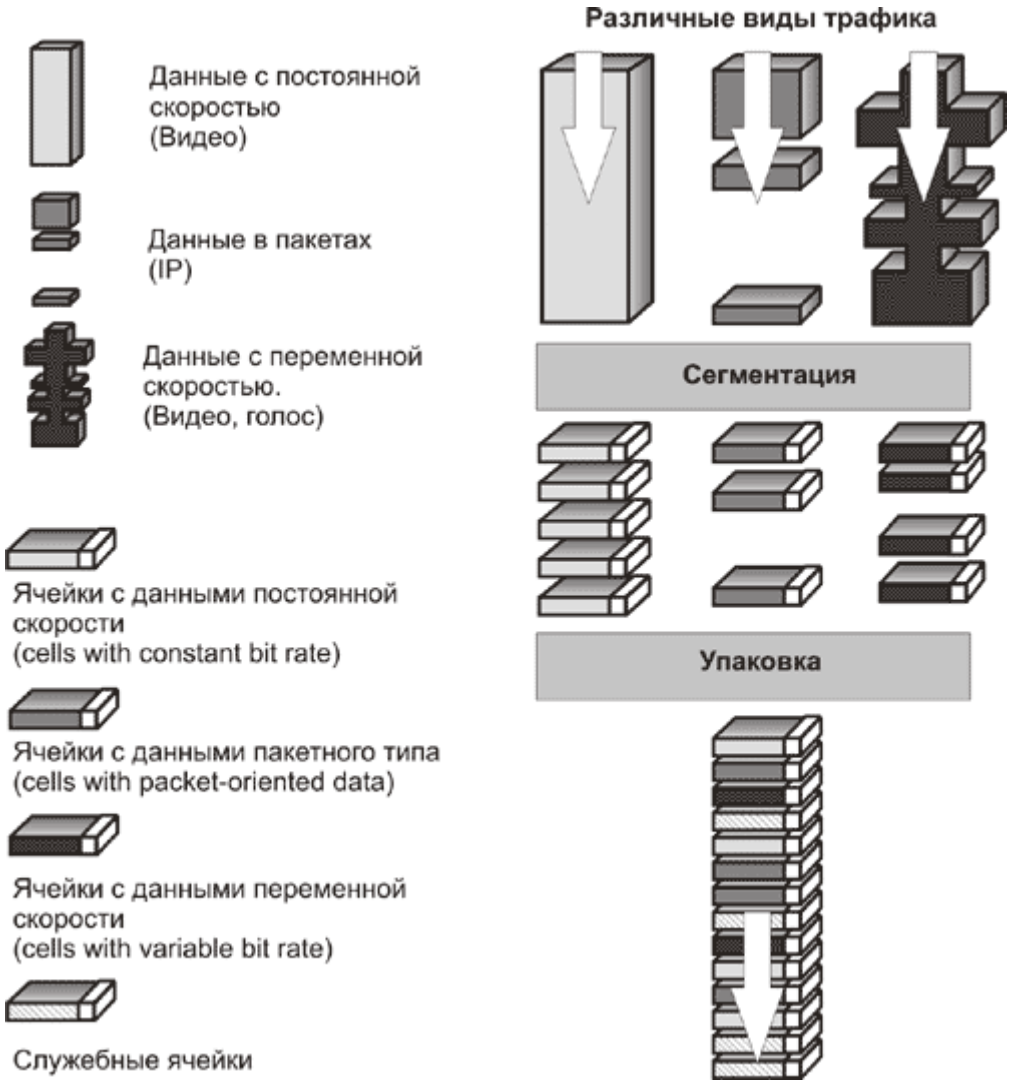

Рис. 2.4. Принцип работы ATM

На размер минимальной порции данных (ячеек в терминологии ATM) влияют несколько факторов. Увеличение размера снижает требования на скорость процессора-коммутатора ячеек, и повышает эффективность использования канала. С другой стороны, чем меньше ячейка, тем более близко к реальному времени возможна передача.

Действительно, пока одна ячейка передается, вторая (пусть самая первоочередная) ждет. Сильная математика, механизм очередей и приоритетов может немного сгладить эффект, но не устранить причину. После достаточно долгих экспериментов в 1989 году для ячейки был определен размер в 53 байта (5 байт служебных, и 48 - данных).

Очевидно, что для разной скорости этот размер может быть разным. Если для скоростей от 25 до 155 Мбит/с подходит 53 байта, то для гигабита 500 байт будут ничем не хуже, а для 10 гигабит - годятся и 5000 байт. Но в этом случае проблема совместимости становится неразрешимой.

Рассуждения носят отнюдь не академический характер - именно ограничение на скорость коммутации поставило технический предел повышению скорости ATM более 622 Мбит, и резко повысило стоимость на меньших скоростях.

Второй компромисс ATM - технология с установлением соединения. Перед сеансом передачи на канальном уровне устанавливается виртуальный канал отправитель-получатель, который не может использоваться другими станциями. Тогда как в традиционных технологиях статистического уплотнения соединение не устанавливается, а в среду передачи помещаются пакеты с указанным адресом.

Для этого в таблицу коммутации заносятся номер порта и идентификатор соединения, который присутствует в заголовке каждой ячейки. Впоследствии коммутатор обрабатывает поступающие ячейки, основываясь на идентификаторах соединения в их заголовках. Опираясь на этот механизм, возможно регламентировать для каждого соединения пропускную способность, задержку, максимальную потерю данных. Т.е. обеспечивать определенное качество обслуживания.

Все перечисленные свойства, плюс хорошая совместимость с иерархией SDH, позволила ATM сравнительно быстро установиться как стандарт магистральных сетей передачи данных. Но с полной реализацией всех возможностей технологии возникли большие проблемы. Как это бывало не раз, локальные сети и клиентские приложения не поддерживали функций ATM. А без этого мощная технология с большим потенциалом становилась только лишним преобразованием между мирами IP (по сути Ethernet) и SDH.

Сложилась весьма неприятная ситуация, которую сообщество ATM попыталось исправить. К сожалению, не обошлось без стратегических просчетов. В реальности, несмотря на все преимущества волоконной оптики по сравнению с медными кабелями, высокая цена интерфейсных плат и портов коммутаторов делала ATM на 155 Мбит/с чрезвычайно дорогим для использования в этом сегменте рынка.

Предприняв попытку определить низкоскоростные решения для настольных систем, ATM Forum ввязался в разрушительные споры по поводу того, на какие скорость и тип соединения следует ориентироваться. Производители разделились на два лагеря сторонников медного кабеля со скоростью 25,6 Мбит/с, и оптического кабеля при скорости 51,82 Мбит/с.

Когда после ряда громких конфликтов (первоначально был выбрана скорость 51,82 Мбит/с), ATM Forum провозгласил 25 Мбит/с в качестве стандарта. Но драгоценное время было потеряно безвозвратно. На рынке технологии пришлось встретить уже не "классический" Ethernet с его разделяемой средой передачи, а Fast Ethernet и коммутируемый 10base-T (с надеждой на скорое появление коммутируемого 100base-T). Высокая цена, небольшое количество производителей, необходимость в более квалифицированном обслуживании, проблемы с драйверами, и т.п. только усугубили ситуацию.

Надежды на внедрение в сегмент корпоративных сетей рухнули, и достаточно слабая "промежуточная" позиция ATM на некоторое время закрепилась. Таково ее положение в

отрасли на сегодня. Однако, и этот вопрос будет рассмотрен еще не раз в следующих главах.

Глава 3. Место Ethernet в провайдинге.

Не важно, как поставлена сеть, важен улов

Такой заголовок связистам старой закалки может показаться кощунством. Ethernet никогда не рассматривался всерьез как протокол транспортного уровня. Это безусловно справедливо для его "классической" модели - разделяемая среда с утилизацией не более 60-70% полосы пропускания канала из-за коллизий, негарантированное качество, отсутствие механизмов приоритезации:

Но так ли это сейчас? Наиболее заметное событие наших дней, коммутируемый Ethernet, добрался до самых малых сетей, и свитч 10/100baseT (IEEE 802.3u) стоит дешевле $10 за порт. Это с соблюдением полнодуплексной передачи (IEEE 802.3x). Более сложные коммутаторы (около $30 за порт) поддерживают приоритезацию (IEEE 802.1p), виртуальные сети (VLAN, 802.1q), алгоритм покрывающего дерева (Spanning Tree Algorithm, IEEE 802.1d), и некоторые другие возможности, необходимые в телекоммуникациях

С другой стороны, резко выросли скорости. Еще весной 1996 года был организован Gigabit Ethernet Alliance. Как закономерный результат, в 1998 году принят IEEE 802.3z, более известный как Gigabit Ethernet (работа по оптоволокну, и на расстояния до 25 метров по витой паре). В 1999 появился IEEE 802.3ab, более известный как 1000base-T (до 100 метров по витой паре). Далее последовал IEEE 802.3ad - поддержка агрегации каналов и объединения в транки: На очереди 10 гигабит.

Кроме этого, для эффективной работы на 3-ем уровне (сетевом по модели OSI) появились мощные корпоративные решения типа MPLS от Cisco (приблизительный аналог технологии установления виртуального соединения в ATM). А некоторые магистральные коммутаторы SDH начали комплектоваться возможностью передачи в том же оптическом кольце Gigabit Ethernet: Процесс проникновения Ethernet в операторские сети идет медленно, но вполне последовательно.

Смешки - наконец Ethernet "добился того, что ATM умел 8 лет назад" неуместны. Решение ATM очень красивое в техническом плане, выверенное и правильное. Но его не подпирает "снизу" многосотмиллионная база инсталлированных портов 10/100/1000base-T. Имея такую массу за спиной, Ethernet'у очень удобно давить ценой. Ведь давно известно - не всегда в соревновании технологий побеждает самое мощное решение. Верх берет самое выгодное - можно вспомнить хотя бы пример архитектуры x86.

Глава 3

Сравнение TDM, ATM, и Ethernet

Еще одно объяснение потенциальной возможности Ethernet занять непривычную нишу транспортных сетей надо искать в физической природе передаваемых данных.

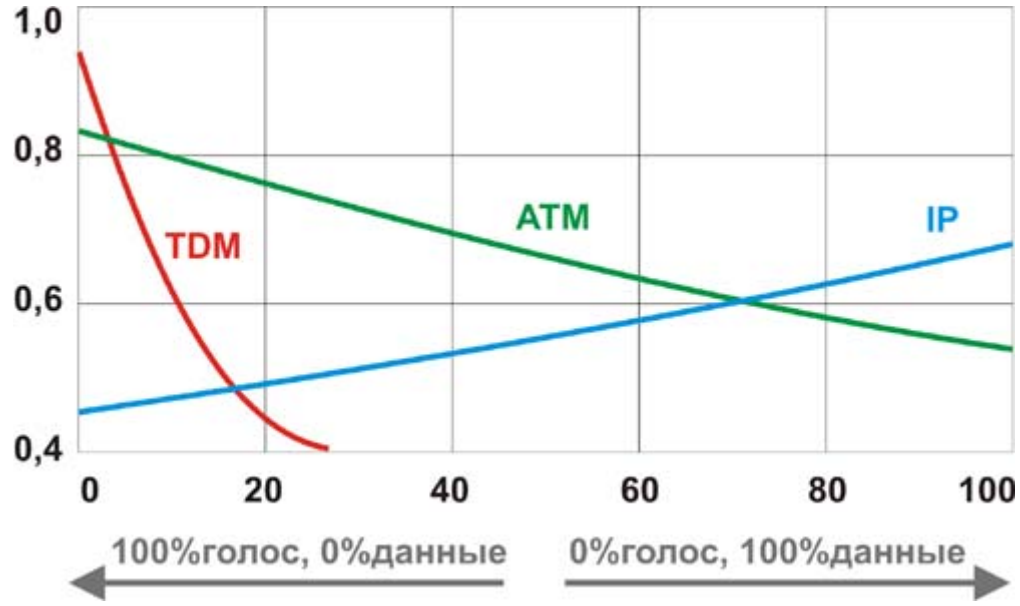

Рис. 3.1. Сравнение видов уплотнения - временного (TDM), и статистического (ATM, Ethernet)

Трафик данных (не голосовой) последние пять лет стал нарастать со скоростью, которую было трудно предугадать. Тем более, с появлением MPEG-4 и ему подобных алгоритмов упали последние надежды, что широкие каналы TDM для передачи данных в реальном времени (потокового видео) когда-нибудь будут востребованы.

В некоторых странах IP трафик по объему уже обогнал телефонию, и близится к заветному рубежу 80%. При превышении которого использование Ethernet становится технически (а не только экономически) обосновано.

Что дальше? Не оттеснит ли передача данных телефонию на второй план в использовании магистральных каналов? Пока об этом говорить всерьез рано. Трафик трафиком, а прибыль, которую получают операторы связи от телефонии, значительно превосходит доход от передачи данных. Да и существующие глобальные сети сориентированы безусловно и целиком на SDH. Так что в этой области доминированию традиционных способов связи почти ничего не угрожает: Пока не угрожает.

Глава 3

Использование Ethernet на "последней миле"

На сегодня Ethernet безусловно доминирует в локальных сетях. Можно сказать, что он вполне пригоден для передачи магистрального IP-трафика (сети Интернет). Но между этими двумя областями лежит печально знаменитая "последняя миля". На которой сегодня в России ничего нет, кроме телефонных медных кабелей сомнительного качества.

Нуждающихся в широкополосных сетях заказчиков можно условно разделить на три категории.

- Корпоративные. Скорее всего, они уже позволили себе качественные каналы и оборудование, не сильно заботясь о стоимости подключения. Консервативно предпочитают многопарную медь, оптоволокно (на западе - T1 или T3) или радиорелейные линии в сочетании со "старыми" провайдерами. Интернет, как правило, используют как дополнение к традиционной телефонии.
- Средний офис. Тут согласны заплатить за подключение до $1-3т. Не слишком требовательны к качеству, но сбои связи более двух-трех часов могут вызвать переход к другому поставщику услуг. Активно используют xDSL, radio-ethernet, оптоволокно, и т.п. Техническая возможность подключения к Интернет за такую сумму может быть найдена практически по любой технологии и зависит скорее от городской коньюктуры. Особых проблем в предложениях от поставщиков услуг такие клиенты не испытывают. Провайдеров огорчает лишь относительная малочисленность данной категории заказчиков. Поэтому рынок уже давно сформирован и "исторически" поделен, ворваться на него при помощи новой технологии (типа xDSL или ethernet) нельзя без больших капитальных вложений и маркетинговых усилий.
- Что остается? Домашний пользователь и малый офис. Этот рынок стремительно растет, потенциально огромен, но: Труден в освоении. Именно на нем (и только на нем) возникает так часто упоминаемая проблема "последней мили". Чего только не изобретают для ее решения. Но традиционный dial-up не сдает позиций.

Поэтому, имеет смысл заострить внимание именно на последнем варианте. Известно большое количество технологий разрубания этого "гордиевого узла". Это отечественных разработки типа Гранчей, экзотические соединений по силовой сети, HomePNA по сети радиовещания, различные варианты радио, кабельное телевидение, лазеры, и многое, многое другое.

Самый перспективный в этом ряду - xDSL. Даже более того, при использовании телефонных коммуникаций ему фактически нет альтернативы. В чем же проблема? По реалиям Российского рынка попытаемся сделать грубый расчет.

"Домашний" пользователь (как и малый офис) не готов платить более $300-500 за подключение, более того, массовый спрос начинается примерно со $100-200. При превышении этих сумм пользователь просто остается "на модеме". Не потому, что так ему удобнее - при домашнем использовании просто нет средств, в случае малого офиса нет осознанной экономической выгоды.

Такой ценовой ценз, по сути, отрезает технологию xDSL от конечного "домашнего" пользователя. Оплатить даже себестоимость подобно подключения он не сможет. Кредитные схемы то же малоэффективны. Предположим, провайдер, надеясь на будущие прибыли, возьмет на себя основные затраты на инсталляцию "порта".

Подсчитаем примерный срок окупаемости. Пусть оконечное оборудование стоимостью до $200 оплатит пользователь. Стоимость оборудования на стороне телефонной станции по самому оптимистическому расчету составит $300-400 за порт (не считая существенных затрат на опорную сеть). Далее, прибыль с одного мегабайта трафика реально близка к $0,1 (при запредельной рентабельности 100%). Потребление домашнего пользователя или малого офиса составляет 50-500 Мб в месяц. Соответственно, прибыль составит $10-30.

С учетом накладных расходов, можно предположить срок окупаемости 3 года и более. Не слишком плохо по мировым меркам, но в России надо быть очень смелым (или очень богатым) предпринимателем, что бы вкладывать деньги в такой проект. Реально это могут себе позволить только монополисты, которые могут диктовать условия, и для которых окупаемость часто не на первом месте.

Остается сказать, что xDSL - это одна из самых дешевых (и эффективных) технологий. В случае с другими вариантами подключения (через кабельное телевидение, оптоволокно, и т.п.) картина получится еще более удручающая.

Глава 3

Ethernet-провайдинг, или домашние сети

Между тем, жизнеспособное решение выросло "само" и совсем не там, где ждали. Преодоление последней мили стало возможно через "большие" сети Ethernet. Но назвать это чисто Российским феноменом нельзя.

Широкополосные каналы доступа в мире уже созрели и поддаются классификации. Говоря в общем, высокоскоростной доступ конечного пользователя можно условно разделить на "американский" и "шведский". Первый ориентирован на подключение каждого абонента прямо к концентратору на узле оператора (например, АТС) отдельным каналом (обычно ISDN, ADSL или кабельное ТВ). "Шведское" решение предусматривает скоростное (как правило, оптоволоконное) подключение к оператору связи проложенной в доме локальной сети Ethernet, а уже через нее - конечного пользователя. Это нельзя назвать "последней милей", скорее "последним дюймом". Но определенная схожесть подходов заметна без труда.

Большинство городов России (но не все) пошли по второму "шведскому" пути. И даже немного дальше. Из-за иной, по сравнению с Европой, экономической ситуации, локальные сети строились не на отдельный дом, а сразу на группу строений, квартал, и даже район.

Наверно, сначала никто не мог предположить, насколько большой запас заложен в технологии Ethernet. Сети строились экспериментально, часто с грубейшими нарушениями норм и правил, "методом тыка". Но работали, несмотря на все нарушения, настолько лучше модемов, что им прощалось многое. Более того, материалы и оборудование для построения таких сетей оказались неимоверно дешевы, и себестоимость широкополосного подключения в $30-50 стала реальностью.

Вот краткое описание "реальных" и "сегодняшних" норм домашних сетей, которые мы подробно и не раз рассмотрим в следующих главах.

- Длина между хабами (репитерами) - до 500 метров для витой пары (при применении нестандартного кабеля), до 350 метров для коаксиального кабеля. При необходимости, для обоих типов носителя возможно увеличение дальности до 800-1000 метров, но это связано с небольшими дополнительными расходами.
- Количество хабов (репитеров) в домене коллизий до 10-12.
- Применение простейших PC под ОС Linux или BSD в качестве маршрутизаторов и серверов.

- Применение самого дешевого китайского оборудования, при цене хаба от $30, кабеля $0,12 метр, сетевых карт - $6.

Это нарушение стандартов, скажете Вы, такая система работать не будет. И во многом будете правы - по нормам серьезных операторов связи за услуги подобного качества деньги брать нельзя.

Однако, ничего не вечно, даже низкий уровень услуг. По мере развития сетей и усиления конкуренции неизбежно улучшится и качество. Ненадежные "медные" линии заменятся на оптику, в узлах появится управляемое оборудование операторского класса. Этот процесс идет непрерывно, и за ним можно наблюдать в настоящий момент.

На следующем рисунке показана "классическая" сеть начального периода строительства. Именно от этого "нулевого" уровня мы будем отталкиваться в дальнейшем изложении.

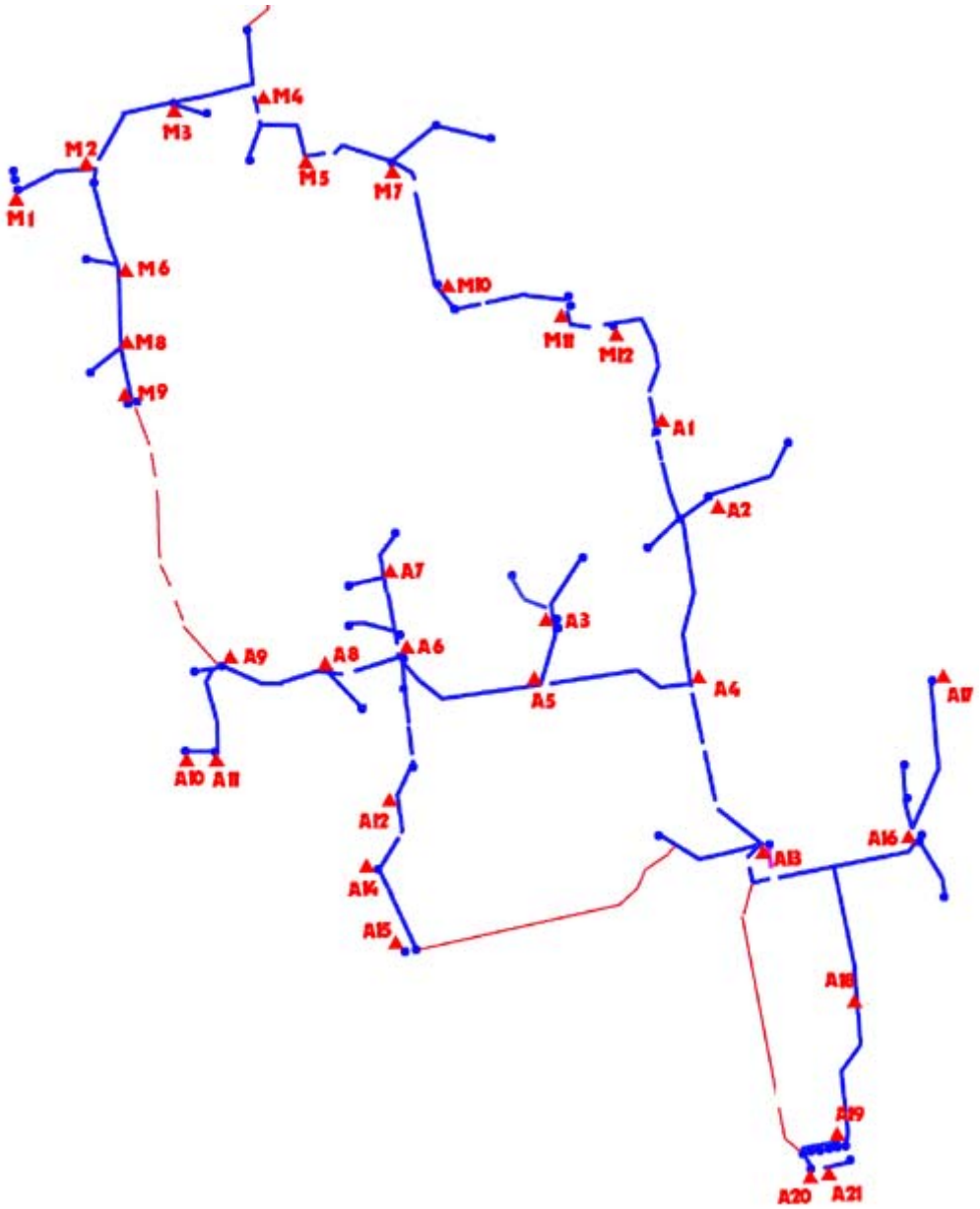

Рис. 3.2. Пример большой локальной сети

Кстати сказать, на рисунке показана часть вполне реальной сети, построенной более 3-х лет назад при моем участии. Срок строительства "с нуля" - 1 года. Рекламные усилия при этом можно считать пренебрежимо малыми.

Диаметр сети составляет примерно 5 км. В качестве магистрали использован кабель П-296, по топологии "витая пара" (обозначен синими линиями). Для задания масштаба, расстояние между точками А4-А13 составляет 485 метров. В сети установлено 33 хаба (обозначены красными треугольниками), в основном Compex 1008. Тремя маршрутизаторами домен коллизий поделен на 5 частей. Тонкими красными линиями отмечены варианты планового соединения сетей в кольца. Сейчас, спустя почти 2 года, сеть в рабочем состоянии, а количество установленных хабов более 50. И все это без серьезных изменений в топологии.

Тем не менее, как с запуском Екатеринбургской транспортной сети АДСЛ, так и снижением цен на оптоволокно, подобное решение безнадежно устарело. Но сеть все еще работает в коммерческом режиме без существенной перестройки и замены оборудования.

Глава 3

Признание домашних сетей

Несмотря на постоянные проблемы с обеспечением качества, пользователя услуга более чем устраивает (в основном из-за низкой цены). Реально два последних года в России и ближнем зарубежье наблюдается просто взрывной рост подобных сетей. И кривая развития даже не думает изменять наклон. Ограничение идет скорее по физической способности провайдеров прокладывать необходимые коммуникации. На практике, подключать более 30 человек в месяц небольшой фирме трудно уже организационно.

Несмотря на колоссальные трудности технического и юридического характера, за несколько лет домашними сетями закрыты многочисленные районы в целом ряде городов России. В Екатеринбурге большинство провайдеров (в том числе наиболее крупных) так или иначе использует технологию Ethernet (самостоятельно, либо через аффилированных партнеров). То есть такой способ оказания телематических услуг не только применяется - он уже признан, как говорится, "де юре".

Так как продвижение новой технологии на рынок занимает определенное время, первое время развитие носило преимущественно экстенсивный характер. По мере роста популярности, очевидно серьезное углубление рынка на уже охваченной территории. Этот процесс экономически хорошо сочетается с улучшением качества услуг.

Чем-то мне это напоминает процесс появления киосков в конце 80-х. И во что они превратились теперь. Не слишком умно было в начале этого пути строить современные стеклянные комплексы. И нельзя представить теперь на улице металлическую, корявую будку, с маленькой, забранной решеткой витриной. Сменилось и название - теперь это не будка, ларек, а остановочный комплекс, мини-магазин. С кассой и вежливыми продавцами.

Подобно этому, и перед домашними сетями скоро встанет (или уже встал) неприятный, но логичный выбор. Исчезнуть (превратиться в любительскую структуру), или перестроиться, легализоваться, в конце концов, сменить название.

Ethernet-провайдинг становится (а кое-где уже стал) вполне респектабельным бизнесом, к которому надо подходить с соответствующей подготовкой. Ее отсутствие грозит как минимум необоснованными затратами, как максимум - быстрым крахом предприятия.

Надеюсь, дальнейшее изложение поможет вам успешно избежать многих ошибок, как в строительстве, так эксплуатации домашних сетей.

Глава 4. Понятие структурированных кабельных систем (СКС).

Стандарты по сетям бывают двух видов: устаревшие и импортные

Конец 80-х годов ознаменован широким распространением персональных компьютеров во всех сферах человеческой деятельности. Не удивительно, что в это же время начался бурный рост компьютерных сетей.

Но проходил он в весьма неоднозначной ситуации, когда существовало несколько несовместимых технологий передачи данных, использовавших вдобавок принципиально разные кабельные системы. Например, Ethernet 10base5 - толстый коаксиальный кабель, 10base2 - тонкий, ArcNet - похожей толщины, но с иным волновым сопротивлением. Экзотический ныне твинаксиал IBM AS/400. Немного позже, в TokenRing начала применяться экранированная витая пара с волновым сопротивлением 150 Ом, а в Ethernet 10baseT - неэкранированная, и с сопротивлением 100 Ом. И это далеко не весь технический ассортимент того времени.

Получалось, что кабельная система - самая трудоемкая в замене, и дорогостоящая часть сети зависела от выбора активного оборудования. И подлежала замене вместе с ним. Конечно, некоторые устройства поддерживали несколько стандартов, но стоили соответственно дороже. Тем более постоянная гонка скоростей сводила впустую все усилия разработчиков.

Инвестиции в инфраструктуру не были защищены, и долго так продолжаться не могло. Для повышения привлекательности идей крупных ЛВС перед заказчиками и сокращения эксплуатационных расходов требовалось поставить кабельную систему "впереди" активного оборудования, структурировать и идеологически объединить с существующими сетями телефонии, сигнализации, наблюдения, кабельного телевидения.

Попытки были предприняты еще в 1983 году, когда AT&T установила первую структурированную кабельную систему. Но большого распространения пример не получил. Серьезно обстановка изменилась только в 1991 году, когда американская Ассоциация электронных отраслей промышленности (EIA) и Ассоциация индустрии связи (TIA) ввели стандарт на телекоммуникационные кабельные системы EIA/TIA 568, пересмотренный и дополненный в октябре 1995 года до используемого сейчас EIA/TIA 568A.

Целью этого стандарта было определение "структурированной кабельной системы" (СКС), которая может поддерживать любые приложения передачи аналоговых, видео и

цифровых данных, и является частью инфраструктуры офиса или промышленного здания. При практическом отсутствии национальных альтернатив, EIA/TIA 568A широко распространился по миру. Именно на его основе были разработаны и приняты международные (ISO/EIC 11801) и европейские (EN50173) стандарты, которые, тем не менее, не нашли такого широкого применения на практике (тем более в России).

В стандарте ANSI/TIA/EIA-568-A описаны требования к производительности и технические характеристики для различных системных конфигураций и компонентов СКС. Он дополняется другими стандартами, соблюдение которых позволяет в полной мере воспользоваться всеми преимуществами СКС. Это ANSI/TIA/EIA-569 (Commercial Building Standard for Telecommunications Pathways and Spaceways), который описывает требования к помещениям, в которых устанавливается СКС и оборудование связи. И ANSI/TIA/EIA-606 (Administration Standard for the Telecommunications Infrastructure of Commercial Buildings), описывающий правила цветовой кодировки, маркировки и документирования смонтированной кабельной системы.

Глава 4. Понятие структурированных кабельных систем (СКС).

Стандарты по сетям бывают двух видов: устаревшие и импортные

Конец 80-х годов ознаменован широким распространением персональных компьютеров во всех сферах человеческой деятельности. Не удивительно, что в это же время начался бурный рост компьютерных сетей.

Но проходил он в весьма неоднозначной ситуации, когда существовало несколько несовместимых технологий передачи данных, использовавших вдобавок принципиально разные кабельные системы. Например, Ethernet 10base5 - толстый коаксиальный кабель, 10base2 - тонкий, ArcNet - похожей толщины, но с иным волновым сопротивлением. Экзотический ныне твинаксиал IBM AS/400. Немного позже, в TokenRing начала применяться экранированная витая пара с волновым сопротивлением 150 Ом, а в Ethernet 10baseT - неэкранированная, и с сопротивлением 100 Ом. И это далеко не весь технический ассортимент того времени.

Получалось, что кабельная система - самая трудоемкая в замене, и дорогостоящая часть сети зависела от выбора активного оборудования. И подлежала замене вместе с ним. Конечно, некоторые устройства поддерживали несколько стандартов, но стоили соответственно дороже. Тем более постоянная гонка скоростей сводила впустую все усилия разработчиков.

Инвестиции в инфраструктуру не были защищены, и долго так продолжаться не могло. Для повышения привлекательности идей крупных ЛВС перед заказчиками и сокращения эксплуатационных расходов требовалось поставить кабельную систему "впереди" активного оборудования, структурировать и идеологически объединить с существующими сетями телефонии, сигнализации, наблюдения, кабельного телевидения.

Попытки были предприняты еще в 1983 году, когда AT&T установила первую структурированную кабельную систему. Но большого распространения пример не получил. Серьезно обстановка изменилась только в 1991 году, когда американская

Ассоциация электронных отраслей промышленности (EIA) и Ассоциация индустрии связи (TIA) ввели стандарт на телекоммуникационные кабельные системы EIA/TIA 568, пересмотренный и дополненный в октябре 1995 года до используемого сейчас EIA/TIA 568A.

Целью этого стандарта было определение "структурированной кабельной системы" (СКС), которая может поддерживать любые приложения передачи аналоговых, видео и цифровых данных, и является частью инфраструктуры офиса или промышленного здания. При практическом отсутствии национальных альтернатив, EIA/TIA 568A широко распространился по миру. Именно на его основе были разработаны и приняты международные (ISO/EIC 11801) и европейские (EN50173) стандарты, которые, тем не менее, не нашли такого широкого применения на практике (тем более в России).

В стандарте ANSI/TIA/EIA-568-A описаны требования к производительности и технические характеристики для различных системных конфигураций и компонентов СКС. Он дополняется другими стандартами, соблюдение которых позволяет в полной мере воспользоваться всеми преимуществами СКС. Это ANSI/TIA/EIA-569 (Commercial Building Standard for Telecommunications Pathways and Spaceways), который описывает требования к помещениям, в которых устанавливается СКС и оборудование связи. И ANSI/TIA/EIA-606 (Administration Standard for the Telecommunications Infrastructure of Commercial Buildings), описывающий правила цветовой кодировки, маркировки и документирования смонтированной кабельной системы.

Глава 4

Принципы построения СКС

Основными признаками СКС считаются **структурированность**, **универсальность**, и **избыточность**.

Рассмотрим **структурированность** как главный, вынесенный в название, термин. Среда передачи сигналов состоит из элементов - кабелей и разъемов. Поэтому, функциональные элементы СКС (как части среды передачи), составляют кабели, оснащенные разъемами в точках подключения или коммутации, и проложенные по определенным правилам (с образованием линий и магистралей).

Для фиксации разъемов используют розетки и панели. Для организации линий применяют короба, лотки, лестницы. Это конструктивные элементы СКС, которые не являются часть среды передачи.

По назначению, структурированную сеть принято разделять на подсистемы. Нельзя сказать, что при этом все становится просто и понятно. Нестыковок достаточно. Так, в американских стандартах такого разграничения нет. Однако специально выделена подсистема администрирования... Ничего удивительного нет, ведь СКС - абстрактный термин, практики работают с СКС AT&T, СКС Lucent, СКС Alcatel и т.п. Иначе говоря, у каждого производителя есть хоть небольшая, но свобода действий, которой они пользуются в полной мере.

Так или иначе, на сегодня предпочтительнее ориентироваться на международные стандарты, которые разделяют три подсистемы: магистраль комплекса, магистраль здания

и горизонтальную подсистему. В общем случае, путаница так велика, что в проспектах ряда компаний можно найти четыре, пять, восемь и даже девять подсистем.

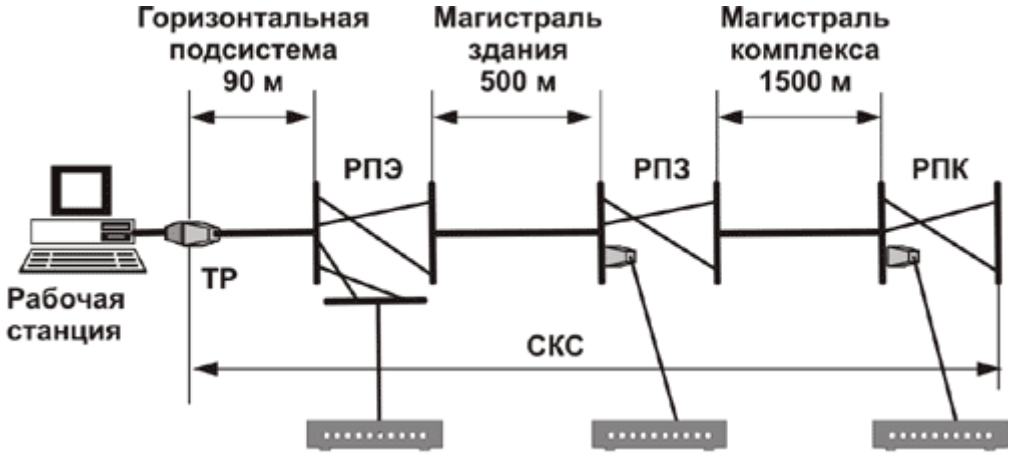

Рис. 4.1. Подсистемы СКС. РПЭ - распределительный пункт этажа, РПЗ - распределительный пункт здания; РПК - распределительный пункт комплекса.

1. Магистраль комплекса служит для соединения между собой различных зданий. Как правило, реализуется на оптоволоконном (реже медном кабеле), и позволяет соединять между собой здания, находящиеся на расстоянии до нескольких километров.
2. Магистраль здания соединяет между собой этажи здания, обеспечивает связь между распределительной панелью здания и панелями этажей. Она должна включать в себя кабель, установленный вертикально между этажными панелями, главную или промежуточную панель в многоэтажном здании, а также кабель, установленный горизонтально между панелями в протяженном одноэтажном здании.
3. Горизонтальная подсистема является частью, которая проложена между телекоммуникационной розеткой на рабочем месте, и этажной распределительной панелью. Каждый этаж здания рекомендуется обслуживать своей собственной горизонтальной подсистемой. На каждое рабочее место должно быть проложено как минимум два горизонтальных кабеля.

Универсальность в СКС достигается благодаря следованию стандартам, которые позволяют перейти от частных к открытым системам, с унифицированными параметрами, поддерживающими работу оборудования (причем как активного так и пассивного) любых производителей. Добиться этого не слишком просто - в отличии от активного оборудования, СКС создают тысячи и десятки тысяч независимых организаций, всегда в единственном экземпляре, и обычно с учетом своих особенностей. При этом изготовители элементов контролируют малое количество инсталляций (или не контролируют их вообще).

Если к этому добавить необходимость использования в СКС единой системы для всех видов коммуникаций, которые должны эксплуатироваться одной службой, по единым методикам и нормам, то создание серьезной сети является совсем не простой задачей. Системные интеграторы все же не зря едят свой хлеб.

Третий основной признак, **избыточность**, не слишком хорошо сказывается на стоимости. Но именно это позволяет строителями создавать системы прежде, чем станут известны

требования пользователей, и обеспечить большой срок службы телекоммуникационной инфраструктуры здания.

В этом заложен достаточно глубокий экономический смысл. Классическая структурированная кабельная система монтируется на этапе строительства здания, или капитального ремонта. И должна служить без изменений до следующего капитального ремонта (обычно 10-15 лет).

Достигается это путем выполнения монтажа системы не из расчета на существующие потребности, а исходя из требований нормативов (реально с существенным запасом). Поэтому практически любые изменения организационной структуры заказчика не могут привести к необходимости модернизации СКС. Для этого должно быть достаточно переключений на распределительных панелях.

Если попробовать кратко сформулировать преимущества СКС над обычными кабельными системами, с которыми строитель (инсталлятор) убеждает заказчика, то получится следующий список:

- для передачи данных, голоса и видеосигнала используется единая кабельная система, которую может обслуживать одно подразделение (экономия на количестве специалистов);
- использование универсальных розеток на рабочих местах позволяет подключать к ним различные виды оборудования, и легко менять его месторасположение;
- оправдывают капиталовложения за счет длительной эксплуатации сети без модернизации (снижение полной стоимости владения);
- возможностями внесения изменений и наращивания мощности без изменения существующей сети (путем замены активного оборудования);
- возможно одновременное использование нескольких различных сетевых протоколов (в настоящее время не актуально);
- не зависят от изменений технологий и поставщика оборудования, используют стандартные компоненты и материалы;
- позволяют комбинировать в одной сети волоконно-оптический и медный кабель.

Глава 4

Проблемы внедрения СКС в небольших сетях

Считается, что СКС приспособлена для зданий с офисной площадью до 1,000,000 м2, и числом пользователей от 50 до 50000 человек, и расстояниями между зданиями до 3 км. Даже при самом поверхностном взгляде на суть вопроса можно заметить, что указанный диапазон возможностей слишком велик. Можно предположить, что для крайних значений, сети будут оптимизированы не лучшим образом.

Действительно, стандарты разрабатывались достаточно давно, и для американского рынка. Наиболее удобны они, соответственно, для средней американской фирмы, владеющей несколькими зданиями, с общей численностью персонала в 500-5000 человек. Для экономических расчетов так же принимались вполне американские зарплаты специалистов, рабочих и служащих.

Не умаляя огромного достоинства методологии СКС для упрощения работы инсталляторов, с точки зрения потребителя можно выделить три основных недостатка.

1. Высокая стоимость строительства, которая является неизбежным следствием избыточности и универсальности.
2. Подмена понятий качества среды передачи данных в сети удобством обслуживания и хорошим внешним видом.
3. Высокая скорость смены технологий, делающая бессмысленным расточительством долгосрочные гарантии работоспособности.

Рассмотрим эти проблемные вопросы более подробно.

Сеть сама по себе сеть передачи данных мало кому нужна. Потребителю необходима выгода (экономия), которую с ее помощью можно получить. А для экономиста (и/или владельца) строительство локальной сети - не более, чем инвестиция. Поэтому более чем уместно задать вопрос о ее окупаемости.

Увы, диспропорция этого аспекта структурированных кабельных систем в России более чем заметна. Конструктивные элементы покупаются за доллары, а экономия затрат от использования сети получается в рублях. Как правило, для больших фирм потребность в высоком качестве и низкие затратах на длительную эксплуатацию в собственном комплексе зданий перекрывают высокие первоначальные вложения.

Но в небольших сетях ситуация совершенно другая. Нужна ли дорогостоящая СКС фирме, где работает менее 50 человек, которая занимает 10-15 комнат в арендованном здании, на 1-2 этажах? А если простой в течении нескольких часов не нанесет заметных убытков? При таком варианте ответ совсем не однозначен, и зависит от многих дополнительных факторов.

Разумеется, дешевая не структурированная сеть - это совсем не значит свалить все активное оборудование в кучу под стол, разбросать кабеля по полу, обжать разъемы отверткой. Недорогие стойки, короба, шкафы, кабеля от проверенных производителей, хорошая маркировка... Такой подход позволяет сильно экономит средства, и дает вполне достойные результаты для бизнеса.

Но, не смотря на большое количество подобных заказчиков, подобный подход часто не находит предложения. Преобладают крайности - или СКС с полной обвязкой (и за полную стоимость), или наплевательское "кабель по плинтусу, а хаб - под стол".

Причина во многом идет от отсутствия внятной количественной оценки. Нет ни методик, ни рекомендаций, которые могли пояснять зависимость качества сети от ее стоимости. Существующие стандарты не более, чем удобный структурированный сборник технических рекомендаций, и для этого просто не предназначены. В недорогих решениях их используют подобно описанию к детскому конструктору, не более того.

Попробуем забыть (не навсегда, конечно) про требования стандартов, и посмотрим, что при этом получается. Приведенная ниже схема не претендует на точность, она лишь призвана наглядно показать возможные пути количественной оценки.

На ЛВС при строительстве (инсталляции) действует три фактора. Исходя из логики, для реально существующей сети они должны образовывать "равновесную" систему, т.е. их векторная сумма будет равна нулю.

Рис. 4.2. Факторы, участвующие в определении свойств локальной сети

- Стоимость установки. Рядовому заказчику совершенно не нужна сама сеть, как предмет или услуга. Его интересует прибыль, которую он с ее помощью может получить. Поэтому, на рисунке показана не "стоимость" (размерная величина), а "экономия расходов", которая может быть выражена в процентах.
- Требование к качеству сети. Под этим понимается создание канала с максимальным соотношением сигнал/шум на приемнике (если опустить прочие, менее значительные параметры типа задержки, скорости распространения, и т.п.). Данная величина то же может быть выражена в относительных величинах, например, подобно ACR, или как процент потерянных пакетов (BER).
- Внешний вид и удобство обслуживания. Хоть это не совсем одно и то же, но на данном этапе не стоит из-за небольших различий усложнять диаграмму. В каких величинах это можно выразить, не совсем понятно. Но очевидно, что и в этом случае можно применить процентную величину, выраженную относительно эталона.

Ключевым звеном схемы является демонстрация того, что качество передачи сигнала, и удобство использования (и внешний вид) совсем не одно и тоже. Наоборот, они противоположны по своему действию. Любой разъем значительно снижает качество передачи. Красивые кабельные каналы обычно увеличивают, а совсем не сокращают длину линии, и т.д. Но более подробно этот вопрос будет рассмотрен в следующих главах, посвященных характеристикам среды передачи сигналов.

Широкому распространению СКС в большой мере способствовало стабильность требований протоколов передачи данных последних 5-10 лет. Действительно, простой

кабель (и разъемы) категории 5 (до 100 МГц) можно было использовать сначала для 10baseT, потом 100baseT, и даже с некоторыми оговорками, для 1000baseT. Из-за этого существенно замедлился процесс принятия стандартов на системы категории 6, и 7, обеспечивающие более широкую полосу пропускания (до 250-500 МГц).

Воодушевленные ситуацией, производители СКС начали давать 15-ти, 20-ти 25-летние и даже пожизненные гарантии. С точки зрения сохранение работоспособности это верно. Но по вероятному сроку службы это скорее иллюзии, которые питают и производители (это выгодно), и заказчики (так спокойнее).

Можно легко связать скорость передачи данных в локальных сетях с пропускной способностью шин компьютеров. Для Intel 80286 или 80386 с шинами ISA (8 Мбайт/с) или EISA (32 Мбайт/с) пропускная способность сегмента Ethernet 10baseT составляла 1/8 или 1/32 канала "память - диск". Для процессоров Pentium и шиной PCI (133 Мбайт/с) эта доля упала до 1/133, что вызвало массовый переход на Fast Ethernet.

Разумно предположить, что Gigabit Ethernet появится в рабочих станциях только после относительно скорого и неизбежного перехода системной шиной значения гигабайта в секунду. При этом большинство кабельных систем категории 5 окажется устаревшими, как это уже было с коаксиальным кабелем, и витой парой категории 3.

Аналогий и примеров подобного рода можно привести много, но смысл от этого изменится незначительно. Пока закон Мура действует, средний срок службы СКС не превысит 6-8 лет, какие бы качественные материалы не были использованы при строительстве. Соответственно, окупаемость системы то же надо рассчитывать исходя из этой величины, а вовсе не срока гарантии.

Глава 4

Применение методов СКС для сетей "последней мили"

Сети "последней мили", построенные по технологии Ethernet, внешне очень мало отличаются от стандартных локальных сетей. Но специфика работы в жилых домах накладывает серьезные ограничения на приведенные выше преимущества СКС. Попробуем прокомментировать основные моменты подробнее.

Таб. 4.1. Принципиальные отличия структурированных кабельных систем и "домашних сетей".

Структурированные кабельные системы (Локальные сети)	"Домашние сети"
Для передачи данных, голоса и видеосигнала используется единая кабельная система, которую может обслуживать одно подразделение (экономия на количестве специалистов).	В сети последней мили (домашней сети) кабельная система используется только для передачи данных, и в подавляющем большинстве случаев не может быть объединена с чем-либо еще в силу организационных причин (разные владельцы, препятствующие стандарты и правила). Кроме этого, большинство

	сетей (телефония, кабельное телевидение) уже построено, и сэкономить при прокладке не удастся.
Стандартами СКС предусмотрено использование магистрали менее 3000 метров.	Сети "последней мили", несмотря на свое название, очень часто выходят за это ограничение.
Качество услуг не нормируется.	Снижение качества услуг (или их временное прекращение) оговаривается регламентами, и должно быть минимизировано. Иначе говоря, существует нормировка качества услуги.
Использование универсальных розеток на рабочих местах позволяет подключать к ним различные виды оборудования, и легко менять его месторасположение;	Устанавливать телекоммуникационные разъемы в жилой квартире по нормам СКС возможно, но явно не рационально. Количество пользователей в квартире определено, неизменно, и его перемещение по дому (а тем более району) маловероятно. Короба использовать крайне нежелательно, подвесных потолков нет. Плюс ко всему, используется другой тип мебели.
Оправдывают капиталовложения за счет длительной эксплуатации сети без модернизации (снижение полной стоимости владения);	Инсталляцию сети крайне сложно приурочить к строительству дома, или капитальному ремонту. Более того, прокладка линий по всем квартирам "заранее" невозможна. Поэтому, сеть просто вынуждена непрерывно модернизироваться на протяжении всего периода существования.
Возможно внесение изменений и наращивание мощности без изменения существующей сети (путем замены активного оборудования);	Это условие применимо, но весьма ограниченно из-за использования недорогих материалов, а так же работы в неприспособленных, плохо защищенных помещениях (либо вообще без таковых).
Возможно одновременное использование нескольких различных сетевых протоколов (в настоящее время не актуально);	Это еще менее актуально в "домашних сетях" ориентирующихся на самые недорогие и распространенные протоколы передачи данных.

На основании сравнения, видно, что сети "последней мили" имеют мало общего с СКС даже без учета ориентации на частного (а не корпоративного) пользователя, с присущими этому сектору рынка низкими стоимостями подключения и эксплуатации, при соответственно пониженном качестве.

Более того, кроме различий в способах построения кабельной системы, появляются дополнительные требования к программному комплексу - биллингу и авторизации, о которых будет рассказано в следующих главах.

Краткие выводы

На основании вышеизложенного материала, можно сделать следующие выводы:

1. Общепринятые способы построения сетей (СКС) могут быть не оптимальны для небольших сетей с числом рабочих мест менее 50, и в каждом отдельном случае требуют специального рассмотрения.

2. Совершенно ясно, что домашние сети не могут являться СКС, это САМОСТОЯТЕЛЬНЫЙ КЛАСС КАБЕЛЬНЫХ СИСТЕМ. Который еще только ждет своих стандартов.

Так как данная книга в основном ориентирована на сети, относящиеся именно к этим двум пунктам, в дальнейшем изложении термин СКС без крайней необходимости не используется. Вместо этого будет сделан упор на физических основах передачи данных, а в дальнейшем - на практических способах построения небольших сетей, и сетей "последней мили".

Глава 5. Небольшие сети для офисов.

Самая длинная дорога начинается с первого шага

Рассматривать построение сетей "в общем" не имеет смысла. Несмотря на то, что во всех случаях используется практически одинаковое оборудование, одинаковая среда передачи, слишком сильно разнится подход для соединения нескольких компьютеров в офисе, и построение структурированной кабельной сети масштаба группы зданий.

Каждый небольшое фрагмент будет одинаков, а вся сеть в целом - различна. В этой главе будут в общих чертах описаны наиболее характерные варианты, такие как простейшая сеть из нескольких компьютеров, сеть малого офиса (5-10 компьютеров), и недорогая сеть небольшой фирмы (до 40-60 компьютеров).

При этом рассмотрение базовых свойств среды передачи и функционирования протоколов разных уровней вынесено в 7, 8 и 9 главы, а подробности технической реализации больших домашних (территориальных) сетей рассмотрены во второй части этой книги.

Если придерживаться формальной логики, то рассматривать практические моменты нужно только после полного описания всех теоретических аспектов. Но, на мой взгляд, углубляться в тонкости функционирования сети можно только после получения практических навыков (или хотя бы понятия о них).

Несколько в стороне будет оставлен вопрос выбора производителя оборудования и материалов. Для недорогих сетей этот вопрос стоит очень остро, и вполне заслуживает отдельной главы (или даже нескольких глав).

Глава 5

Соединение в сеть двух компьютеров.

Как самое большое здание может быть построено из небольших кирпичиков, так и прокладка коммуникаций любого масштаба сводится в конечном итоге к соединению между собой двух активных устройств (компьютеров, коммутаторов, повторителей, маршрутизаторов).

Для простейшей сети кроме двух компьютеров потребуются два сетевых адаптера, и соответствующим образом оконцованный кабель (коаксиальный или витая пара). Процесс установки адаптеров, как правило, весьма прост, и в дополнительном пояснении не нуждается. В крайнем случае, его можно провести по описанию, которое должно прилагаться к программному обеспечению на оборудование.

Таким образом, для соединения двух компьютеров в сеть Ethernet необходимо провести следующие операции:

- изготовление кабеля, и его подключение к сетевым адаптерам;
- настройка компьютеров.

Дополнительную сложность вызывает то, что первый пункт зависит от среды передачи, и должны быть рассмотрен отдельно для разных случаев (коаксиального кабеля и витой пары). Несмотря на то, что "коаксиал" уже давно не применяется в больших сетях, он остается удобным средством для соединения нескольких компьютеров с минимальными затратами. Поэтому его необходимо описать (хоть и достаточно кратко).

Подготовка к работе с витопарным кабелем (UTP)

Для работы потребуется витая пара, два разъема RJ-45, обжимное устройство. И примерно 1 минута на сам процесс. Но сначала надо определиться с выбором материалов и инструмента.

Витая пара. Так как для протоколов 10/100baseT используется только две пары, то можно использовать кабель 2-х или 4-х парный. При использовании 4-х парного варианта две пары остаются в резерве (могут быть использованы, например, в 1000baseT).

Следует различать кабель с проводником из монолитной проволоки толщиной 0,5 - 0,65 мм (solid), и многопроволочные конструкции, в которых проводники состоят из нескольких (обычно 7) тонких проволок 0,2 мм. Второй вариант имеет значительно более плохие электрические характеристики, и используется только для изготовления коммутационных шнуров, которым необходима большая гибкость.

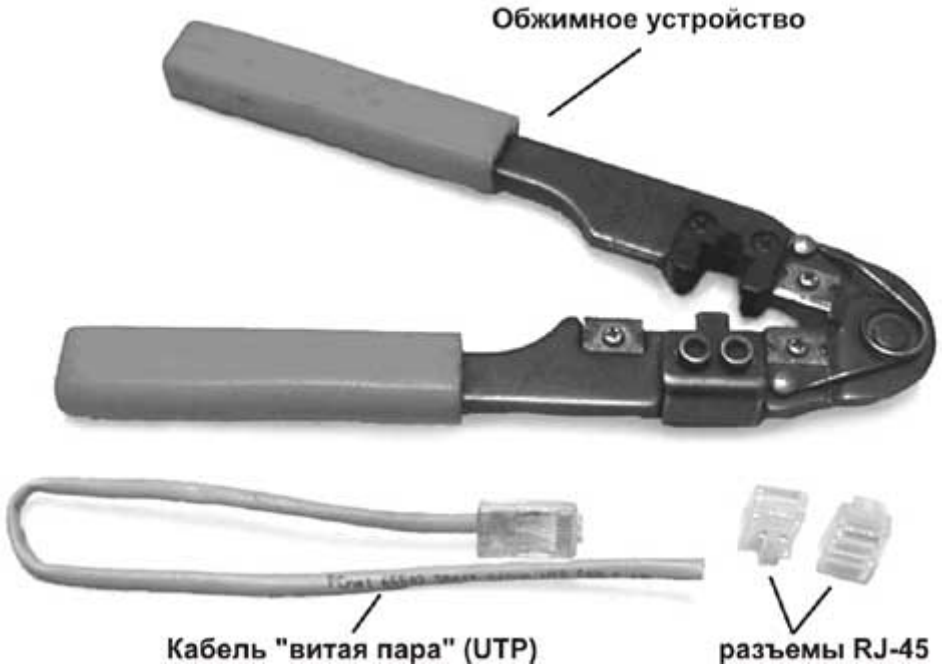

Рис. 5.1. Инструменты и материалы, необходимые для установки разъемов на витопарный кабель.

Штекерные разъемы RJ-45 (вилки). Тип разъема должен соответствовать используемому кабелю. При внешнем сходстве, конструкция врезного контакта для проводника из монолитной проволоки немного отличается от контакта, используемого в многопроволочной конструкции. Это важный момент, и ошибка в выборе рано или поздно приведет к плохому контакту со всеми вытекающими последствиями.

Второе ограничение - в сети нужно использовать разъемы соответствующей категории (3 или 5). Различие в них весьма условно, и носит скорее косметический характер. Ранее в 5 категории часто использовался специальный пластиковый вкладыш, в который укладываются проводники перед введением внутрь разъема. Его назначение - обеспечить минимальную длину расплетения пар, и тем самым улучшить электрические характеристики среды передачи.

В настоящее время преимущественно используют разъемы 3 и 5 категории одинаковой конструкции. Проводники вводятся внутрь по специальным желобкам в корпусе. Это требует несколько большей квалификации от монтажников, но в общем не представляет трудности.

Обжимной инструмент. Существует очень много разновидностей по цене от $5 до $50. Результат применения разных типов примерно одинаковый, отличие состоит скорее в долговечности и удобстве работы. В любом случае, даже инструмент начального уровня должен иметь ножи для обрезки кабеля и снятия изоляции. На практике, наиболее распространен тип HT-210 (Hanlong), который и будет использован в примерах ниже по тексту.

В самом крайнем случае можно обжать разъем подручным инструментом (отверткой). В опытных и твердых руках результат получится вполне сносным, но рекомендовать такой подход как "обычный" ни в коем случае нельзя.

Глава 5

Установка разъемов на витопарный кабель (UTP)

Порядок работы при установке разъемов лучше всего расписать по операциям, и сопроводить их фотографиями.

1. Необходимо ровно отрезать кабель. Даже если старый срез хорошо выглядит, вполне возможно, что под оболочку проникла влага или грязь. Желательно пожертвовать 5-10 сантиметрами, чем рисковать получить некачественное соединение.

2. Снятие оболочки. Для установки разъема нужно освободить от оболочки примерно половину дюйма (1,25 см) проводников. Большинство обжимных инструментов имеют для этого специальное приспособление - пара лезвий и ограничитель. Нужно вставить конец кабеля до упора, и надрезать изоляцию. Именно надрезать, а не прорезать - важно не повредить жилы кабеля. В материале оболочки должно быть достаточно мела для легкого "отламывания" по получившейся линии надреза.

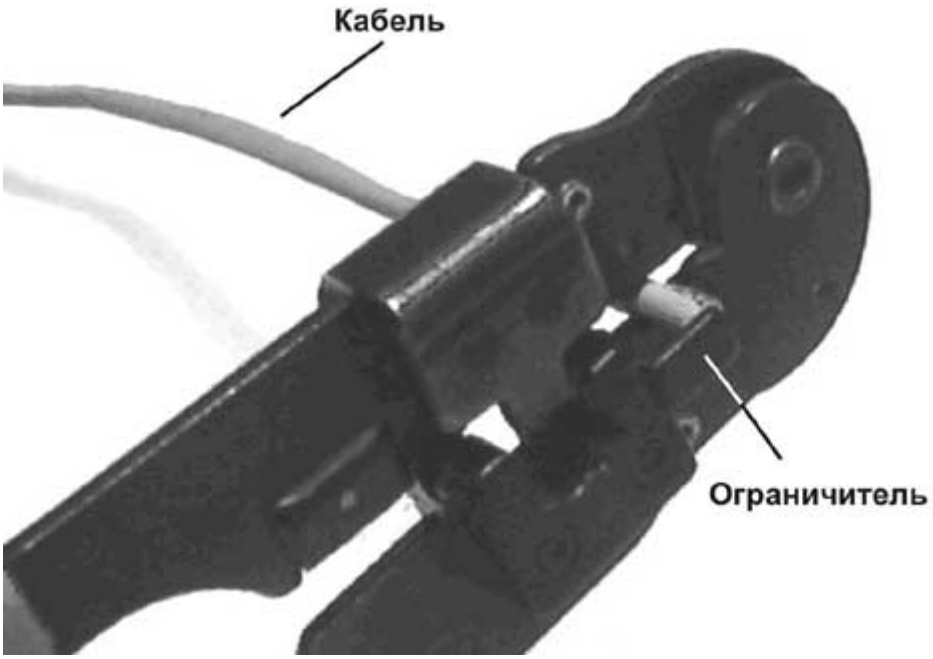

Рис. 5.2. Снятие оболочки кабеля.

3. Сортировка и выравнивание проводников. В принципе, нет никакой разницы, какая из пар кабеля будет подключена к передатчику сетевого адаптера, а какая к приемнику. Главное, что бы были подключены именно пары, а не проводники из разных пар.

Очевидно, что значительно проще делать все разъемы одинаково, а еще лучше по общему для всех разъемов в мире стандарту. Благо, что он есть - EIA/TIA-568B.

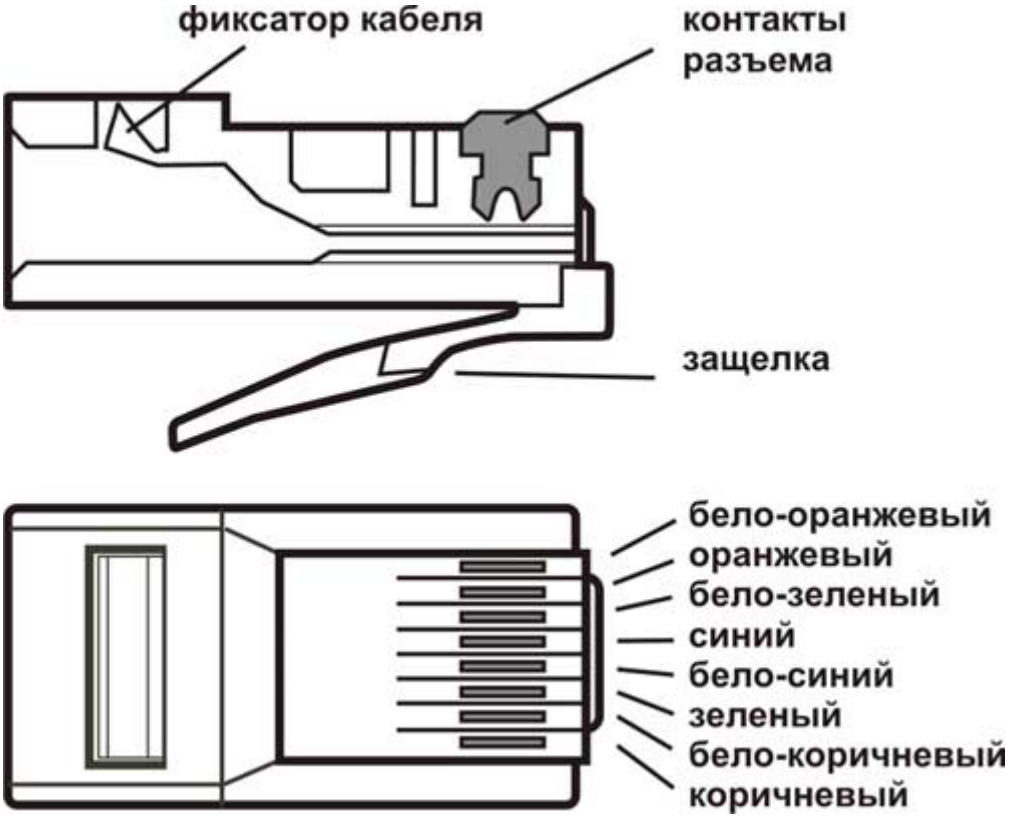

Рис. 5.3. Разъем RJ-45 и порядок обжима проводников.

Можно заметить, что пары подключаются к следующим контактам - 1-2, 3-6, 4-5, 7-8. В 10/100baseT используется только первые две пары контактов - 1-2 и 3-6, остальные являются резервными. Если используется 2-х парный кабель, то подключать пары нужно именно к этим контактам, оставляя остальные свободными.

Для сортировки проводников неизбежно придется расплетать пары. Это нужно делать на минимальную длину (по стандарту не более чем на 1,25 см), как можно меньше нарушая структуру пар, геометрические размеры и шаг повива не задействованной в разъеме части кабеля.

После того, как проводники будут ровно уложены, и выпрямлены, нужно выровнять край - немного подрезать на одну длину.

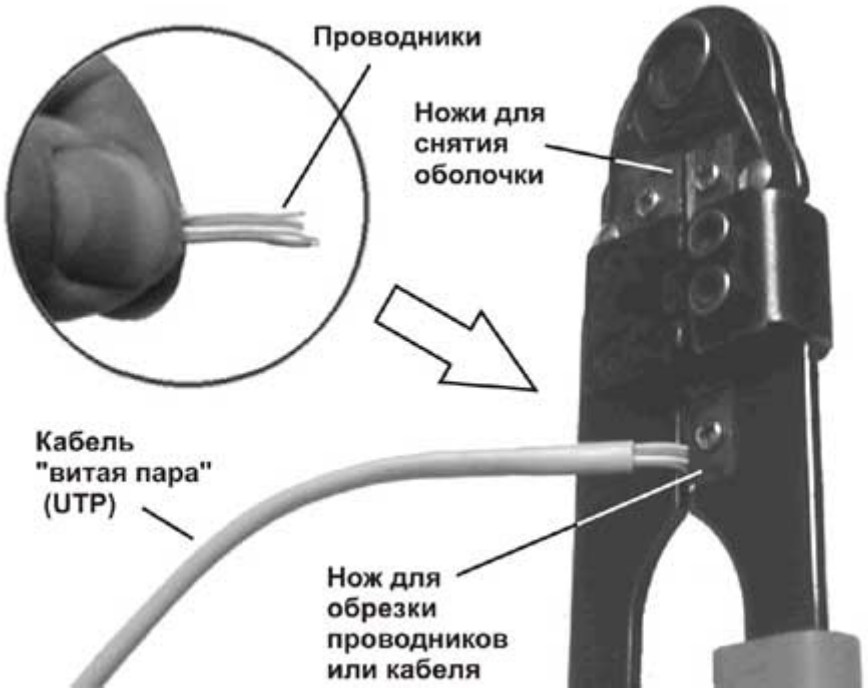

Рис. 5.4. Выравнивание проводников перед введением в разъем.

4. Вставлять проводники в разъем нужно плавно и не торопясь. Каждая жила должна попасть в свой паз внутри RJ-45, и дойти до упора. Процесс удобно контролировать через прозрачный корпус разъема (при необходимости можно использовать лупу). Если какой-либо проводник не прошел до конца, нужно вытащить кабель целиком из разъема и повторить процесс начиная с п. 3.

5. Далее нужно как можно глубже засунуть в корпус разъема край оболочки кабеля. По крайне мере, он должна заходить "за" фиксатор, что бы после обжима удерживаться последним.

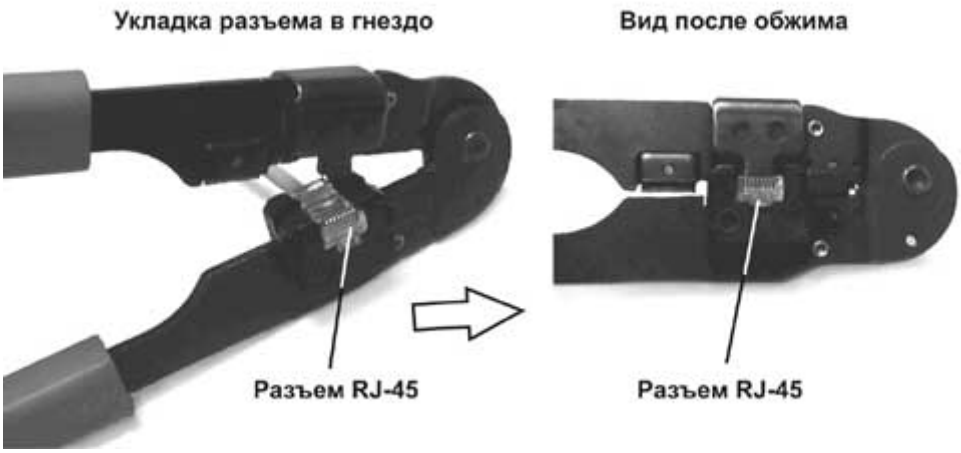

Рис. 5.5. Обжим разъема RJ-45.

6. Перед обжимом желательно еще раз убедиться, что все жилы и оболочка кабеля находятся на положенных местах. После этого можно вставить разъем в соответствующее гнездо на инструменте, и в одно движение (но плавно), произвести обжим. При этом острые кромки контактов прорежут изоляцию, и обеспечат надежный контакт. А фиксатор будет утоплен внутрь корпуса, дополнительно закрепляя кабель.

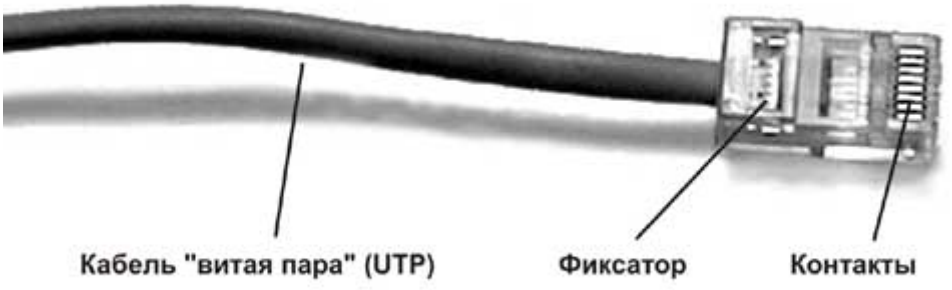

Рис. 5.6. Готовый разъем RJ-45 на кабеле.

7. Разъем готов. Перед использованием его желательно осмотреть, обращая особое внимание на состояние контактов. Все они должны выступать из корпуса на равную высоту.

Подобную последовательность действий нужно выполнить с другим концом кабеля. При этом, необходимо особо отметить, что существует две разновидности кабелей - прямые (контакты 1-2 и 3-6 первого разъема соединяются с контактами 1-2 и 3-6 второго) и перекрестные (контакты 1-2 и 3-6 первого разъема соединяются с контактами 3-6 и 1-2 второго).

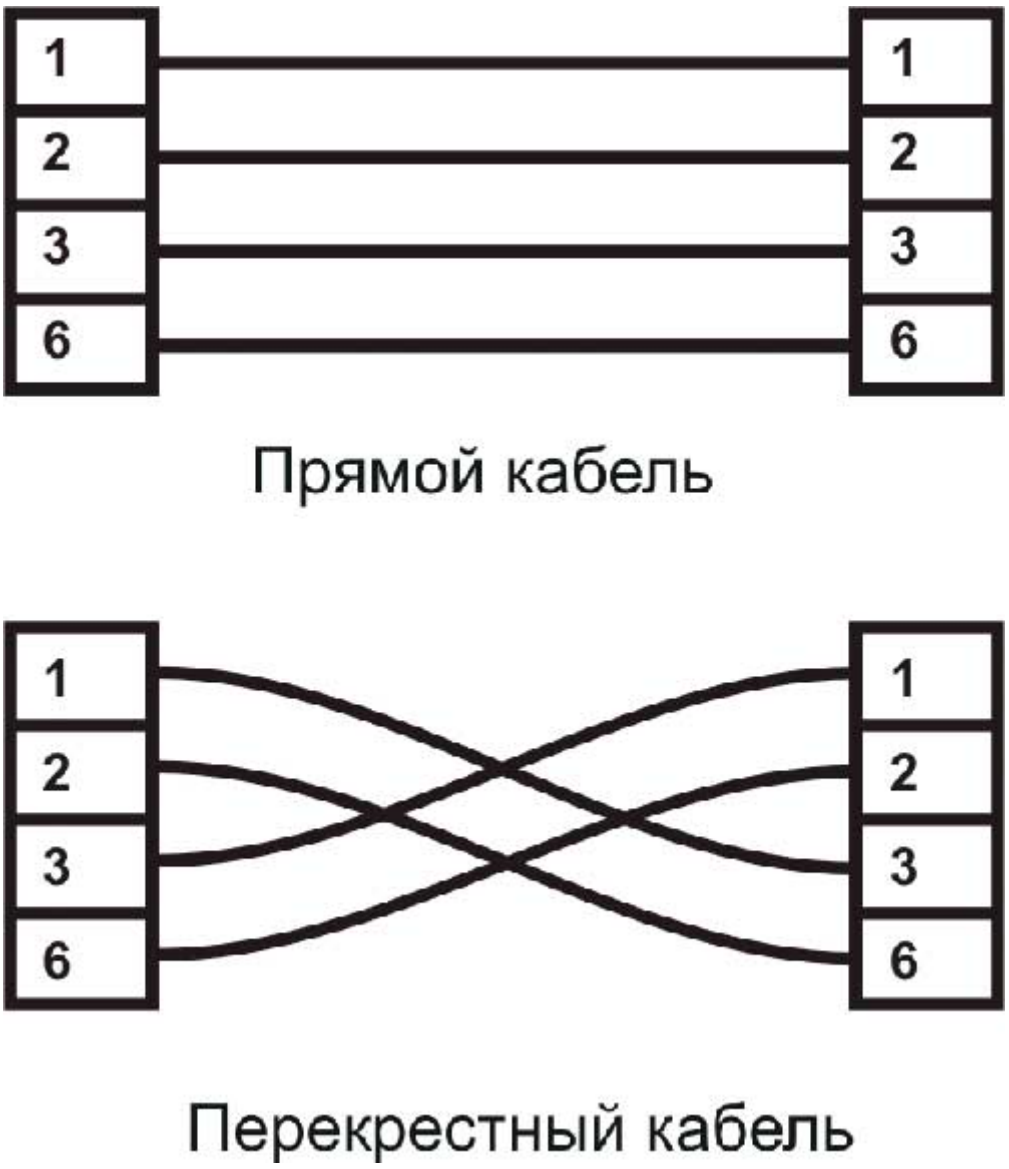

Рис. 5.7. Прямой и перекрестный кабель

Физический смысл достаточно прост - передатчик одного устройства должен быть соединен с приемником другого. Поэтому, для соединения одинаковых устройств (например, двух компьютеров) нужно использовать перекрестный кабель. В хабах, коммутаторах, и подобном оборудовании конструктивно заложена перекрестная разводка, и для их соединения с компьютером используется прямой вариант кабеля.

В то же время, например два хаба, два коммутатора, или хаб с коммутатором можно соединять двумя вариантами. Либо перекрестным кабелем в обычные порты, либо прямым кабелем в порты uplink (в некоторых моделях для изменения разводки порта используется специальный переключатель). В новом активном оборудовании эта проблема обычно решена кардинально - введена функция автовыбора, поэтому будет нормально работать любой вариант разводки пар в кабеле.

Для дополнительной защиты кабеля от механических повреждений, около разъема может быть использован защитный колпачок. Простая и дешевая мера, которой, к сожалению часто пренебрегают. Кроме этого, некоторые типы защитных колпачков защищают от обламывания (при грубом обращении) защелки разъема RJ-45.

Для установки разъема в гнездо сетевого адаптера дополнительных навыков не требуется - ошибиться совершенно не возможно. Единственное, на что стоит обратить внимание - проверить качество фиксация (разъем не должен вываливаться без нажатия на соответствующий элемент).

Глава 5

Подготовка к работе с коаксиальным кабелем (RG-58)

Для работы потребуется коаксиальный кабель, два разъема, два Т-коннектора, два терминатора, устройство для обрезки, и обжимные клещи (crimping tool). Сам процесс может занять сравнительно много времени, около 3-5 минут.

Коаксиальный кабель. Существует много типов коаксиального кабеля - от РК-50 Российского производства, до весьма сложных (и дорогих) конструкций иностранных производителей. Отличие может быть в диаметре, материале диэлектрика, центральной жилы, экрана. Поэтому под каждый тип кабеля могут потребоваться свои особенные разъемы.

Но на практике наиболее распространен кабель RG-58, для которого разработаны разъемы типа BNC.

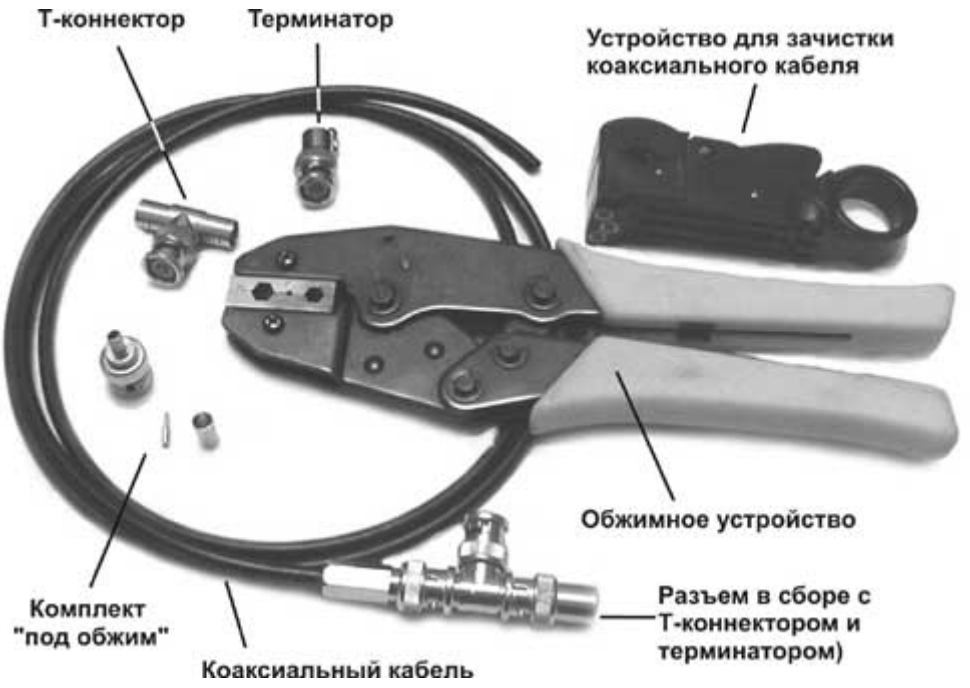

Рис. 5.8. Инструменты и материалы, необходимые для оконцовывания коаксиального кабеля.

Разъемы типа BNC. В общем, все типы разъемов можно разделить на 3 большие группы. Для пайки (например, отечественные СР-50-74-ПВ), под обжим, и навинчивающиеся (twist-on). Первый вариант несколько надежнее, долговечнее, и даже дешевле остальных. Но требует большого времени, инструмента и высокой квалификации монтажников.

Вариант с использованием обжима наиболее распространен. Как главный недостаток такого разъема можно назвать одноразовость. В случае повреждения соединения его придется отрезать, и установить новый.

Навинчивающие разъемы редко встречаются, дороги, относительно не надежны. Единственный плюс - легкость монтажа даже в полевых условиях.

Обжимное устройство (инструмент). Более всего внешним видом напоминает большие кусачки сложной конструкции. Подавляющее большинство моделей позволяет выполнить две операции - общим центрального контакта, и обжим оплетки на хвостовике. Для этого применяются разные фасонные штампы на губках обжимного устройства.

Следует отметить следующую особенность устройства одной из самых распространенных моделей. В ней предусмотрен храповой механизм, который препятствует разжиманию губок инструмента до полного обжима разъема. При этом работа неизбежно проводится "в одно движение" - именно так, как нужно для обеспечения надежного и долговечного контакта.

Приспособления для зачистки изоляции. Конструкция коаксиального кабеля заметно сложнее, чем витой пары. Соответственно, операция по снятию части изоляции более трудоемка, требует специального приспособления. При некотором навыке, ее можно проделать при помощи скальпеля, но это будет по истине "ювелирная работа".

Т-коннекторы и терминаторы. Присоединяются к уже закрепленному на кабеле разъему. Т-коннекторы служат для подключения кабеля к сетевому адаптеру, а так же сборки кабелей в единую шину (или подключения терминатора). Терминатор - это, по сути, заглушка, соединяющая центральную жилу и оплетку через активное сопротивление, совпадающее по величине с волновым сопротивлением кабеля (для Ethernet 50 Ом). Служит нагрузкой, в которой электромагнитные волны гасятся не вызывая отраженного сигнала.

Кусачки, или бокорезы. Можно использовать любой (вплоть до ножниц или ножа) инструмент, способный разрезать тонкий коаксиал, и в случае необходимости "подровнять" кончик центральной жилы или остатки оплетки. Некоторые наборы для работы с коаксиальным кабелем комплектуются специальными кусачками с полукруглыми ножами. Они удобны в массовой работе, но не более того.

Установка разъемов на коаксиальный кабель (RG-58)

Для описания установки коаксиального разъема применим уже знакомый по витой паре пооперационный метод.

1. Начать лучше всего с той же самой операции, что и для витой пары - обрезания небольшого кончика кабеля. Хотя на первый взгляд коаксиальный кабель выглядит плотным монолитом, его оплетка очень легко "набирает" воду. А наличие влаги вовсе не способствует возникновению качественного контакта. 2. Зачистка изоляции. Для коаксиального кабеля это весьма деликатная операция, при проведении которой используется специальный инструмент, отдаленно напоминающий бельевую прищепку. Кабель RG-58 (подобно веревке) закладывается под подпружиненную часть. По инструкции, конец кабеля не должен выступать за габарит устройства. Но в реальности удобнее оставить "снаружи" небольшой запас в 3-5 мм. Это позволит позже исправить некоторые ошибки в работе (если они, конечно, возникнут). 3. Затем устройство

несколько раз поворачивается вокруг кабеля, разрезая находящимися внутри ножами изоляцию на фиксированную глубину. Надо отметить, что под каждый тип кабеля может потребоваться индивидуальная настройка ножей.

Рис. 5.9. Надрезание изоляции коаксиального кабеля

4. После надрезания изоляции нужно осторожно удалить отрезанные части. Если все было сделано правильно, то внешний вид конца кабеля должен соответствовать показанному на Рис. 5.10, и образовывать аккуратные "ступеньки" - оплетка, изолятор - центральная жила.

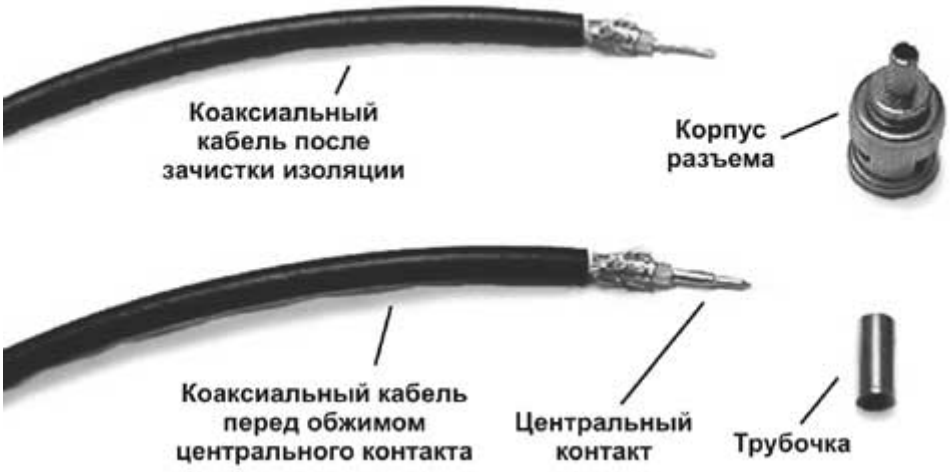

Рис. 5.10. Вид кабеля после зачистки изоляции.

5. Далее нужно надеть на центральную жилу контакт. При этом нужно, что бы кончик проводника полностью умещался внутри контакта, а последний краем плотно прилегал к срезу диэлектрика. Но при этом остаток жилы должен быть достаточно длинным, что бы надежно удерживаться всей внутренней поверхностью контакта после его обжимания.

6. Обжимание центрального контакта не требует особых навыков. Достаточно обычной аккуратности. Перепутать штамп почти невозможно, а способ укладки хорошо виден на Рис. 5.11.

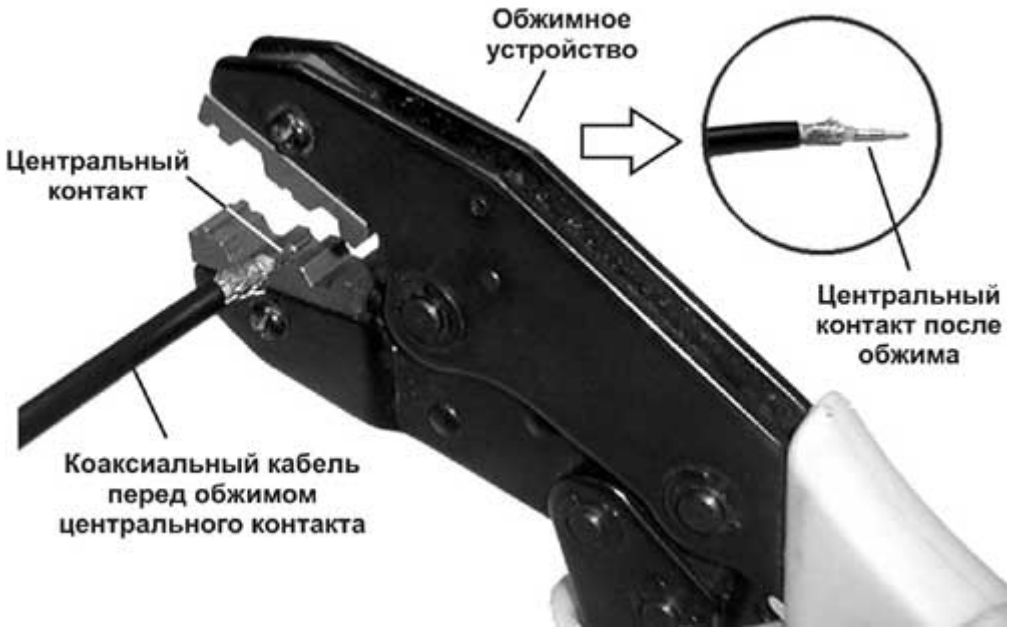

Рис. 5.11. Обжимание центрального контакта.

Главное не повредить рабочую часть центрального контакта, для чего при обжиме она должна находиться в специальной прорези.

7. Далее нужно надеть на конец кабеля корпус разъема. Но перед этим - не забыть про трубочку, при помощи которой обжимается оплетка. Строго говоря, ее желательно надеть в самом начале работы, еще до надрезания - тогда не будет мешать оплетка. Но не поздно это сделать и непосредственно перед установкой корпуса.

Рис. 5.12. Разъем перед обжиманием оплетки.

Оплетку (и фольгу, если она есть) нужно аккуратно расправить, и пустить поверх хвостовика корпуса разъема. Если кабель имеет редкую или непрочную оплетку, то желательно ее собрать в несколько более плотных "косичек". Затем нужно поставить трубочку на место.

8. Далее нужно поместить разъем в обжимное устройство, и: обжать. Распространенные модели инструмента позволят сделать это только "в одно движение", и только с определенным усилием.

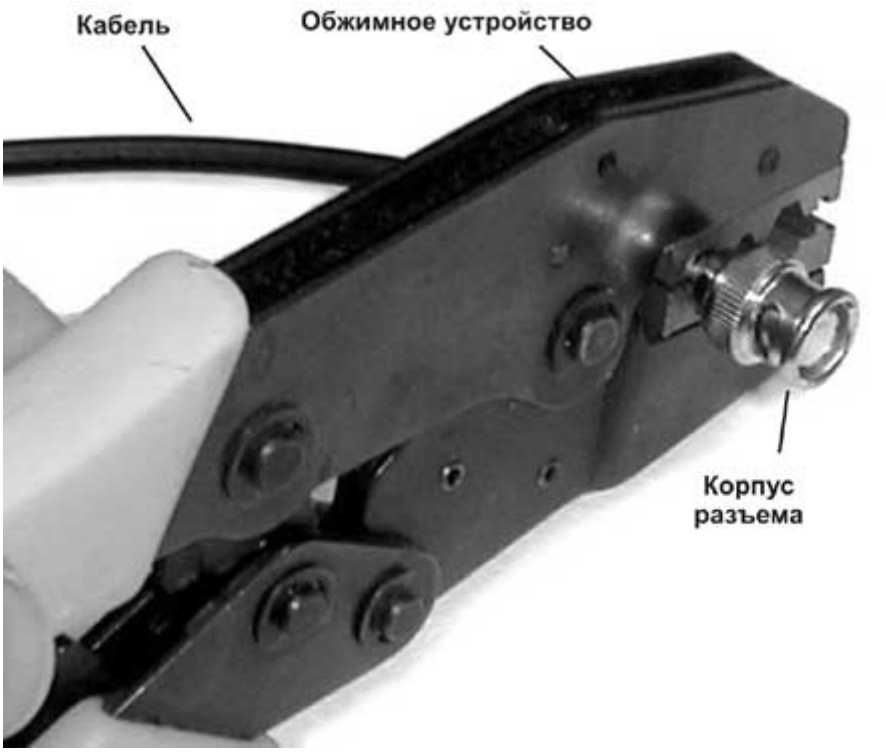

Рис. 5.13. Обжим оплетки BNC разъема.

9. Остается присоединить к разъему Т-коннектор, терминатор, и кабель можно присоединять к сетевому адаптеру.

Рис. 5.14. Кабель готов к использованию.

Кабель готов к использованию, и его можно присоединять в сетевому адаптеру. Ошибиться при выполнении этой операции почти невозможно.

Основные моменты настройки компьютеров

Останавливаться подробно на этом этапе создания сети не имеет большого смысла. Перечислить все множество протоколов и операционных систем трудно. Тем более, нельзя в рамках данной книги охватить все разнообразие особенностей программного обеспечения. Но хотя бы основные моменты установления связи систем с ОС Windows по протоколу TCP/IP нужно показать.

Будем исходить из предположения, что сетевые карты установлены. При этом на рабочем столе должен появиться значок "сетевое окружение".

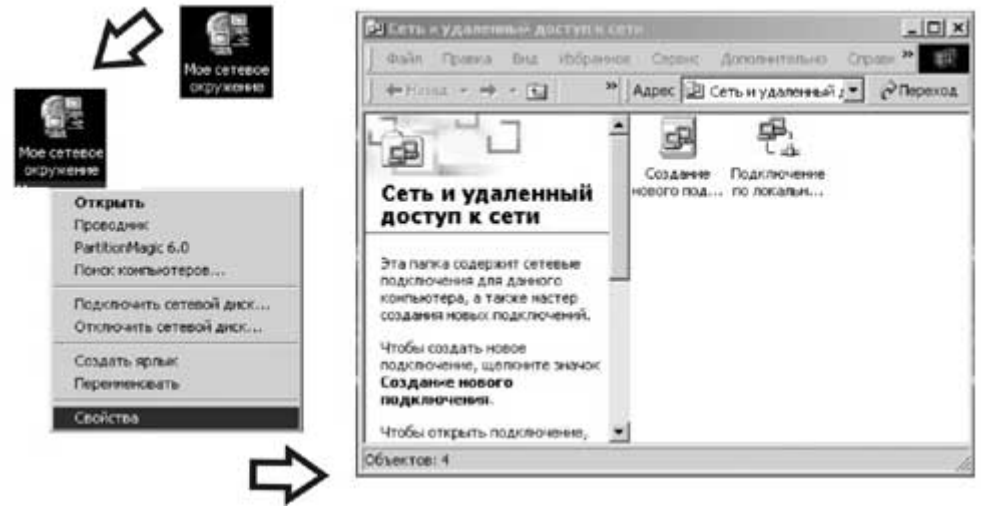

Рис. 5.15. Выход с папку "сеть и удаленный доступ к сети".

Выйти в папку "сеть и удаленный доступ к сети" весьма не сложно - по правой кнопке мыши на пиктограмме "сетевое окружение" выбирается строка "свойства".

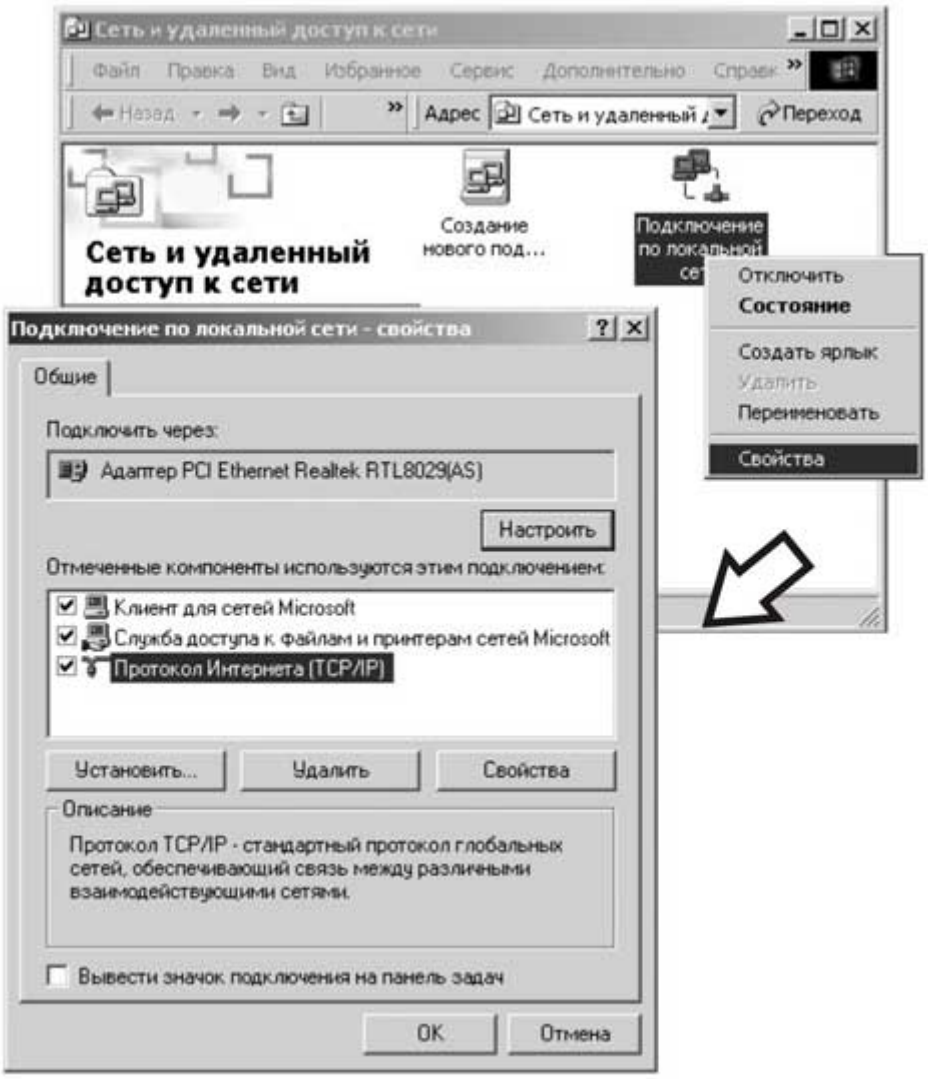

Рис. 5.16. Подключение по локальной сети - свойства.

Далее нужно выбрать пиктограмму "подключение по локальной сети - свойства", и открыть соответствующее окно. "Клиент для сетей Микрософт" установится автоматически, в любом случае. "Служба доступа к сетям и принтерам:" используется при работе через сетевое окружение, и для доступа в Интернет, например, не нужна.

В случае необходимости, нужную службу или протокол можно легко добавить или убрать при использовании соответствующих кнопок.

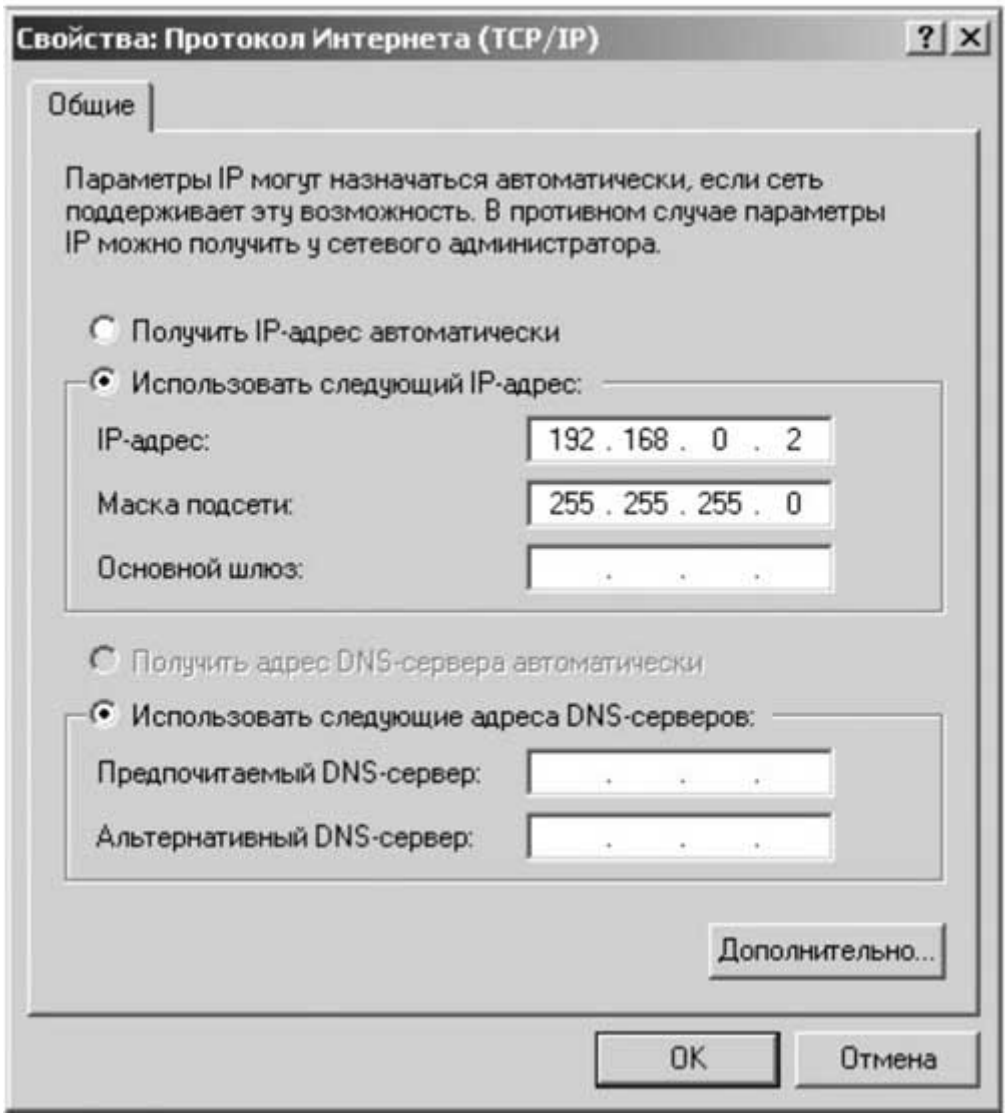

Рис. 5.17. Протокол Интернета TCP/IP.

Некоторой настройки требует "Протокол Интернета TCP/IP". В соответствующих полях нужно прописать в явном виде IP-адрес компьютера. На Рис. 5.17. использован адрес 192.168.0.2 и маска 255.255.255.0.

Прописывать адрес шлюза, и DNS для простой сети нет необходимости.

Работоспособность полученной сети удобно проверять командой ping. Для этого из командной строки запускается ping 192.168.0.1 (адреса, с которым нужно связаться). Если получается ответ типа "Ответ от 192.168.0.1: число байт=32: время=1мс TTL=64", то все сделано нормально, и на уровне IP сеть работает. Если ответ "Превышен интервал времени для запроса", то что-то сделано не правильно, и нужно искать причину неисправности.

При успешном испытании сети можно настраивать необходимое программное обеспечение более высокого уровня - обмен файлами, ftp, http, использование базы данных, и т.п. Но этот момент лежит уже далеко за рамками данной книги.

Глава 5

Создание сети малого офиса (5-10 рабочих мест)

После успешного соединения в сеть двух компьютеров, можно постараться расширить сеть до 5-10 машин. С выделенным сервером, принтером, и доступом в Интернет. Несмотря на небольшую величину, такие проекты вполне востребованы. Именно такую конфигурацию имеет подавляющее большинство сетей малых офисов.

Попробуем конкретизировать задачу для некой средней фирмы.

Предположим, для работы на одном из этажей арендованы 2-3 комнаты средних размеров, для 7-8 сотрудников. Серьезных требований по надежности, и скорости не ставится. Все несколько проще - на сервере хранятся общие файлы, работает бухгалтерская программа. Для совместного пользования выделен сетевой принтер начального уровня. И, конечно, вся эта сеть подключена к провайдеру Интернет посредством канала Ethernet.

Выбор идеологии

Очевидно, что задачу можно решить разными способами, с разной стоимостью, надежностью, и долговечностью. Что важнее, что предпочесть?

В Главе 4 было показано, что традиционный подход построения структурированных кабельных сетей (СКС) может повлечь лишние затраты. Для их оптимизации нужно задать еще некоторые дополнительные условия, позволяющие выбрать идеологию построения ЛВС. Этот процесс удобно показать в виде следующей блок-схемы:

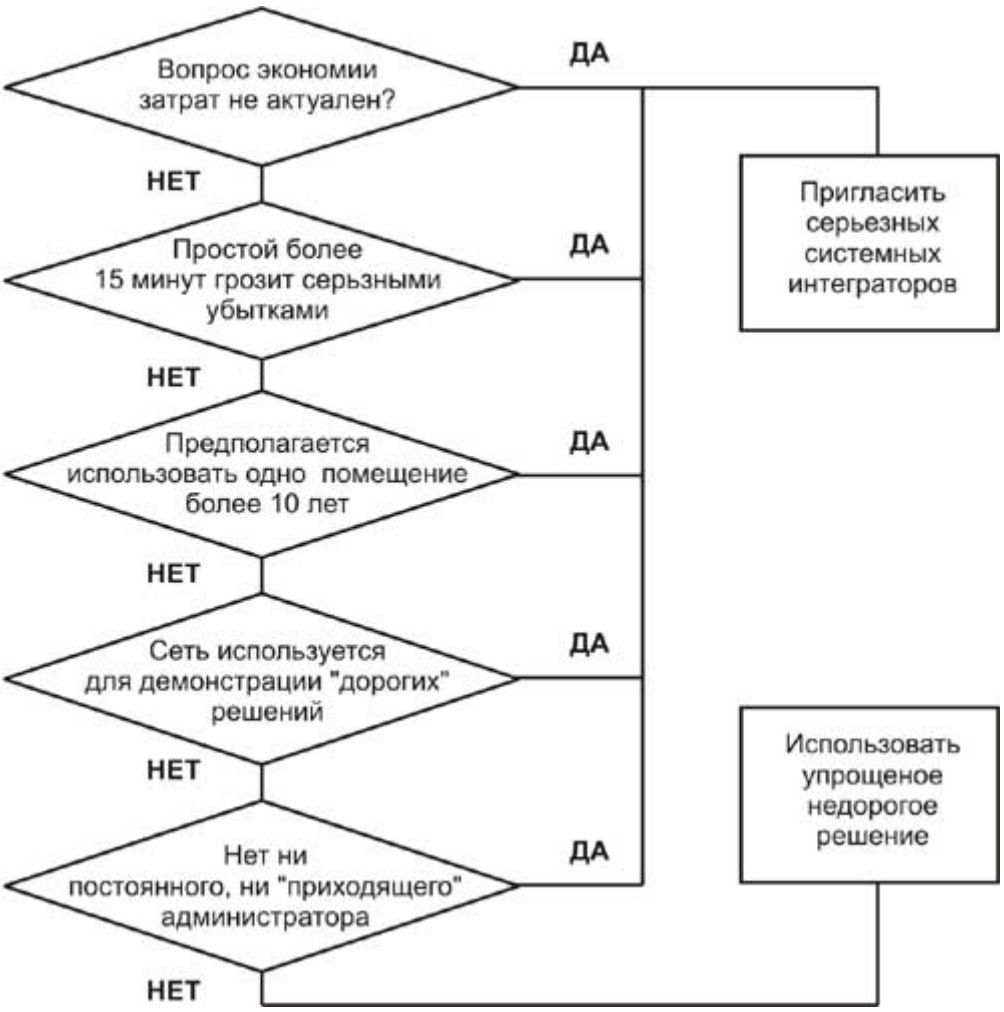

Рис. 5.18. Выбор идеологии построения сети.

Так как данная книга посвящена строительству недорогих сетей своими силами, при несоблюдении указанных условий нельзя предложить иного выхода, как обратиться к серьезным системным интеграторам. Которые смогут качественно, быстро, но совсем не дешево построить нужную вам сеть. В остальных случаях вполне возможно решить задачи с меньшими затратами.

Однако, категорически не рекомендуется впадать в противоположную крайность, и пытаться построить сеть на остатках коаксиального кабеля и списанных сетевых адаптерах. Это, разумеется, возможно, но имеет смысл только для 2-3 компьютеров при серьезнейшей нехватке ресурсов, например в школьном кабинете информатики.

Что из себя будет представлять оптимальное на сегодня решение? Для офисной сети нет никакого смысла ограничиваться 10 мегабитами, и, тем более, использовать коаксиальный кабель. Так же отошла в прошлое разделяемая среда - неуправляемые коммутаторы по стоимости сравнялись с хабами (подробно особенности активного оборудования описаны в 10 главе).

Использование кроссов, специальных телекоммуникационных шкафов представляется не целесообразным. Но настенные короба совсем не помешают. Розетки крайне желательны, но, в крайнем случае, можно обойтись и без них.

Составление эскизного проекта

При наличии большого опыта и некоторого запаса расходных материалов, можно обойтись без эскизного проекта. Уж слишком прост рассматриваемый вариант сети для реализации на практике. Но даже в этом случае не помешает сделать простейший набросок, и подписать его у заказчика (или руководителя). Как показывает практика, бумага с подписью слишком часто бывает не лишней.

Основная проблема при разработке подобного проекта - выбрать наилучший путь прокладки кабелей от рабочих мест, и размещения коммутатора. Тут очень много зависит от планировки, материала и толщины стен, и общие рекомендации дать сложно. Тем не менее, задача эта не сложная, и для ее решения вполне достаточно здравого смысла. В любом случае, эскиз весьма условен, и небольшие коррекции по мере строительства сети пойдут ему только на пользу.

Особое внимание нужно обратить на вопросы электропитания коммутатора и сервера. Оно должно быть достаточно надежным. Иногда имеет смысл отремонтировать старую розетку, или поставить новую. Так же не помешает подвести хорошее защитное зануление/заземление. Удлинители крайне не желательны - при уборках или перемещениях мебели они страдают в первую очередь.

Вот пример простого эскизного проекта:

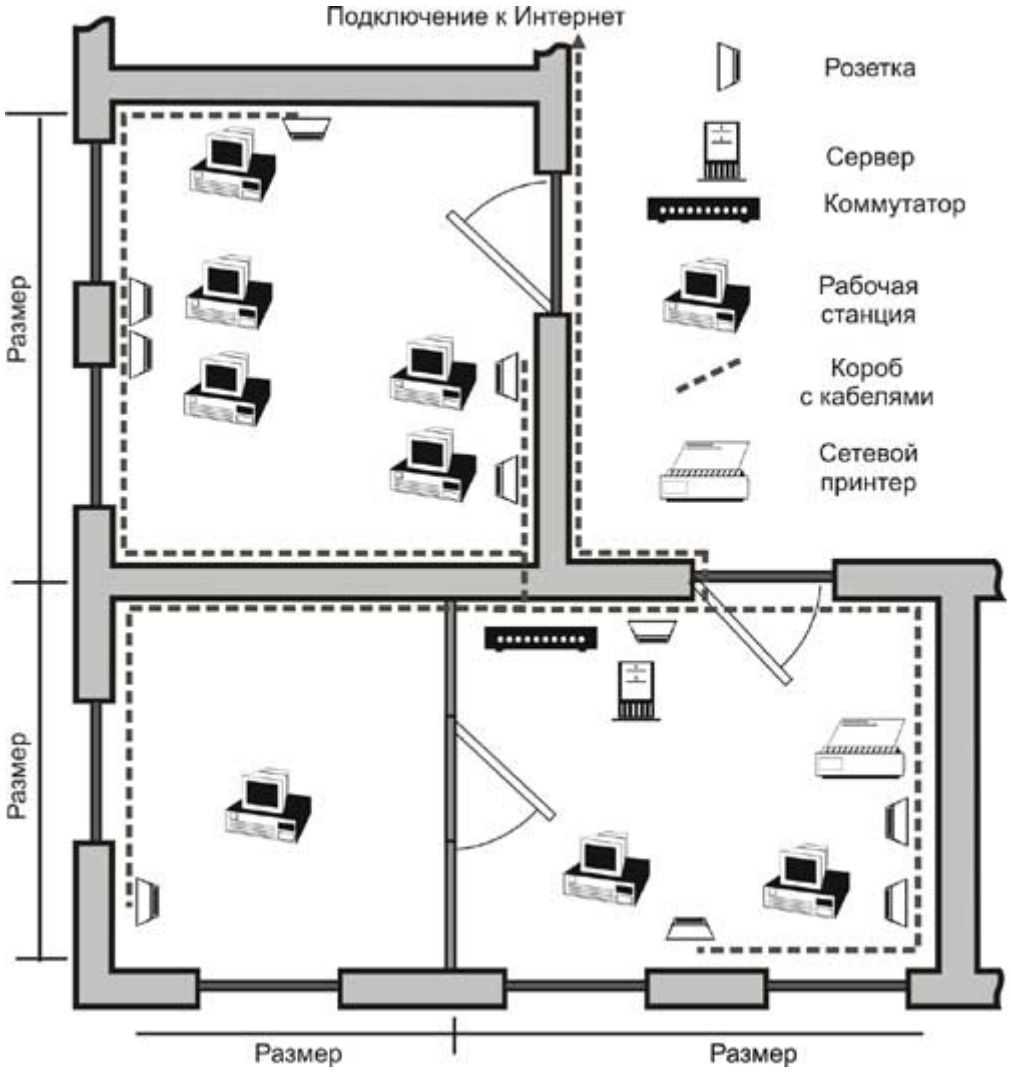

Рис. 5.19. Эскизный проект построения сети.

На основании плана (и геометрических размеров помещения) нужно определиться с закупкой оборудования и материалов по следующим позициям:

1. сетевые карты;
2. коммутатор;
3. кабель;
4. штекерные разъемы (вилки);
5. гнездовые разъемы (розетки);
6. абонентские кабеля;
7. короба и декоративные элементы;
8. расходные материалы;
9. инструменты и приспособления.

Выбор конкретной фирмы-изготовителя вопрос достаточно сложный. На этот счет есть множество мнений, а их противостояние часто не уступает по накалу знаменитому "Intel против AMD". Замечу лишь, что для решения простых задач вполне годится материалы и оборудование даже малоизвестных марок типа Genius, Surecom, Eline, Compex, и им подобных. Конечно, при использовании более известных брендов (3com, Cisco, Intel, и т.д.) сеть хуже работать не будет. Но вероятно, что адекватного выигрыша в скорости и долговечности получить не удастся из-за условий, описанных выше.

В крайнем случае, можно воспользоваться консультацией фирмы-продавца. Нужно просить "средние" решения, и с очень большой вероятностью это будет как раз то, что нужно.

Отдельно нужно рассмотреть случай, когда параллельно локальной сети делается телефонная разводка от мини-АТС. Для небольшого офиса это скорее не типичный случай, чем общепринятая практика, поэтому подробнее этот вариант будет рассмотрен в следующем примере. Но надо отметить, что требования к качеству кабельной системы для передачи голоса очень низки по сравнению с передачей данных, и при необходимости прокладка производится без каких-либо проблем.

Практическая прокладка сети

Ну вот, эскиз сделан, материалы закуплены, оборудование в наличии. Можно начинать строительство сети.

Первое, что необходимо сделать - это исследовать ситуацию с силовой проводкой. Очень неприятно, когда кабель под напряжением 220 Вольт попадает под бур перфоратора при изготовлении отверстия в стене, или гвоздь при прибивании короба. Конечно, если силовая проводка разводится одновременно с коммуникациями ЛВС, проблемы не возникает. Но когда кабеля уже уложены в стенах, к ним нужно относиться с большой осторожностью. Не стоит надеяться, что строители соблюли все требования ГОСТов и здравого смысла. Трассы могут иметь весьма неочевидные (и даже тупиковые) ответвления, или изгибы.

Для обнаружения скрытой проводки применяют специальные пробники (датчики электромагнитного поля). Приборы это простые, не дорогие, и весьма надежные. Если под рукой их не оказалось, то придется руководствоваться общими признаками - розетками, выключателями, распределительными коробками. Обычно силовая проводка проходит в стенах на 10-15 см. ниже потолка, но осторожность лишней не будет.

Однако, опасность силовой проводки заключается не только в возможности повреждения кабелей. При близком расположении с витой парой, на последнюю возможны наводки, влекущие сбои связи. Чем ближе расположены кабеля друг к другу, и чем больший ток протекает по силовой цепи, тем сильнее негативное влияние.

В некоторых национальных стандартах этот параметр очень жестко нормируется (вплоть до разнесения кабельных систем на 60 см. друг от друга). В Российской практике, инсталляторы СКС используют более либеральные правила. Внутриофисная проводка (мощность потребления менее 2 киловатт) не представляет угрозы целостности данных, и сети могут монтироваться рядом, или в одном и том же коробе (по соображениям электробезопасности короб должен иметь внутреннюю перегородку).

Второй по важности вопрос - отверстия в стенах и перегородках. Мало того, что эту грязную часть работы желательно пройти до распаковки из коробок красивой фурнитуры, и тем более, активного оборудования. Вполне может оказаться, что в самом удобном "на бумаге" месте стена окажется совершенно непроходимой. Или неожиданно подвернется силовая проводка. Будет очень неприятно, если заранее прибитый короб закончится на расстоянии 10 см. от нового отверстия. Наставить его не сложно, но "заплатки" никогда не улучшали внешний вид коммуникаций.

В зависимости от задач можно использовать разное оборудование. Для деревянной, или тонкой кирпичной стены (в один, максимум два киприча) вполне можно обойтись бытовой электродрелью с соответствующим сверлом. Для преодоления более серьезных преград (от 15 сантиметров до 1 метра) не обойтись без перфоратора. Устройство это дорогое, и при разовых работах проще всего взять в аренду вместе с соответствующими бурами.

Часто проще обойти капитальную стену в дверном проеме, как это сделано на эскизе (Рис. 5.19) для кабеля подключения ЛВС к Интернет, чем делать сложные отверстия. Экономия даже 5-10 метров кабеля не стоит затрат на использование дорогого инструмента (в отличие от строительства СКС, где такие аргументы в расчет не принимаются, да и с перфораторами профессионалам намного проще).

Следующая стадия - подготовка трасс для прокладок кабеля. В простом случае это означает установку коробов, потому что для небольших и недорогих сетей другие методы практически не используются. Но это не значит, что прокладки за подвесным потолком, под полом, или в других местах не целесообразны. Скорее наоборот, эти способы наиболее просты, экономичны. Просто из-за малого количества кабелей трассы специально не готовятся, а вопросы локального крепежа решаются простейшими способами при строительстве сетей.

Но вернемся к коробам. Их ассортимент достаточно широк, но общий принцип один. К стене прикрепляется основа короба, которая после укладки кабеля закрывается декоративной крышкой. Розетка (корпус с разъемом гнездового типа внутри) может крепиться как снаружи короба, так и быть частью его конструкции. Последнее красивее, надежнее, но немного дороже.

Крепить короба можно на шурупы, саморезы, болты, гвозди, двухсторонний скотч в зависимости от материала стен. Горизонтальные прогоны выполняются обычно на высоте около 60-80 сантиметров от пола. Стыковать друг с другом их можно при помощи конструкционно-декоративных элементов, правильно подобрать которые без

консультации продавца будет весьма затруднительно (этим нужно озаботиться на стадии закупок).

Прокладка кабеля не требует особых навыков. Следует только избегать изгибов с малым радиусом, и повреждения внешней оболочки. Тонкие короба (на 2-3 кабеля) по мере прокладки закрывают декоративной крышкой. В более толстых кабель сначала закрепляют от выпадывания специальными держателями из пластмассы (при их отсутствии сгодится плотный картон).

Если кабель прокладывается "верхом", то нужно помнить, что стандартами прямо запрещается укладывать его на каркас подвесного потолка. Это логично, так как создает дополнительную нагрузку, мешает работе других служб, эксплуатирующих здание, и вызывает дополнительный риск повреждения коммуникаций.

По правилам, полагается крепить кабель к стенам, или к специальным несущим тросам (струнам). Но реально, делать это ради 2-3 "витых пар" не имеет смысла. Нагрузка явно незначительная, помеха небольшая, а требования по надежности рассматриваемых вариантов невысоки. Зато прокладка очень проста и не требует больших трудозатрат. Так и лежат в большинстве случаев небольшие сети за подвесным потолком:

Кроме этого, возможны прокладки кабелей под фальш-полом, внутри перегородок, и многие другие варианты, предусмотреть которые заранее не представляется возможным. Единственное, что можно отметить особо - укладку витой пары по плинтусу (или прямо по стене) "под гвоздик". Страшного в этом ничего нет, но все же рекомендовать такой вариант для офиса не стоит (хотя порой он применяется в промышленных помещениях даже в СКС).

Оставшиеся после укладки кабелей концы нужно завести на разъемы, которые устанавливаются в розетки (нужно разделять розетку как декоративный элемент, и закрепленный в ней разъем как часть среды передачи). Розетки можно условно разделить на используемые для установки на стену, и в короб. Настенные модели не отличаются большим разнообразием конструкций - встречаются телефонные, 3 категории с креплением проводников "под винт", и более современные, с врезными контактами через изоляцию.

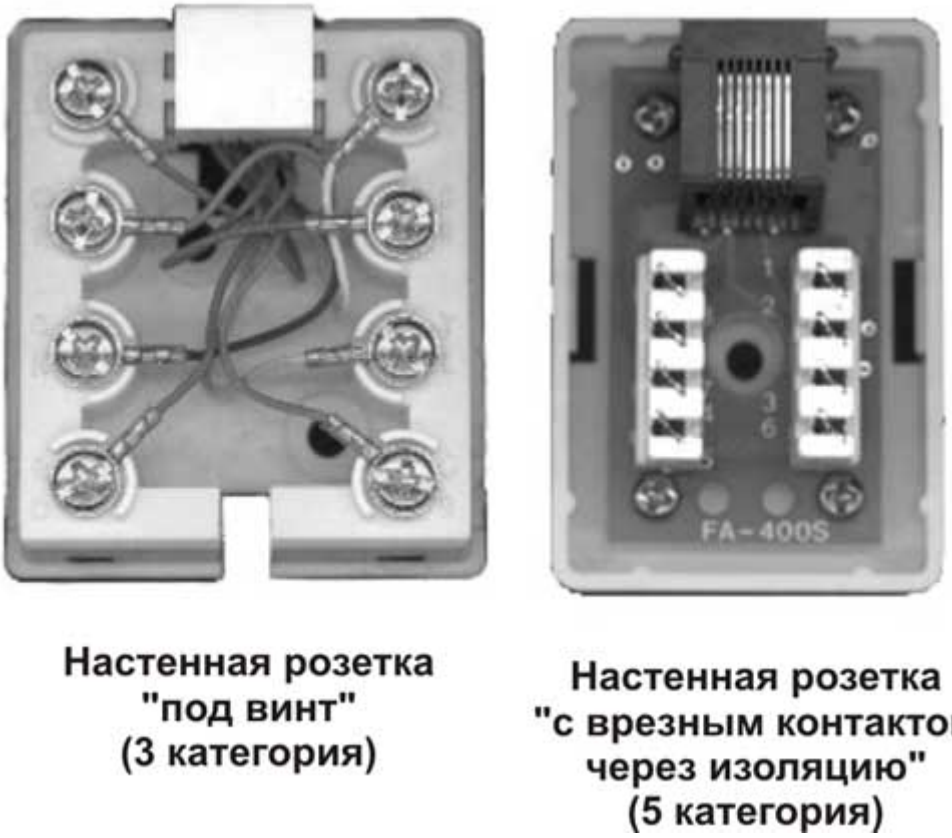

Рис. 5.20. Настенные розетки

Работа с ними не слишком сложна, но винтовое соединение не проходит по требованиям 5 категории, а врезной контакт требует специального (но весьма не дорогого) инструмента.

Для достижения более красивого внешнего вида предпочтительно использовать розетки, которые монтируются внутрь короба. Это более современный, и более качественный подход, поэтому модельный ряд значительно более разнообразен. Хотя основа разъема всегда одна и та же (врезной контакт через изоляцию), способов установки проводников множество. Удобно, что большая их часть не требует специального инструмента для подсоединения (например, поворотные элементы Legrand).

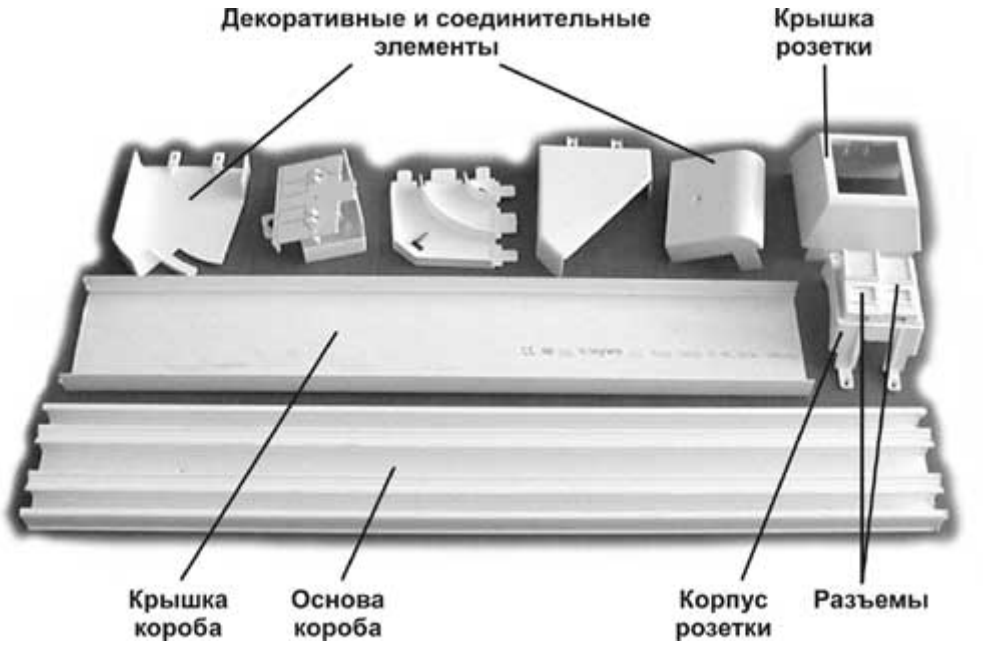

Рис. 5.21. Розетка для установки в короб, и часть короба

Разъемы, установленные в розетках, соединяются с компьютерами при помощи специальных абонентских кабелей (шнуров, патчкордов), представляющих собой отрезок гибкой витой пары длиной 1-3 метра с разъемами штекерного типа (RJ-45) на концах. Разумеется, можно использовать самодельные кабели, но технически это не оправдано. Абонентское окончание сети наиболее подвержено физическим воздействиям, и достаточно малейшей ошибки при изготовлении, что бы абонентский кабель вышел из строя в самый неприятный момент.

Концы кабеля, которые подключается к активному оборудованию (коммутатору), так же можно развести подобным образом. Сети с установленными в ряд 5-8 розетками встречаются, и ничего экстраординарного собой не представляют. Но технической необходимости в таком решении нет, так как переключения будут выполняться относительно редко, и не непосредственно пользователем, а более квалифицированным персоналом (обычно сисадмином).

Намного проще обжать витую пару разъемами штекерного типа (RJ-45), и напрямую подключить к коммутатору. Последний при этом можно аккуратно повесить на стену. При этом несколько страдает внешний вид, но стоимость понижается, а надежность увеличивается (нет промежуточной пары разъемов).

В более крупных сетях целесообразно применять разделку кабелей с использованием коммутационных панелей или кроссов, но в простой сети на 8-10 пользователей это излишне.

Маркировка, установка активного оборудования

В маркировке построенной сети нет ничего сложного. Нужно, что бы любой конец кабеля (даже не разделанный) был промаркирован. Желательно, что бы маркировка была нанесена на эскизный проект в виде подписей, или специальных таблиц.

Но важность этого нехитрого мероприятия такова, что вполне заслуживают отдельного подзаголовка хотя бы по следующей причине: хорошо известно, насколько часто

требование маркировки не соблюдается. И так же известно, сколько проблем это причиняет в дальнейшем. Сэкономленные при строительстве 2-3 часа, зачастую оборачиваются в дальнейшем серьезными работами по прокладке новых коммуникаций.

Технически выполнить маркировку можно самыми разными способами. Например, нанесение надписей на оболочку кабеля специальным маркером (или даже шариковой ручкой), приклеивание скотчем бумажной "записки", специальные пластиковые метки: Либо вставки в розетки, кросса, коммутационной панели.

Годится все, что даст возможность однозначно определить начало и конец каждого кабеля в сети. Причем не только на следующий день после окончания строительства, но и спустя 2-3 года.

После строительства (инсталляции) кабельной системы остается только установить активное оборудование, и программное обеспечение.

При этом используются самые различные варианты. Например, коммутатор можно установить на стену, за подвесной потолок, на стол, или еще каким-либо образом. Главные требования - отсутствие возможности механического повреждения, надежное электропитание, и пожаробезопастность.

Если в офисе есть мини-АТС, то более чем целесообразно разместить активное оборудование локальной сети рядом с ней. А кабельную разводку пустить в одном и том же коробе, устанавливая на рабочих местах сдвоенные розетки.

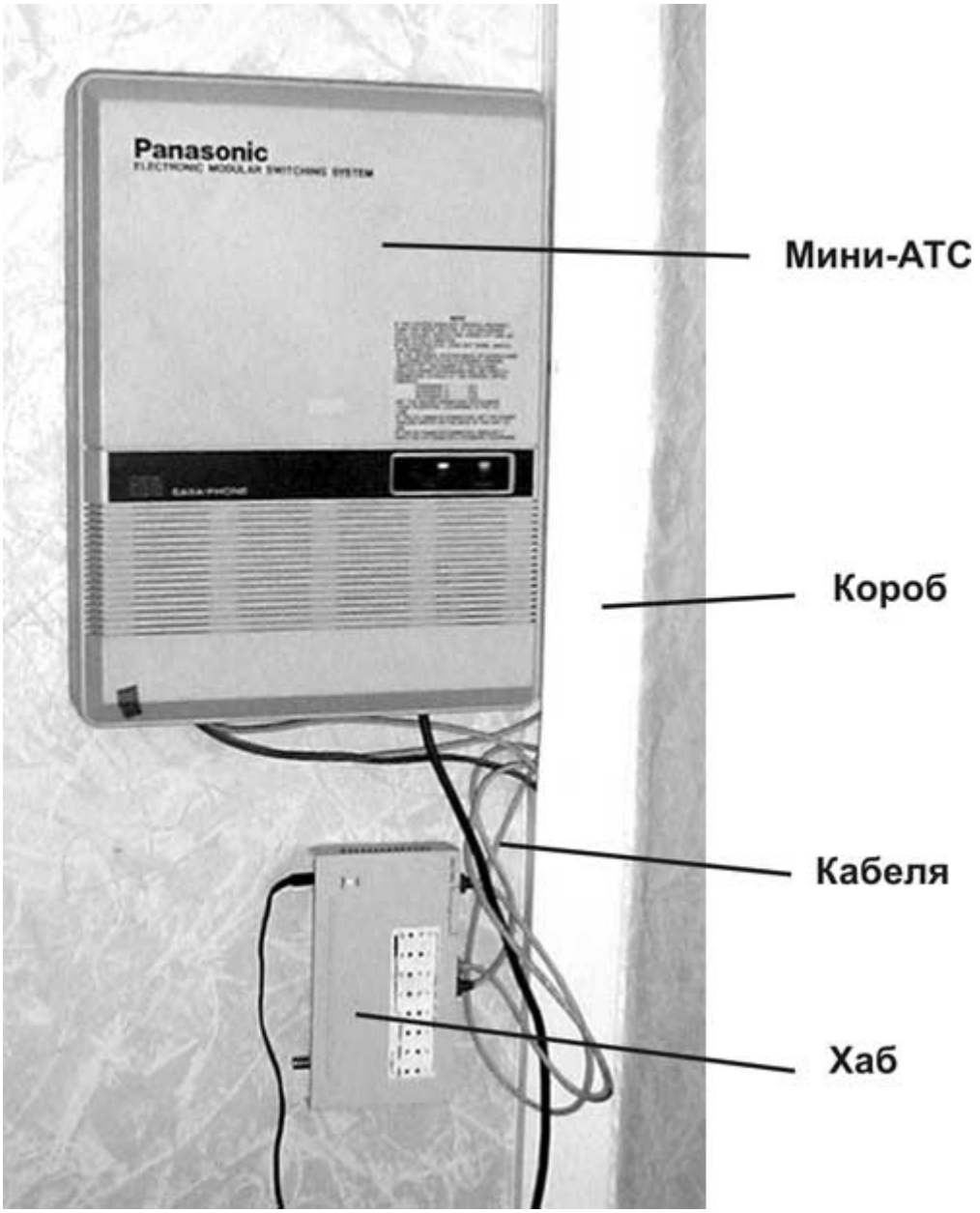

Рис. 5.22. Пример установки активного оборудования (хаб и миниАТС).

При необходимости можно использовать специальные настенные шкафы (как рассчитанные на 19-ти дюймовое оборудование, так и нет). Для улучшения технических или эксплуатационных показателей небольшой сети это не нужно. Но очень часто шкафы приходится использовать из соображений внешнего вида. Так, например, на Рис. 5.19 активное оборудование желательно установить почти перед дверью в комнату руководителя, на самом видном месте. Очевидно, что без дорогостоящего шкафа (да еще известного производителя) никак не обойтись по имиджевым соображениям.

Если же планировка и размеры арендуемых помещений позволяют выделить удобный "угол", в который не заглядывают посетители, и который не бросается на глаза сотрудникам, вполне можно обойтись вариантом, показанном на Рис. 5.22.

Сеть небольшой фирмы (40-60 рабочих мест)

Строго говоря, для таких объемов уже вполне экономически и технически оправдано строительство структурированной кабельной сети (СКС). Недорогая сеть, построенная только в расчете на существующие рабочие места, и с распределенным по территории активным оборудованием, целесообразна скорее как временный вариант, чем долгосрочное решение.

С другой стороны, в России огромное число предприятий с подобной численностью сотрудников не имеет твердой уверенности в продлении краткосрочных договоров аренды. На практике мне не раз приходилось видеть, как новый арендатор был вынужден демонтировать оставшуюся от предыдущей фирмы (и очень не дешевую) сеть из-за самых различных причин. Начиная от отсутствия необходимости в передаче данных вообще, до иного, чем прежде, расположения комнат.

Кроме этого, финансовое положение заказчиков часто не способствует большим капитальным затратам... В таких условиях вкладываться в инфраструктуру просто рискованно.

Данный вариант мало отличается от рассмотренного выше, и скорее является наиболее простым вариантом его развития. Поэтому, ограничимся кратким рассмотрением идеологии, и некоторыми технические особенности построения подобных сетей.

Идеология сети

Предположим, что нужно объединить рабочие места на предприятие, которое занимает по несколько комнат на каждом из 3 соседних этажей в многоэтажном доме контор. Для этого можно представить весь проект как совокупность небольших сетей из 5-10 рабочих мест в соседних комнатах (сети рабочих групп), связанных вместе. Таким образом, задача построения сети из 40-60 рабочих мест сводится к объединению в одной точке 6-8 небольших сетей масштаба отдела или рабочей группы.

С точки зрения идеологии СКС, это не слишком правильный подход, чреватый невысокой надежностью сети, и ведущий со временем к высоким эксплуатационным расходам. Особенно надо отметить, что сеть из 5-10 рабочих мест можно вполне развить до 40-60, не меняя общей структуры и идеологии. Но увеличивать сеть далее, без изменения концепции, по меньшей мере, не рационально как по техническим, так и экономическим соображениям.

Данный вариант является, на мой взгляд, пограничным размером сети, которую имеет смысл делать с нарушением стандартов СКС (и, тем более, своими силами). При этом выбор (см. Рис. 5.18) должен делаться еще более жестко, чем в рассмотренном выше примере.

Тем не менее, если принято недорогое решение, рассмотрим его особенности. Главное отличие - центральный узел, который связывает коммуникации рабочих групп в единую сеть. С технической точки зрения это коммутатор, с одной стороны связывающий коммутаторы рабочих групп друг с другом, с другой - обеспечивающий подключение серверов и других общих ресурсов.

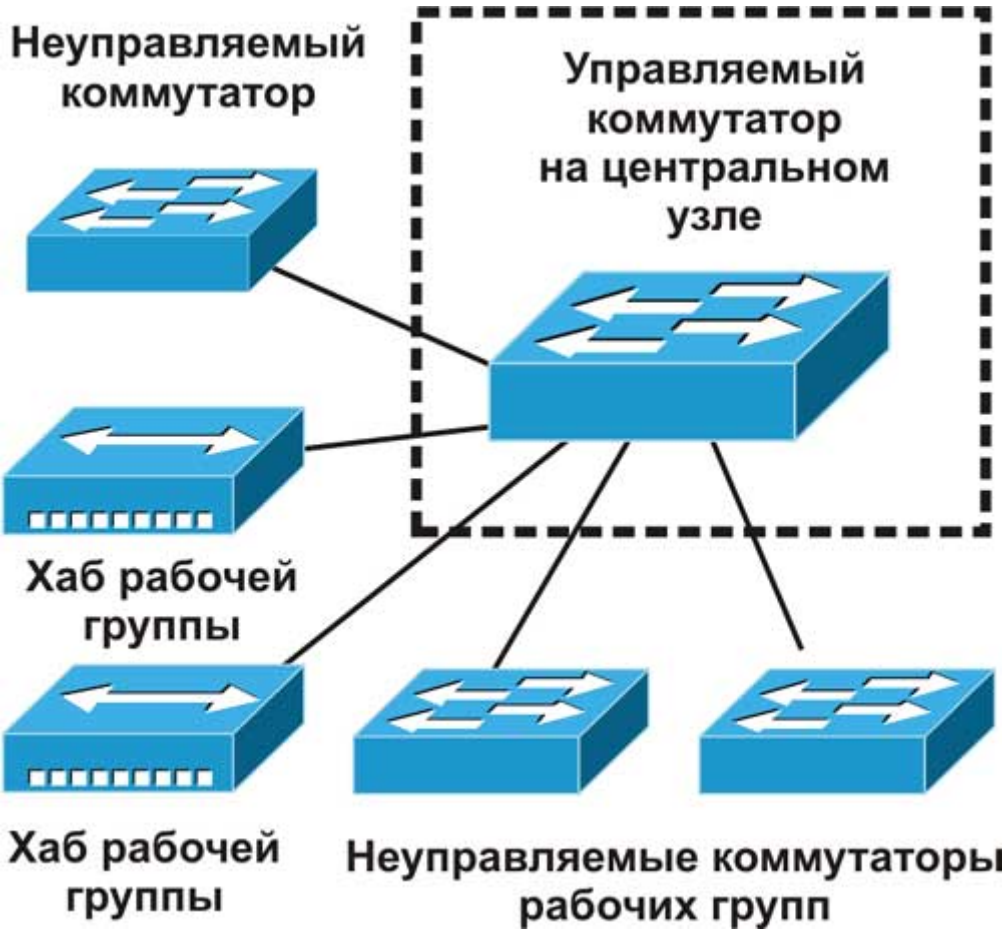

Рис. 5.23. Структура сети небольшого предприятия

В самом простом случае роль центрального коммутатора может выполнять такой же свитч, как и в сетях рабочих групп. Но все же предпочтительнее использовать более мощный управляемый коммутатор известного производителя. Ведь если выход из строя (или сбой) свитча рабочей группы вызовет простой 5-10 человек, то центрального узла - все 40-60.

Так же желателен более строгий подход к установке оборудования. Простой навесной (или напольный) шкаф с коммутационной панелью, источником бесперебойного питания, и другими необходимыми составляющими становится необходимостью, а не роскошью. Стоимость при этом растет на проценты, а надежность сети порой повышается в разы.

Нужно отметить, что при использовании управляемых коммутаторов можно значительно более гибко управлять построенной сетью. Например, создать виртуальные сети (VLAN), установить пониженную скорость, собирать статистику, осуществлять мониторинг, и многое другое (более подробная информация по активному оборудованию содержится в Главе 10).

Кроме этого, при том падении цен на Gigabit Ethernet, которое происходит в настоящий момент, вполне оправдано подключение серверов по протоколу 1000baseT. И об этом стоит серьезно задуматься перед покупкой центрального коммутатора.

Особенности практической реализации сети.

Основным отличием кабельной инфраструктуры небольшого предприятия от сети рабочей группы является наличие межэтажных линий (вертикальная разводка в терминологии СКС). Для их прокладки используются специальные шахты слаботочной проводки, которые обычно используются для телефонии и охранной сигнализации.

Бывают случаи, когда для силовой, и для слаботочной проводки используется одна и та же шахта. При этом через кабеля 220/380 Вольт могут идти весьма большие токи, способные вызвать наводки на витую пару. Да и с точки зрения электробезопасности в этом случае не все обстоит хорошо. Выходы есть - это прокладка в металлорукаве, в отдельной трубе, использование экранированной витой пары. В самом крайнем случае остается вариант строительства сети с применением оптоволокна.

Расположение шахт оказывает самое непосредственное влияние на топологию сети, и это надо учитывать еще на стадии составления эскизного проекта. Так же важно предусмотреть способ ввода (и вывода) витой пары в шахту. Иногда это можно сделать по специальным коммуникациям (например, трубам, уложенным в стены или пол), но чаще приходится что-то придумывать, например пробивать специальные отверстия.

Проблема непроходимости межэтажных пролетов достаточно редко встречается в административных или офисных знаниях, но в возможности прокладки желательно убедиться еще до начала работ. При этом единственным надежным способом проверки можно признавать экспериментальную протяжку, так как внешний вид бывает обманчив. Может сложиться ситуация, когда одна из шахт здания забита до предела, а другая почти пуста. И небольшое изменение топологии на стадии разработки эскиза сэкономит много времени при прокладке.

Практические приемы преодоления межэтажных пролетов не сложны. Берется упругая проволока диаметром 2-4 мм, и метров 3-4 длиной, на ее конце делается плоская петля для облегчения прохождения препятствий. Желательно заизолировать проволоку изолентой или кембриком, так как даже в шахтах слаботочной проводки можно попасть в кабель 220В. Телефонисты для этих целей очень часто используют кусок стеклопрутка (можно найти внутри оптоволоконных кабелей многих типов).

Затем проволока (или пруток) проталкивается через шахту слаботочной проводки (обычно по специальным пластиковым или металлическим трубам). К оставшемуся концу изолентой туго приматывается витая пара (без выступающих частей), и протаскивается по шахте. На следующем этаже операция повторяется.

В реальности, не всегда бывает просто сделать даже такую внешне простую операцию, и к ней для более подробного рассмотрения придется вернуться во второй части книги (строительстве домашних сетей).

Вторая особенность строительства коммуникаций, связывающих рабочие группы, это необходимость вести значительную связь в помещениях общего пользования. Например, коридорах, переходах, лестничных площадках, и т.п. При этом могут возникнуть очень сложные вопросы с собственником помещений, охранными службами, и т.п. Это то же желательно учитывать и прорабатывать заранее.

В третьих, как уже говорилось несколькими абзацами выше, центральная точка нуждается в значительно лучшей оформлении и оборудовании, чем коммутаторы рабочих групп. Связано это как с большей стоимостью простоя, так и с необходимостью хоть как-то управлять сетью.

К тому же, кроме коммутатора наверняка будет один, а скорее и несколько серверов. Им то же не помешает установка в шкаф, источник бесперебойного питания, и квалифицированное обслуживание.

Более того, для сети такого размера необходимо место для администратора. Даже если он "приходящий", без этого обойтись будет трудно.

И последняя (но очень важная) особенность рассматриваемого типа сетей. При количестве сотрудников в 40-60 человек можно с уверенностью сказать, что на предприятии есть мини-АТС. Если она уже установлена, и кабельная инфраструктура разведена, то вопросов не возникает.

Но при совместном строительстве обоих сетей (вычислительной и телефонной) очевидно, что нужно использовать одни и те же трассы и короба. В стандартах СКС это не только допускается, но и прямо рекомендуется, поэтому сложностей с подбором материалов не возникнет.

Глава 6

Глава 6. Домашние (территориальные) сети.

Сорока и плотвица, чебак и птица клест,
"ты рыба или птица" ей задали вопрос.
И гордо шаркнув лапкой, прищурив левый глаз,
ответила Оляпка - "я птица водолаз"
Детская песенка про Оляпку.

Вопрос оказания провайдинговых услуг через сети Ethernet уже несколько раз был затронут в данной книге (например, в Главе 3). Пришло время подробнее остановиться на основных принципах построения подобных сетей, положить некий теоретический базис под практические материалы 2 части.

Не вдаваясь глубоко в исторические детали, можно сказать, что технология ethernet и сеть Internet долгое время жили независимой жизнью. В провайдинге использовались синхронные и асинхронные каналы до 115/128к, для богатых организаций потоки E1-E3. Технологии надежные, универсальные, но дорогие и относительно низкоскоростные.

С другой стороны, развивались локальные сети. За кратчайший период появилось множество стандартов (и не меньше устаревших было "забыто"). Коаксиальный кабель сменила более удобная и дешевая витая пара. Скорость с 2 Мб выросла сначала до 10, потом до 100, и наконец 1000. Теперь на подходе 10 Гигабит, и конца этой гонке не видно. При всем этом стоимость оборудования не только не увеличивалась, а стремительно падала до каких-то нелепо малых цен, обусловленных немыслимыми в телекоммуникациях тиражами.

Рис. 6.1. Смена поколений. Хаб 3com Office connect и адаптер 3com 900 в масштабе со старым модемом.

Нельзя сказать, что Ethernet как вид передачи данных был удобен для предоставления доступа к Интернет. Скорее наоборот, имел массу недостатков. Но большинство компьютеров в больших и малых фирмах уже было к этому моменту соединено локальными сетями. В результате множество пользователей связалось с Интернет именно при помощи существующих ЛВС.

До Ethernet-провайдинга оставался один шаг, и, разумеется, он был сделан. Подключение через Ethernet, как коммерческая услуга, появилось сравнительно недавно. Еще год-два назад крупные провайдеры стыдливо замалчивали такой вид подключения в своих прайсах, считая его не серьезным. Это направление не звучало в маркетинговых программах, не предлагалось менеджерами, не рекомендовалось в "умных" книгах.

Но конкуренция сделал свое дело. Молодые и энергичные провайдеры быстро нащупали эту незанятую нишу, и серьезно потеснили на рынке домашнего пользователя и малого офиса старожилов рынка. Подключая клиентов по Ethernet, они предоставляли настолько быстрый и дешевый канал, что на сравнительно низкий уровень сервиса мало кто обращал внимание.

Так возник Ethernet-провайдинг - массовое коммерческое оказание телематических услуг с использованием технологии Ethernet.

Понятно, что для фирмы, занимающейся услугами подобного рода, построение надежной, и относительно недорогой сети является едва ли не самым важным вопросом. И, как было показано в Главе 4, использовать опыт структурированных кабельных сетей нужно с серьезными оговорками.

Глава 6

Дилемма 10/100.

Как ни странно, но начать разговор о технологиях придется с экономики. Вернее, со скорости передачи данных, которую желательно использовать в домашних (территориальных) сетях. Причина этого достаточно проста - неизбежный (по целому ряду экономических и технических причин) уход от идеологии СКС ведет к серьезной зависимости кабельной системы от используемой технологии передачи данных.

Если при строительстве серьезной корпоративно сети декларируется пригодность кабельной инфраструктуры к передаче данных любого стандартного типа, и с любой стандартной скоростью, в Ethernet-провайдинге ситуация противоположная. Сеть создается для вполне определенной технологии (Ethernet), и вполне определенной скорости передачи данных.

Из этого следует несколько выводов:

1. Нет понятия законченной сети - она строится по мере необходимости (и ремонтируется) все время. Хороший и весьма близкий пример - абонентская часть телефонной сети.

2. Инфраструктура создается не для удовлетворения собственных потребностей, а как средство, необходимое для продажи услуг. Соответственно, появляется вполне экономический расчет продажи не абстрактной выгоды от использования, а пропускной способности.

3. Динамика развития отрасли такова, что инвестиции на данном рынке должны окупиться быстрее, чем за 3-5 лет. Далее не обойтись без коренной реконструкции инфраструктуры (в первую очередь активного оборудования).

Особо нужно отметить, что такой подход отнюдь не значит, что на сети, спроектированной под соответствие требованиям 3-ей Категории, никогда не будет работать протокол, предусматривающий 100-мегабитную (или значительно большую) скорость. Ограничение - не самоцель, а лишь экономический расчет продажи сети. Как только появится технология, в которой высокая скорость сочетается нетребовательностью к качеству абонентской разводки, и сравнимой стоимостью - ее надо будет немедленно взять на вооружение. Хорошей демонстрацией потенциальных возможностей старых кабельных систем могут служить стандарты 100C5 или 10baseT4, не получившие, к сожалению, широкого распространения. Но наличие технологий передачи более 10 мегабит по электрической проводке позволяют предположить реальную возможность передачи 200-300 мегабит по витой паре 3-ей категории.

Посмотрим, что же продает Ethernet-провайдер. Ответ простой - услуги и трафик. К трафику мы еще вернемся, сначала обратим внимание на услуги.

Не только в домашней сети, в интернете вообще очень сложно продать услуги. Если у пользователя есть канал передачи данных, он обычно в состоянии сам позаботиться о сервисе (посредником вклиниться реально, но скорее пока это из раздела фантастики). Традиционный хостинг, ASP-провайдинг, требования безопасности, антивирусы, и т.п. фактически не востребованы в этом сегменте рынка.

IP-телефония более реальный сервис, но это скорее отдельный бизнес, не имеющий особого отношения к сети. Что остается? Видео по заказу (пока никто не наказывает за пиратство), радиотрансляции. Это хорошо, и технически возможно, остается только придумать, как за это получать реальные деньги.

Можно сказать, что на сегодня единственный источник прибыли Ethernet-провайдера (и в значительной степени традиционного ISP) - перепродажа трафика. Он покупается оптом подешевле, продается в розницу, но дороже. Схема древняя и простая, следовательно, можно сделать вполне реальное экономическое обоснование выбору скорости.

Пусть средний пользователь тратит до $20-30. Хоть 30 скорее то, что хочется, а не то, что есть, примем эту величину за основу. Далее, мы имеем расценки на трафик, которые диктуют транспортные операторы - это примерно $50 за гигабайт для провайдера, и примерно $100 для конечного пользователя. Кроме этого, предположим, что есть и внутригородской (внутрироссийский) трафик по льготной цене (например, $3 за гигабайт), который составляет 80% от общего потребления.

Проделав не сложные расчеты, можно получить, что 10-ти мегабитный канал с 30% загрузкой способен передать 700 Гб в месяц, на сумму $3000. А этого более чем достаточно на 100 пользователей. В реальности, цены на трафик значительно выше, а значит, количество пользователей можно смело увеличить в 2-3 раза.

Посмотрим на проблему с другой стороны. Может быть, трафик имеет резкие пики во времени? Но это явно не так. Частный пользователь и малый офис дают кривую, существенно более гладкую, чем корпоративный ADSL (и это вполне объяснимо). Более того, получать данные с большой одномоментной скоростью просто неоткуда - Интернет в массе до сих пор мыслит категориями dial-up, со всеми вытекающими последствиями.

Может быть, проще строить сразу с запасом, что бы не переделывать в будущем? Но компьютерная индустрия не оставляет места иллюзиям. Активное оборудование устаревает стремительно, и не стоит рассчитывать срок его службы более, чем в 5 лет. То же самое относится к наружной проводке (правда, уже по причинам большой агрессивности внешних условий).

Можно возразить, что активное оборудование на 100 мегабит стоит всего на 20-30% дороже 10 мегабит. Но это то же деньги, причем не разовые - ведь эксплуатационные затраты то же выше на похожую величину. Готов ли конечный пользователь заплатит эти лишние деньги? Для предположения отрицательного ответа не нужно проводить специального исследования. Все и так ясно…

Еще один аргумент за более высокую скорость - конкурентное преимущество. Кажется, что стоит сказать клиенту, что "у нас в 10 раз быстрее", как он немедленно покинет чужую сеть...

Однако, в реальности это не так. Не менее 50% абонентов вообще не примут сказанного в расчет. 40% спросят стоимость трафика и абонентской платы, и будут долго прикидывать что выгоднее. А оставшиеся 10% (вероятно, игроки в Квейк или КС) с радостью переключатся... Но только бесплатно. Зато все посмотрят на офис, лицензии, вежливость технической поддержки, скорость устранения неполадок, и многое другое.

Поэтому, как и в любом традиционном бизнесе, конкурентное преимущество получит сеть с лучшими экономическими показателями. А вот тут-то сэкономленные 20-30% весьма и весьма пригодятся. Это лишний подарок к празднику, пять копеек скидки в тарифе, круглосуточная техподдержка, квалифицированный персонал, и многое другое...

Порой говорят, что сеть "тормозит", даже 100 Мбит недостаточно. Ответ простой - и гигабита не хватит... пока трафик внутри сети не учитывается. Пользователь любит халяву. Не только Российский, кстати (но это уже совсем другая история). Если ему дать возможность, он загрузит копированием CD-дисков 100 мегабит, а копированием DVD - гигабит. И даже не поморщится.

Решающее все проблемы средство одно - подсчет трафика на порту. Тогда 10-ти мегабит хватит надолго... Но реально это сделать не так-то просто, нет такого оборудования (и программного обеспечения) за небольшие деньги. Поэтому на сегодня логичнее (а главное, дешевле) делать 100-мегабитную магистраль, а пользователей жестко ограничивать 10-тью. Это даст возможность минимально защитить бекбон от перегрузки.

Вполне рационально дизайном сети ограничить возможности прямой связи между абонентами, а большинство ресурсов сделать платными... Однако, это совсем не означает содрать три шкуры с пользователя. Скорее наоборот - каждый заплатит именно за то, что использовал (и вполне вероятно, меньше "среднего по всем абонентам").

Значительно хуже ситуация, когда бесплатность видеоархива, игрового сервера и внутрисетевого трафика покрывается высокими расценками за внешний Интернет. Из сети вымываются потребители наиболее выгодного (при продаже) ресурса, что плохо как им самим, так провайдеру. Известны на первый взгляд странные случаи, когда модем используется для дешевого окачивания сайтов, найденных при подключении через Ethernet. Если услуга неудобна для наиболее платежеспособного пользователя, бизнес не сможет быть успешным.

В заключение остается добавить, что большая часть вышесказанного не относится к любительским сетям, которые не ставят целью получение максимальной прибыли. Это случай особый, и экономические критерии к нему малоприменимы.

Глава 6

Основные понятия.

Большинство домашних сетей начиналось стихийно, с одного дома. При этом активное оборудование размещалось в соответствии с сиюминутными, часто весьма причудливыми, требованиями. В результате обычно получалась весьма причудливая топология, сочетающая различные типы кабелей, хабов, маршрутизаторов, коммутаторов, и т.п. Но по мере превращения Ethernet-провайдинга в бизнес, задачи менялись, и подобный подход уже не может в полной мере удовлетворить потребности рынка.

Необходим "промышленный" подход к строительству "домашних" сетей, их структурирование, определение минимальных отраслевых стандартов.

Если обратиться к стандартам структурированных кабельных систем (СКС), то них для кабельной системы определены следующие элементы:

- Магистральная кабельная система группы зданий (включает в себя соединения каждого распределителя здания с распределителем группы зданий)
- Магистральная (вертикальная) кабельная система здания (обеспечивает соединение каждого из распределителей этажа с распределителем здания)
- Горизонтальная кабельная система этажа (кабель от розетки пользователя до этажного распределителя).

Для "домашних" (территориальных, кампусных) сетей горизонтальная кабельная система в ее традиционном виде не имеет смысла, так как на одном этаже редко бывает более 2-3

пользователей. По сути, можно представить, что в жилом доме роль горизонтальной разводки выполняет "подъездное" распределение.

Из-за малого количества пользователей в доме (обычно менее 20-30) нет необходимости выделять каждый подъезд в отдельную подсистему со своим активным (или пассивным) оборудованием. Более того, в ряде случаев это даже вредно из-за сложностей организации распределителей в реальных условиях.

Еще одной особенностью подобных сетей является фактическое отсутствие коммутационных (распределительных) панелей - их роль выполняет активное оборудование. В дальнейшем, по мере увеличения количества абонентов, и широкого использования многопарных кабелей, необходимость в них неизбежно возникнет. Но пока мне представляется преждевременным использовать коммутационные панели как необходимый структурный элемент.

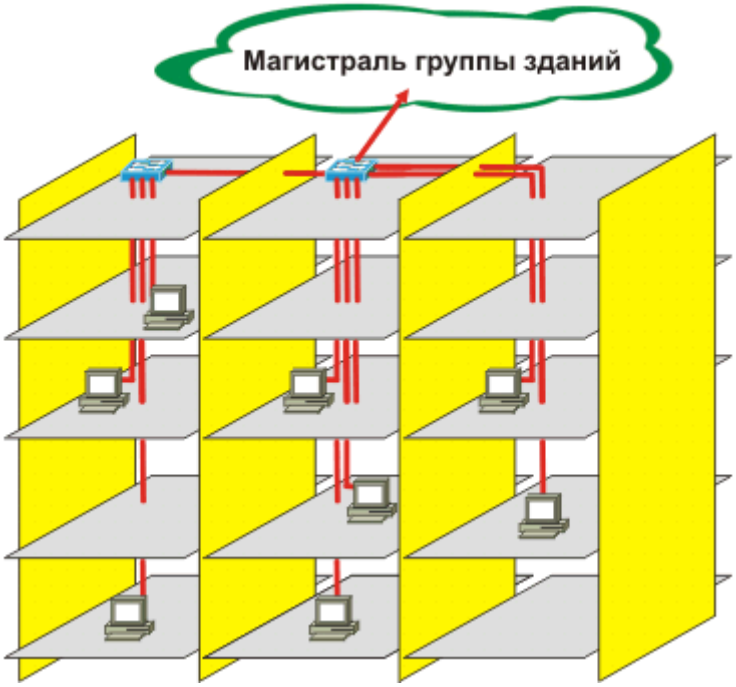

Рис. 6.2. Топология сети внутри здания.

Учитывая эти особенности, для "домашних" сетей можно определить следующие структурные элементы:

1. Абонентская система здания. Как следует из названия, она служит для подключения конечных пользователей к активному (редко пассивному) оборудованию Ethernet-провайдера внутри одного дома.
2. Магистральная кабельная система. Служит для объединения активного оборудования абонентских систем здания в единую инфраструктуру, и их соединения с другими сетями (в том числе Интернет).

Основываясь на этих определениях, рассмотрим подробнее основные варианты построения сетей, начиная с магистралей и заканчивая абонентской системой.

Магистральная кабельная система.

Магистральная кабельная система

Основная задача этой части сети - обеспечение надежной связи каждого здания со шлюзом сети Интернет и (или) центральными сервисами. Основными свойствами, которые характеризуют сеть, можно назвать топологию и материал кабелей.

С последним все более или менее понятно (и будет рассмотрено подробно в следующих главах). Но кратко можно сказать, что может быть оптоволокно, или витая пара, пусть иногда весьма непохожая на привычную 5-ю категорию (например, П-296). Начнем описание "домашних сетей" с рассмотрения топологий, применяемых при их строительстве.

"Начинающая" сеть (гирлянда).

Фундаментальным признаком начинающей сети можно считать отсутствие упорядоченной структуры, и особенно, явно выраженных магистралей. Кабель, проложенный первоначально для одного отдаленного пользователя, может в любой момент стать основой для подключения еще нескольких домов (с десятками абонентов). При этом активное оборудование (и его месторасположения) остается прежним.

В общем, такая сеть напоминает постоянно и беспорядочно растущий организм. Очень велико влияние субъективных (или попросту случайных) факторов. Соответственно, невозможно предсказать, какую форму примет сеть через значительный промежуток времени.

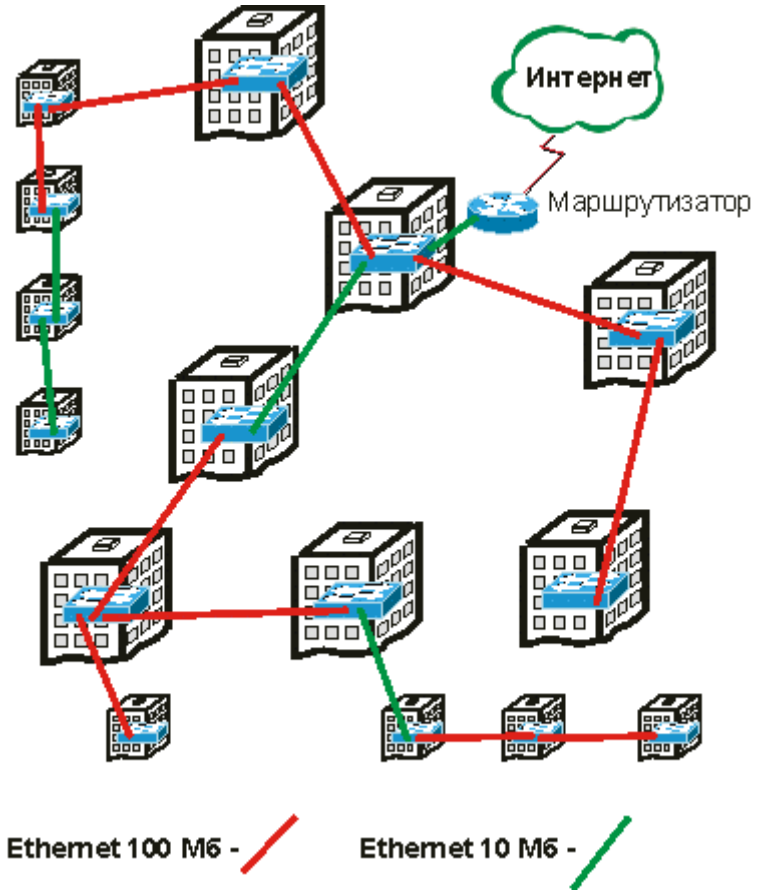

Рис. 6.3. "Начинающая" сеть.

Более всего такая сеть похожа на елочную гирлянду. Активные устройства соединены последовательно на нескольких "лучах", которые, в свою очередь, могут иметь многочисленные разветвления.

Подобная сеть очень дешева, и вполне способна развиваться за счет подключения новых пользователей. До определенных пределов она достаточно надежна, и обеспечивает приемлемую скорость, поэтому почти все начинающие Ethernet-провайдеры проходили этот этап.

Но при росте сети, последовательно соединенные коммутаторы (хабы) оказываются слабым звеном. Отказы недорогого оборудования в тяжелых условиях совсем не редки по самым разным причинам - "зависание", сбои питания, повреждения в грозы, замокания, воровство, вандализм, и т.п. А неисправность любого устройства в цепочке влечет неработоспособность всей подключенной к нему линии. При этом наиболее удаленным абонентам придется мириться с большими простоями.

Вывести однозначные рекомендации сложно - условия могут сильно отличаться не только в разных городах, но и районах. Но в среднем, с точки зрения надежности, можно признать нерациональным построение цепочки более чем из 2-3 активных устройств. В целом, это совпадает с рекомендациями стандартов СКС, только надо учитывать, что в их основу положены существенно более надежные решения, и большого "запаса" по этому параметру "домашняя" сеть иметь не будет.

Поэтому традиционный вопрос начинающих сетестроителей "сколько можно соединить последовательно коммутаторов, или хабов" представляется совсем в ином свете. Если принимать во внимание только техническую (или теоретическую) работоспособность, данные можно передавать и по линии из 30-50 коммутаторов. Но строить такую сеть, мягко говоря, не рационально - практика показывает, что уже при 15-20 последовательно соединенных устройствах (причем нет разницы, какого типа применяется оборудование) сеть становится практически неработоспособной (разумеется, с точки зрения последнего абонента в "гирлянде").

Из вышесказанного можно сделать следующие выводы. На сегодня такой способ развития имеет смысл только в небольших городах с низким платежеспособным спросом, и при отсутствии конкуренции. Тут ему нет альтернативы.

Второй вариант применения "начинающей" сети удобен как временный вариант минимизации расходов в случае возможности аренды надежной и относительно недорогой опорной сети. При этом на первом этапе несколько пользователей могут быть подключены небольшой "гирляндой", а в случае увеличения их количества переведены на отдельный (арендованный или приобретенный) магистральный канал (оптоволокно, xDSL, и т.п.).

"Звезда" или "кольцо".

Традиционно считается, что локальные сети должны строиться по топологии "звезда", а кольцевая архитектура присуща серьезным телекоммуникационным системам на основе SDH/ATM (это очень эффективное средство повышения надежности в телефонии, где несколько АТС могут продолжать работать независимо от вышедшего из строя узла).

Однако, любая многосвязная архитектура более надежна, чем простое соединение. И кольцо Ethernet не исключение. С распространением недорогих коммутаторов, поддерживающих STP (протокол покрывающего дерева), использование резервных связей стало достаточно простым процессом, не требующим вмешательства администраторов сети. При использовании "кольца" в случае выхода из строя какого-либо узла (или части кабельной системы) работоспособность сети в целом сохраняется.

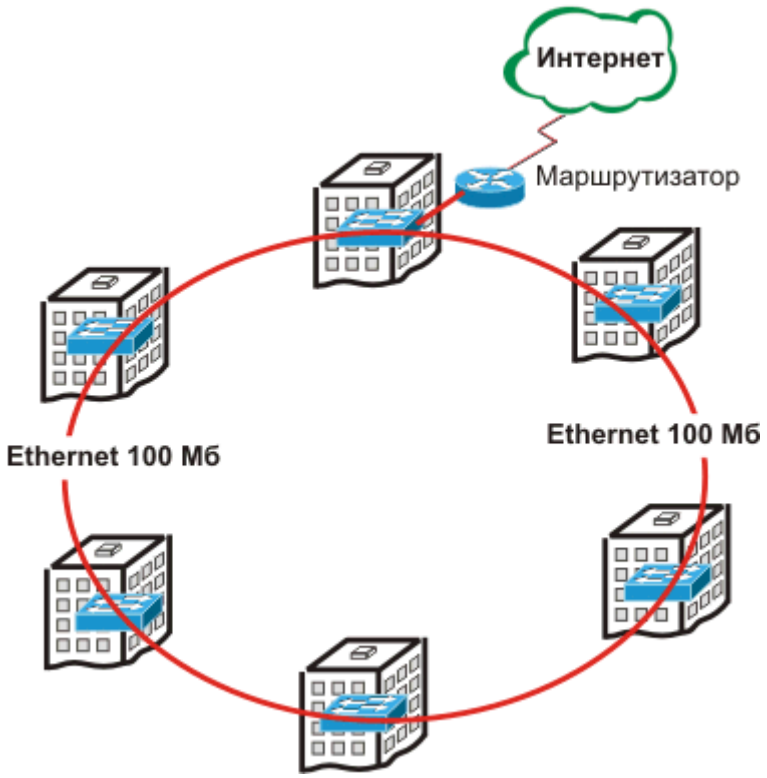

Рис. 6.4. Магистраль в виде кольца.

В свою очередь, "Звезда" несколько лучше приспособлена для предоставления обычной для локальной сети централизованной услуги. Действительно, в ЛВС почти всегда есть сервер или маршрутизатор, для доступа к которому (по большому счету) и построена сеть. Общение пользователей "напрямую" не слишком нужно, а часто и просто запрещено по соображениям безопасности.

Кроме этого, кольцевая топология является избыточной по числу связей, а значит и более дорогой. А вопрос надежности стоит не слишком остро из-за небольших размеров "обычной" ЛВС.

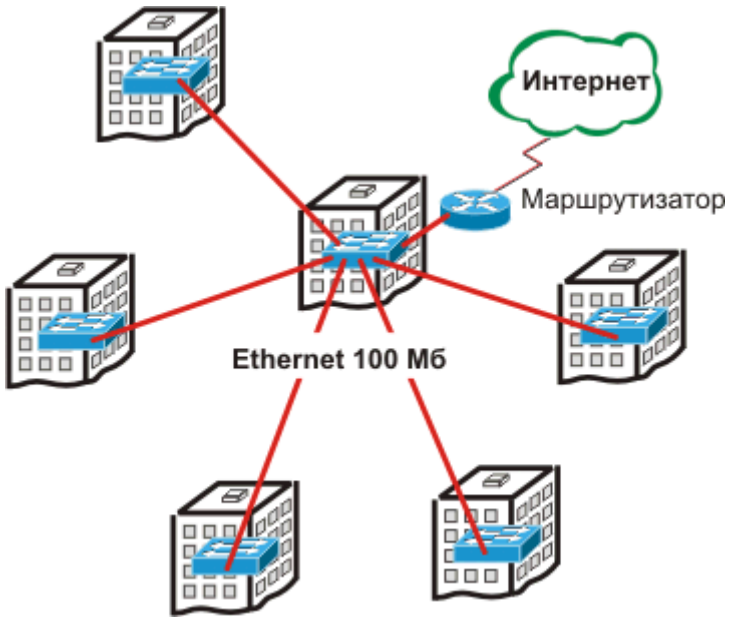

Рис. 6.5. Магистраль в виде звезды.

Какая топология более предпочтительна для домашней сети? Вопрос сложный и далеко не однозначный. Даже в корпоративных сетях до недавнего времени в качестве альтернативы единого центра (магистрали, вырожденной до внутренней шины коммутатора) предлагалось решение на безе распределенной магистрали (обычно на основе технологии FDDI).

Ethernet вытеснил FDDI, предложив STP с похожими возможностями, по сути "в нагрузку" к обычному активному оборудованию. Но выбор архитектуры магистрали от этого не стал проще - наличие недорогой альтернативы часто вызывает желание улучшить сеть. При этом нельзя не учитывать, что достоинства и недостатки есть у обоих способов.

Сравнение топологий "звезда" и "кольцо"

Особенности	Звезда	Кольцо
Возможность использования недорогого активного оборудования без поддержки STP	Да	Нет
Сохранение работоспособности всех пользователей сети в случае повреждения кабеля.	Нет	Да
Возможность организации дополнительного (резервного) канала без перестройки топологии сети.	Нет	Да
Сохранение связи между узами в случае отказа центрального оборудования.	Нет	Да
Возможность строительства магистралей по частям.	Да	Нет
Малая зависимость от особенностей места строительства.	Да	Нет

Кроме перечисленных, большое влияние на выбор топологической схемы могут оказать множество субъективных факторов. Например, исторически сложившиеся кабельные линий, местные условия прокладки, или финансовые возможности. В общем, можно сделать вывод, что "кольцо" несколько более предпочтительно по условиям надежности,

но для его выбора необходимы большие первоначальные вложения и наличие самой технической возможности строительства "кольца".

Понятно, что практике очень редко можно встретить идеальные топологические решения. Реальность, в большой мере, путь компромисса. Вопрос не стоит или-или. Нужно оптимальное решение - и часто оно будет являться синтезом рассмотренных выше схем. Поэтому, будет полезно рассмотреть несколько типичных примеров подобного подхода.

Глава 6

Выбор топологии в реальных условиях.

Основной бич домашних сетей - это трудности прокладки кабелей. Спроектировать и построить инфраструктуру крупного предприятия или межстанционные соединения АТС можно не считаясь с затратами, подстраивая "под проект" местные условия. В случае необходимости - выкопать новый туннель, возвести эстакаду, проложить подводный кабель, и т.п.

Ситуация недорогих сетей принципиально иная, и в этом их коренное отличие. Домашним сетям неизбежно приходится подстраиваться под застройку города. В некоторых местах прокладка невозможна, где-то нежелательна, или имеет высокую стоимость. Масса на первый взгляд незначительных помех часто превращает подобные работы в "шаманство", требуя от проектировщика глубоких знаний местных условий.

Основным вариантом, который сложно уложить в описанные в предыдущей главе схемы, является линейный.

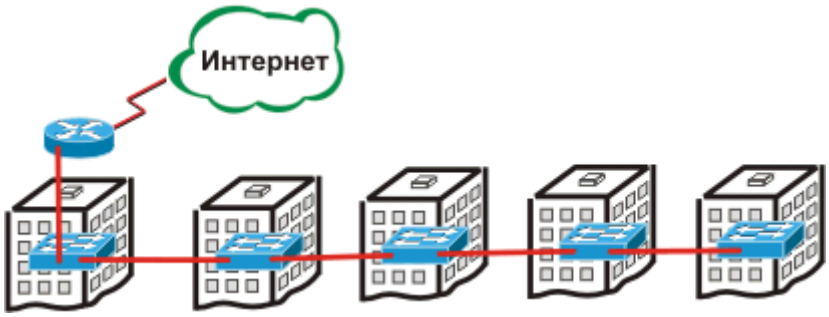

Рис. 6.6. Линейная магистраль.

В таком виде сеть представляет собой уже рассмотренную выше "гирлянду", в ее самом примитивном и ненадежном виде. Отказ любого промежуточного узла вызывает прекращение услуги абонентам, подключенным далее по линии.

Вдобавок, приходится констатировать, что это один из самых распространенных на сегодня типов небольших сетей. Такой форме способствуют особенности линейной городской застройке, экономия магистрального кабеля, стремление с минимальными затратами "дотянуться" до "перспективного" дома (или хорошего друга), и т.п.

Что же можно сделать для увеличения надежности линейной структуры?

Наиболее очевидным вариантом будет превращение "гирлянды" в "звезду". Пусть кабеля лежат рядом, или даже в одной оболочке, такой подход позволит избежать зависимости всей сети от локального сбоя электропитания или неисправностей активного оборудования. Иначе говоря, все узлы могут работать с центральным независимо друг от друга.

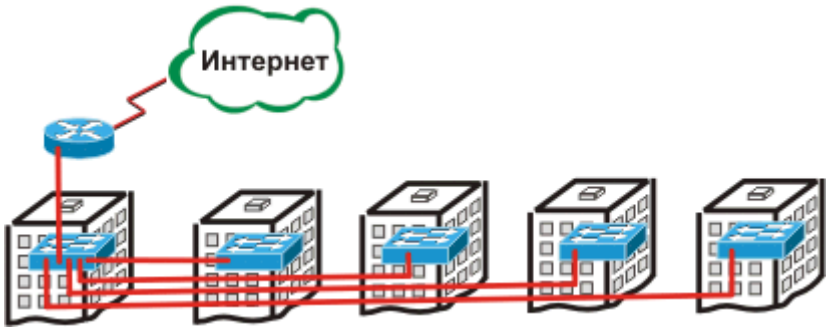

Рис. 6.7. Звезда, растянутая в линию.

Можно заметить, что в этом нет ничего нового, именно так обычно строится внутридомовая проводка телефонии или СКС. Подобно этому, для магистрали использование одного физического кабеля может с успехом применяться, особенно в сетях среднего и небольшого размера.

Но, как правило, это технически осуществимо (и рентабельно) только в случае использования оптоволокна. Большое количество волокон в одном кабеле стоит не слишком дорого (хоть и вполне ощутимо). В то же время, для медных многопарных кабелей при таком подходе нет места - 100-200 метров, вот предел их работы. А это очень мало для междомовых магистралей.

Очевидно, что для любой среды передачи кабель будет самым уязвимым звеном. Его повреждение вызовет отказ всех расположенных далее узлов без исключения. Это основной и неустранимый недостаток "линейной звезды".

В случае применения отдельного кабеля главным недостатком становится его большой расход. Кроме этого, использовать специальные решения типа П-296 сложно - пучок толстых кабелей (около 14 мм диаметром каждый) будет хорошо виден, и может легко привлечь нежелательное внимание. К тому же выглядит это весьма некрасиво даже на большой высоте.

Вдобавок, кабеля хоть и разделены, но идут по одной трассе. Поэтому вероятность их одномоментного отказа остается вполне вероятной.

Описанных выше проблем можно избежать, если применить "линейное кольцо". Действительно, совсем не обязательно замыкать магистраль при помощи своих кабелей. Это вполне можно сделать и "через интернет" (либо какую-либо иную сеть передачи данных).

Рис. 6.8. Кольцо "через Интернет" в "линейной" сети.

При этом понадобится несколько более тонкая настройка программной части сети. В пользовательском компьютере может быть установлен только один "шлюз по умолчанию" (маршрутизатор, которому отправляются дейтаграммы IP, адресованные во внешние сети).

Соответственно, в случае повреждения линии в какой-либо точке желательна (но в общем случае не обязательна) автоматическая "подмена" основного канала резервным. Это сравнительно просто сделать используя фиктивные адреса пользователей, и несколько более сложно для реальных. Но в целом не представляет собой неразрешимой задачи.

Как и в "классическом" кольце, общий отказ возможен только при одновременной неисправности двух активных устройств или повреждения кабелей в двух точках. Понятно, что вероятность такого события невелика, и можно получить вполне надежную сеть при "линейной" топологии ценой оплаты "запасного" канала подключения к Интернет.

Нужно отметить, что резервные коммуникации могут быть значительно менее скоростными, чем основные. А значит, сравнительно не дорогими, вполне по карману Ethernet-провайдеру средней величины.

Еще одним вариантом "линейного кольца" можно считать "гирлянду", в которой предусмотрена "обратная петля". Т.е. одна пара волокон в кабеле проходит через все активные устройства по очереди, а вторая идет цельной, и соединяет первый и последний узел сети.

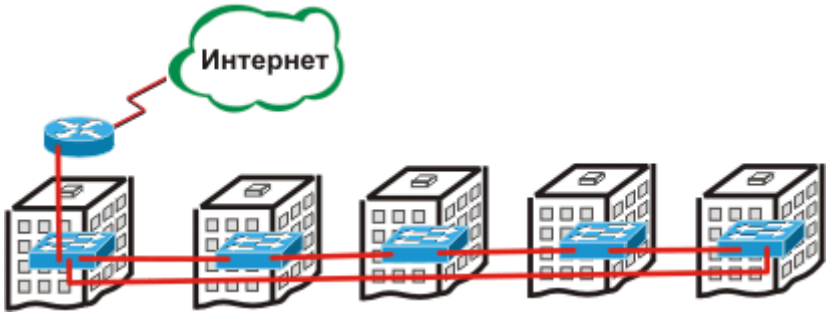

Рис. 6.9 Кольцо "с обратной петлей".

Этот вариант позволяет надежно и недорого защититься от отказов активного оборудования, но уязвим от повреждения кабеля. Тем не менее, это, пожалуй, лучший способ для небольшой сети линейной топологии, в которой построение обычного кольца слишком сложно или дорого.

Но что делать, если финансовое положение начинающей сети не позволяет использовать оптоволокно в "линейной звезде", "обратной петле", или схемы, которые используют резервирование "через Интернет"? В этом крайнем случае ситуацию может облегчить (но не исправить полностью) следующая топология:

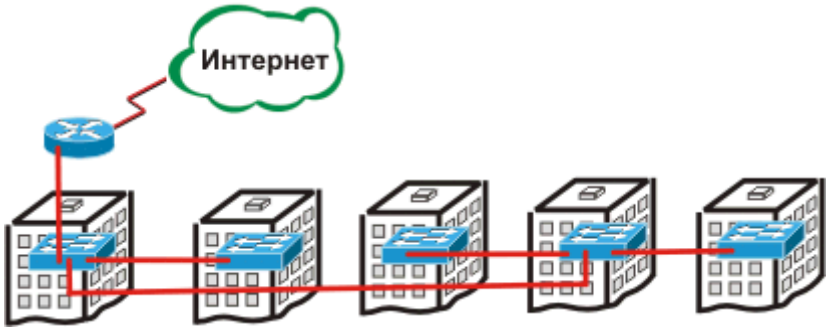

Рис. 6.10. Вариант сети в условиях максимальной экономии.

Т.е. ни в коем случае не следует стремиться построить длинную "гирлянду" из последовательных активных устройств. Значительно более целесообразно выделить магистраль, использующую минимальное количество оборудования. Пусть иногда понадобится "возвращаться" - расход кабеля при этом не так и велик…

Зато общая надежность значительно возрастет. Например, для недорогого П-296 (П-270) вполне достижимо 400-500 метров без повторителей. Значит, на сеть радиусом в 1,5 км (а это достаточно много) понадобится всего 4-5 устройств. В то время, как при построении "гирлянды" количество повторителей составит 15-20 штук.

При этом, по всей вероятности, придется отказаться от 100baseT в пользу 10baseT. Пусть медленнее, но надежнее. Не нужно хорошо разбираться в теории вероятностей, что бы сделать вывод о времени простоя сети при разных топологиях построения. Очевидно, что "гирлянда" будет больше ремонтироваться, чем работать.

В заключение, для иллюстрации общих принципов, хотелось бы привести схему вполне реальной (не придуманной) сети. Увы, карту расположение домов пришлось убрать из соображений безопасности прокладок.

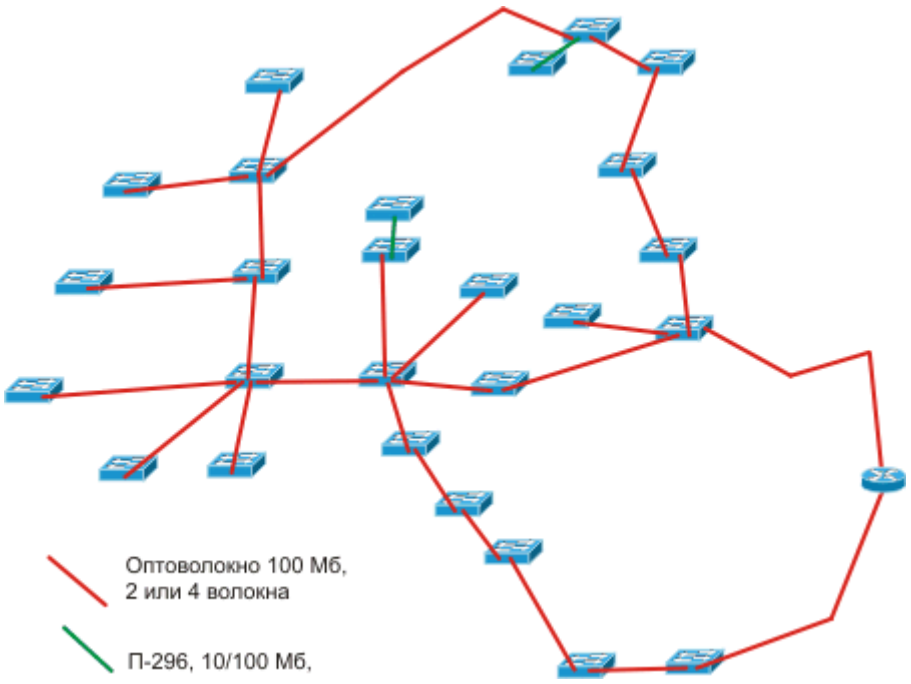

Рис. 6.11. Пример реальной домашней сети.

Можно видеть два связанных кольца, в которых часть узлов является центром небольших "звезд". Таким образом, полностью вывести сеть из строя достаточно сложно. Обрыв любого кабеля на кольце не остановит работу. А оконечные разветвления позволяют охватить значительную территорию (практически весь жилой район).

По сути, это компромисс "звезды" и "кольца", адаптированный под имеющиеся дома, с учетом минимальных затрат кабеля и оборудования. И все это с сохранением достаточной потенциальной надежности.

В заключение можно порекомендовать творчески относиться к проектированию сети, порой самые эффективные решения не очевидны на первый взгляд. А небольшое усложнение/удорожание может привести к существенному росту надежности всей системы в целом.

Глава 6

Абонентская система здания.

Основное назначение абонентской системы здания (иначе говоря, внутридомовой разводки) - подключение конечных пользователей к активному (очень редко пассивному) оборудованию Ethernet-провайдера внутри одного дома. В функциональном плане эта цель почти совпадает (в терминах СКС) с горизонтальной кабельной системой, но прокладка сети в жилом доме обладает целым рядом отличительных признаков.

Во-первых, как было показано выше, оптимально в качестве базового протокола использовать 10baseT, требования которого к качеству коммуникаций невысоки (достаточно Категории 3). Основным материалом бесспорно можно считать витую пару 5-той категории. Единственное, на что при этом стоит обратить внимание - это количество

пар в кабеле. Спецификации Ethernet 10/100baseT явно определяют необходимый минимум - 2 пары, максимальное их количество не ограничено, и может быть выбрано "по потребности" (например, достаточно широко используются 25 и 50 парные кабеля).

Во-вторых, из вполне понятных экономических соображений, Ehternet-провайдерам приходится подстраиваться под архитектурные особенности зданий. Нельзя прокладывать коммуникации, невзирая на расходы, как это принято при инсталляции СКС (тем более, совмещать их со строительством или капитальным ремонтом). Поэтому желательно еще на стадии проекта (или эскиза) учесть пропускную способность шахт слаботочной проводки, вводов, возможность крепления кабелей, предусмотреть защиту активного оборудования от злоумышленников, и многое другое.

В-третьих, не известно заранее ни количество, ни расположение абонентов. Подводить кабеля ко всем квартирам без исключений имеет смысл только в "элитных" домах. В большинстве зданий по статистике подключается в первый год не более 10% жильцов, и такие затраты просто не обоснованны. В результате абонентская система растет постоянно, по мере увеличения количества абонентов.

Учитывая вышесказанное, рассмотрим наиболее важный аспект в строительстве абонентской системы здания - топологию сети, которая определяется в основном местоположением активного оборудования.

Хаотичное расположение оборудования

Подобная топология достаточно типична для начинающих сетей. Само название говорит о том, что упорядоченной структуры нет, оборудование ставилось "где удобно", и, скорее всего, "когда угодно". Например, нужно подключить соседа - ставится хаб (коммутатор) в подъездном щитке. Или оказалось слишком велико расстояние до соседнего дома, в результате на чердаке (техэтаже) поставлено активное устройство. А то и еще проще - в момент прокладки не удалось получить доступ на один из этажей, нет никого из жильцов - и поставлен еще один разветвитель.

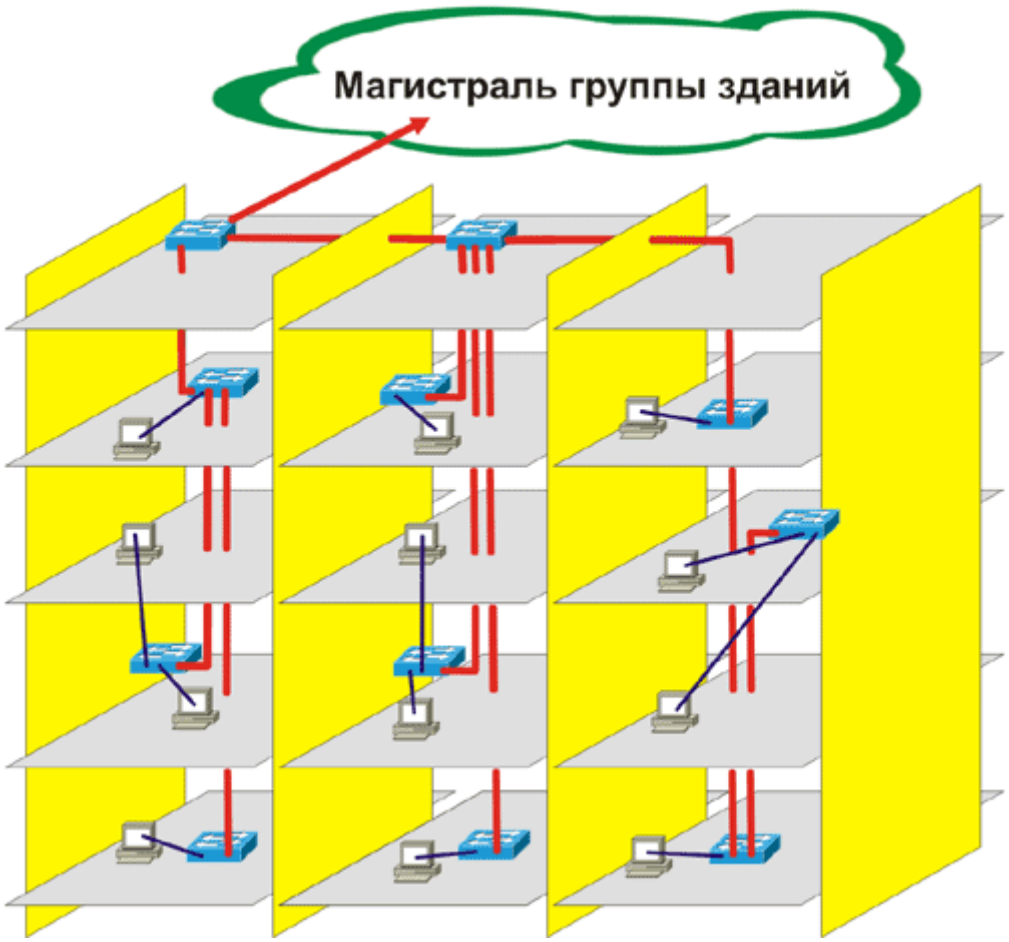

Рис. 6.12. Абонентская система здания с хаотичным расположением оборудования.

Таким образом, причин (и мотиваций) может быть много, от вполне резонных, до сиюминутных. Результат обычно получается вполне работоспособным, но до определенных пределов, за которыми может последовать частичная или полная неработоспособность сети (часто с труднообъяснимыми симптомами).

Можно согласиться, что современное активное оборудование очень дешево, надежно, и позволяет легко создавать разветвленные запутанные сети. Плюс к этому, используется минимальное количество кабеля, и проводятся самые простые монтажные работы.

Но для промышленного использования такой вариант не годятся по следующим причинам:

- Отдельное электропитание каждого устройства вызывает необходимость подключения к силовой сети во множестве точек. Пока это делается пиратским способом, особых сложностей не видно (кроме заметного снижения надежности и повышения сложности работ). Но как только потребуется официальная сдача сети, пусть даже самой первичной инстанции (ЖЭК, ДЭУ), быстро выяснится вся сложность ситуации. Как минимум, потребуется электрический счетчик, щиток под него, предохранители... В общем, можно без преувеличения сказать, что проблемы с пожарной инспекцией, энергосбытом, ГСН, и другими инстанциями будут фактически неразрешимы.
- Для оказания качественной услуги, надежной авторизации и защиты абонентов необходим удаленный контроль каждого пользователя на порту активного оборудования (а не на шлюзе доступа к Интернет). Однако, до выпуска недорогих

малопортовых управляемых коммутаторов еще достаточно далеко, их отличие в стоимости от простейших хабов (являющихся в настоящее время фундаментом хаотичных сетей), пока достигает сотен долларов. Таким образом, рассматриваемая сеть с точки зрения администраторов является "черным ящиком", процессы внутри которого не поддаются контролю, и, тем более, управлению.

- Обслуживание активного оборудования едва ли не самая большая статья расходов Ethernet-провайдеров. Очевидно, что гораздо проще следить за состоянием одного мощного коммутатора, чем десятка небольших хабов, рассеянных по дому (да еще с не всегда очевидным местоположением, доступом, и правом собственности). То же самое в полной мере относится и к защите от злоумышленников - чем меньше устройств, тем их проще защитить.

Полагаю, что каждого из перечисленных пунктов в отдельности достаточно для создания мотивации к переходу на другие схемы построения абонентских систем здания (конечно, при наличии финансовых возможностей).

Структурирование по подъездам

В этом варианте пользователи подключаются к "своему", обслуживающему каждый отдельный подъезд устройству (хабу, коммутатору). Оборудование всех подъездов подключено к одному коммутатору, который, в свою очередь, каким-либо образом включен в магистраль.

Этот вариант является фактическим отражением офисных локальных сетей. Только роль "вертикальной" межэтажной магистрали играют "межподъездые" связи, а разводка внутри подъезда аналог горизонтальной кабельной системы этажа в терминах СКС.

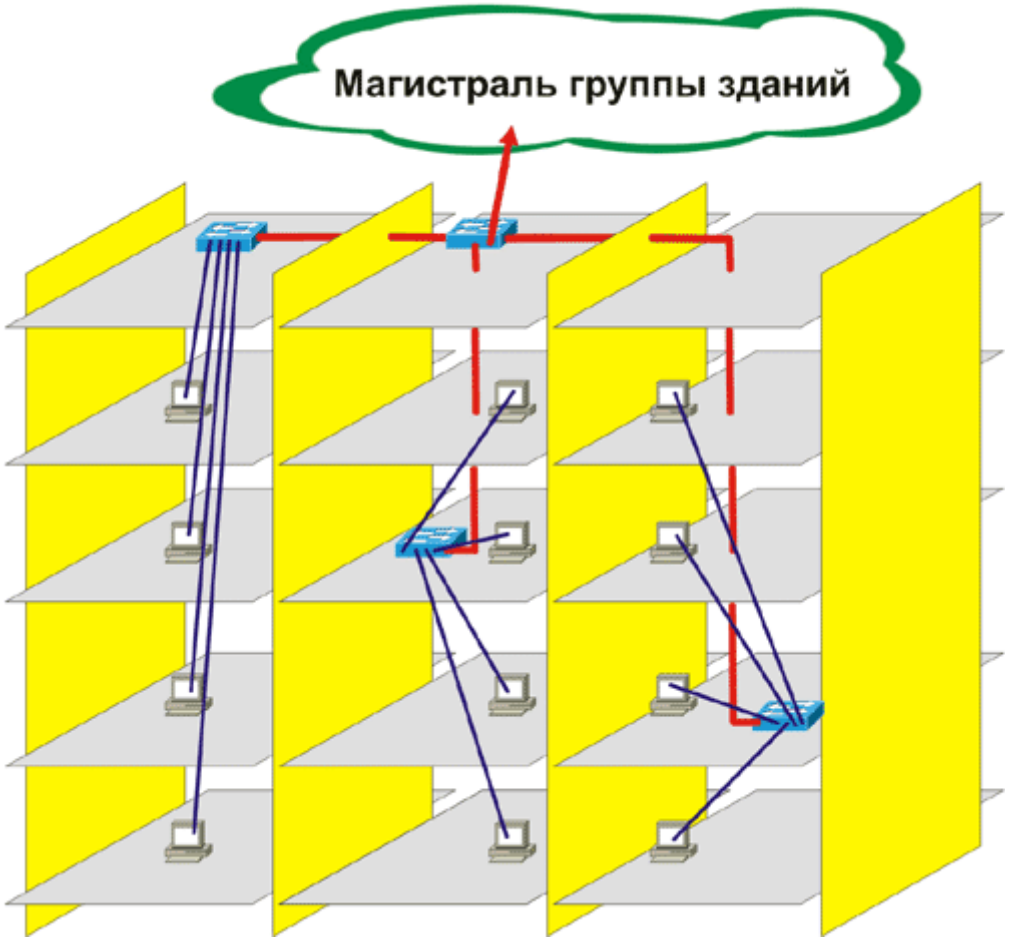

Рис. 6.13. Структурированная по подъездам абонентская система здания.

Такая схема может применяться, если в подъезде имеется достаточное количество абонентов (не менее 10-15), которые оправдывают размещение отдельного коммутатора.

Наиболее правильное место размещения с точки зрения топологии сети - один из средних этажей. Однако, как правило, архитектурой отечественных зданий это не предусмотрено, и приходится искать место на техэтаже, в подвале, лифтовой, и т.п. местах. При этом может проявиться главный недостаток централизованных схем - узость шахт слаботочной проводки. К сожалению, с этим приходится считаться, и ниже будет приведено несколько способов уменьшения остроты проблемы.

Второй существенный недостаток. Хоть устройство и всего одно на подъезд, сдача "инстанциям" может оказаться слишком дорогой, особенно в старых домах, где есть сложности с удобным местом размещения и "правильным" подводом питания. Хотя нельзя не признать, что если есть потребность в установке коммутатора в каждом подъезде (много абонентов), должно хватить средств и на легализацию.

Один дом - один распределительный пункт

Предельная централизация абонентской системы здания - установка оборудования в одной точке дома, в которую сходятся кабельные линии от всех абонентов.

Протокол 10baseT позволяет на современных кабелях Категории 5 нормально работать на расстояниях до 200-т метров (а часто и более). Учитывая, что высота 10-ти этажного дома около 30 метров, длина на подъезд - примерно 25-30 метров, вполне достаточно одного активного устройства на 7-8 подъездов. В случае, если здание очень большое, целесообразно рассматривать его логически как несколько домов, соединенных магистралями (в том числе оптоволоконными).

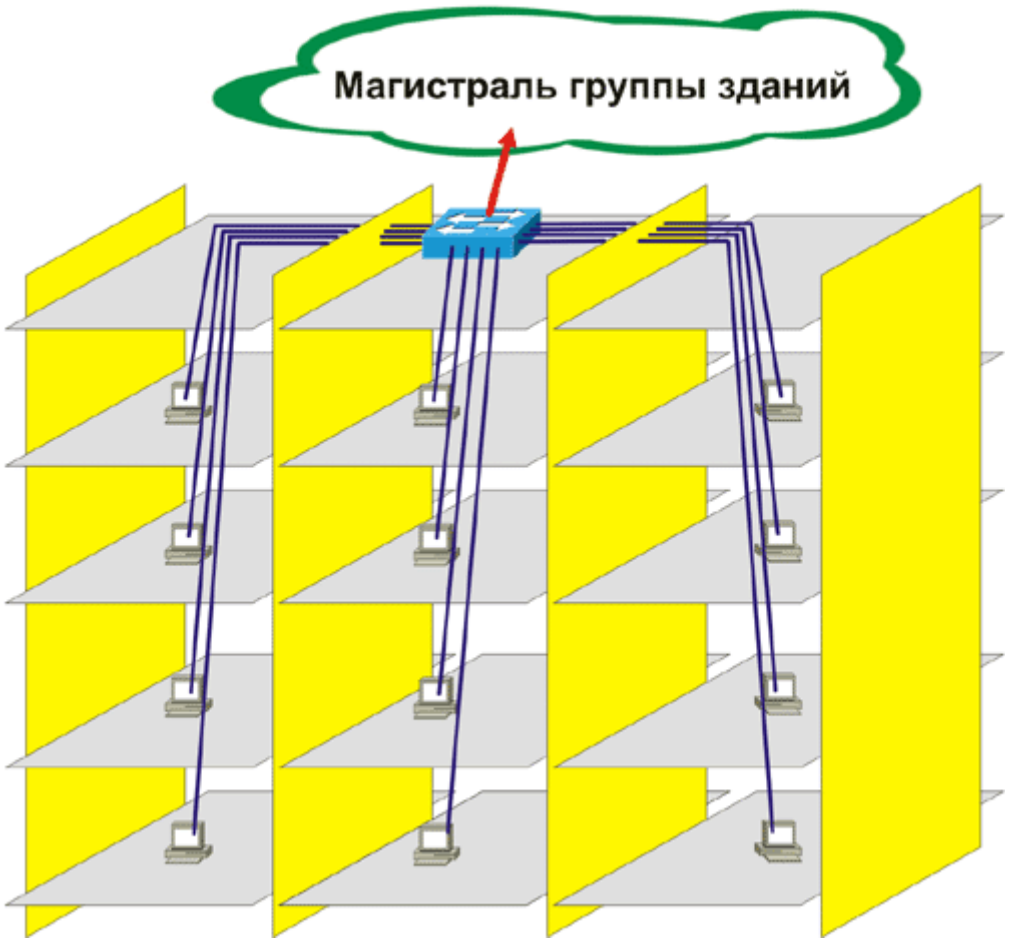

Рис. 6.14. Абонентская система здания с одной точкой коммутации.

Преимущества перед предыдущей схемой очевидны - установка, подвод питания, обслуживание, защита от злоумышленников - все в одном месте. Но недостатки тоже имеются, главным образом это кабельные линии большей протяженности и большой толщины.

Что лучше выбрать? Решение придется принимать в основном из архитектурных соображений. Если протащить толстые пучки кабелей через шахты слаботочной проводки реально, то вариант с одним распределительным пунктом будет более предпочтителен. То же самое можно сказать, если в подъезде приходится прокладывать новые кабельные каналы (это нередкий случай в старых домах, где слаботочная проводка не предусмотрена вообще).

Когда коммуникационные трубы слишком узкие, строение многоэтажное (более 10-12 этажей), и много абонентов (или большие перспективы их появления), целесообразно использовать структурную схему, ориентированную на установке активного оборудования в каждом подъезде.

Централизованная схема удобнее в относительно невысоком здании (менее 10-12 этажей), и числом абонентов в подъезде менее 10-15. Практически, под это определение попадает около 90% отечественных домов, поэтому можно считать данный вариант основным.

Можно подчеркнуть дополнительное преимущество схемы с одним распределительным пунктом в доме. При развертывании сети часто бывает, что пользователей мало (всего 1-2 на дом). Понятно, что ставить в этой ситуации несколько активных устройств сразу не

выгодно. А когда сеть разрастется, не придется менять ее топологию - достаточно вместо 6-портового хаба поставить мощный 25-ти коммутатор, или даже что-то более серьезное. Кабельная система здания может остаться прежней.

Минимизация толщины кабельного пучка

Так или иначе, но чем тоньше кабель, тем проще его использовать на реальных объектах. При этом стандартный для офисных локальных сетей 4-х парный кабель является, пожалуй, наименее подходящим решением из-за наличия 2-х неиспользуемых пар. Поэтому, в стесненных условиях целесообразно подключать один кабель сразу к двум портам (разделяя пары через розетку или плинт).

Еще больший выигрыш дает 25-ти или 50-ти парный кабель. Экономия толщины в этом случае идет за счет одной на все пары внешней оболочки, и более плотной упаковки пар. Но возникает проблема этажной разводки - делать ее полностью, на каждом этаже, малореально (дорого и заметно снизится качество электрического тракта). Решить задачу можно следующими способами:

Выводить из под общей оболочки несколько пар на каждом этаже (2, 4, 6 или более), а остальные пускать дальше не разрезая. Но мне, к сожалению, не известен "красивый" способ сделать это. Можно аккуратно вскрыть оболочку вдоль многопарного кабеля на длину порядка 10 см, обрезать нужные пары с одной стороны, и вывести их наружу. Далее, закрыть надрез (скорее всего изолентой), и подсоединить выведенные пары к тонкому кабелю (2-х или 4-х парный), которым выполнена проводка до пользователя.

Более правильно с точки зрения стандартов будет разделать весь многопарный кабель на одном из средних этажей на специальном плинте ("Крона" или "110"), затем развести по абонентам подъезда обычной витой парой. Недостатки - больший расход кабеля, относительно дорогостоящий плинт (порядка $20), необходимость запаса сечения кабельных каналов на "обратную" прокладку.

Однако, не смотря на внешние сложности, использовать многопарный кабель при массовых прокладках очень удобно. 25-парный кабель позволяет подключить 12 абонентов (эквивалентен шести обычным 4-х парным витым парам, но значительно тоньше, и удобнее в работе).

Последнее время некоторые Ethernet-провайдеры стараются проложить по стояку слаботочной проводки подъезда 25-парный кабель сразу, "на вырост". Подключение пользователей к нему делается позже, по мере необходимости. Со стороны оборудования весь кабель заводится на 50-100 парный плинт, а далее (иногда через грозозащиту) в коммутатор.

Такой подход позволяет подключать до 12 абонентов в каждом подъезде напрямую к коммутатору. При большем количестве пользователей придется прокладывать дополнительный кабель (не обязательно многопарный).

Дополнительно остается "неправильный", но дешевый выход - подключить нескольких соседей на один хаб, и передать его последним на полное "самообслуживание". Иногда это удобно как для провайдера (его ответственность заканчивается на "входящем" порту хаба), так и абонентам - они сэкономят на подключении.

Глава 7. Электрическая среда передачи данных.

Радиотехника - наука о контактах.

Какими бы своеобразными не казались Ethernet-решения для построения "последней мили", они имеют твердую основу в теории построения локальных сетей. В этой главе будут рассмотрены два основных способа построения кабельных систем с электрической средой - на основе коаксиального кабеля и витой пары. Нестандартные типы кабелей, которые часто используются в Ethernet-провайдинге для экономии средств и достижения большей дальности (скорости, надежности), принципиально не отличаются от вышеуказанных, и будут отдельно рассмотрены в следующих главах.

По этой теме существует поистине огромное количество материалов. Пересказывать их подробно в рамках настоящей книги не имеет смысла. Поэтому постараюсь без излишних подробностей изложить основные тезисы, которые будут подробно раскрыты в последующих главах. А наибольшее внимание будет уделено, конечно, витой паре - как основному в настоящее время способу построения Ethernet-сетей 10/100baseT.

Основной упор будет делаться на тех материалах и оборудовании, которое обычно используется в недорогих Ethernet-сетях (которые, в свою очередь, послужили прототипом сетей последней мили). Технологии, интересные с точки зрения построения больших по размерам локальных сетей, но не получившие широкого распространения в России, экзотические, либо устаревшие, будут рассмотрены отдельно.

Глава 7

Сети на основе коаксиального кабеля.

На сегодня это далеко не самая распространенная, и не самая удобная технология. Но начать изложение с него нужно по историческим причинам. Первые сети Ethernet были построены на протоколе 10base5, использующей в качестве электрической среды передачи данных "толстый" коаксиальный кабель (ThickNet). Использовать его практически оказалось не слишком удобно, и практически сразу появился более простой и дешевый вариант 10base2, использующий "Тонкий" коаксиальный кабель (ThinNet).

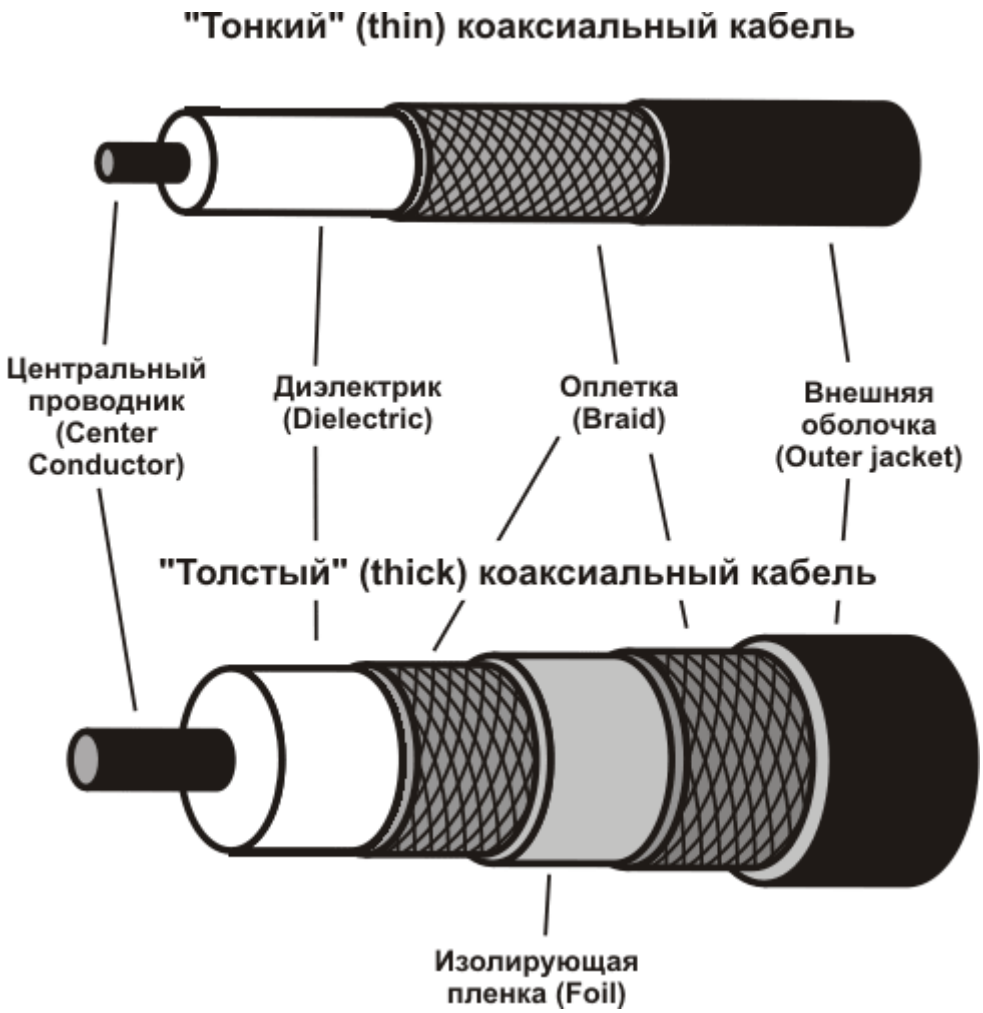

Рис. 7.1. Коаксиальные кабели

Как правило, "толстый" коаксиал производился ярко-желтого цвета. "Тонкий" изготовляли черным, реже серым. Из-за высокой цены и сложностей в инсталляции, первый вариант в России воспринимается как экзотика, и найти работающую сеть на его основе - огромная проблема. Тем не менее, общее представление о нем желательно иметь. Возможно, не будь эта технология столь дорогой и устаревшей, она смогла бы, благодаря удобной топологии и работе на большие расстояния, найти широкое применение в домашних (кампусных) сетях.

В сетях 10base5 и 10base2 применяются только кабеля, имеющие волновое сопротивление 50 Ом. В качестве основного топологического элемента, используется сегмент. Так называется общая длина кабеля между двумя терминаторами, устанавливаемыми на обоих концах сети (один из них должен быть заземлён).

В случае, если необходима сеть большего размера, несколько сегментов (или компьютеров) можно соединить при помощи репитеров (repeater), которые восстанавливают уровень сигнала и передают его на несколько портов.

В сети не может быть более 5 сегментов, 4 репитеров, и только 3 сегмента могут иметь подключенные устройства. Остальные 2 служат только для увеличения протяженности сети. Это ограничение более известно, как правило (5/4/3), и применяется ортодоксальными стандартами для всех сетей Ethernet.

Особенности сетей, использующих "толстый" коаксиальный кабель и протокол передачи данных 10base5, показаны на следующей схеме.

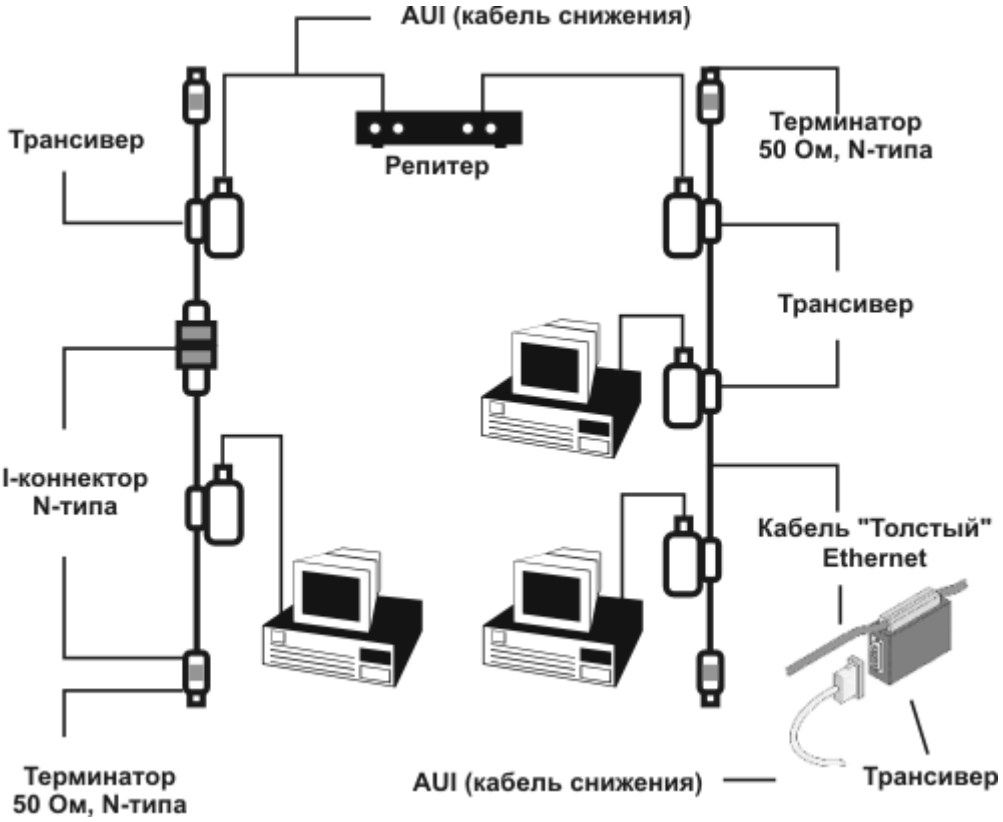

Рис. 7.2. Схема сети на "толстом" коаксиальном кабеле

- Каждый компьютер подсоединяется к главному кабелю (магистраль, backbone) с помощью специального "кабеля снижения" (drop cable). Этот кабель, в свою очередь, присоединяется к AUI-порту сетевого адаптера.
- Стандарт 10Base5 поддерживает до 100 узлов на сегмент (расстояние между узлами кратно 2,5 метрам).
- Максимальная длина не более 500 метров;
- Главный кабель RG-8, RG-11. Сокращение RG означает кабель, от "Radio Grade" - волновод.
- Используются коннекторы N-типа.
- Напряжение пробоя изоляции между узлами - 5 кВ.
- Наружный диаметр 10 мм, центральный проводник - 2,17 мм, затухание на частоте 10 МГц в районе 70 dB/км (подробнее значение этого параметра будет дано в разделе, посвященном кабелям на основе витой пары).
- Кабель снижения состоит из витых пар, может иметь длину до 50 метров. Используются разъемы типа DB15 (15 контактов), более известные под названием "AUI". Внешне они похожи на известные DB9 (RS-232, 9 контактов).

Особенности сетей, использующих "тонкий" коаксиальный кабель и протокол передачи данных 10base2 показаны ниже.

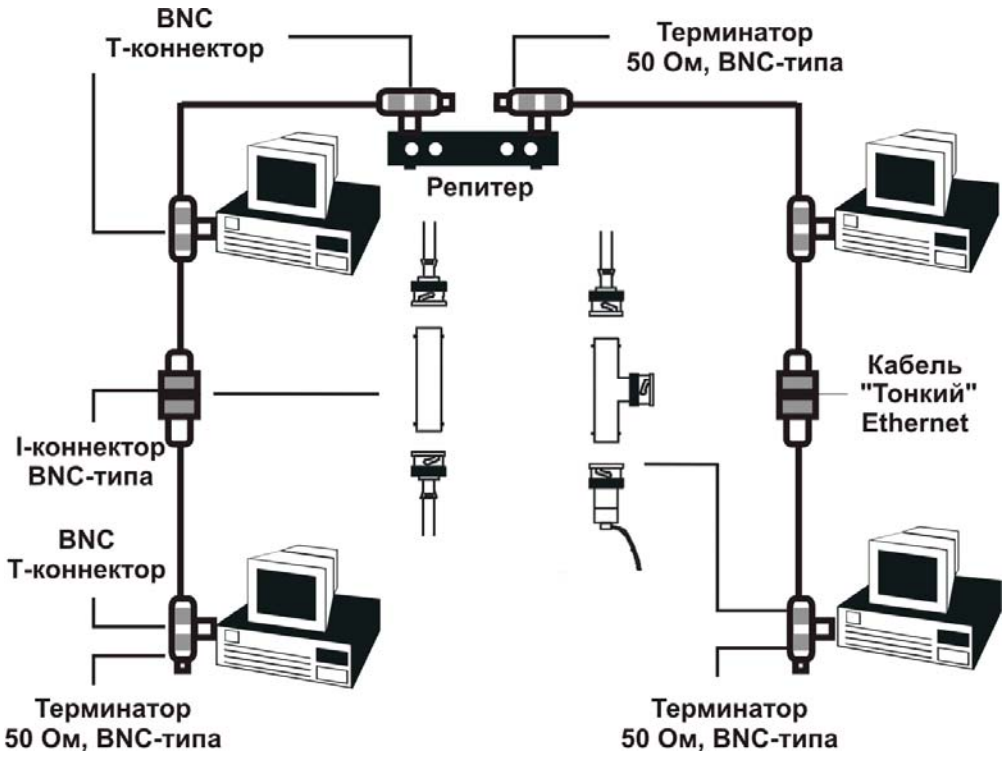

Рис. 7.3. Схема сети на "тонком" коаксиальном кабеле

- К одному сегменту не может быть подключено более 30 устройств, длина которого должна составлять не более 185 м. Минимальное расстояние между ними составляет 0.5 метра. Таким образом, в локальной вычислительной сети может быть максимум 90 компьютеров.
- Кабель RG58/U (одна центральная жила), RG58A/U, RG58C/U (негорючий материал диэлектрика).
- Напряжение пробоя изоляции между узлами - 100 Вольт.
- Наружный диаметр около 5 мм, центральный проводник - 0,8 мм, затухание на частоте 10 МГц около 160 dB/км.
- Применяются разъемы BNC-типа. Для подключения сетевых адаптеров к кабелю используются специальные Т-коннекторы (T-Connector).

Сети на "тонком" коаксиальном кабеле сравнительно широко распространены. Эта технология до недавнего времени была достаточно удобна для небольших (до 5-10 компьютеров) сетей. Как основное достоинство по сравнению с витой парой выделялось отсутствие активного оборудования. Однако, в последнее время применяющиеся в подобных сетях хабы (коммутаторы) так сильно подешевели, что делать новую сеть на коаксиальном кабеле не имеет ни малейшего смысла.

Аргументы против коаксиального кабеля достаточно серьезны:

- ограничение скорости в 10 Мбит;
- коаксиальный кабель примерно на 30-40% дороже, чем витая пара;
- низкая технологичность инсталляции, сложность в эксплуатации;
- рассоединение шины в любом месте полностью нарушает работоспособность сети, вызывая известный среди сетевых администраторов прошлого "бег вдоль сети с терминатором";
- низкая устойчивость к статическому напряжению и грозовым наводкам;

Все эти причины привели к тому, что в корпоративных сетях (и по распространенному стандарту TIA-568A) коаксиальный кабель просто не рассматривается как возможная среда передачи данных. По возможности, его стараются не применять даже для телевизионной проводки.

Глава 7

Витая пара (Twisted Pair).

Наиболее популярным материалом для построения современных компьютерных сетей является витая пара. На сегодня это недорогой и универсальный кабель для создания локальных коммуникаций практически любого уровня сложности. Постараемся объяснить, почему она получила такое широкое распространение.

Общее понятие о витой паре

Витая пара - это изолированные проводники, попарно свитые между собой некоторое число раз на определенном отрезке длины, что требуется для уменьшения перекрестных наводок между проводниками. Такие линии как нельзя лучше подходят для создания симметричных цепей, в которых используется балансный принцип передачи информации.

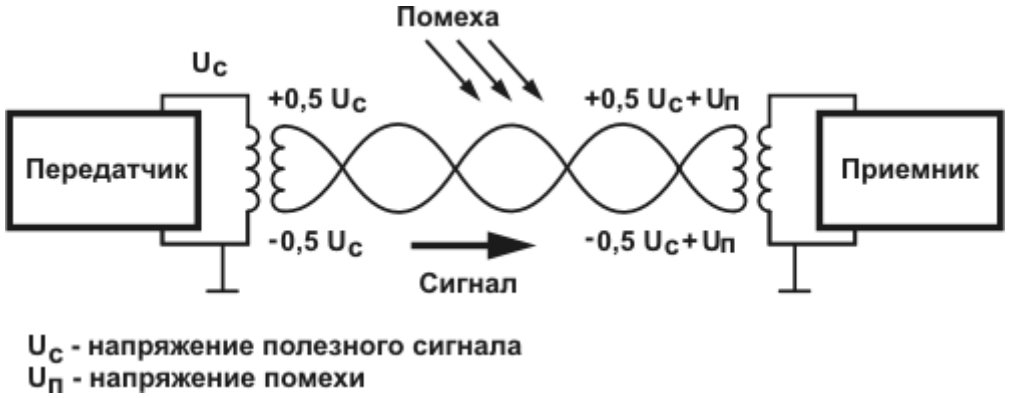

Рис. 7.4. Симметричная цепь

Приемник и передатчик гальванически развязаны друг от друга согласующими трансформаторами. При этом во вторичные обмотки (сетевые адаптеры) подается только разность потенциалов первичной обмотки (непосредственно протяженной линии). Из-за этого необходимо отметить два важных момента.

- Токи в любой точке идеальной витой пары равны по значению, и противоположны по направлению. Следовательно, векторы напряженности электромагнитного поля каждого из проводников противоположно направлены, и суммарное ЭМИ отсутствует. Под идеальной витой парой понимается линия, в которой проводники бесконечно плотно прилегают друг к другу, имеют бесконечно малый диаметр, и ток, протекающий через них, стремится к нулю.
- Метод накладывает некоторые ограничения на протокол передачи (невозможность передачи постоянной составляющей), но значительно более устойчиво к внешним влияниям (по сравнению, например, с несимметричным RS-232). Из рисунка 5.5. видно, что результирующее напряжение наводки на вторичной обмотке будет

синфазным, соответственно не передастся на вторичную обмотку (сетевой адаптер).

Разновидности витопарных кабелей

Витая пара не была новым изобретением. До этого она уже многие десятки лет успешно использовалась в телефонии, и остается только удивляться, почему ее перенос на почву Ethernet прошел только сентябре 1990 года, когда был официально принят стандарт 10baseT. Вполне естественно, что это была витая пара 3 категории, с очень большим, в десятки сантиметров, шагом скрутки проводов в паре, и небольшой, до 20 МГц, полосой пропускания (т.е. были взяты прямо из телефонной проводки). Компьютерные кабеля отличало только оформление - 4 пары под одной оболочкой.

Немного позже, одновременно с появлением Fast Ethernet в 1995 году, был введен новый стандарт на кабель Категории 5 (Level 5), с шагом скрутки, меняющемся для разных пар от 12 до 32 мм (например, ряд от Lucent - 15, 13, 20, 24 мм). Делается это для уменьшения перекрестных наводок, о которых будет рассказано ниже. Такой кабель обеспечивает передачу сигналов с частотой до 100 Мбит. Далее, несколько лет назад, появилась Категория 5e (до 125 МГц), в разработке Категоря 6 (до 200 МГц) и Категория 7 (до 600 МГц).

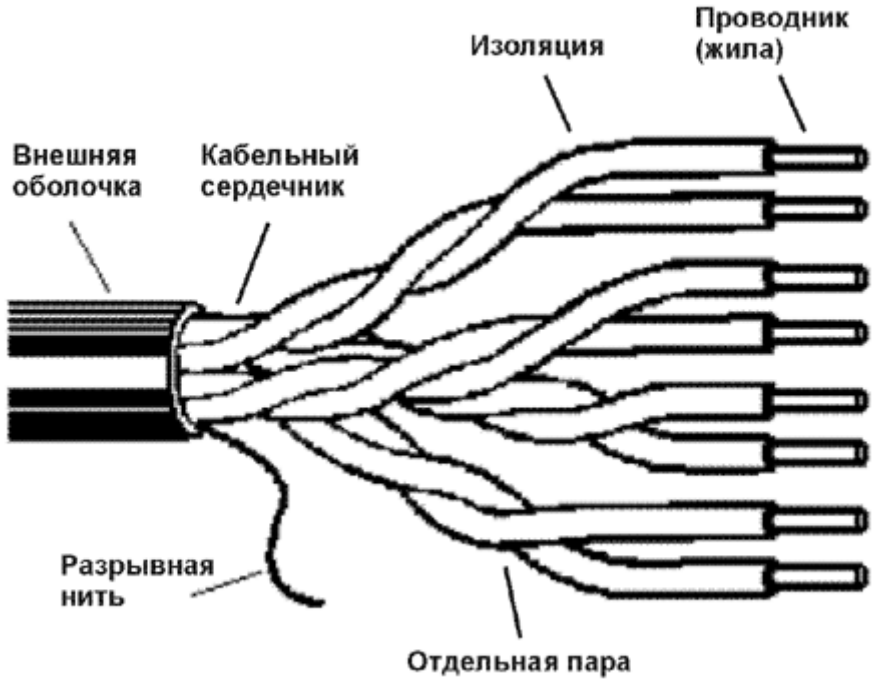

Рис. 7.5. Конструкция витой пары

Предполагаю, что подробно пояснять конструкцию витопарного кабеля нет необходимости - все понятно из рисунка. Как правило, кабель имеет 4 пары в одной оболочке. Немного реже встречаются 2-х парные варианты, которые можно применять с ограниченным числом сетевых протоколов.

Проводники изготовлены из монолитной медной проволоки толщиной 0,5 - 0,65 мм. Кроме метрической, применяется система AWG, в которой эти величины составляют 24

или 22 соответственно. Толщина изоляции - около 0,2 мм, материал обычно поливинилхлорид (английское сокращение PVC), для более качественных образцов 5 категории - полипропилен (PP), полиэтилен (PE). Особенно высококлассные кабеля имеют изоляцию из вспененного (ячеистого) полиэтилена, которые обеспечивают низкие диэлектрические потери, или тефлона, который обеспечивающий уникальный рабочий диапазон температур.

Разрывная нить (обычно капрон) используется для облегчения разделки внешней оболочки - при вытягивании она делает на оболочке продольный разрез, которы открывает доступ к кабельному сердечнику, гарантированно не повреждая изоляцию проводников.

Внешняя оболочка имеет толщину 0,5-0,6 мм, и обычно изготавливается из привычного поливинилхлорида с добавлением мела, который повышает хрупкость. Это необходимо для точного облома по месту надреза лезвием отрезного инструмента. Кроме этого, начинают применяться так называемые "молодые полимеры", которые не поддерживают горения, и не выделяют при нагреве галогенов. Их широкому внедрению пока мешает только более высокая (на 20-30%) цена.

Самый распространенный цвет оболочки - серый. Оранжевая окраска, как правило, указывает на негорючий материал оболочки, который позволяет прокладывать линии в закрытых областях. В общем случае, цвета не обозначают особых свойств, но их применение позволяет легко отличать коммуникации с разным функциональным назначением, как при монтаже, так и обслуживании.

Отдельно нужно отметить маркировку. Кроме данных о производителе и типе кабеля, она обязательно включает в себя метровые или футовые метки

Конструкция кабельного сердечника достаточно разнообразна. В недорогих кабелях пары уложены в оболочке "как попало". Более качественные варианты предусматривают парную (по две пары между собой) или четверочную скрутку (все четыре пары вместе). Последний вариант позволяет уменьшить толщину сердечника и достигнуть лучших электрических характеристик. Но относительно высокая стоимость не позволила этим типам кабеля получить широкое распространение в России (и тем более, в недорогих домашних сетях).

Форма внешней оболочки так же может быть различна. Чаще других применяется самая простая - круглая, а для 2-х парных кабелей - овальная. Только для прокладки под половым покрытием, по очевидной причине, используется плоский кабель.

Отдельно стоят кабеля для наружной прокладки. Они обязательно имеют влагостойкую оболочку из полиэтилена, которая наносится (как правило) вторым слоем поверх обычной, поливинилхлоридной. Кроме этого, возможно заполнение пустот в кабеле водоотталкивающим гелем, и бронирование с помощью гофрированной ленты.

По наличию (или отсутствию) экрана, различают несколько типов кабелей:

- UTP (unshielded twisted pair), что означает незащищенная витая пара (НЗВП), то есть кабель, витые пары которого не имеют индивидуального экранирования;
- FTP (Foiled Twisted Pair) - фольгированная витая пара. Имеет общий экран из фольги, однако у каждой пары нет индивидуальной защиты;

- STP (shielded twisted pair) - защищенная витая пара (ЗВП), каждая пара имеет экран;
- ScTP (Screened Twisted Pair) - экранированный кабель, который может как иметь, так и не иметь защиту отдельных пар;

Экран выполняется либо плетеным из медной проволоки (хорошая защищает от низкочастотных наводок), либо из токопроводящей фольги (пленки), которая блокирует высокочастотное электромагнитное излучение. Так же на практике часто используют двойные экраны (HIGHT Screen), в которых используются оба способа.

Эффект от применения экрана на первый взгляд достаточно прост - уменьшение внешних наводок на экранированную пару (или несколько пар), и снижение уровня их электромагнитного излучения "наружу".

Но общий экран вызывает рост NEXT (перекрестных наводок, подробно рассмотренных ниже) из-за отражения от экрана, на 10-20%. Далее, экранирование увеличивает затухание в кабеле вследствие добавочной емкости между экраном и витыми парами. Но и это не все. Монтаж экранированной системы значительно более сложен (дорог), требует хорошего подбора всех элементов. А самые незначительные ошибки способны ухудшить, а не улучшить параметры линии.

Это достаточно, что бы большинство производителей СКС отказалось от применения FTP или ScTP. Но это не снижает значение экрана в условиях очень высокого уровня внешних помех, или при большой вероятности "грозовой" наводки. Последнее существенно практически для всех внешних прокладок.

Однако, нужно подчеркнуть - в домашних сетях (с использованием любого типа кабеля) не создается экранированной кабельной системы. При заземлении экрана появляются лишь отдельные экранированные линии. Наиболее хорошей аналогией будет прокладка обычной витой пары в металлической трубе (этот способ часто применяют в условиях монтажа сетей в промышленных помещениях).

Экран, индивидуальный для каждой пары, действительно позволяет улучшить электрические показатели кабеля, но вызывает значительный рост стоимости, а так же веса и объема. Поэтому, такой вариант имеет смысл использовать в самых крайних случаях.

По вышеизложенным причинам, а именно, благодаря низкой цене, удобному и легкому монтажу, широкое распространение получила только незащищенная витая пара (UTP). Именно она является основой всех современных компьютерных сетей.

Параллельно с уже рассмотренными, используется еще два основных типа кабелей, имеющих несколько другое функциональное применение.

Для магистральных прокладок часто используют кабеля с 10, 25, 50, 100 и более, парами в одной оболочке. Тут ассортимент производителя достаточно широк, что бы удовлетворить любые требования. Есть многоэлементные кабеля, объединяющие одной оболочкой множество 2-х или 4-х парных элементов. Есть многопарные, в которых все витые пары находятся под одной оболочной, и для удобства монтажа разделены на пучки полиэтиленовыми ленточками.

Для подключения абонентского оборудования, и коммутации используются гибкие кабеля (шнуры, патч-корды). Из-за необходимости устойчивости к постоянным изгибам, проводник у них выполнен не из одной, а из семи более тонких медных проволок толщиной около 0,2 мм каждая (многопроволочная конструкция). Той же цели служит более толстая (до 0,25 мм) изоляция, и внешняя оболочка повышенной гибкости.

Из-за большего, в сравнении с обычным, затухания использовать кабель для шнуров оправдано только на небольшие расстояния, как правило, не более 5 метров с каждой стороны линии.

Параметры, определяющие электрические свойства витой пары

Электрические свойства витой пары, как обычной направляющей системы электромагнитных колебаний характеризуются сопротивлением R, индуктивностью проводников L, емкостью C, и проводимостью изоляции G.

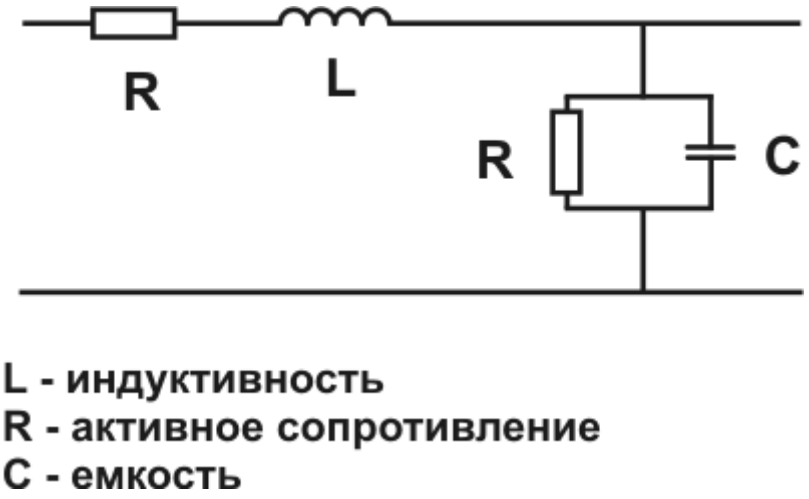

Рис. 7.6. Упрощенная эквивалентная электрическая схема витой пары

Величины R и G обуславливают тепловые потери в меди и диэлектрике соответственно. L и C определяют реактивность системы, или, иначе говоря, ее частотные свойства.

Активное сопротивление R постоянному току зависит от материала проводника, его геометрических размеров, и его температуры. По распространенному стандарту EIA/TIA-568A это значение не должно превышать 19,2 Ом на короткозамкнутом шлейфе длиной в 100 метров при температуре 20° C. Эту величину можно легко измерить простым омметром.

С увеличением частоты сигнала, активное сопротивление растет. Это обусловлено прохождением тока в основном по части, обращенной к другому проводнику (эффект близости). Вытеснение тока к поверхности проводника (скин-эффект) для проводов тоньше 0,8 мм мало заметен, но какое-то минимальное влияние на уменьшение эффективного сечения то же оказывает.

Проводимость изоляции G является мерой качества материала и его нанесения на поверхность отдельного проводника. Сопротивление току утечки связанное с несовершенством диэлектрика, может достигать нескольких единиц гигаом, и на сегодня его можно не учитывать. Поэтому, в основном на проводимость изоляции влияют затраты на поляризацию диполей материала диэлектрика.

Особенно много их содержится в поливинилхлориде, часто используемом для витой пары низкой категории. В более качественных кабелях обычно используются полиэтилен или тефлон, рассеяние энергии в которых гораздо ниже. Еще ниже этот показатель для вспененных материалов, применяемых для кабелей высшего класса.

Индуктивность L можно разделить на внешнюю (определяемую геометрией и магнитными свойствами проводника), и внутреннюю (создаваемую магнитным полем протекающего тока). Внутренняя индуктивность имеет слабую тенденцию к уменьшению с ростом частоты.

Два проводника, составляющих пару, можно рассматривать как конденсатор, емкость которого, C, не зависит от частоты. Она определяется материалом изоляции, геометрическими размерами проводников, и расстоянием между ними. По стандарту, для современных кабелей, величина емкости составляет не более 5,6 нФ.

Особо нужно отметить, что применение экрана вызывает рост емкости примерно на 30%, что существенно снижает его эксплуатационные свойства такого кабеля.

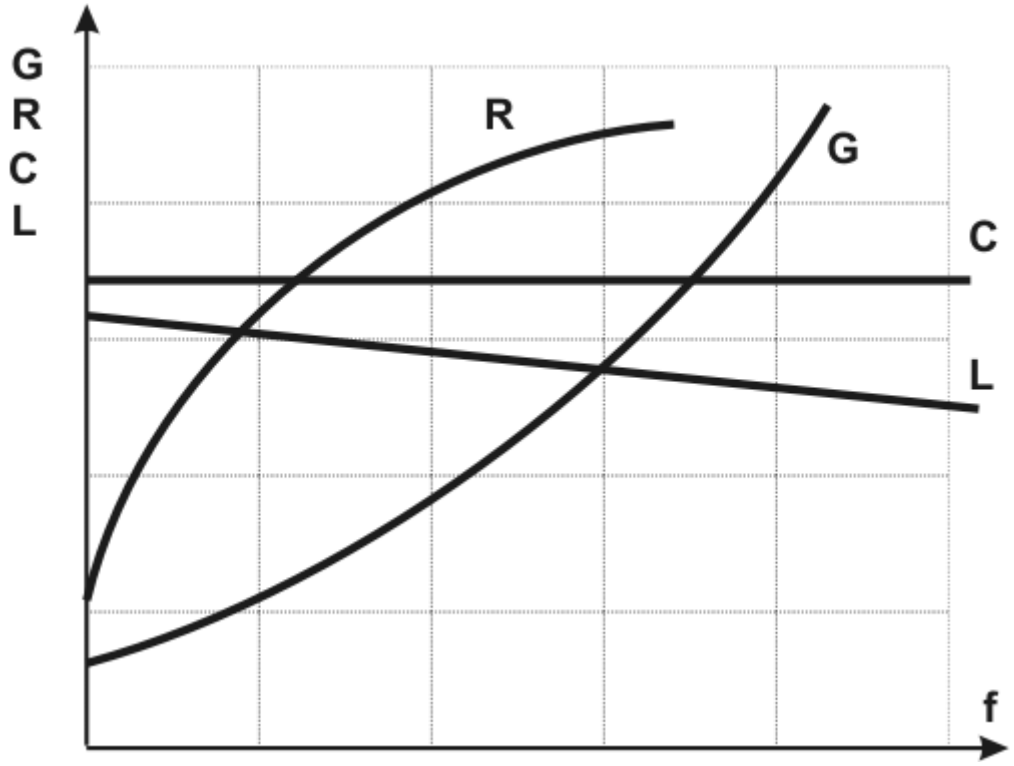

Рис. 7.7. Частотная зависимость электрических свойств витой пары

На основании перечисленных электрических параметров, может быть рассчитано волновое сопротивление. Сделать это можно по формуле $Z = v(R+jwL)/(G+jwC)$, которую для высоких частот Ethernet можно упростить до $Z = vL/C$. В рабочем диапазоне кабеля эта величина должна составлять 100 ± 15% Ом.

Волновое сопротивление хорошо характеризует однородность тракта передачи электромагнитной энергии. Его неоднородности неизбежно вызывают отражения части сигнала, и ухудшение качества линии. Поэтом, достаточно очевидно, что все составляющие, включая сетевые адаптеры, должны иметь одинаковое волновое сопротивление. Иначе, можно сказать, должны быть согласованы.

Как правило, неоднородности волнового сопротивления на реальных коммуникациях являются следствием некачественного монтажа (изгиб, давление, растяжение, перекручивание). Более подробно этот вопрос будет рассмотрен в разделе, посвященном рефлектоскопии.

Глава 7

Витая пара (соотношение сигнал и шум).

Несмотря на первоочередное физическое значение основных электрических параметров, использовать их для реальной оценки качества среды передачи не целесообразно. Тем более, исторически сложилось, что для оценки качества передачи требуется знать только соотношение двух базовых параметров - сигнала и шума. Это достаточно логично, ведь для корректной интерпретации принятого сигнала не важно абсолютное значение амплитуды, она может составлять и 0,001 В, и 1000 В. Необходимо, что бы полезный сигнал был различим на фоне шума (превышал уровень помех).

Поэтому нормируются производителем и определяются при тестировании линии именно те параметры, с помощью которых можно легко сопоставить уровни сигнала и шума. При этом в качестве основной единицы измерения выбраны Децибелы (дБ).

Это условное обозначение, позволяющее сравнивать и количественно оценивать уровни сигналов, относящиеся к процессам в различных средах и измеряемым в различных единицах. Важно помнить, что децибелы определяют отношение уровней, а не абсолютную величину, и для преобразования в них применяется следующая формула: X(дБ) = 20*log10(P1/P2), где P1 и P2 - два сравниваемых значения.

Рассмотрим наиболее важные из параметров, определяющих физические свойства линии передачи данных. Наиболее существенное влияние на них оказывает затухание (ослабление) - отношение мощности сигнала на выходе из передатчика к мощности сигнала на входе в приемник той же линии. Обуславливает постепенную потерю энергии сигнала в среде передачи, в результате которой мощность полезного сигнала уменьшается.

A = 20*log10 (P передатчика / P приемника)

Для оценки качества кабеля часто используется коэффициент затухания alfa, который отражает ослабление сигнала на единицу длины:

alfa(дБ/метр) = A (дБ) / L (м), где L - длина кабеля.

Нужно различать собственное (в идеальных условиях), и рабочее затухание кабеля. Наименьшим оно будет в случае равенства волнового сопротивления источника сигнала, приемника, и самого кабеля (отражение электромагнитной энергии будет отсутствовать). Иначе говоря, должна быть обеспечена согласованная нагрузка.

Так как затухание прямо пропорционально сопротивлению витой пары, то из рисунка 7.7. следует вывод, что оно растет по мере увеличения частоты сигнала, постепенно стабилизируясь на высоких частотах.

К сожалению, затухание далеко не полностью описывают картину прохождения сигнала по реальному кабелю. При передаче сигналов по неидеальной витой паре, часть энергии рассеивается в окружающем пространстве в виде электромагнитных волн (а не только в виде тепла). Причем, чем больше будет отличаться от идеальной витая пара (будет разбалансированной), тем больше будет энергия такого излучения.

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

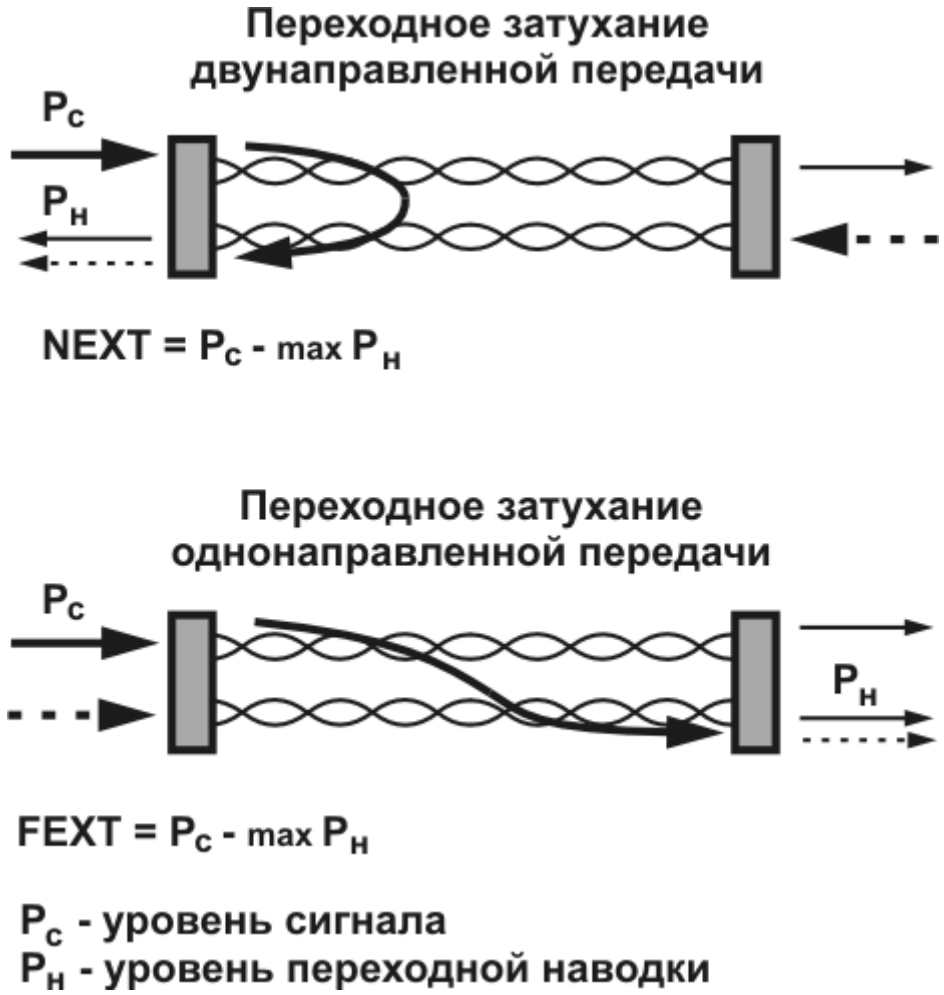

Рис. 7.8. Переходные наводки

Необходимо различать NEXT (Near End Crosstalk) - переходное затухание двунаправленной передачи, и FEXT (Far End Crosstalk) - переходное затухание однонаправленной передачи (английское слово Cross часто сокращают как X). Надо отметить, что дословно NEXT означает перекрестные наводки на ближнем, а FEXT - на дальнем конце кабеля.

Таким образом, в зависимости от типа передачи (или от места измерения, по другой трактовке), можно применять следующие соотношения: NEXT (FEXT) = 20*log10 (Pc/Pн), где Pc - мощность сигнала, а Pн - мощность сигнала, наведенная на другой витой паре).

Связана такая серьезная терминологическая путаница с тем, что 10/100baseT имеет одну пару на передачу, а другую на прием. При этом понятие однонаправленных наводок не

имеет практического смысла (как не имеет смысла понятие наводки на источник сигнала). Естественно, первоначальные определения давались по принципу "как проще", потом они "устоялись" в нормативах, документации, технологическом оборудовании, и изменить их стало практически невозможно.

Таким образом, чем выше NEXT и FEXT, тем меньше уровень имеет наводка в соседних парах, и тем выше качество кабеля. Это объясняет выбор в качестве базового такого неочевидного параметр, как перекрестное затухание (а не более понятной инженерам наводки). Из маркетинговых соображений, лучший кабель не должен иметь более низкие числа в малопонятных неспециалистам характеристиках.

Вполне закономерно, что наводки зависят от частоты, так как параллельно идущие проводники можно рассматривать как обкладки конденсатора. Стандарт EIA/TIA-568A нормирует минимально допустимые значения для переходного затухания двунаправленной передачи (при кабеле 100 метров длиной) по следующей формуле:

NEXT(f) = NEXT(0,772) - 15*log10(f/0,772), где NEXT(0,772) - минимально допустимое переходное затухание двунаправленной передачи на частоте 0,772 МГц (составляет 43 дБ для кабеля 3 категории, и 64 дБ для 5 категории), а f (МГц) - частота сигнала.

На основе описанных параметров несложно вывести критерии, напрямую показывающие соотношение сигнал/шум (а значит, и качество линии) в логарифмическом виде. В кабельных системах для этого используется следующая пара параметров. ACR (attenuation to crosstalk ratio), дословно переводится как "отношение затухания к наводкам", и ELFEXT (equal level far end crosstalk) - "равноуровневые наводки на дальнем конце". Эти параметры не определяются путем измерений, а рассчитываются по следующим формулам:

ACR = NEXT - A, ELFEXT = FEXT - A.

Физический смысл ACR достаточно прост - это превышение сигнала над уровнем собственных шумов при двунаправленной передачи сигналов, а ELFEXT - однонаправленной.

Так как основным видом помех в кабелях компьютерных сетей являются наводки, то использование параметра ACR позволяет однозначно определить верхнюю границу частоты электрического тракта передачи (либо любой его части). Считается, что среда передачи может обеспечить устойчивую полнодуплексную работу любого приложения с такой граничной частотой, на которой параметр ACR составляет 10 дБ.

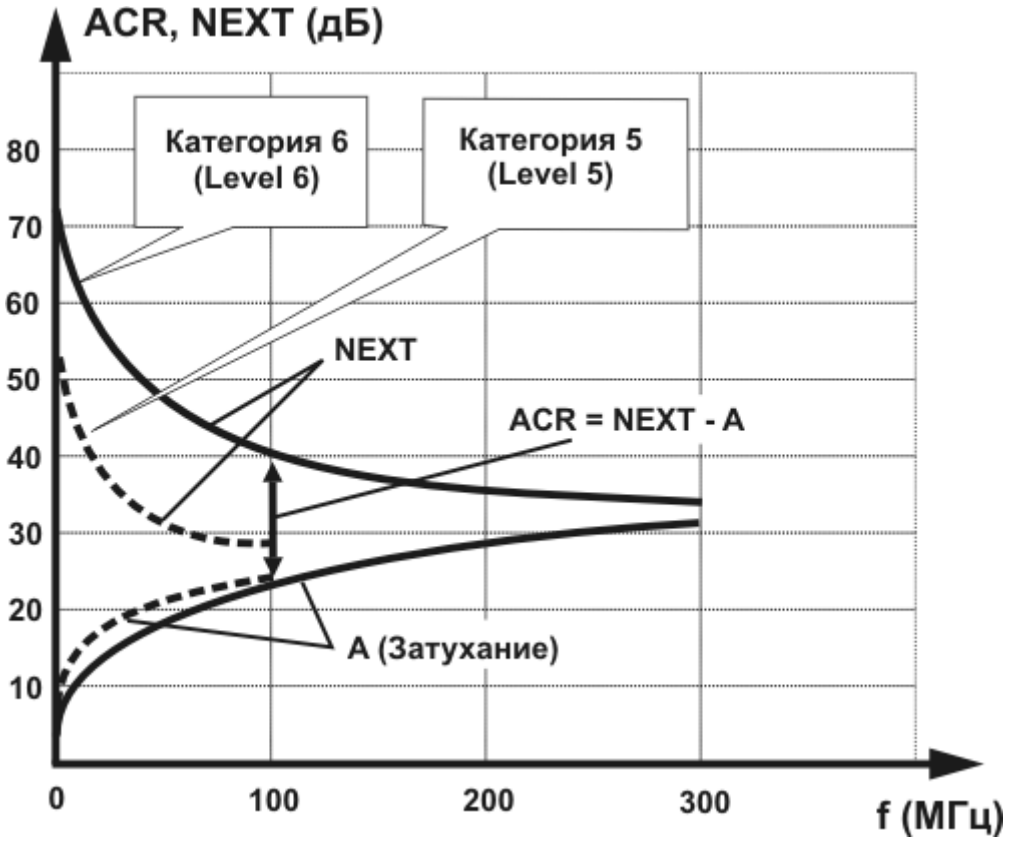

Рис. 7.9. Граничная частота среды передачи

Приведенный график очень наглядно показывает картину возможности приема сигнала заданной частоты от параметров кабеля. Особенно хорошо это видно для нестандартных кабелей, и в следующих главах к этой иллюстрации мы еще не раз вернемся.

Для иллюстрации, рассмотрим стандартный кабель длиной 100 метров в сети 100baseT. По нормам, затухание не должно превышать 24 дБ. В десятичных величинах это значит уменьшение сигнала в 251 раз. Уровень наводок на входе в приемник для комбинации худших пар ограничен величиной 27,1 дБ. Это значит, что мощность наводок в 513 раз меньше мощности сигнала передатчика смежной пары. Сигнал превышает наводки на 3,1 дБ или в 2,04 раза.

Есть еще несколько параметров, которые действующими стандартами не нормируются, но на высокоскоростную передачу данных могут влиять.

Прежде всего, это относительная скорость распространения сигналов (NVP, Nominal Vilocity of Propagation), выражающее в процентах замедление сигналов в витой паре относительно скорости света в вакууме. Параметр может оказаться важен для корректной работы высокоскоростных приложений. Так же рефлектометры его используют для определения расстояния до аномалии.

Задержка (Delay) в передаче сигнала по одному кабелю, определяется разной электрической длиной пар с разным шагом скрутки и разным материалом изоляции. Для протоколов 10/100baseT это практически не имеет значения, но уже для 1000baseT некоторые специфические виды кабелей (например, с разным материалом диэлектрика в парах) могут вызвать серьезное рассогласование сигнала.

В заключение раздела нужно сказать, что с увеличением скоростей передачи данных, все большее количество параметров приходится принимать во внимание при построении сетей. Описанных вполне достаточно для 10/100/1000baseT. Но, к сожалению, это не значит, что для следующих протоколов не придется учитывать еще какие-либо особенности электрической среды, образуемой витопарным кабелем.

Глава 7

Типы и использование электрических разъемов.

Согласно известной поговорке, электроника - наука о контактах. Это верно и для сетей. Место и способ соединения по праву можно назвать важнейшим элементом кабельной структуры. Как правило, уменьшить перекрестные наводки в кабелях оказывается намного проще, чем компенсировать разбалансировку, вызванную расплетением витых пар в разъемах. Так, достаточно часто в литературе встречается ссылка на распространенность ситуации, при которой параметры кабеля длиной 90 метров примерно на порядок лучше, чем у кабеля такой же длинны с двумя разъемами на концах.

Основные понятия

Разъем можно определить как окончание кабеля для коммутируемого электрического или оптического разъемного соединения. Коннектор - часть кабельного разъема, обеспечивающая электрическое подключение проводников. Именно этот элемент конструкции должен обеспечить неразъемный контакт проводников кабеля в разъеме, и разъемный - для соединения самих кабелей.

Соединения кабелей, в свою очередь, могут быть симметричными и несимметричными. При этом, несимметричные кабельные разъемы не требуют для стыковки дополнительных элементов (классический пример - витая пара) подразделяются на гнездовые и штекерные, например RJ45 (RJ - registered jack, любой разъем, применяемый для соединений, описанных в Code of Federal Regulations, глава 74, часть 68). В отличие от них, симметричные разъемы (например, BNC) подключают друг к другу с помощью соединителей, которые часто называют I-коннекторами.

Надо специально отметить, что конструкции разъемов достаточно разнообразны, и иногда четко определить название того или иного элемента бывает затруднительно.

Наиболее распространенный способ неразъемного подключения проводников - "врезной контакт сквозь изоляцию" (КСИ в русскоязычной литературе, IDC - в англоязычной), разъемного - подпружиненные контакты.

Технология КСИ изобретение достаточно не новое, и первоначально использовалась для монтажа телефонных кроссов и слаботочных сетей. Такой способ надежнее, чем механический, и в десятки раз технологичнее пайки. Врезной контакт (из-за ограниченного доступа кислорода к месту контакта), не окисляется, не подвержен воздействиям, вызванным перепадом температур. Более того, часто в месте врезки происходит процесс диффузии - медь проводника и материал коннектора проникают друг

в друга, увеличивая площадь контакта. Поэтому с годами электрические параметры таких соединений даже улучшаются.

На сегодня, врезной контакт через изоляцию практически полностью вытеснил другие способы создания неразъемных соединений.

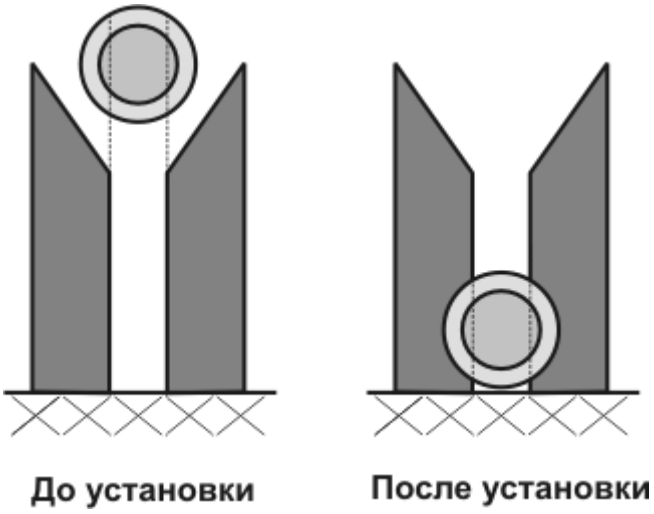

Рис. 7.10. Врезной контакт сквозь изоляцию

Группы двойных пружинящих контактов, которые объединяет коннектор, напоминают гребенку, в которой боковые поверхности зубцов представляют из себя тонкие электропроводные лезвия. При подключении проводники по одному проталкиваются между двух соседних зубцов, ножи которых прорезают изоляцию и часть проводника, обеспечивая тем самым электрический контакт.

Для уменьшения разбалансировки, вызванной нарушением скрутки витых пар, разработчики используют конструкцию, позволяющую расплетать витую пару на минимальную длину. Кроме этого, в некоторых типах разъемов гнездового типа для компенсации применяют печатные платы, которые устраняют разбалансировку всего соединения в целом (включая соответствующие штекерные разъемы).

Методы создания канала

Вообще говоря, этот пункт общий как для электрических, так и оптических сред передачи данных. Поэтому, мне пришлось долго колебаться в выборе места для этих материалов. В результате возобладала точка зрения, что при общей идеологии, в деталях витопарные и оптоволоконные сети сильно отличаются. И их проще для создания целостной картины рассматривать раздельно.

Второй, порой "путающий" момент. Необходимо различать коммутацию пакетов (или каналов), подробно рассмотренную в первых главах, и механическую коммутацию кабельных сетей, кратко рассмотреть которую предполагается в данном разделе.

Рассмотрим общий вид кабельного канала.

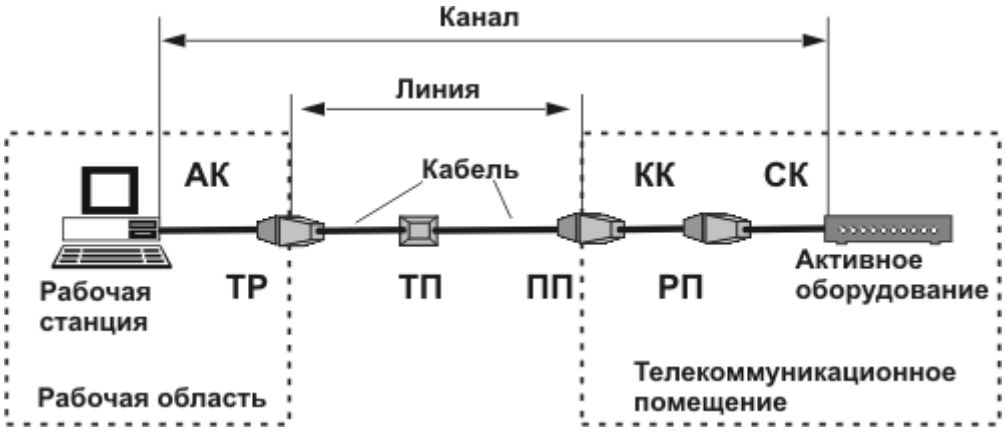

Рис. 7.11. Создание канала

На рисунке, АК - абонентский кабель, КК - коммутационный кабель, СК - сетевой кабель, ТР - телекоммуникационный разъем, РП - распределительная панель, ПП - промежуточная панель, ТП - точка перехода. Таким образом, для подключения оборудования используются абонентский кабель, телекоммуникационный разъем, две панели и два соединительных кабеля - сетевой и коммутационный (обычно они не отличаются друг), и соединение точки перехода.

Отметим, что в стандарте TIA/EIA-568A закреплены два метода создания канала: подключением (interconnection), и коммутацией (cross connection). Причем первый является частным случаем второго - в нем отсутствует промежуточная панель и коммутационный кабель.

Рассмотрим подробнее компоненты канала.

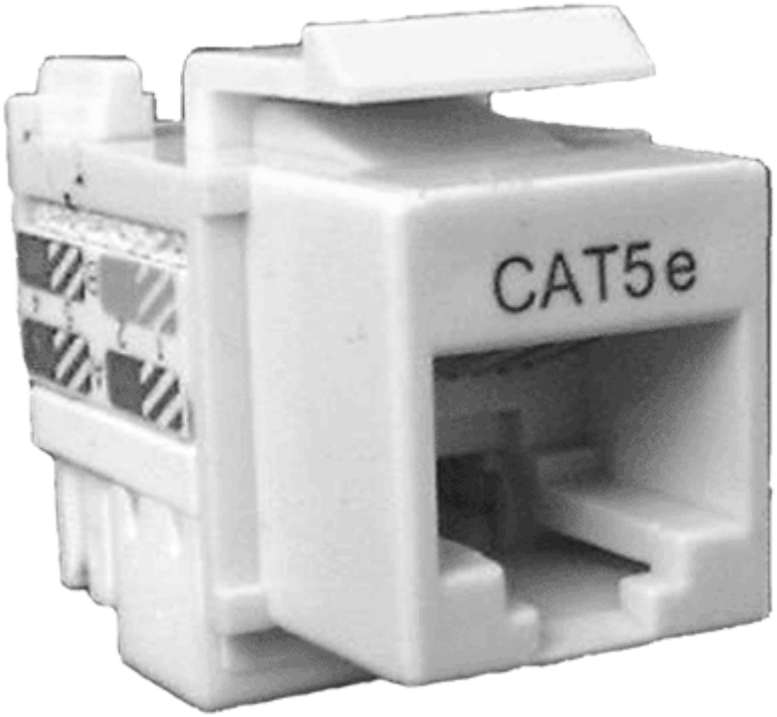

Рис. 7.12. Пример телекоммуникационного разъема

Телекоммуникационный разъем (telecommunication outlet) может быть расположен на стене, полу или в другой точке рабочей области. Как правило, каждое рабочее место оборудуется двумя разъемами (под компьютер и телефон), смонтированными в одной розетке.

Контакты штекера скользят в момент подключения по контактам гнезда, и образуют "контактную шину" с хорошими электрическими параметрами за счет большой длины поверхности. Материалом коннекторов обычно служит берилливая бронза с напылением золота.

Для перекоммутации соединений не нужно специальных навыков, и проводить ее можно от 750 до 10000 раз (в зависимости от исполнения разъема), с помощью стандартных сетевых или коммуникационных кабелей.

Распределительные (РП), так и промежуточные панели (ПП) можно разделить на три вида:

1. Коммутационные (распределительные) панели (patch panels) предназначены для размещения сетевых окончаний симметричных электропроводных кабелей. Коммутация осуществляется с помощью модульных гнездовых разъемов на лицевой стороне, а подключение проводников кабелей к врезным коннекторам - на тыльной. Для наглядности, можно представить панель в виде большого числа телекоммуникационных разъемов, объединенных одним конструктивным элементом.

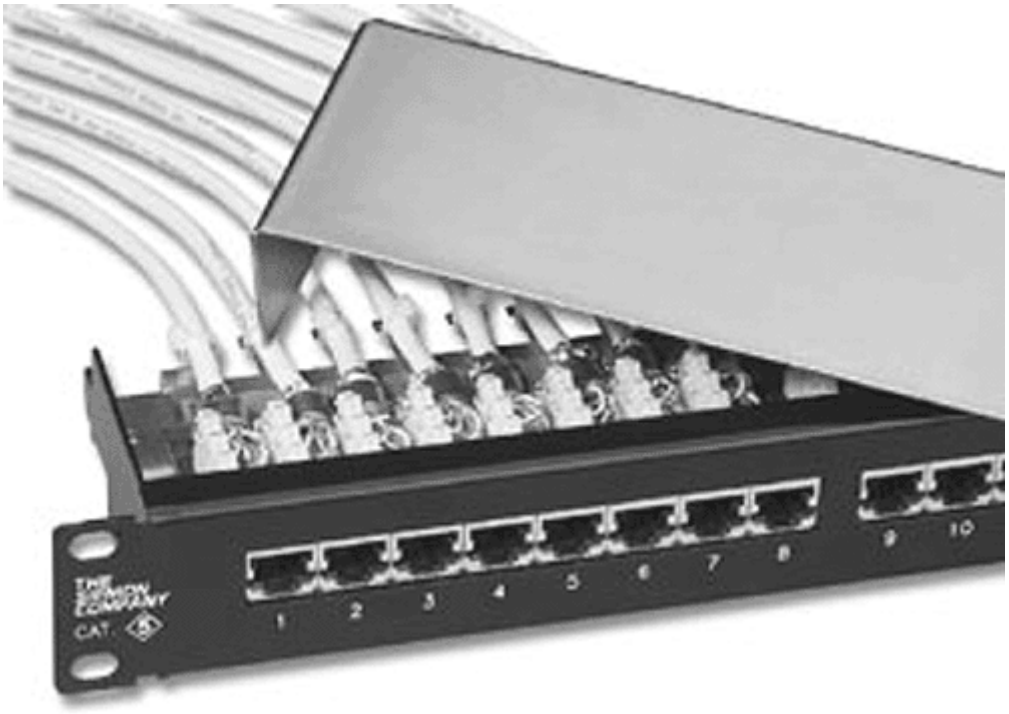

Рис. 7.13. Коммутационная панель

2. Соединительные панели (interconnect panels) обеспечивают разъемные соединения коаксиальных кабелей (BNC) или оптических волокон. При этом, к лицевой стороне подключают разъемы соединительных кабелей, к тыльной - оснащенные разъемами линии связи. Более подробно они будут рассмотрены в главе, посвященной оптической среде передачи.

3. Кросс (distribution frames) представляет собой поле с врезными контактами, которые обычно располагаться на лицевой стороне конструктивного блока. Соединения осуществляются коммутационными кабелями, оснащенными специальными разъемами или перемычками - одиночными витыми парами без разъемов.

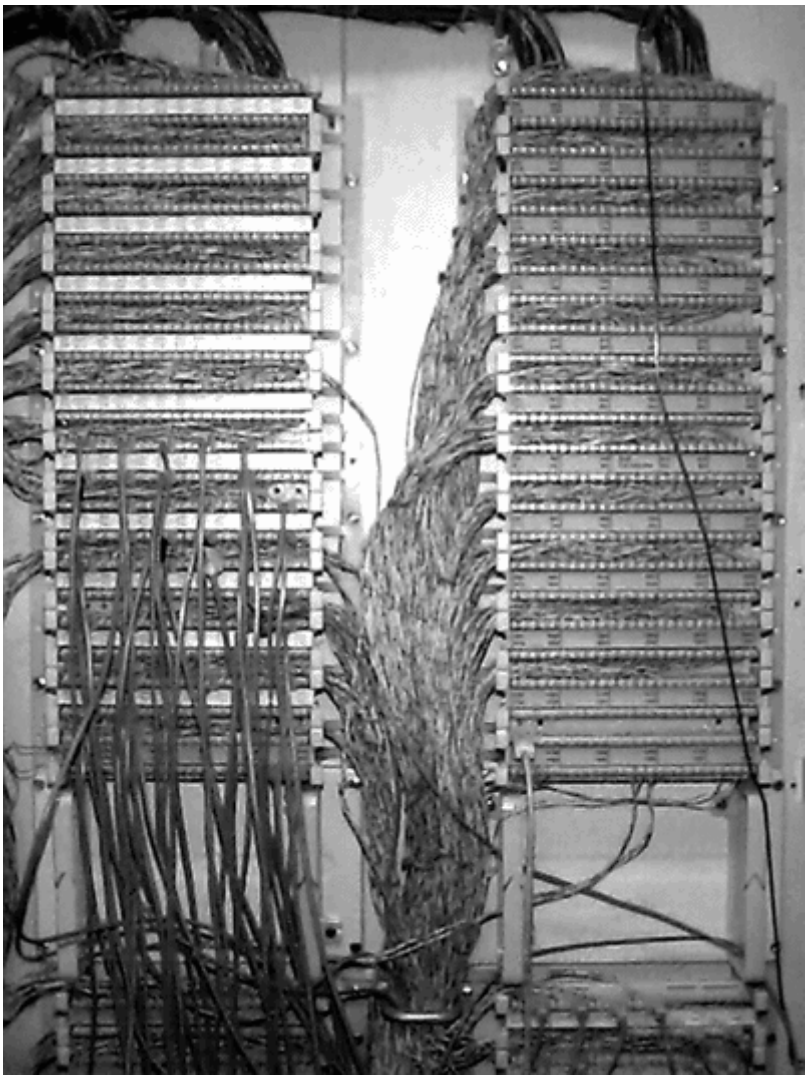

Рис. 7.14. 110 Кросс (Lucent)

Кроссовые панели с врезными контактами дешевле модульных, и обеспечивают большую гибкость и плотность соединений. Однако заделка проводов в них требует специальных инструментов (или специальных коммутационных кабелей, как в кроссе 110 типа), и определенных навыков.

Кроме того, существуют некоторые ограничения на число повторных заделок проводов в контакты с целью перекоммутации электрических цепей. Как правило, один и тот же контакт можно использовать не более 250 раз. Здесь следует, однако, отметить, что необходимость в таком количестве изменений на практике возникает крайне редко.

Все типы панелей устанавливаются в телекоммуникационных помещениях (шкафах), где обеспечивается необходимое для нормальной работы пространство, электропитание, обогрев, вентиляция.

Абонентские, сетевые и коммутационные кабеля часто называют одним термином - шнур, корд, patch cord. Действительно, обычно во всех случаях используется один и тот же тип кабеля. Единственный распространенный на практике обратный случай - коммутационный кабель для кроссов 110 типа, где используется специальный разъем на одном или обоих концах.

Рис. 7.14. Абонентский кабель и разъемы

Общая длина абонентских, коммутационных и сетевых кабелей, образующих канал, обычно ограничивается 10 метрами из-за большого, по сравнению с обычным, затухания в гибком кабеле.

В качестве разъемов используются RJ45. Контактная пластина, запрессованная в прозрачный корпус, имеет острые выступы, которые при обжиме обеспечивают надежное соединение по способу "врезной контакт через изоляцию". Существуют разные типы контактных пластин. Для монолитного проводника лезвия охватывают проводник сверху, и с разных сторон, а для многопроволочного - одно лезвие входит посередине между проволок. Так же существуют и универсальные конструкции.

В гнезде разъем RJ45 удерживается благодаря гибкой пластмассовой защелке.

Точка перехода (Transition Point) - место, в котором выполняется соединение двух кабелей разных типов (например, круглого кабеля с плоским), или разветвление многопарного

кабеля на несколько четырехпарных. В точке перехода не допускается подключение сетевого оборудования и выполнение переключений.

Кроме перечисленного, для фиксации разъемов используют розетки, панели, в организации каналов применяют короба, лотки, лестницы. Все это - конструктивные элементы, которые будут кратко рассмотрены в следующих главах.

Глава 7

Измерение параметров среды передачи.

Как уже говорилось выше, для определения качества линий используют величины, измерянные специальным оборудованием. По их результатам можно достаточно точно оценить пригодность сети к эксплуатации.

Если специалисты плохо представляют себе значение тестируемых параметров, или надеются на полное соответствие стандартов, объявляемых производителями материалов и оборудования, то процесс сертификации больше похож на церемонию. Более того, гарантии соответствия стандартам сами по себе бесполезны для пользователей, их интересует работа реальных протоколов, требования которых могут неожиданно разойтись с "гарантированными" параметрами линии.

Вариантов разрешение такой ситуации по сути два. Можно надеяться на высокое качество материалов и оборудования известных фирм (это совсем не дешево). Или необходимо хорошо представлять роль измеряемых величин в передаче электрических сигналов, что позволяет менее критично подходить к выбору производителя, но требует высокой квалификации специалистов.

Перечень измеряемых параметров

Спецификации стандарта TIA TSB-67 полевого тестирования определяют функции тестирования, конфигурации и минимально необходимую точность измерений, необходимые для сертифицирования кабельной системы на соответствие определенным классам приложений.

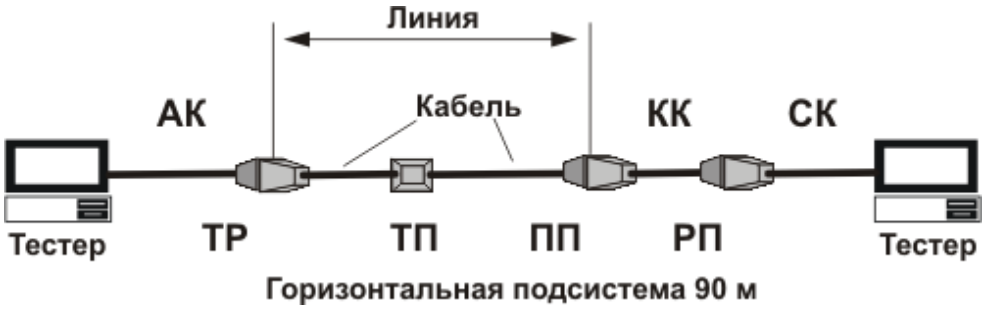

Рис. 7.16. Схема тестирования канала по TIA TSB-67
АК - абонентский кабель, КК - коммутационный кабель, СК - сетевой кабель, ТР - телекоммуникационный разъем, РП - распределительная панель, ПП - промежуточная панель, ТП - точка перехода.

В рамках данной книги имеет смысл говорить только о двух классах:

Класс C (кабеля категории 3) - приложения высокоскоростной цифровой передачей данных. Рабочие характеристики кабельных линий определены до 16 МГц. Наиболее распространенным представителем этого класса является протокол Ethernet 10baseT.

Класс D (кабеля категории 5) - приложения очень высокой скорости передачи данных. Рабочие характеристики кабельных линий, определены до 100 МГц. Как правило, в качестве протокола используется Ethernet 100baseT.

Приложения класса E (250 МГц) и F (600 МГц) пока недостаточно распространены даже в высокоскоростных сетях, и, тем более, не применяются при создании коммуникаций "последней мили".

Таб. 7.1. Основные электрические параметры, тестируемые в симметричных кабельных линиях

Измеряемый параметр	Выявление неполадок	Соответствие стандарту
Волновое сопротивление (impedance)	-	100 Ом +/- 15%
Задержка распространения (propagation delay)	-	Да
Электрическая длина	-	До 95 метров
Сопротивление петли постоянному току	-	До 40 Ом
Затухание (attenuation)	Да	Да
NEXT	Да	Да
Порядок соединения проводников, экранов (если они есть), наличие обрывов или коротких замыканий	Да	-

Кроме этого, при наличии неполадок может быть определено расстояние до места неисправности.

Необходимо помнить, что определить отдельно параметры кабелей и разъемов недостаточно, поскольку в результате монтажа существенно повышается уровень собственных шумов системы. Более того, именно расплетение витых пар при монтаже разъемов считаются основным источником возникновения помех.

Наиболее важные параметры линии

Будет полезно привести основные параметры качества витой пары 3 и 5 категории. Запоминать их не имеет смысла, тем более, они есть практически в любом описании стандарта EIA/TIA-568A. Но хотя бы самое общее представление о порядке величин желательно все же иметь.

Таб. 7.2. Максимально допустимое затухание для кабелей категории 3 и 5

Частота, МГц	Затухание, дБ, 100м, Категория 3	Затухание, дБ, 100м, Категория 5
1,0	3,7	2,5
4,0	6,6	4,8
10,0	10,7	7,5
20,0	-	10,5
100,0	-	23,2

Таб. 7.3. Минимальное значение NEXT для кабелей категории 3 и 5

Частота, МГц	Затухание, дБ, 100м, Категория 3	Затухание, дБ, 100м, Категория 5
1,0	39	54
4,0	29	45
10,0	23	39
20,0	-	37
100,0	-	27

Таб. 7.4. Задержка распространения

Тип кабеля	Задержка, мс	Частота, МГц
Категория 3	1,0	10
Категория 5	1,0	10

Из последней таблицы видно, что задежка даже по нормам мало зависит от категории кабеля.

Основные способы измерения

Известно три типа приборов, применяемых для проверки электрических параметров линий передачи данных.

Самые простые, мультиметры (электрические тестеры) позволяют измерять ток, напряжение, и активное сопротивление. Несмотря на такой скромный перечень возможностей, их вполне достаточно для определения простых ошибок, допущенных при монтаже, и дефектов кабеля. Главный их плюс - низкая цена (менее $10) и доступность. Подробнее работа с ними будет описана в следующих разделах.

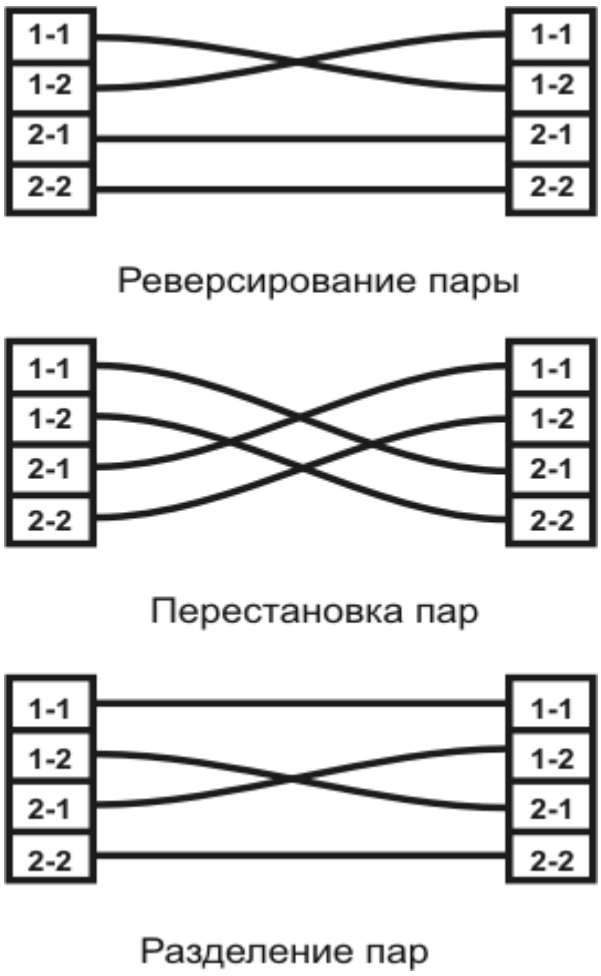

Рис. 7.17. Типовые ошибки при монтаже разъемов

1. Реверсирование пары (Reversed Pair). На разных сторонах линии взаимно меняются номера контактов одной пары. Для 10/100baseT это не приводит к нарушению нормальной работы (за редчайшими, но возможными исключениями).
2. Перестановка пар (Transposed Pairs). Подключение любой из пар к контактом другой пары на противоположной стороне линии. Практически всегда приводит к потере связи (исключение - активное оборудование, имеющее автоопределение перекрещенных линий).
3. Разделение пар (Split Pair). Этот дефект в телефонии более известен как "разнопарка". К контактам разъема, предназначенным для подключения одной пары, присоединяются проводники из разных пар. Это приводит к резкому ухудшению электрических характеристик, но не всегда к полной невозможности работы линии. Поэтому, такой дефект может долгое время оставаться незамеченным, и перестать работать в самый неожиданный (или неприятный) момент.

Теоретически, при помощи различных схем и простых приборов (достаточной точности) можно измерить (или вычислить) все характеристики линии, описанные выше. Но на практике трудоемкость процесса столь велика, что для этого используются специальные полевые тестеры. Несмотря на их высокую цену, от $500 за прибор начального уровня, до нескольких тысяч (или более) долларов за промышленное устройство, они очень широко применяются при построении сетей.

Так как часто монтируют кабельные системы, и устанавливают активное оборудование разные бригады (или даже фирмы), то проверить функционирование сети при реальной работе затруднительно. Тем более, на уровне протоколов дать объективную оценку электрических параметров невозможно.

Поэтому именно результаты измерения являются основанием для принятия построенной сети заказчиком (результаты приемо-сдаточных испытании).

Тестеры всегда состоят из двух частей, базового блока и инжектора, подключаемых с разных сторон линии. За несколько секунд производится все измерения, результат которых, в зависимости от модели устройства, может быть показан, распечатан, занесен в память.

Кроме тестеров, в магистральных сетях часто используют рефлектометры, позволяющие получить представление о линии с помощью отраженного от неоднородностей сигнала. В локальных сетях они применяются очень редко из-за сложной трактовки результатов и высокой стоимости.

Вообще говоря, измерениям свойств линий можно посвятить не один параграф, а несколько больших и серьезных книг. Но если вернуться к реальности, то самый простой полевой тестер начального уровня стоит более $500. Поэтому в рамках данного материала целесообразно ограничиться описанием использования простого мультиметра. Оно будет кратко рассмотрено в следующих главах совместно с практическими вопросами прокладки кабелей.

Глава 8. Оптическая среда передачи данных.

Кто мудр, испытывать не станет, ни женщин, друг мой, ни стекла.

Передача данных при помощи оптической связи использовалась задолго до изобретения электричества. Атмосферные способы то исчезали из практики, то вновь появлялись на новом этапе технического развития. Последний "взлет" закончился в 70-х годах прошлого века, когда лазеры были признаны дорогими и не надежными игрушками. Большее применение получили способы передачи в радиодиапазоне.

На сегодня, лазерные атмосферные линии является скорее экзотикой, чем практикой, хотя даже в России устройств этого типа выпускаются более-менее серийно.

Зато побочная ветвь оптической связи - передача информации через волновод из кварцевого стекла (SiO_2) - переживает бурный рост, и применяется чем дальше, тем шире. Так, оптоволоконные кабеля уже полностью вытеснили медные (электрические) на магистральных каналах, и стремительно подбирается к конечному пользователю.

Физический принцип, лежащий в основе передачи сигналов по оптическому волокну прост и далеко не нов. Еще в 1870 г. в Лондонском Королевском обществе Дж. Тиндаль продемонстрировал непрямолинейное распространение света внутри струи жидкости, основанное на отражении света от границы сред (воздуха и воды).

Практическое применение этого эффекта стало возможно после двух принципиальных технологических "прорывов". В 1967 г. Жорес Алферов создал первые полупроводниковые гетеролазеры, работоспособные при комнатной температуре. Чуть позже, в 1970 г., на фирме "Корнинг" была получена первая миля сверхчистого кварцевого волокна, пригодного для оптической связи.

На основе этих технологий, в 1975 году было внедрено первое поколение передатчиков сигналов. Основу составлял светоизлучающий диод, работающий на длине волны 0.85 мкм в многомодовом режиме. Не прошло и трех лет, как появились одномодовые диодные лазеры на 1.3 мкм. А в 1982 году пошло в серию третье поколение, работающее на длине волны 1.55 мкм.

1988 год ознаменован вводом в действие первой трансатлантической ВОЛС ТАТ-8. В настоящее время близка к покорению другая часть рынка. Настольные системы, соединенные в локальную сеть при помощи оптоволокна, вполне реальны и лишь слегка экзотичны.

Основными достоинствами оптоволокна является практически не ограниченная пропускная способность, индифферентность к электрическим (например, атмосферным) наводкам, и высокая долговечность. К недостаткам можно отнести относительно дорогой кабель и активное оборудование, и высокую сложность монтажа.

На сегодня, применение оптоволокна в небольших локальных сетях не оправдано ни экономически, ни технически. Но для сетей "последней мили" оптическая среда передачи данных является практически единственным способом строить большие и надежные сети "воздушным" способом.

Глава 8

Физические параметры оптических волокон.

Принцип работы оптоволоконной линии не сложен. Источником распространяемого по оптическим кабелям света является светодиод (или полупроводниковый лазер), а кодирование информации осуществляется двухуровневым изменением интенсивности света (0-1). На другом конце кабеля принимающий детектор преобразует световые сигналы в электрические.

Для передачи информации мало создать световую волну, надо ее сохранить и направить в нужном направлении. В однородной среде свет (электромагнитная волна) распространяется прямолинейно, но на границе изменения плотности среды по оптическим законам происходит изменение направления (отражение), или преломление.

В используемых в настоящее время схемах луч от светодиода или лазера впускают в более плотную среду, ограниченную менее плотной. При правильном подборе материалов, происходит эффект полного отражения (преломление отсутствует). Таким образом, транспортируемый сигнал "идет" внутри замкнутой среды, проделывая путь от источника сигнала до его приемника.

Остальные элементы кабеля - лишь способ предохранить хрупкое волокно от повреждений внешней средой различной агрессивности.

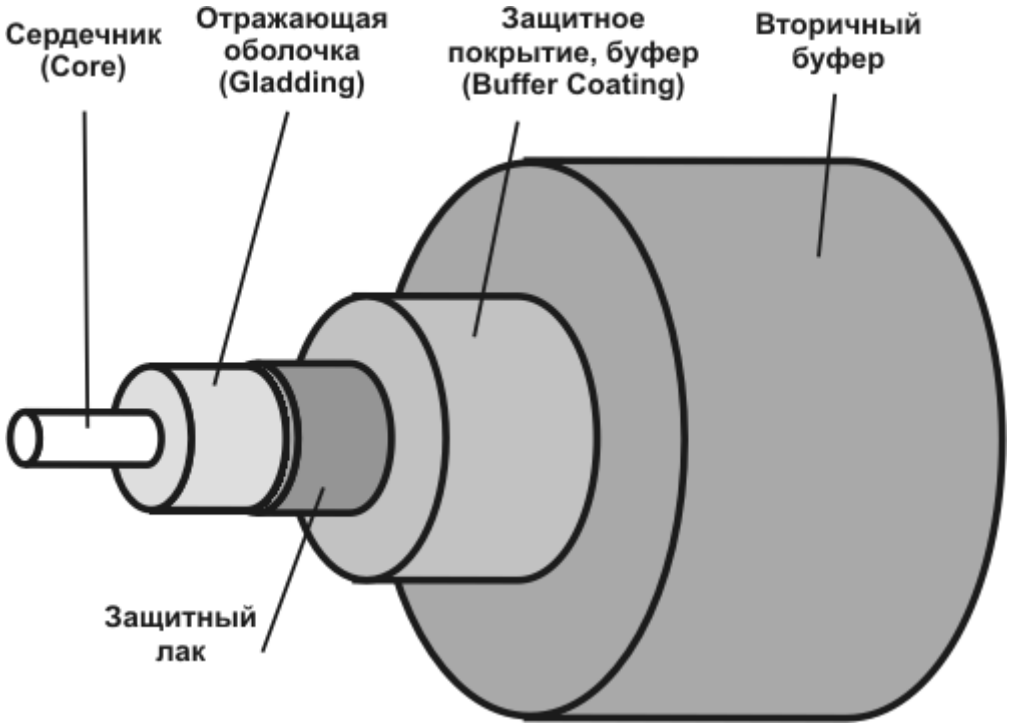

Рис. 8.1. Конструкция оптического волокна

Сложность конструкции скорее кажущаяся, чем реальная. Основные элементы показаны на рисунке. Внешний диаметр отражающей оболочки унифицирован для всех типов кабелей и составляет 125±2 мкм. В этот размер входит и 2-3 мкм. слой лака, который служит защитой от влаги и связанной с ней коррозии.

Первичную механическую прочность и гибкость рассматриваемой конструкции придает защитное покрытие из эпоксиакриолата, часто называемое буфером. Как правило, для удобства монтажа его окрашивают в разные цвета. Толщина покрытия составляет 250±15 мкм. Кроме этого, для лучшей защиты волокна и более удобного монтажа разъемов часто применяются конструкции с вторичным буфером диаметром 900 мкм, который без зазора уложен на первичный.

Рассмотрим подробнее оптические параметры волокна. Все распространенные типы волокон характеризуются двумя важнейшими параметрами: затуханием и дисперсией.

Затухание характеризует потерю мощности передаваемого сигнала на заданном расстоянии, и измеряется в дБ/км, где Децибел - логарифмическое выражение отношения мощности, выходящей из источника P1, к мощности, входящей в приемник P2, дВ = 10*log(P1/P2). Потери в 3 дБ означают, что половина мощности потеряна. Потеря 10 дБ означает, что только 1/10 мощности источника доходит до приемника, потери 90%. Волоконно-оптические линии как правило способны нормально функционировать при потерях в 30 дБ (прием всего 1/1000 мощности).

Есть два принципиально различных физических механизма, вызывающих данный эффект.

- Потери на поглощение. Связаны с преобразованием одного вида энергии в другой. Электромагнитная волна определенной длины вызывает в некоторых химических

элементах изменение орбит электронов, что, в свою очередь, ведет к нагреву волокна. Естественно, что процесс поглощение волны тем меньше, чем меньше ее длина, и чем чище материал волокна.

- Потери на рассеяние. Причина снижения мощности сигнала в этом случае - означает выход части светового потока из волновода. Обусловлено это обычно неоднородностями показателя преломления материалов. Известно, что с уменьшением длины волны потери рассеивания возрастают.

Рис. 8.2. Окна прозрачности оптических волокон

В теории, лучших показателей общего затухания можно достичь на пересечении кривых поглощения и рассеивания. Реальность несколько сложнее, и связана с химическим составом среды. В кварцевых волокнах (SiO2) кремний и кислород проявляют активность на определенной длине волны, и существенно ухудшают прозрачность материала в двух окрестностях.

В итоге образуются три окна прозрачности, в рамках которых затухание имеет наименьшее значение. Самые распространенные значения длины волны:

0.85 мкм;
1.3 мкм;
1.55 мкм.

Понятно, что именно под такие диапазоны разработаны специальные гетеролазеры, на которых основываются современные ВОЛС (волоконно-оптические системы связи).

Надо специально заметить, что влияние частоты сигнала на реальные технологии сегодняшнего дня очень большое. Для примера, инфракрасный луч проходит в волокне с небольшим затуханием 10 км, красный свет (длина волны 0,65 мкм) пройдет лишь 0,5 км, а синий (0,43 мкм) и вообще меньше 50 м.

Оптический бюджет.

Каждый компонент оптоволоконной линии имеет свою величину оптических потерь. Допустимые потери оптического сигнала на всём пути от передатчика до приёмника часто называют оптическим бюджетом. Рассчитывается он на основании информации, предоставленной производителем оборудования.

Упрощенно можно представить себе расчет оптического бюджета в виде следующей схемы:

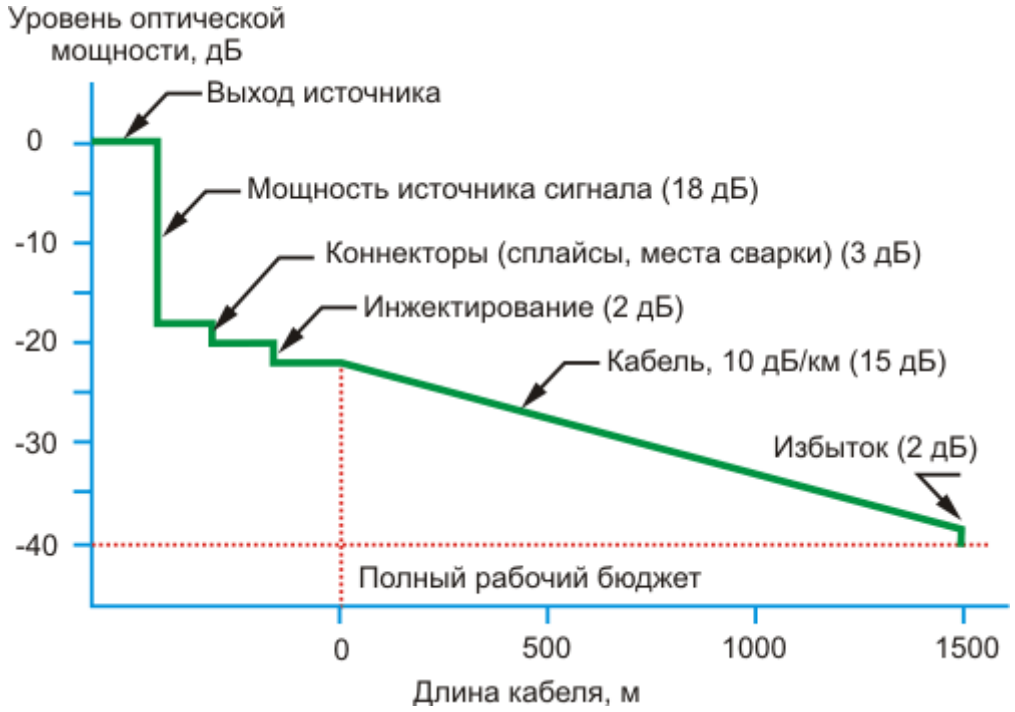

Рис. 8.2b. Оптический бюджет

Потери на инжектирование возникают при вводе излучения от источника в волокно, и зависят в основном от диаметра сердечника. Потери на сплайсах, местах сварки при их наличии в линии должны быть включены подобно потерям коннекторах.

Так же рекомендуется учитывать, что мощность лазера (светодиода) несколько уменьшается с течением времени. Обычно на ремонт и старение эмиттера отводится от 3 до 6 дБ.

Дисперсия.

Второй важный параметр оптического волокна - дисперсия. Он означает рассеяние во времени спектральных и модовых составляющих оптического сигнала. Существуют три типа дисперсии: межмодовая, материальная и межчастотная.

- Межмодовая дисперсия обусловлена неидеальностью современных источников света, которые испускают волны в нескольких направлениях, и далее они проходят по разным траекториям (иначе говоря - будут иметь разные моды). Как следствие, лучи достигнут приемника в разные моменты времени.
- Материальная дисперсия обусловлена зависимостью показателя преломления от длины волны. Если распределение плотности волокна будет неравномерным, то волны, проходящие путь по разным траекториям, будут иметь разные скорости распространения. И, соответственно, попадать в приемник в разное время.

- Межчастотная дисперсия. Источники излучения не идеальны, и испускают волны различной длины. В кварцевом стекле более короткие волны распространяются быстрее, а следовательно достигают конца световода в разные моменты времени.

Все виды дисперсии отрицательно влияют на пропускную способность оптоволоконного канала. Так как в настоящее время используются только цифровые способы передачи информации, то световой сигнал поступает с передатчика импульсами. И чем сильнее размыт по времени импульс на выходе (эффект дисперсии), тем сложнее его правильный прием. Иначе говоря, дисперсия накладывает ограничение на дальность передачи и на верхнюю частоту передаваемых сигналов.

При оценке пользуются термином "полоса пропускания", который понимается как величина, обратная к уширению импульса при его прохождении по оптическому волокну расстояния в 1 км. Измеряется полоса пропускания в МГц*км.

Специально нужно отметить, что потери, вызванные затуханием и дисперсией, равномерно распределяются по всей длине кабеля. Какие-либо помехи отсутствуют, если не принимать во внимание системы с частотным уплотнением, которые в недорогих сетях еще долго не получат распространения.

Глава 8

Одномодовые и многомодовые оптические волокна

Несмотря на огромное разнообразие оптоволоконных кабелей, волокна в них практически одинаковые. Более того, производителей самих волокон намного меньше (наиболее известны Corning, Lucent и Fujikura), чем производителей кабелей.

По типу конструкции, вернее по размеру серцевины, оптические волокна делятся на одномодовые (ОМ) и многомодовые (ММ). Строго говоря, употреблять эти понятия следует относительно конкретной используемой длины волны, но после рассмотрения Рисунка 8.2, становится понятно, что на сегодняшнем этапе развития технологий можно это не учитывать.

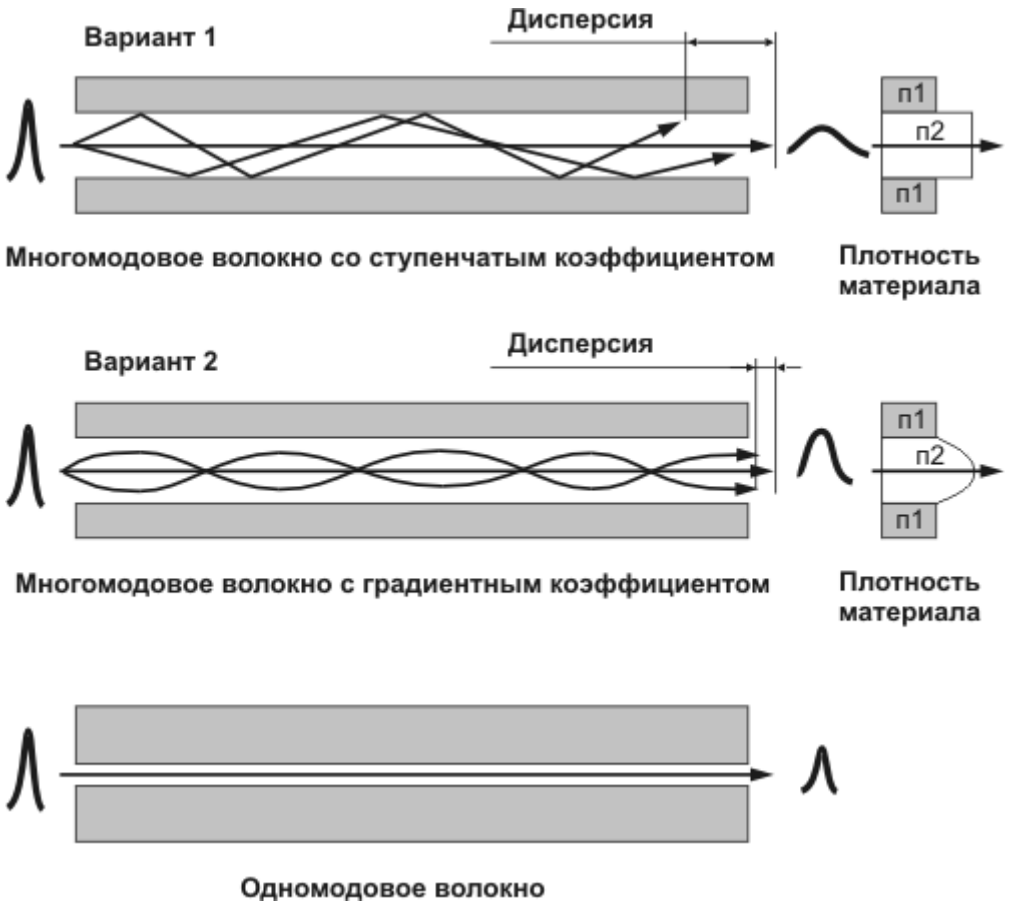

Рис. 8.3. Одномодовые и многомодовые оптические волокна

В случае многомодового волокна диаметр сердечника (обычно 50 или 62,5 мкм) почти на два порядка больше, чем длина световой волны. Это означает, что свет может распространяться в волокне по нескольким независимым путям (модам). При этом очевидно, что разные моды имеют разную длину, и сигнал на приемнике будет заметно "размазан" по времени.

Из-за этого хрестоматийный тип ступенчатых волокон (вариант 1), с постоянным коэффициентом преломления (постоянной плотностью) по всему сечению сердечника, уже давно не используется из-за большой модовой дисперсии.

На смену ему пришло градиентное волокно (вариант 2), которое имеет неравномерную плотность материала сердечника. На рисунке хорошо видно, что длины пути лучей сильно сокращены за счет сглаживания. Хотя лучи, проходящие дальше от оси световода, преодолевают большие расстояния, они при этом имеют большую скорость распространения. Происходит это из-за того, что плотность материала от центра к внешнему радиусу уменьшается по параболическому закону. А световая волна распространяется тем быстрее, чем меньше плотность среды.

В результате более длинные траектории компенсируются большей скоростью. При удачном подборе параметров, можно свести к минимуму разницу во времени распространения. Соответственно, межмодовая дисперсия градиентного волокна будет намного меньше, чем у волокна с постоянной плотностью сердечника.

Однако, как бы не были сбалансированы градиентные многомодовые волокна, полностью устранить эту проблему можно только при использовании волокон, имеющих достаточно

малый диаметр сердечника. В которых, при соответствующей длине волны, будет распространяться один единственный луч.

Реально распространено волокно с диаметром сердечника 8 микрон, что достаточно близко к обычно используемой длине волны 1,3 мкм. Межчастотная дисперсия при неидеальном источнике излучения остается, но ее влияние на передачу сигнала в сотни раз меньше, чем межмодовой или материальной. Соответственно, и пропускная способность одномодового кабеля намного больше, чем многомодового.

Как это часто бывает, у более производительного типа волокна есть свои недостатки. В первую очередь, конечно, это более высокая стоимость, обусловленная стоимостью комплектующих, и требованиями к качеству монтажа.

Таб. 8.1. Сравнение одномодовых и многомодовых технологий.

Параметры	Одномодовые	Многомодовые
Используемые длины волн	1,3 и 1,5 мкм	0,85 мкм, реже 1,3 мкм
Затухание, дБ/км.	0,4 - 0,5	1,0 - 3,0
Тип передатчика	лазер, реже светодиод	светодиод
Толщина сердечника.	8 мкм	50 или 62,5 мкм
Стоимость волокон и кабелей.	Около 70% от многомодового	-
Средняя стоимость конвертера в витую пару Fast Ethernet.	$300	$100
Дальность передачи Fast Ethernet.	около 20 км	до 2 км
Дальность передачи специально разработанных устройств Fast Ethernet.	более 100 км.	до 5 км
Возможная скорость передачи.	10 Гб, и более.	до 1 Гб. на ограниченной длине
Область применения.	телекоммуникации	локальные сети

Глава 8

Разновидности оптоволоконных кабелей

Классифицировать ВОК очень сложно в силу большого разнообразия. Количество типов и материалов сердечника, изоляции, упрочняющих слоев может легко дезориентировать даже специалиста. Поэтому, после классификации "обзорного типа", подробно остановимся только на разновидностях, обычно применяемых для недорогих наружных магистралей.

По назначению, волоконно-оптические кабеля (ВОК) можно разделить на:

- Монтажные (соединительные). Используются для механической коммутации и подключения аппаратуры;

- Объектовые. Используются для высокоскоростных соединений внутри строений. Как правило, в них используются покрытие, слабо распространяющее горение, выделяющих малое количество дыма, и не содержащее галогенов (LSF/OH - low smoke and fume zero halogen);
- Городские, Зоновые. Соединяют здания, районы, города области. Обычно сети, построенные с их использованием, имеют протяженность от 1-2 до 100 км.
- Магистральные. Предназначены для передачи информационных потоков на большие расстояния. Для этого используются кабеля с очень качественными оптическими волокнами.

По месту прокладки:

- По подземным коммуникациям телефонных и других служб;
- Предназначенные для прокладки в грунте. Усиленная броня, защита от грызунов.
- Подвесные (на столбах освещения, трубостойках, контактных опорах железных дорог, опорах ЛЭП, и т.п.). Длина пролета может доходить до 450м.
- Подводные.

Рассмотрим подробнее конструкцию кабелей. Ее выбор для построения сети "последней мили" достаточно ограничен. Это должны быть недорогие кабеля с небольшим количеством волокон (обычно не более 8), хорошо приспособленные для работы на открытом воздухе.

Из всего многообразия, хорошо отвечают этим условиям только модульные конструкции (multitube cable, многотрубочный кабель).

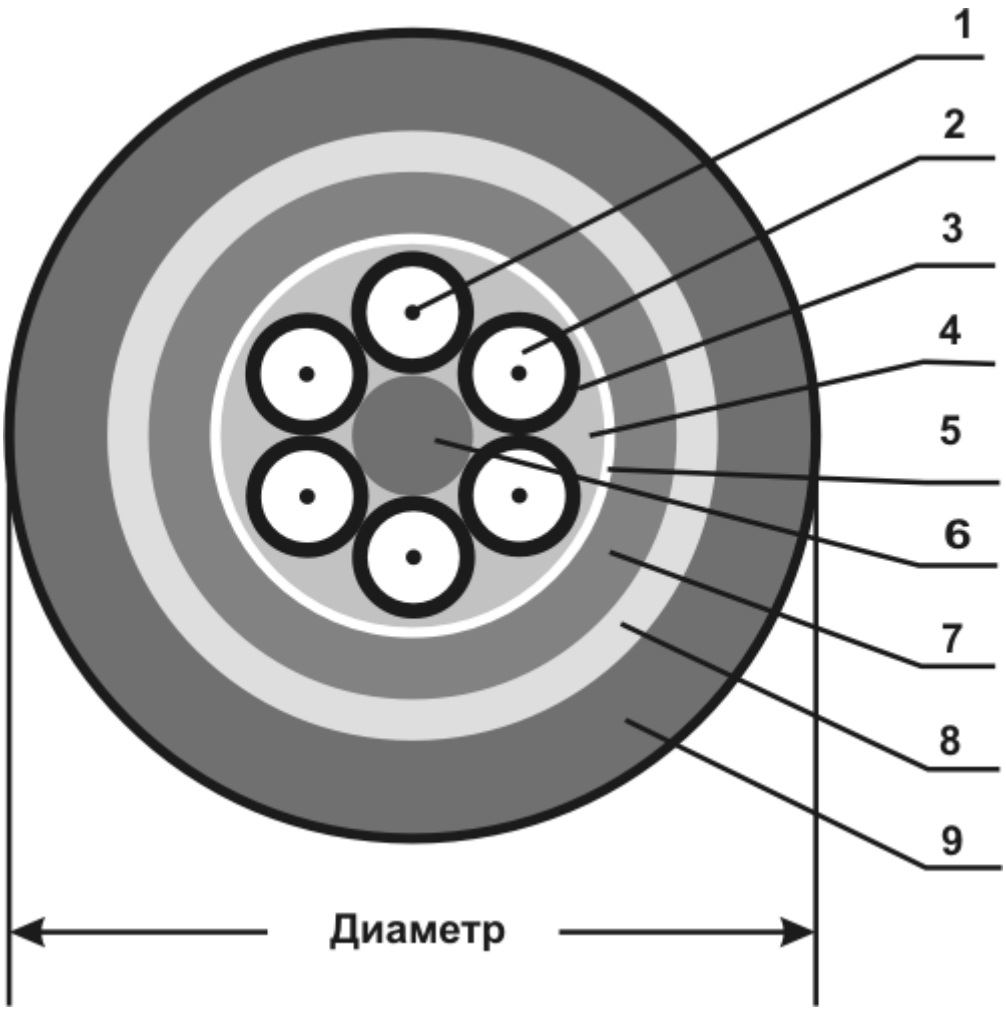

Рис. 8.4. Типовая конструкция кабельного сердечника модульного типа.
1 - оптическое волокно в буфере (ОВ) или служебная жила (СЖ) из мягкой медной проволоки; 2 - гидрофобный заполнитель (ГЗ); 3 - оболочка оптического модуля (ОМ); 4- гидрофобное заполнение; 5 - скрепляющий элемент, обычно обмотка полиэтилентерефталатной пленкой; 6 - центральный силовой элемент (ЦСЭ); 7- промежуточная оболочка кабеля; 8 - силовой элемент; 9 - защитная оболочка из ПЭ.

Модули (трубки из полибутилентерефталата или полиэтилена (ПЭ) диаметром около 2 мм) имеют традиционную повивную скрутку вокруг центрального элемента (стеклопластиковый пруток, металлический трос или даже проволока). Иногда в конструкцию вводят сплошные кордели заполнения (КЗ) из ПЭ или модули без оптического волокна.

Оптические волокна свободно уложены в трубки модуля (от 1 до 12 волокон) с легким повивом вдоль внешней стенки. Кроме этого в модули могут быть заложены капроновые волокна для амортизации и специальный гель для защиты от влаги. Эти меры позволяют очень надежно предохранить хрупкое волокно от нагрузок при упругом растяжении и изгибе.

Если учитывать промежуточную оболочку, силовой элемент (высокопрочные нити, броню из проволок или стальной ленты), и защитную оболочка из полиэтилена толщиной до нескольких миллиметров, такая конструкция ВОК представляется очень надежной, и при правильном выборе способной выдержать любые условия эксплуатации.

Вот типовые характеристики современных кабелей для внешней прокладки:

- Внешний диаметр - 10-20 мм;
- температурный диапазон монтажа - от -10°С до +50°С;
- температурный диапазон эксплуатации - от -40°С до +60°С;
- минимальный радиус изгиба при прокладке - 15 внешних диаметров;
- минимальный радиус изгиба при эксплуатации - 20 внешних диаметров;
- максимально допустимое усилие на растяжение - 2500-10000 Н;
- максимально допустимое усилие на сдавливание - 2000-4000 Н;

Виды кабелей, в которых модуль не заполнен гелем, предназначены для проводки внутри здания, и использовать их для внешних прокладок крайне не желательно. Влага медленно, но верно будет снижать прозрачность оптоволокна.

Примерно то же самое относится к вариантам кабелей, предназначенных для прокладки внутри помещений, у которых волокно находится внутри монолита из пластиката (буфера 900-мкм). Этот кабель удобен в работе, недорог, но недостаточно устойчив к низким температурам и влаге. Нужно специально отметить, что в последнее время появились конструкции, избавленные от этих недостатков. Но, как правило, они имеют стоимость, превышающую средний уровень.

Маркировки ВОК по своему разнообразию не уступают вариантам конструкций. Для примера, приведем маркировку отечественных подвесных кабелей для внешней прокладки.

ОКА-MNП-XX-YY-Z(F), где ОК - оптический кабель, А - силовой элемент из арамидных нитей, М - модульная конструкция, N - количество элементов в повиве, П - тип центрального силового элемента - стеклопластиковый пруток, XX - тип оптического волокна, YY - предельное значение затухания, дБ/км, Z - количество оптических волокон, F - допустимое растягивающее усилие.

Отдельно нужно отметить очень удобные для воздушных коммуникаций самонесущие ВОК с сечением в виде восьмерки. Стальной или диэлектрический несущий трос таких кабелей заключен в полиэтиленовую оболочку и крепится к основной конструкции перепонкой и того же полиэтилена. Такие кабеля легко крепить даже с помощью подручных материалов.

Глава 8

Виды и типы разъемов

При всех достоинствах оптических волокон, для монтажа сетей их необходимо соединять. Именно сложность этого процесса для световодов из кварцевого стекла является основным сдерживающим фактором оптоволоконной технологии.

Несмотря на весь прогресс технологии последних лет, непрофессионалам доступно только соединение кабелей, не имеющих особых требований по качеству. Серьезные работы по монтажу магистралей регионального значения требуют наличия дорогостоящего оборудования и высоко квалифицированного персонала.

Но для создания междомовой разводки "последней мили" такие сложности уже не нужны. Работы доступны специалистам без серьезной подготовки (или вообще без нее), комплект

технологического оборудования стоит менее $300. В сочетании с этим, огромные (не побоюсь этого слова) преимущества оптоволокна над медными кабелями при воздушных прокладках делают его очень привлекательным материалом для домашних сетей.

Рассмотрим подробнее виды и способы соединения оптических волокон. Для начала, нужно принципиально разделить сростки (неразъемные соединения), и оптические разъемы.

В сравнительно небольших сетях (до нескольких километров диаметром) сростки не желательны, и их следует избегать. Основной на сегодня способ их создания - сварка электрическим разрядом.

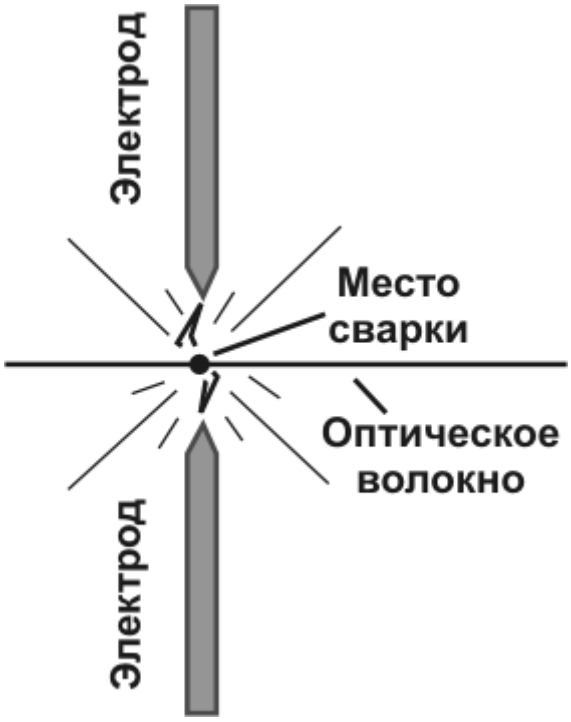

Рис. 8.5. Принцип сварки оптического волокна.

Такое соединение надежно, долговечно, и вносит ничтожно малое затухание в оптический тракт. Но для сварки нужно весьма дорогостоящее оборудование (в районе нескольких десятков тысяч долларов), и сравнительно высокая квалификация оператора.

Обусловлено это необходимостью высокоточного совмещения концов волокон перед сваркой, и соблюдения стабильных параметров электрической дуги. Кроме этого, нужно обеспечить ровные (и перпендикулярные оси волокна) торцы (сколы) свариваемых волокон, что само по себе является достаточно сложной задачей.

Соответственно, выполнение таких работ "от случая к случаю" своими силами не рационально, и проще пользоваться услугами специалистов.

Так же подобный способ часто используется для оконечивания кабелей путем сварки волокон кабеля с небольшими отрезками гибких кабелей с уже установленными разъемами (pig tail, буквально - поросячий хвост). Но с распространением клеевых соединений, сварка постепенно сдает позиции при терминировании линий.

Второй способ создания неразъемных соединений - механический, или с использованием специальных соединителей (сплайсов). Первоначальное назначение этой технологии - быстрое временное соединение, используемое для восстановления работоспособности линии в случае разрыва. Со временем, на "ремонтные" сплайсы некоторые фирмы начали давать гарантию до 10 лет, и до нескольких десятков циклов соединения-разъединения. Поэтому целесообразно выделить их в отдельный способ создания неразъемных соединений.

Принцип действия сплайса достаточно прост. Волокна закрепляются в механическом кондукторе, и специальными винтами сближаются друг с другом. Для хорошего оптического контакта в месте стыка используется специальный гель с похожими на кварцевое стекло оптическими свойствами.

Несмотря на внешнюю простоту и привлекательность, способ не получил широкого распространения. Причин этому две. Во-первых, он все-таки заметно уступает по надежности и долговечности сварке, и для магистральных телекоммуникационных каналов не пригоден. Во-вторых, он обходится дороже, чем монтаж клеевых разъемов, и требует более дорогого технологического оборудования. Поэтому, он достаточно редко применяется и при монтаже локальных сетей.

Единственное, в чем эта технология не знает себе равных - это скорость выполнения работ, и не требовательность к внешним условиям. Но этого на сегодня явно не достаточно для полного завоевания рынка.

Рассмотрим разъемные соединения. Если предел дальности действия высокоскоростных электропроводных линий на основе витой пары зависит от разъемов, то в оптоволоконных системах вносимые ими дополнительные потери достаточно малы. Затухание в них оставляет около 0,2-0,3 дБ (или несколько процентов).

Поэтому вполне возможно создавать сети сложной топологии без использования активного оборудования, коммутируя волокна на обычных разъемах. Особенно заметны преимущества такого подхода на небольших по протяженности, но разветвленных сетях "последней мили". Очень удобно отводить по одной паре волокон на каждый дом от общей магистрали, соединяя остальные волокна в коммутационной коробке "на проход".

Что основное в разъемном соединении? Конечно, сам разъем. Основные его функции заключаются в фиксация волокна в центрирующей системе (соединителе), и защите волокна от механических и климатических воздействий.

Основные требования к разъемам следующие:

- внесение минимального затухания и обратного отражения сигнала;
- минимальные габариты и масса при высокой прочности;
- долговременная работа без ухудшения параметров;
- простота установки на кабель (волокно);
- простота подключения и отключения.

На сегодня известно несколько десятков типов разъемов, и нет того единого, на который было бы стратегически сориентировано развитие отрасли в целом. Но основная идея все вариантов конструкций проста и достаточно очевидна. Необходимо точно совместить оси волокон, и плотно прижать их торцы друг к другу (создать контакт).

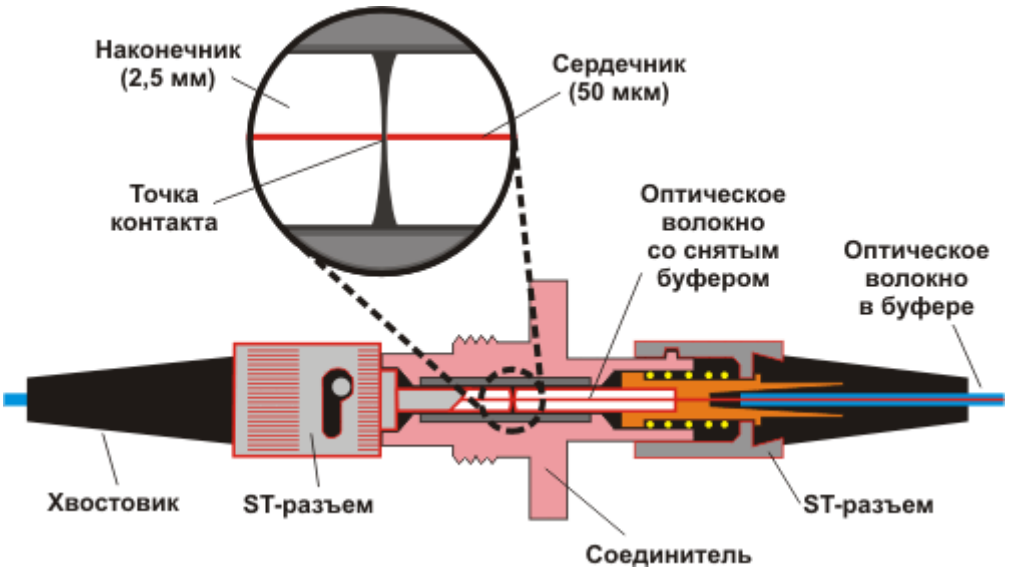

Рис. 8.6. Принцип действия оптоволоконного разъема контактного типа

Основная масса разъемов выпускается по симметричной схеме, когда для соединения разъемов используется специальный элемент - coupler (соединитель). Получается, что сначала волокно закрепляется и центрируется в наконечнике разъема, а затем уже сами наконечники центрируются в соединителе.

Таким образом, можно видеть, что на сигнал влияют следующие факторы:

- Внутренние потери - вызванные допусками на геометрические размеры световодов. Это эксцентриситет и эллиптичность сердцевины, разность диаметров (особенно при соединении волокон разного типа);
- Внешние потери, которые зависят от качества изготовления разъемов. Возникают из-за радиального, углового смещения наконечников, непараллельности торцевых поверхностей волокон, воздушного промежутка между ними (френелевские потери);
- Обратное отражение. Возникает из-за наличия воздушного промежутка (френелевское отражение светового потока в обратном направлении на границе стекло-воздух-стекло). Согласно стандарта TIA/EIA-568A, нормируется коэффициент обратного отражения (отношение мощности отраженного светового потока к мощности падающего). Он должен быть не хуже -26 дБ для одномодовых разъемов, и не хуже -20 дБ для многомодовых;
- Загрязнение, которое, в свою очередь, может вызвать как внешние потери, так и обратное отражение.

Несмотря на отсутствие официально признанного всеми производителями типа разъема, фактически распространены ST и SC, весьма похожие по своим параметрам (затухание 0,2-0,3 дБ).

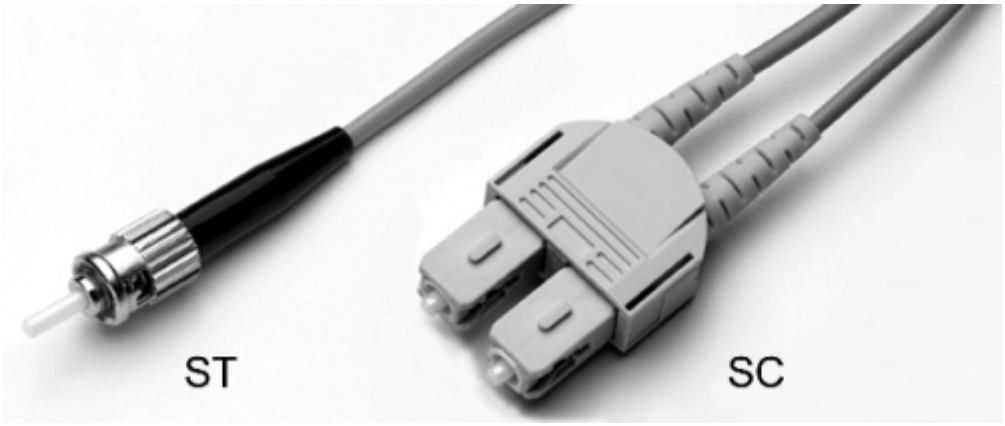

Рис. 8.7. Разъемы оптических волокон.

ST. От английского straight tip connector (прямой разъем) или, неофициально Stick-and-Twist (вставь и поверни). Был разработан в 1985 году AT&T, ныне Lucent Technologies. Конструкция основана на керамическом наконечнике (феруле) диаметром 2,5 мм с выпуклой торцевой поверхностью. Фиксация вилки на гнезде выполняется подпружиненным байонетным элементом (подобно разъемам BNC, использующимся для коаксиального кабеля).

Разъемы ST - самый дешевый и распространенный в России тип. Он немного лучше, чем SC, приспособлен к тяжелым условиям эксплуатации благодаря простой и прочной металлической конструкции (допускает больше возможностей для применения грубой физической силы).

Как основные недостатки, можно назвать сложность маркировки, трудоемкость подключения, и невозможность создания дуплексной вилки.

SC. От английского subscriber connector (абонентский разъем), а иногда используется неофициальная расшифровка Stick-and-Click (вставь и защелкни). Был разработан японской компанией NTT, с использованием такого же, как в ST, керамического наконечника диаметром 2,5 мм. Но основная идея заключается в легком пластмассовом корпусе, хорошо защищающим наконечник, и обеспечивающим плавное подключение и отключение одним линейным движением.

Такая конструкция позволяет достичь большой плотности монтажа, и легко адаптируется к удобным сдвоенным разъемам. Поэтому разъемы SC рекомендованы для создания новых систем, и постепенно вытесняют ST.

Дополнительно нужно отметить еще два типа, один из которых используется в смежной отрасли, а другой постепенно набирает популярность.

FC. Очень похож на ST, но с резьбовой фиксацией. Активно используется телефонистами всех стран, но в локальных сетях практически не встречается.

LC. Новый "миниатюрный" разъем, конструктивно идентичный SC. Пока достаточно дорог, и для "дешевых" сетей его применение бессмысленно. Как главный аргумент "за" создатели приводят большую плотность монтажа. Это достаточно серьезный довод, и в отдаленном (по телекоммуникационным меркам) будущем вполне возможно, что он станет основным типом.

Глава 8

Конструкционные элементы (шкафы и муфты)

Как правило, оптоволоконные кабеля разделываются с большим запасом по длине свободных волокон. Первоначально это было обусловлено сложностью соединения. Процесс скола, сварки мог повторяться далеко не один раз, и каждая попытка требовала несколько десятков сантиметров волокна. С тех пор технология усовершенствовалась явно недостаточно, что бы можно было обойтись без этого.

Кроме этого, кабель необходимо жестко зафиксировать, волокна уложить по достаточно большому радиусу, надежно закрепить необходимые элементы (сплайсы, гильзы, соединители). К созданному соединению нужно обеспечить доступ, предусмотреть возможность переключений или модификации.

Попробуем дать определения основным конструкционным элементам, при помощи которых реализуются эти задачи.

Шкафы оптические (распределительные) предназначены для организации разъемного соединения нескольких оптических кабелей, и выполнения переключений в процессе эксплуатации сети. Как правило, они применяются при переходе с линейных (внешних) оптоволоконных кабелей на линии, прокладываемые внутри зданий, или для подключения активного оборудования.

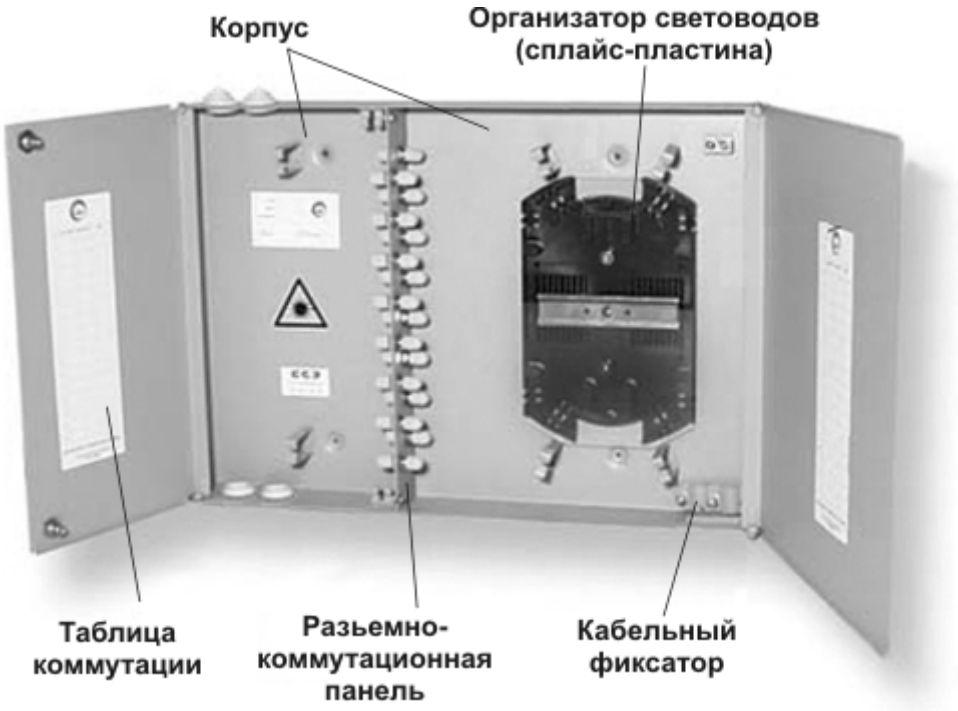

Рис. 8.8. Конструкция настенного оптического шкафа

Шкаф представляют собой устанавливаемый на стене или на любой стойке универсальный металлический корпус, в котором имеется разъёмно-коммутационная

панель, на которую монтируются оптические соединители. С одной стороны к ним подключаются разъемы одного (или нескольких) разделанных в шкафу кабелей, с другой - присоединяемых. Роль последних очень часто выполняют гибкие коммутационные шнуры, с помощью которых выполняются коммутации или подключается активное оборудование.

Обычно коммутационная панель, дополнительно к прямому назначению, разделяет внутренне пространство шкафа на секцию для размещения сращиваемых световодов, и секцию коммутационных соединений. В недорогих конструкциях роль кроссовой панели может выполнять внешняя стенка корпуса.

Свободные волокна (технологический запас) закрепляется на специальном организаторе световодов (сплайс-пластине), которая обеспечивает их фиксацию с соблюдением минимально допустимого радиуса изгиба. Там же при необходимости предусматривается крепление сросток (защитных гильз, или сплайсов).

Иногда как отдельный элемент выделяется кабельный фиксатор, при помощи которого кабель прикрепляется к корпусу шкафа.

Нужно отметить, что для установки в 19-ти дюймовую стойку существуют элементы, практически полностью совпадающие с оптическими шкафами как по назначению, так и по конструкции. Но называются они коммутационные полки. На особенностях их конструкции останавливаться подробно нет смысла, так как они предназначены для использования в структурах с большой плотностью оптических портов, к которым сети "последней мили" не относятся.

Для создания неразъемных соединений используются оптические муфты. Они предназначены для восстановления оболочек кабеля, и обеспечения прямого сращивания и разветвления кабелей. Применяются они в самых разных условиях, и поэтому их конструкция отличается большим разнообразием.

Рис. 8.9. Конструкция муфты.

Конструкция муфт достаточно проста. Это герметически закрытый корпус, в котором размешен организатор световодов (сплайс-кассета), и предусмотрено крепление кабелей. В общем случае, муфта не предназначена для коммутации или обслуживания. Но многие конструкции позволяют выполнять частичную модификацию соединения без полной замены конструкции.

Согласно технических требований, муфты должны обеспечивать размещение в них запаса длин оптических волокон с диаметром укладки не менее 750 мм, быть стойкими к воздействию растягивающих усилий 50...80% от нормируемого растягивающего усилия кабеля, для монтажа которого они предназначены.

Можно попытаться классифицировать оптические муфты следующим образом:

- по материалу корпуса: нержавеющая сталь, полиэтилен или различные конструкционные пластмассы (например полипропилен);
- по способу герметизации корпуса и вводов оптического кабеля: при помощи термо-усаживающегося материала, либо механически при помощи стяжек, винтов и различных герметизирующих прокладок;
- по месту применения: в грунте, в кабельной канализации, на воздухе, на опорах;
- по способу ввода кабелей можно различать прямые, разветвительные и тупиковые муфты;
- по емкости (количеству соединяемых волокон), и возможности ее модульного наращивания (увеличения количества сплайс-кассет).

В общем, можно сказать, что грань между оптическими шкафами и муфтами весьма условна. Есть достаточно примеров конструкций, которые могут быть с равным правом отнесены к любому из этих двух типов. Так, достаточно распространены муфты под размещение разъемных соединений. С другой стороны, часто используются шкафы для размещения сросток - например при переходе с одного типа кабеля на другой.

Но для потребителя это разнообразие очень удобно. Выбор конструкций большой, и всегда можно найти именно то, что наилучшим образом отвечает техническим потребностям.

Глава 9. Сетевые протоколы.

Контора пишет...

В Главах 7 и 8 были показаны физические линий передачи данных, по которым можно передавать электрические или оптические импульсы с заданной частотой и формой сигнала. Теперь нужно рассмотреть тот путь, который проходят данные от шины компьютера до передатчика сетевого адаптера.

Вопрос весьма объемный, и нужно его упорядочить, разбить на небольшие, относительно независимые части. Для этого даже существует несколько вполне логичных моделей. Однако решить, какая из них более удобная, порой не могут даже специалисты. Поэтому подход в изложении материала будет вполне традиционен - краткий обзор разных методик, и пристальное внимание техническим особенностям.

Глава 9

Модели коммуникации.

Из давнего 1984 года дошла до настоящего времени семиуровневая эталонная модель коммуникации OSI (Open System Interconnection, Взаимодействия Открытых Систем). Предложена она была Международной организацией по стандартизации (ISO) для упрощения взаимодействия соединений между большим числом сетей разного типа. Основная идея - каждый уровень предполагает, что напрямую взаимодействует с подобным уровнем другого устройства, хотя на самом деле может соединяться только с соседними уровнями своего узла.

Такой подход должен был привести к открытой и независимой от поставщиков базовой сетевой технологии (согласованного набора протоколов и реализующих их программно-аппаратных средств, достаточных для построения вычислительной сети).

С методологической же точки зрения, модель OSI служит основой для описания сетевой стратегии, разделяя для этого задачу на семь относительно автономных уровней, и определяя их функции и правила взаимодействия.

1. Физический уровень (Physical). Определяет такие характеристики, как уровень напряжения, синхронизацию изменений напряжения, скорость передачи физической информации и другие характеристики физических сред передачи данных, и параметров электрических сигналов. Как основная величина используется бит (bit).
2. Канальный уровень (Data link). Обеспечивает безошибочную передачу данных через физический канал. Он оперирует блоками данных, которые называются кадрами (frame). В протоколах канального уровня заложена определенная процедура доступа к среде, и способы адресации кадров.
3. Сетевой уровень (Network). Обеспечивает работу в сети с произвольной топологией, при этом он не берет на себя никаких обязательств по надежности передачи данных. В качестве объекта передачи используется дейтаграмма.
4. Транспортный уровень (Transport). Описывает протокол передачи данных с требуемым уровнем надежности (transport protocol). Например, он должен обладать необходимыми средствами для нумерации, установления соединения, упорядочивания пакетов.
5. Сеансовый уровень (Session). Содержит средства управления диалогом двух или нескольких узлов (session protocol). Предоставляет средства синхронизации в рамках процедуры обмена сообщениями.
6. Уровень представления (Presentation). Используется для работы с внешним представлением данных, выполнения преобразования между различными их видами (presentation protocol). Как пример, можно привести операции, компрессии или шифрования.
7. Прикладной уровень (Application). Определяет сетевые сервисы, используемые конечными пользователями и приложениями (Application protocol). Как пример, можно привести передачу файлов, подключение удаленных дисков, управление удаленным сервером.

С точки зрения практического применения, для организации межсетевого взаимодействия необходимы только процессы, соответствующие первым трем уровням эталонной модели OSI (физического, канального и сетевого). Именно они связаны с сетевым оборудованием - адаптерами, хабами, мостами, коммутаторами, маршрутизаторами. Функции более высокого уровня реализуются операционными системами и приложениями конечных узлов. Особо можно выделить транспортный уровень, который играет роль посредника между этими двумя группами протоколов.

Однако, для описания локальных сетей оказалась более удобной четырехуровневая модель TCP/IP. Transmission Control Protocol/Internet Protocol (TCP/IP) - это стандарт стека протоколов, разработанный более 20 лет назад по инициативе Министерства обороны США для связи нескольких сетей между собой. Существуют они в виде спецификаций RFC (Request for Comment) - последовательной серии документов, описывающих функционирование сети Internet.

1. Уровень IV. Соответствует физическому и канальному уровням модели OSI, и определяет метод инкапсуляции пакетов IP в кадры сетевой технологии. Не регламентируется, но поддерживает Ethernet и большинство известных стандартов (PPP, Frame Relay, X.25, и др.).
2. Уровень III, межсетевого взаимодействия, по значению соответствующий сетевому уровню модели OSI. В качестве основного используется дейтаграмный (без гарантии доставки) протокол IP, изначально предназначенный для передачи информации в глобальной сети. Так же применяются протоколы сбора маршрутной информации RIP (Routing Internet Protocol), и OSPF (Open Shortest Path First), а также протокол межсетевых управляющих сообщений ICMP (Internet Control Message Protocol).
3. Уровень II. Носит название основного, и соответствует транспортному и сеансовому уровню модели OSI. Определяет функционирование протокола управления передачей TCP, и протокола дейтаграмм пользователя UDP (User Datagram Protocol). TCP образует виртуальное соединение (сессию) между прикладными процессами, и обеспечивает надежную передачу сообщений. Протокол UDP обеспечивает передачу пакетов дейтаграммным способом, и выполняет только функции связующего звена между III и I уровнями.
4. Уровень I, или прикладной. К этим протоколам и сервисам относятся такие широко используемые, как FTP (копирования файлов), эмуляции терминала telnet, почтовый SMTP, гипертекстовые сервисы доступа WWW и многие другие.

Связь между моделью OSI и стеком TCP/IP можно показать следующим образом.

Таб. 9.1. Связь между моделью OSI и стеком TCP/IP

<table>
<tr><th>Модель
OSI</th><th>Протоколы информационного обмена</th><th>Стек
TCP/IP</th></tr>
<tr><td>7</td><td rowspan="2">HTTP, SNMP, FTP, Telnet, SSH, и много других</td><td rowspan="2">I</td></tr>
<tr><td>6</td></tr>
<tr><td>5</td><td rowspan="2">TCP, UDP, DNS, NetBios</td><td rowspan="2">II</td></tr>
<tr><td>4</td></tr>
<tr><td>3</td><td>IP, ARP(RARP), ICMP, RIP, DHCP</td><td>III</td></tr>
<tr><td>2</td><td rowspan="2">Ethernet, ATM, Frame Relay, SDH
(Для стека TCP/IP не регламентируется)</td><td rowspan="2">IV</td></tr>
<tr><td>1</td></tr>
</table>

Кроме этих двух основных моделей встречаются и другие способы описания сетевых протоколов. Так, часто канальный уровень модели OSI разделяют на два подуровня. Или разделяют физический и канальный уровень в стеке TCP/IP. Но широкого распространения эти методы не получили, и подробно их рассматривать не имеет смысла.

Физический уровень.

Особенности физического уровня модели OSI удобно рассматривать с использованием следующего рисунка:

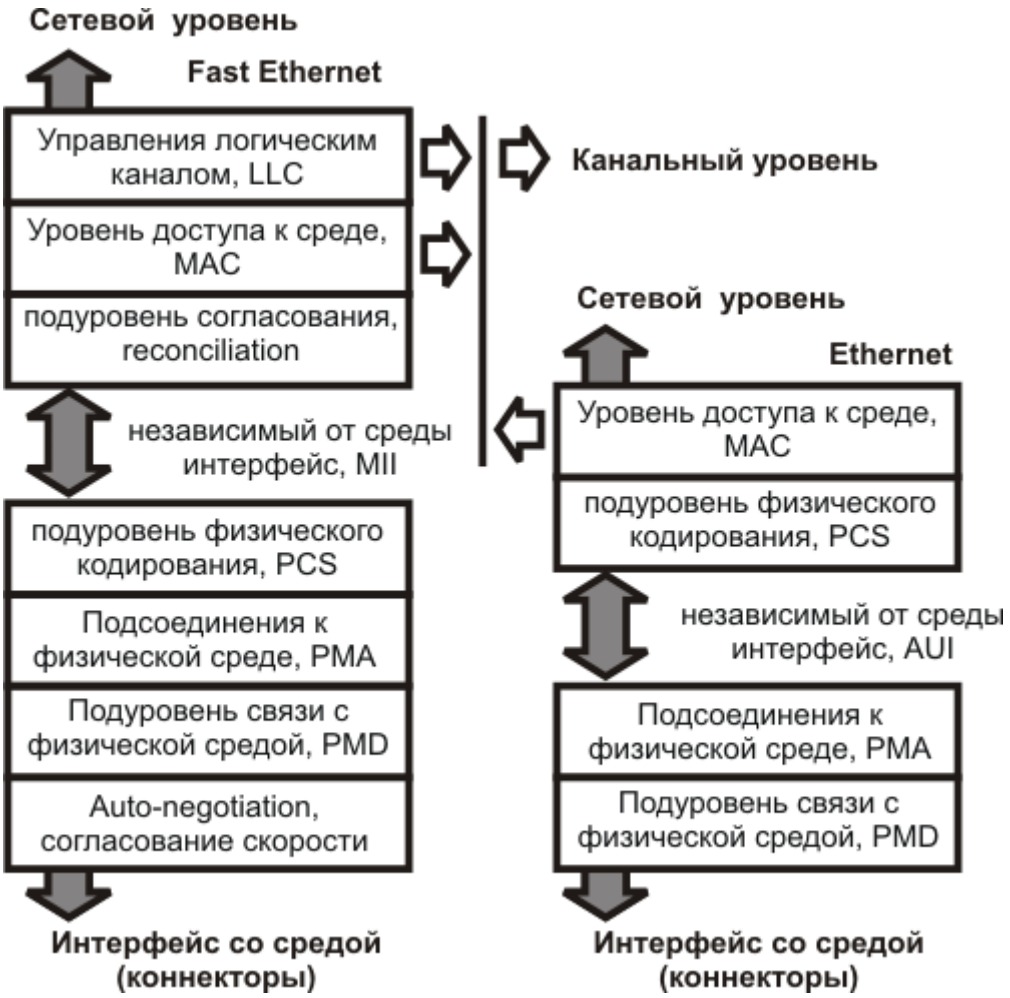

Рис. 9.1. Физический и канальный уровень модели OSI для Ethernet и Fast Ethernet

Можно выделить следующие подуровни:

- Reconciliation - подуровень согласования. Служит для перевода команд MAC-уровня в соответствующие электрические сигналы физического уровня.
- MII - Medium Independent Interface, независимый от среды интерфейс. Обеспечивает стандартный интерфейс между MAC-уровнем и физическим уровнем.
- PCS - Physical Coding Sublayer, подуровень физического кодирования. Выполняет кодирование и декодирование последовательностей данных из одного представления в другое.
- PMA - Physical Medium Attachment, подуровень подсоединения к физической среде. Преобразует данные в битовый поток последовательных электрических сигналов, и обратно. Кроме того, обеспечивает синхронизацию приема/передачи.

- PMD - Physical Medium Dependent, подуровень связи с физической средой. Отвечает за передачу сигналов в физической среде (усиление сигнала, модуляция, формирование сигнала).
- AN - Auto-negotiation, согласование скорости. Используется для автоматического выбора устройствами протокола взаимодействия.
- MDI - Medium Dependent Interface, зависимый от среды интерфейс. Определяет различные виды коннекторов для разных физических сред и PMD-устройств.

Необходимо подчеркнуть различия между классическим Ethernet 802.3i (10 Мбит) и Fast Ethernet 802.3u, объединяющий FX, TX, и T4. В первом роль связующего звена между MAC-уровнем и PHY играл интерфейс AUI. Так как кодирование было всегда одинаковым (Манчестер-2), то схема была простой. Поэтому AUI располагался между подуровнем физического кодирования сигнала и подуровнем физического присоединения к среде. Усложнение Fast Ethernet повлекло и изменение схемы. Добавилось несколько блоков, и интерфейс MII занял место над подуровнем кодирования сигнала, который, в свою очередь, логически вошел в PHY.

Надо так же отметить, что подуровень согласования скоростей (AN) используется не во всех способов передачи. Например, его нет в 10baseT, 10/100baseF.

Подробное рассмотрение подуровней лучше вести "снизу", от физической среды. Так же, в предыдущих главах были подробно рассмотрены вопросы подсоединения к физической среде (MDI), и формирования сигналов (PMD).

Согласование скорости (Auto-negotiation)

К концу 90-х годов сложилась ситуация, при которой в одной и той же сети, по одним и тем же кабелям могло работать сразу пять протоколов - 10base-T, 10base-T full-duplex, 100base-T, 100base-T4, 100base-T full-duplex. Немного позже к ним присоединился 1000base-T. Оставить "ручное" управление таким хозяйством было бы слишком жестоко по отношению к сетевым администраторам.

Первоначально протокол автоматического согласования скорости работы под названием Nway предложила компания National Semiconductor. Немного позже, он был принят в качестве стандарта IEEE 802.3u (Auto-negotiation).

Логично предположить, что возможны два варианта - либо оба договаривающихся устройства поддерживают Auto-negotiation, либо только одно. В первом случае адаптеры (или коммутаторы) должны выбрать наиболее предпочтительный протокол из поддерживаемых (порядок см. выше). При втором варианте более умное устройство должно поддержать единственный вариант, на который способен партнер (как правило, 10Base-T).

Процесс авто-переговоров начинается при включении питания устройства, или команде управляющего устройства (если оно имеется). Для согласования используется группа импульсов, которые называются Fast Link Pulses (FLP). Оборудование, не поддерживающие Auto-negotiation, воспринимают их как служебные сигналы проверки целостности линии 10Base-T (link test pulses).

Устройство, начавшее процесс auto-negotiation, посылает своему партнеру пачку импульсов FLP, в котором содержится 8-битное слово, кодирующее предлагаемый режим

взаимодействия. При этом протокол предлагается самый приоритетный из поддерживаемых.

Если подключенное к линии оборудование поддерживает Auto-negotuiation, и может работать в предложенном режиме, то оно посылает подтверждающее слово, и переговоры заканчиваются. При невозможности работы в предложенном режиме, устройство-партнер отвечает своим предложением, которое и принимается для работы.

Часто возникают проблемы, если настройки negotiation на портах устройств отличаются друг от друга. Нужно либо оба связанных порта устанавливать в режим auto, либо оба зажимать на конкретные значения.

Несколько иначе обстоит дело с оборудованием, поддерживающим только 10Base-T. Такие устройства каждые 16 миллисекунд посылают импульсы для проверки целостности линии, и не отвечают на запрос FLP. Если сетевой адаптер или коммутатор получает в ответ на свой запрос только импульсы проверки целостности линии, он прекращает согласование и устанавливает такой же режим работы.

Глава 9

Присоединение к физической среде (PMA).

Этот подуровень наиболее важный для понимания взаимодействия устройств на физическом уровне. Пожалуй, не будет преувеличением сказать, что именно в нем заключается ключ технологии Ethernet, все его главные отличия от других способов передачи данных. Соответственно, без понимания этих процессов невозможно использовать все возможности Ethernet, особенно при работе за пределами стандартов, присущей многим домашним (территориальным) сетям. И так как данная книга посвящена именно им, то на эту главу придется очень часто ссылаться.

Доступ к среде передачи

Пожалуй, можно сказать, что основное назначение устройства физического уровня - доступ к среде. Как уже говорилось в второй главе, в Ethernet используется CSMA/CD (carrier-sense multiple access/collision detection) - множественный доступ с контролем несущей / обнаружением коллизий. Физическая среда делится между всеми устройствами, и одновременно передавать сообщение может только одно из них.

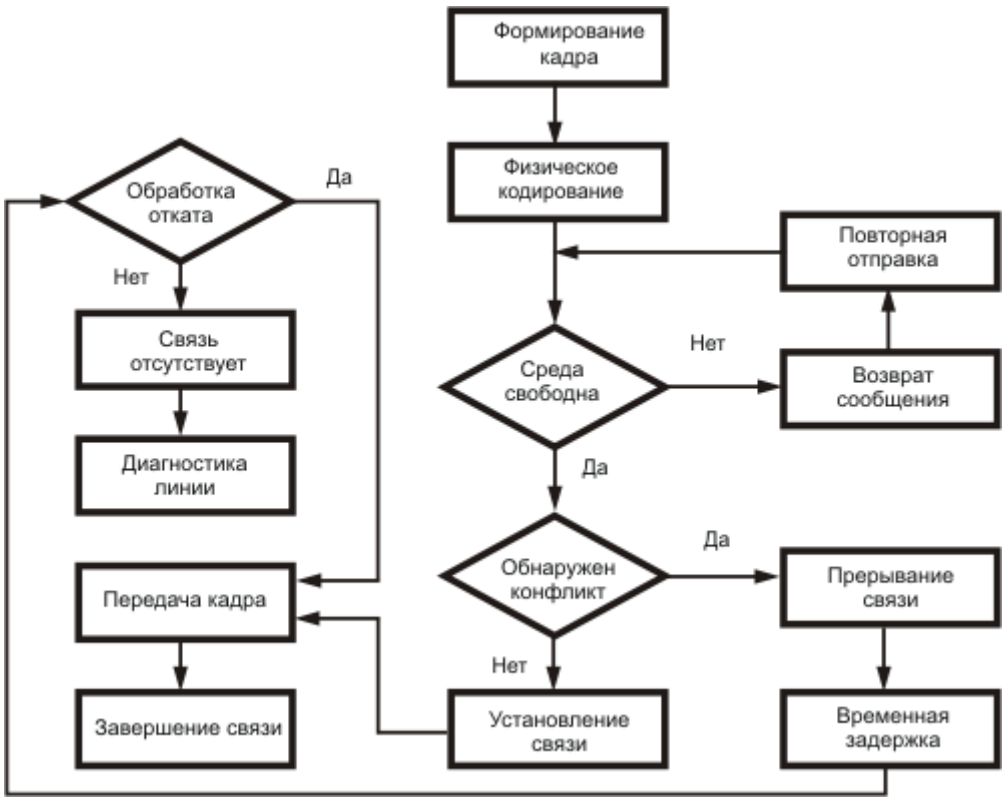

Рис. 9.2. Принцип установления связи в сети Ethernet.

Принцип работы на первый взгляд достаточно прост. Нужно сначала убедиться, что канал свободен, и установить связь. В случае, если среда занята - подождать, когда она освободится. Если в течение заданного промежутка среда не освобождается - сформировать сигнал ошибки.

В сетях Ethernet признаком свободной среды является "отсутствие несущей" (10 МГц). Наоборот, в стандарте Fast Ethernet признаком свободного состояния шины является передача по ней специального Idle-символа (11111) соответствующего избыточного кода, который поддерживает синхронизм и проверяет целостность сети.

Что бы одно устройство не смогло монопольно использовать канал, используют простой механизм. После передачи каждого кадра делаются специальные перерывы в передаче, которые называются межкадровыми интервалами (Inter Packet Gap, IPG). Его длительность для Ethernet (10 Мбит) составляет 9,6 мкс, а для Fast Ethernet в 10 раз меньше, 0,96 мкс.

Значительно более сложной проблемой являются коллизии, или ситуации одновременной параллельной передачи двумя (или более) устройствами. Происходит это из-за того, что сигнал проходит между узлами не мгновенно. И за время его распространения другие сетевые устройства вполне могут начать передачу. При этом происходит "столкновение", в котором искажаются оба пакета. Такая ситуация вполне штатная, и даже неизбежная в некоммутируемом Ethernet.

Распознавание коллизий

Для распознавания коллизий каждое устройство прослушивает сеть во время, и после передачи кадра. Если получаемый сигнал отличается от передаваемого, то станция определяет эту ситуацию как коллизию. В сетях Fast Ethernet, станция, обнаружившая

коллизию, не только прекращает передачу, но и посылает в сеть специальный 32-битный сигнал, называемый jam-последовательностью. Его назначение - сообщить всем узлам сети о наличии коллизии.

В любом случае, после обнаружения коллизии, передача должна быть повторена по достаточно сложному алгоритму отката, показанном на следующем рисунке:

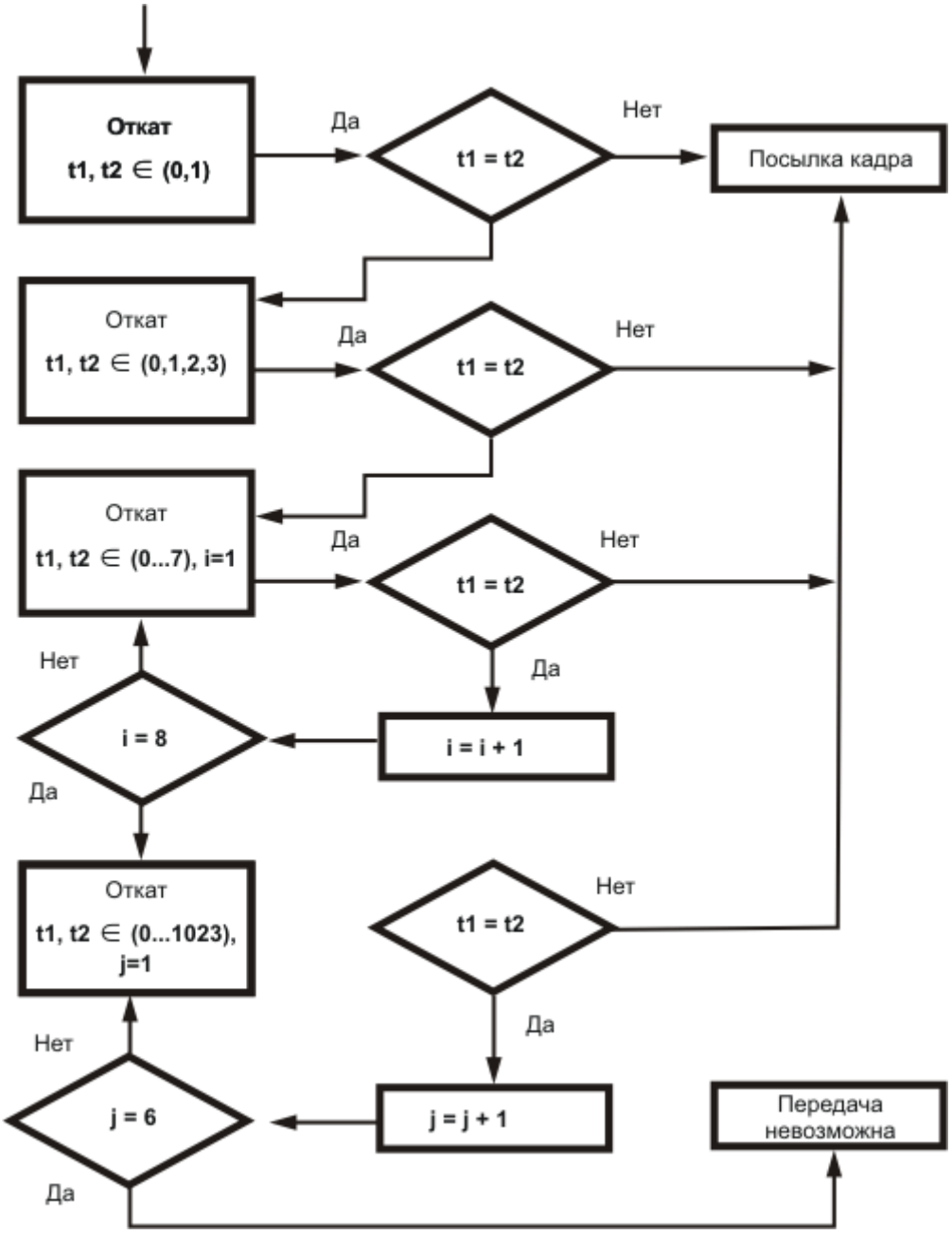

Рис. 9.3. Реализация повторения передачи (отката) при коллизии в сетях Ethernet.

Ключевым моментом является выбор задержки (T) передачи перед повтором, которая равна случайно выбранному из заданного диапазона количеству интервалов (N) времени (t). Иначе говоря, T = N*t, где t = 51,2 мкс. Всего предпринимается 16 попыток передать кадр. В случае невозможности это сделать формируется сообщение об ошибке.

Очевидно, что для переповтора кадра при коллизии, устройство должно ее обнаруживать. Если передающие узлы будут находиться на большом расстоянии друг от друга, то может

случиться, что передача одного из них закончится раньше, чем будет распознана коллизия.

Так как для кадров Ethernet на канальном уровне подтверждение доставки не предусмотрено, то пакет будет просто потерян. Повторить передачу может только протокол более высокого (не ниже транспортного) уровня. Но это уже займет значительно больше времени (в сотни раз).

Можно видеть, что необходимость корректного обнаружения коллизий накладывает ограничение на минимальный размер пакета и расстояние между узлами сети.

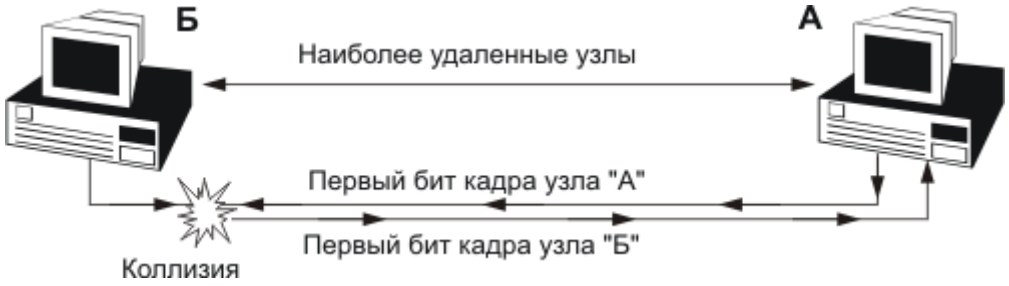

Рис. 9.4. Определение коллизий

Строго говоря, кадры формируются, и повторяются при коллизии на MAC-уровне. Но состояние среды определяется на физическом уровне, и именно он определяет ход процесса доступа к среде. Однако, разделять описание по разным пунктам не целесообразно.

Для передачи в Ethernet выбран минимальный размер кадра на MAC-уровне 512 бит, или 64 байта. При скорости 10 Мбит/с для передачи требуется 51,2 мкс. Самая неблагоприятная ситуация возникнет, когда узел сети "Б" начнет передачу перед самым приходом пакета от узла "А", начавшего передачу ранее. В этом случае сигнал "Б" должен достигнуть узла "А", раньше, чем он закончит передачу.

Нужно специально отметить, что в описании процесса распознавания коллизий часто используется термин "столкновения" пакетов, с последующим его распознаванием передатчиком. Это совершенно не верно отражает происходящие физические процессы, но, вероятно, повышает наглядность объяснения.

Скорость распространения электромагнитного или оптического сигнала в среде передачи составляет около 2/3 от скорости света в вакууме (3x108 м/с), или 200 м/мкс. Несложно подсчитать, что за 51,2 мкс сигнал успеет пройти почти 12 километров. Соответственно, расстояние между узлами может составлять до 6 километров, если не происходит задержек по другим причинам. В реальности это неизбежно происходит в тракте сетевого адаптера и на повторителях (хабах).

Сложно сказать, что учитывали разработчики при выработке стандартов на 10Base5, но в нем максимальное расстояние между узлами составляет 2500 м. Далее, в 10baseT, оно еще уменьшилось до 500 за счет сохранения прежнего количества повторителей - но без какого-либо технического обоснования. В Fast Ethernet (100 Мбит) кадр передается в канал всего за 5 мкс, поэтому ограничения на расстояния намного более жесткие.

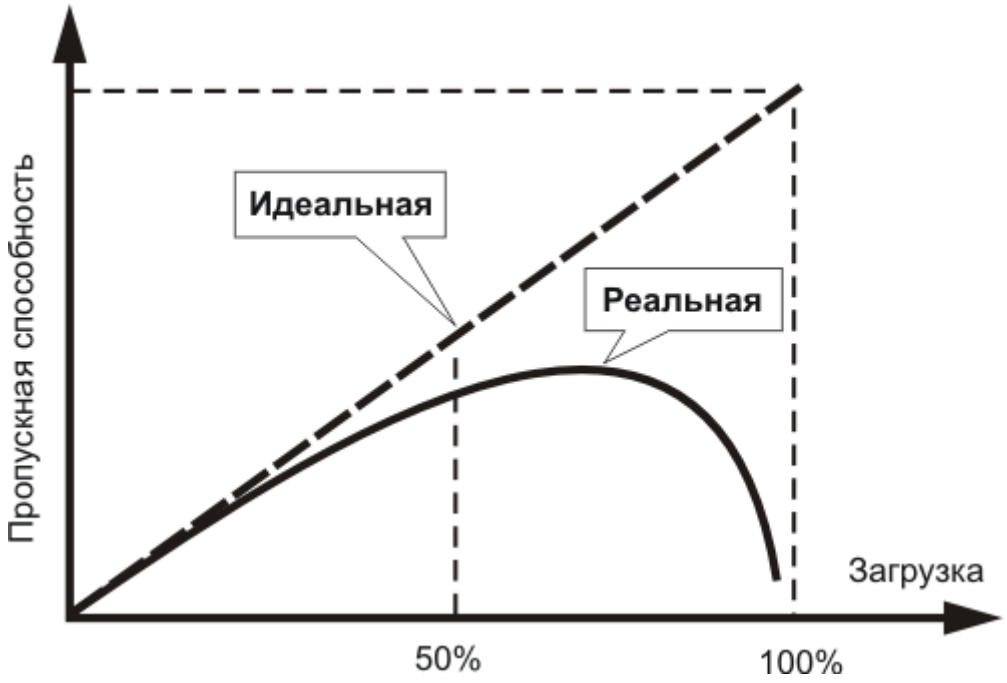

Рис. 9.5. Пропускная способность Ethernet

Легко видеть, что в случае большой загруженности сети вероятность возникновения коллизий резко возрастает, и пропускная способность сети уменьшается из-за многочисленных попыток передачи одних и тех же кадров. Для описания этого явления даже вводят специальный термин - деградация производительности.

Ну, а практической рекомендацией будет простой. Не использовать некоммутируемый Ethernet при загрузке более 30-40%.

Глава 9

Коммутируемый Ethernet.

Принципиально меняет ситуацию использование коммутируемого Ethernet. В нем используются специальные устройства - коммутаторы (свитчи), которые, на основании адресов узлов сети могут устанавливать независимые друг от друга соединения между пользователями.

В этом случае каждое устройство может принимать и передавать данные независимо друг от друга. Соответственно, механизм доступа к среде сильно упрощается. Понятие коллизий отсутствует, нет ограничения на расстояние передачи, нет деградации производительности. Именно это позволяет использовать Ethernet в операторских решениях, на равных конкурируя с намного более сложными и дорогостоящими технологиями детерминированного доступа к среде.

При работе в полнодуплексном режиме компьютер может в любой момент отправлять кадры в коммутатор, так как если бы он был один (не принимая во внимание другие компьютеры). В реальности часто встречается ситуация, когда несколько компьютеров отправляют кадры одному, и их поток превышает возможности передачи. Порт коммутатора неизбежно столкнется с перегрузками.

Если это будет происходить недолго, поможет буфер входного порта. Но для работы при долговременной перегрузке необходимо предусмотреть механизм управления потоком кадров. Для этого коммутатор может использовать кадры "паузы" технологии Advanced Flow Control, описанной в стандарте IEEE 802.3x.

К сожалению, эта удобная технология не приемлема при работе в полудуплексном режиме, с сетевыми адаптерами не поддерживающими 802.3x. В этом случае для управления потоком кадров коммутатор может использовать два метода, основанных на нарушении некоторых правил доступа к среде передачи данных.

Для Fast Ethernet используется метод обратного давления (backpressure). При этом коммутатор для "подавления" активности какого-либо устройства искусственно генерирует коллизии на этот порт, посылая ему jam-последовательности.

Второй метод (на сегодня неактуальный), применяемый для Ethernet (10 Мб), основан на агрессивном поведении коммутатора. В этом случае порт использует межкадровый интервал в 9,1 мкс, вместо 9,6 мкс, положенных по стандарту. Как следствие, порт коммутатора монопольно захватывает шину, направляя сетевому адаптеру только свои кадры и разгружая свой внутренний буфер. Похожий способ используется для захвата шины после коллизии, когда он выдерживает интервал отсрочки, равный 50 мкс вместо положенных 51,2 мкс.

Кодирование битовой последовательности

Что бы избежать в дальнейшем терминологической путаницы, нужно разделить кодирование битовой последовательности в электрический сигнал, и кодирование данных, которое преобразует одну последовательность битов в другую. Процессы эти принципиально различны по сути, но логически тесно связаны. Дело в том, что для разных способов передачи применяются разные формы представления данных.

Рассмотрим операции, которые требуются для передачи и последующего приема битовой последовательности:

- синхронизация тактовой частоты передатчика и приемника;
- преобразование последовательности битов в электрический сигнал;
- уменьшение частоты спектра электрического сигнала с помощью фильтров;
- передача урезанного спектра по каналу связи;
- усиление сигнала и восстановление его формы приемником;
- преобразование аналогового сигнала в цифровой.

Битовый поток передается со скоростью, определяемой числом бит (дискретных изменений сигнала) в единицу времени. Тактовая частота, измеряемая в герцах, означает число синусоидальных изменений сигнала в единицу времени.

Такое очевидное соответствие часто вызывает ошибочное сопоставление скорости передачи данных и тактовой частоты. Но на практике все сложнее. Данные могут передаваться не только битами, но и их группами, иметь не два, а 3, 5, и более уровней напряжения. Или даже передаваться по нескольким парам параллельно.

Классический Ethernet, пожалуй, последняя из распространенных технологий передачи данных в которой кодирование данных не применяется. При помощи алгоритма Манчестер-2 в линию передаются битовые последовательности (прямо с MAC-уровня).

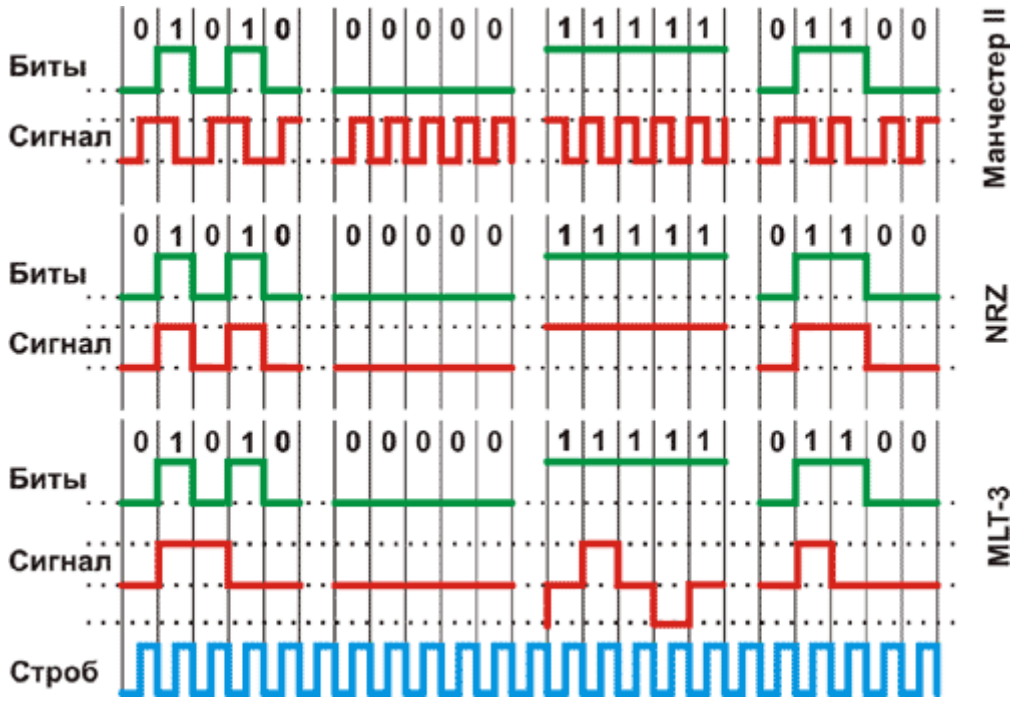

Рис. 9.6. Кодирование Манчестер-2, NRZI, MLT-3.

Из рисунка легко видеть, что в этом случае сигнал имеет две несущие частоты. При передаче только нулей, или только единиц - 10 МГц, и 5 МГц при чередовании нулей и единиц.

Большое достоинство этого кода - отсутствие постоянной составляющей при передаче длинной серии нулей или единиц. Изменение сигнала в центре каждого бита позволяет не принимать специальных мер для синхронизации приема-передачи.

Следующий простейший двухуровневый код - NRZ (Non Return to Zero), или "без возврата к нулю". Нулевому значению соответствует нижний уровень сигнала, единице - верхний. Переходы электрического сигнала происходят на границе битов.

Достоинство кода в его простоте. Из рисунка видно, что кодировка по сути отсутствует. Еще один плюс - даже при самой неудачной последовательности данных (чередование нулей и единиц) скорость передачи данных вдвое превышает частоту. Для других комбинаций частота будет меньше, и при одинаковых битах частота изменения сигнала равна нулю.

К недостаткам NRZ (или инвертированного NRZI) можно отнести то, что он не имеет синхронизации. Поэтому, применяют искусственные меры - например не допускают появления длинных последовательности одинаковых байтов, или используют специальный стартовый служебный бит.

Используется кодировка NRZI в основном для работы с оптоволоконной средой (PHY FX), и протоколами 100Base-FX.

Код трехуровневой передачи MLT-3 (Multi Level Transmission - 3) несколько похож на NRZ, только с тремя уровнями сигнала. Единице соответствует переход с одного уровня сигнала на другой, и изменение уровня сигнала происходит последовательно, с учетом предыдущего перехода. Максимальной частоте сигнала соответствует передача

последовательности единиц, при передаче нулей сигнал не меняется. Основной недостаток кода MLT-3 такой же, как и NRZ - отсутствие синхронизации.

Применение MLT-3 - сети 100base-T на основе витой пары (PHY TX). Наличие двух методов кодирования для протоколов одной скорости вызвано отличием физических сред. Для оптоволокна технически невозможно использовать кодирование, отличное от двухуровневого, но оно имеет достаточно широкую полосу пропускания. С другой стороны, витая пара очень критична к полосе пропускания, и трехуровневое (или пятиуровневое для 1000base-T) кодирование позволяет значительно снизить частоту несущей.

На рисунке 9.7. электрические сигналы изображены в виде прямоугольников. Но в реальности формировать такую их форму очень сложно, и применяются гармонические (синусоидальные) колебания. Если говорить точнее, то используется сумма основной составляющей (несущей частоты), и высших гармоник, задающих форму импульсов. Совокупность нескольких таких колебаний называется спектр.

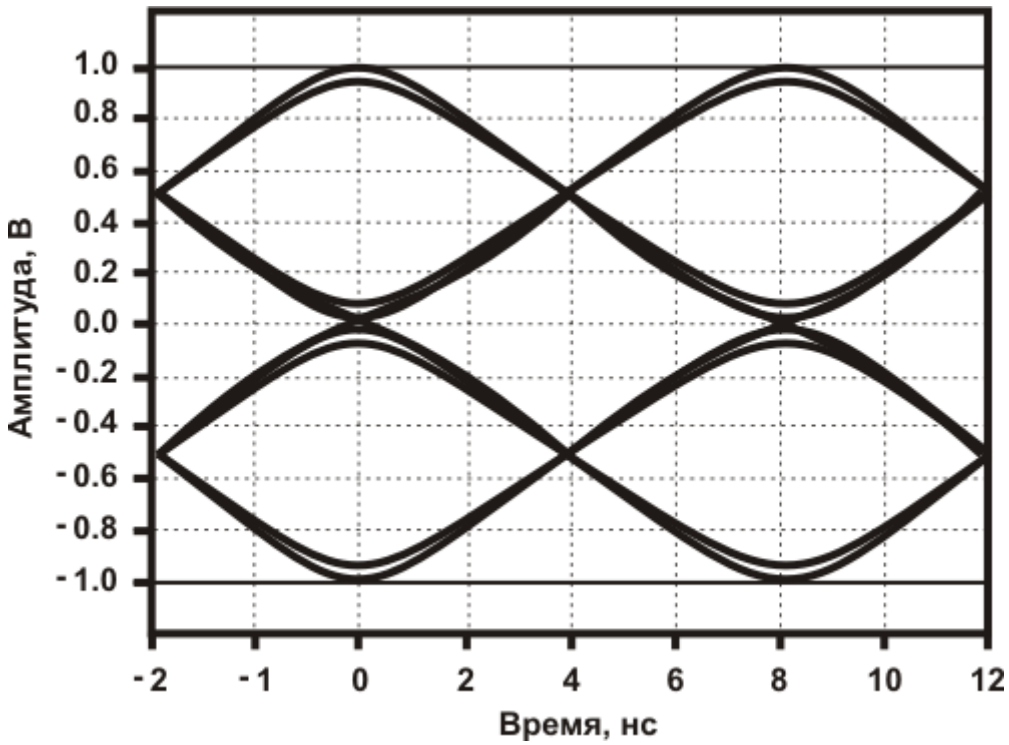

Рис. 9.7. Реальный вид сигнала при использовании протокола 100baseT (MLT-3).

В теории, цифровой метод передачи позволяет восстановить исходный сигнал только несущей спектра. Но в реальности удовлетворительной помехоустойчивости удается достигнуть только с использованием первой гармоники. Это удваивает ширину спектра, необходимого для передачи сигналов.

Так, из рисунка 9.7. можно видеть, что для передачи 100 Мбит информации с использованием метода кодирования MLT-3, необходима несущая, частотой 25 Мгц. С учетом первой гармоники, требования повышаются до 50 МГц. А с учетом избыточного кодирования 4B/5B, необходимо уже 62,5 МГц.

Аналогично, для передачи 10 Мбит с кодировкой Манчестер-2, требуется полоса пропускания в 20 Мгц. Эта величина окончательная, так как в этом случае избыточное кодирование не применяется.

Физическое кодирование (PCS)

Как уже было показано выше, коды MLT-3 и NRZI не являются самосинхронизирующимся. Передача длинной последовательности единиц или нулей подряд приведет к потере несущей, и ошибкам приема.

Для исключения таких цепочек применяют кодирование данных 4B/5B, в котором используется пяти-битовая основа для передачи четырех-битовых сигналов. Кроме синхронизации, этот метод улучшает помехоустойчивость благодаря контролю принимаемых данных на пяти-битном интервале. Очевидная цена кодирования данных - снижение на 25% скорости передачи полезной информации.

Преобразованный пяти-битовый сигнал имеет 16 значений для передачи информации, и 16 избыточных значений, из которых для служебных сигналов отведены девять символов, а семь комбинаций, имеющие более трех нулей - не используются. Исключенные сигналы (01 - 00001, 02 - 00010, 03 - 00011, 08 - 01000, 16 - 10000) интерпретируются символом V (VIOLATION - сбой).

Наличие служебных символов позволяет применять схему непрерывного обмена сигналами между передатчиком и приемником. Это позволяет сетям 100base-T осуществлять более эффективные методы доступа к физической среде по сравнению с 10Base-T.

Необходимо обратить внимание, что именно методам кодирования обязан рост скоростей передачи как в Ethernet, так и других технологий передачи данных (например xDSL), с использованием прежней кабельной инфраструктуры. Выше показано, как переход на другой способ кодирования способен снизить требуемую полосу пропускания почти на 40%.

Еще более заметно это на протоколе 1000base-T - в нем современные методы кодирования успешно используются для серьезного повышения скорости передачи. Если посмотреть на проблему с другой стороны, то можно показать возможность передачи с небольшой скоростью 10 мегабит на расстояние до 3 километров. Подробнее этот вопрос будет рассмотрен в следующих главах.

В заключение, отметим еще один важный момент. В PHY TX есть специальный механизм шифрования-дешифрования (scrambler/descrambler). Определен он в спецификации ANSI TP-PMD, и используется для равномерного распределения сигнала по частотному спектру. Что, в свою очередь, уменьшает электромагнитное излучение кабеля.

Независимый от среды интерфейс (MII) и подуровень согласования (Reconciliation)

Во времена использования 10base5 для доступа к конкретной среде передачи данных применялось отдельное устройство (трансивер), которое было логически связанно с сетевым адаптером или повторителем специальным кабелем снижения (до 50 метров длиной, амплитуда сигнала 12 вольт, 15 контактов в разъеме). При этом на логическом уровне использовался независимый от конечной среды передачи интерфейс AUI (Attachment Unit Interface, интерфейс подключения устройства). Кодирование данных не

производилось вообще, а кодирования битовой последовательности в электрический сигнал происходило в сетевом адаптере.

Введение стандарта Fast Ethernet (802.3u) потребовало новой, более скоростной и удобной связи MAC и PHY уровней. Для этого используется независимый от среды интерфейс (MII), имеющий, в случае внешнего исполнения, большой по размеру разъем с 40 контактами, длину кабеля не более 1 метра, и амплитуду сигналов в 5 вольт.

Но обычно на практике шина MII интегрирована в одной микросхеме с другими логическими элементами сетевого адаптера (повторителя), и имеет структуру, далекую от канонического вида.

Канал передачи данных от подуровня MAC к PHY образован 4-битной шиной данных, которая синхронизируется тактовым сигналом, генерируемым PHY, а также сигналом "Передача", исходящим от MAC-подуровня. Подобно устроен прием данных - это другая 4-битной шина, синхронизирующаяся тактовым сигналом и сигналом "Прием", которые генерируются PHY.

Обмен командами управления идет по отдельной двухпроводной шине. Подуровни могут передавать друг другу сообщения об возникших ошибках ("ошибка приема", "ошибка передачи"). Кроме этого, данные о конфигурации, состоянии порта и линии хранятся соответственно в регистрах управления (Control Register) и статуса (Status Register).

- Регистр управления. Используется для установки скорости и параметров работы порта.
- Регистр статуса. Содержит информацию о действительном состоянии работы порта.

Кроме связи между подуровнями, в повторителе (хабе, репиторе) интерфейс MII может применяться для соединения нескольких устройств PHY.

Роль подуровня согласования (Reconciliation), несмотря на его выделение в отдельный функциональный блок, весьма прозаична. При переходе от шины AUI к MII интерфейс MAC-подуровня был сохранен. Соответственно, возникла потребность его согласования с новой шиной MII, что и было сделано с помощью этого подуровня.

Глава 9

Канальный уровень.

Задача канального уровня - обеспечить взаимодействие устройств внутри локальной сети путем передачи специальных блоков данных, которые называются кадрами (frame). В процессе формирования они снабжаются служебной информацией (заголовком), необходимой для корректной доставки получателю, и, в соответствии с правилами доступа к среде передачи, отправляются на физический уровень.

При приеме данных с уровня PHY необходимо выделить кадры, предназначенные данному устройству, проверить их на отсутствие ошибок, и передать сервису или протоколу, которому они предназначались.

Нужно обратить внимание, что именно канальный уровень отправляет, принимает, и повторяет кадры в случае коллизии. Но определяет состояние разделяемой среды физический уровень. Поэтому процесс доступа (с необходимым уточнением) подробно описан в предыдущей главе.

Информационное взаимодействие на канальном уровне сетей стандарта Ethernet так же, как и на физическом, принято разделять на дополнительные подуровни, которые не были предусмотрены стандартом OSI-7.

- LLC (Logical Link Control). Уровень управления логическим каналом;
- MAC (Media Access Control). Уровень доступа к среде.

Подуровень MAC

В идеология множественного доступа к среде Ethernet передачу данных приходится реализовать по широковещательному принципу "каждый для всех" (broadcasting). Это не может не наложить отпечаток на процесс формирования и распознавания кадров. Рассмотрим строение кадра Ethernet DIX, как наиболее часто используемого для передачи IP трафика.

Для идентификации устройств используются 6-ти байтовые MAC-адреса, которые отправитель обязательно должен указать в передаваемом кадре. Старшие три байта представляют собой идентификатор производителя оборудования (Vendor codes), младше - индивидуальный идентификатор устройства.

За уникальность последних несет ответственность производитель оборудования. С идентификаторами производителя дело обстоит сложнее. Существует специальная организация в составе IEEE, которая ведет список вендоров, выделяя каждому из них свой диапазон адресов. Кстати, занести туда свою запись стоит совсем не дорого, всего US $1250. Можно отметить, что создатели технологии Ethernet, Ксерокс и DEC, занимают первую и последнюю строчку списка соответственно.

Такой механизм существует для того, что бы физический адрес любого устройства был уникальным, и не возникло ситуации его случайного совпадения в одной локальной сети.

Нужно особо отметить, что на большинстве современных адаптеров можно программным путем установить любой адрес. Это представляет определенную угрозу работоспособности сети, и может быть причиной тяжелых "мистических" неисправностей.

MAC-адрес может быть записан в различной форме. Наиболее часто используется шестнадцатеричная, в которой пары байтов отделяются друг от друга символами "-" или ":". Например, сетевая карта Realtek, установленная в моем домашнем компьютере, имеет адрес 00:C0:DF:F7:A4:25.

MAC-адрес позволяет выполнять единичную (Unicast), групповую (Multicast) и широковещательную адресацию кадров (Broadcast).

Единичная адресация означает, что узел-источник направляет свое сообщение только одному получателю, адрес которого явно указывается.

В режиме групповой адресации кадр будет обработан теми станциями, которые имеют такой же Vendor Code, как и у отправителя. Признаком такой посылки является "1" в

младшем бите старшего байта MAC-адреса (X1:XX:XX:XX:XX:XX). Такой формат достаточно удобен для "фирменного" взаимодействия устройств, но на практике используется достаточно редко.

Другое дело широковещательная посылка, в которой адрес получателя кодируется специальным значением FF-FF-FF-FF-FF-FF. Переданный пакет будет принят и обработан всеми станциями, которые находятся в локальной сети.

Таблица 9.2. Формат кадра Ethernet

Preamble Преамбула	SFD	DA Адрес назначения	SA Адрес Источника	Type/Length Тип/Длина	Data Данные	FCS Контрольная сумма
7 байт	1 байт	6 байт	6 байт	2 байта	46-1500 байт	4 байта

Для успешной доставки одного адреса назначения явно недостаточно. Нужна дополнительная служебная информация - длина поля данных, тип сетевого протокола и др.

- Преамбула (Preamble). Состоит из 8 байтов. Первые семь содержат одну и ту же циклическую последовательность битов (10101010), которая хорошо подходит для синхронизации приемопередатчиков. Последний (Start-of-frame-delimiter, SFD), 1 байт (10101011), служит меткой начала информационной части кадра. Это поле не учитывается при определении длины кадра и не рассчитывается в контрольной сумме.
- MAC-адрес получателя (Destination Address, DA).
- MAC-адрес отправителя (Source Address, SA). Первый бит всегда равен нулю.
- Поле длины либо тип данных (Length/Type, L/T). Два байта, которые содержат явное указание длины (в байтах) поля данных в кадре или указывают на тип данных. Ниже, в описании LLC будет показано, что возможно простое автоматическое распознавание разных типов кадров.
- Данные (Data). Полезная нагрузка кадра, данные верхних уровней OSI. Может иметь длину от 0 до 1500 байт.
- Для корректного распознавания коллизий необходим кадр не менее чем из 64 байт. Если поле данных менее 46 байт, то кадр дополняется полем заполнения (Padding).
- Контрольная сумма (Frame Check Sequence, FCS). 4 байта, которые содержит контрольную сумму всех информационных полей кадра. Вычисление выполняется по алгоритму CRC-32 отправителем и добавляется в кадр. После приема кадра в буфер, приемник выполняет аналогичный расчет. В случае расхождения результата вычислений, предполагается ошибка при передаче, и кадр уничтожается.

Подуровень LLC

Данный подуровень обеспечивает единый, независимый от используемого метода доступа, интерфейс с верхним (сетевым) уровнем. По сути, можно сказать, что на нем определяется логическая структура заголовка кадра Ethernet.

Как ни странно, единый стандарт не определен до сих пор. Так как особых технических трудностей при определении типов кадров устройствами не оказалось, на практике могут параллельно использоваться четыре модификаций:

- 802.3/LLC (или кадр Novell 802.2)
- Raw 802.3 (или кадр Novell 802.3)
- Ethernet DIX (или кадр Ethernet II)
- Ethernet SNAP

Причина вполне обычна. Технология Ethernet начала свое развитие задолго до принятия стандартов IEEE 802. Первоначально подуровень LLC не выделялся из общего протокола и, соответственно, в специальном заголовке не было нужды. После принятия стандартов IEEE, и появления двух отличных друг от друга форматов кадров канального уровня, понадобился механизм согласования. Попытка введения нового, "объединяющего" варианта заголовка, привела к возникновению очередного формата кадра.

Что бы не слишком запутаться в частных (и не слишком важных) отличиях, рассмотрим только наиболее широко распространенный в локальных сетях кадр Ethernet DIX (Ethernet II), структура которого уже была рассмотрена в описании подуровня MAC.

Как наиболее важный момент, необходимо отметить смысл поля Length/Type (длина/типа данных). 2-байтовое поле Length (Длина) кадра Raw 802.3, в кадре Ethernet DIX используется в качестве поля типа протокола (Type), и явно указывает на тип протокола верхнего уровня, вложившего свой пакет в поле данных кадра. Если подходить строго, то видно, что к Ethernet DIX название Length (Длина) не имеет отношения. Но терминология устоялась, и проще пойти на неоднозначную формулировку, чем ее ломать.

Автоматическое распознавание типов кадров Ethernet выполняется достаточно просто, и поддерживается подавляющим большинством сетевых устройств. Так, для отличия Ethernet DIX от Raw 802.3 в поле Type указываются значения, превышающие значение максимальной длины поля данных (1500 байт). Например, для IP используется код 0800, для IPX - 8037, X.25 - 0805, и т.п.

Так же, в случае наличия полей LLC, несложно отличить кадр Ethernet SNAP от 802.3/LLC. Но эти форматы не используются в 10/100baseT, и подробно останавливаться на них в рамках данного изложения не имеет смысла.

Кадры Ethernet с тегами VLAN 802.1q

Первое время массовому внедрению Ethernet не мешали "врожденные" недостатки стандарта (в особенности полное отсутствие средств обеспечения безопасности). Но сети быстро росли, и ограничения начали всерьез сдерживать технологию в целом.

Для решения проблемы было предложено несколько "фирменных" методов маркировки фреймов (например ISL, VLT), однако на сегодня имеет смысл говорить только о стандарте 802.1q. Его смысл достаточно прост - в заголовок добавляется 4 байта, в которых содержится информация о номере виртуальной сети (vlan), и информация о приоритете.

Таким образом, заголовок приобретает следующий вид:

Preamble Преамбула	SFD	DA Адрес назначения	SA Адрес Источника	Ether Type	Метка	Type/Length Тип/Длина	Data Данные	FCS Контр. сумма
7 байт	1 байт	6 байт	6 байт	2 байта	2 байта	2 байта	46-1500 байт	4 байта

Поле EtherType, TPID (Tagged Protocol Identifier) содержит код 0x8100. Оно соответствует полю тип протокола стандартного поля кадра Ethernet и указывает на необходимость обработки кадра согласно требованиям IEEE 802.1q.

Поле "Метка" надо рассмотреть подробнее:

Приоритет	CFI	VLAN ID
3 байта	1 байт	12 байт

Поле приоритета кадра - 3 бита, 1-битовое поле CFI (Canonical Format Identifier) и 12-битовое поле VID (идентификатор виртуальной сети) называются TCI (Tagged Control Information).

Такое решение позволило решить проблемы приоритезации и разделить одну сеть на множество отдельных виртуальных сетей. Т.е. основные проблемы оказались решены.

Однако, тут не обошлось и без проблем. Прежде всего, фрейм ethernet увеличил длину до 1522 октетов, и с 802.1q может корректно работать далеко не всякое старое оборудование (регулируется спецификацией 802.3ac). Да и вообще, нововведение серьезно усложнило коммутаторы - для распознавания тегов о них требуется большая мощность, и для соблюдения приоритетов - несколько очередей в исходящих буферах. А для установки тегов приоритета более того. Способность анализировать более высокие протоколы (например 4-го уровня по модели OSI), и исходя из порта назначения и настроек устанавливать тэги.

Во-вторых, внедрение дополнительных тегов не решило всех проблем Ethernet - количество VLAN ограничено 4096. С приоритетами до сих пор оборудование разных брендов обращается довольно произвольным образом...

Тем не менее, стандарт 802.1q позволил сильно усложнить структуру сетей, и добавил принципиальные возможности. Сейчас без него просто невозможно представить сколь-нибудь большую сеть.

Глава 9

Сетевой уровень.

Этот уровень первоначально использовался для образования единой транспортной системы, объединяющей несколько сетей, не зависимо от способа передачи данных. В качестве блока данных сетевого уровня используется дейтаграмма, который предназначен для доставки некоторого фрагмента передаваемого сообщения. Такой подход позволяет отделить процесс передачи данных от прикладных программ, позволяя обрабатывать сетевой трафик одинаковым способом для любых приложений.

По сети произвольной топологии дейтаграмма перемещается на основании адреса пункта назначения и адреса источника, и делает это независимо от всех остальных дейтаграмм. В качестве примера протоколов сетевого уровня можно привести X.25, IPX, и, конечно, популярнейший на сегодня Internet протокол - IP.

Кроме этого, для осуществления своих функций, сетевой уровень имеет возможности структуризации сети и согласования различных методов работы канального уровня.

Наиболее важный вопрос передачи данных, адресация, может быть решен двумя способами. Во-первых, с использованием совпадающих, во-вторых - различных сетевых и канальных адресов. Первый способ (например, протокол IPX) упрощает администрирование локальной сети. Второй обеспечивает гибкость, независимость от аппаратной части, и логическое единство адресного пространства. Эти преимущества позволили способу адресации, использующему различные сетевые и канальные адрес, получить распространение в сети Интернет (под названием Internet Protocol, IP), практически вытеснив все остальные способы передачи данных.

Все остальные протоколы (кроме ARP/RARP, который часто относят к протоколу канального уровня) используют IP для передачи данных между узлами сети.

Логика передачи пакетов на сетевом уровне

Как было описано выше, взаимодействие на канальном уровне ограничивается локальной сетью, и механизм передачи кадров между разными сетями отсутствует (без их фактического объединения). Поэтому реально кадры Ethernet передают не данные, а дейтаграммы сетевого уровня, которые занимают место данных.

Устройства, способные выделять IP дейтаграммы из кадров, определять их маршрут назначения, и упаковывать дейтаграммы опять в кадры канального уровня (обычно, уже другой сети), называются маршрутизаторами (router). Таким образом, упрощенно можно представить Интернет как совокупность сетей разного типа, объединенных посредством маршрутизаторов.

Для определения маршрута следования дейтаграммы, используются специальные таблицы маршрутизации, которые могут быть задана администратором (статически), или определена маршрутизатором при помощи специальных (и достаточно сложных) протоколов взаимодействия (динамически).

При этом для каждой сети, или группы сетей задаются правила (адреса маршрутизатора), в соответствии с которыми должны быть переданы дейтаграммы для достижения узла назначения. Причем в качестве правил могут быть указаны только адреса, до которых может быть проведена непосредственная доставка (next hop routing). Таким образом, на каждом маршрутизаторе задаются только адреса сетей, с которыми он имеет прямую связь, а не полную информацию о маршруте.

Более того, нет необходимости одного "сквозного" протокола для всего пути дейтаграммы. Для ее передачи между компьютерами, которые подключены к разным локальным сетям (подсетям), нужно провести следующие действия.

1. Отправитель посылает кадр, включающий IP дейтаграмму с адресом получателя, устройству, определенному как шлюз локальной сети (маршрутизатор). Для получения кадра шлюз должен быть подключен к той же локальной сети, что и отправитель;
2. Маршрутизатор получает кадр, извлекает из него IP-дейтаграмму. По адресу назначения, в соответствии с таблицей маршрутизации, формирует кадр канального уровня, и направляет его в соответствующую подсеть следующему шлюзу согласно таблице маршрутизации.

3. Операция повторяется до тех пор, пока IP-дейтаграмма не достигнет маршрутизатора, подключенного к той же подсети, что и получатель. В этом случае кадр будет оправлен непосредственно получателю.

Исходя из такого способа доставки сообщений, удобно, что бы каждый из узлов имел уникальный сетевой адрес, состоящий из двух частей - адреса сети (Net ID) и адреса узла (Host ID). Для установки соответствия между адресами канального и сетевого уровня используется специальный протокол разрешения адресов (Address Resolution Protocol, ARP). При составлении и модификацией таблиц маршрутизации используются RIP (Routing Internet Protocol) и OSPF (Open Shortest Path First), а также протокол межсетевых управляющих сообщений ICMP (Internet Control Message Protocol).

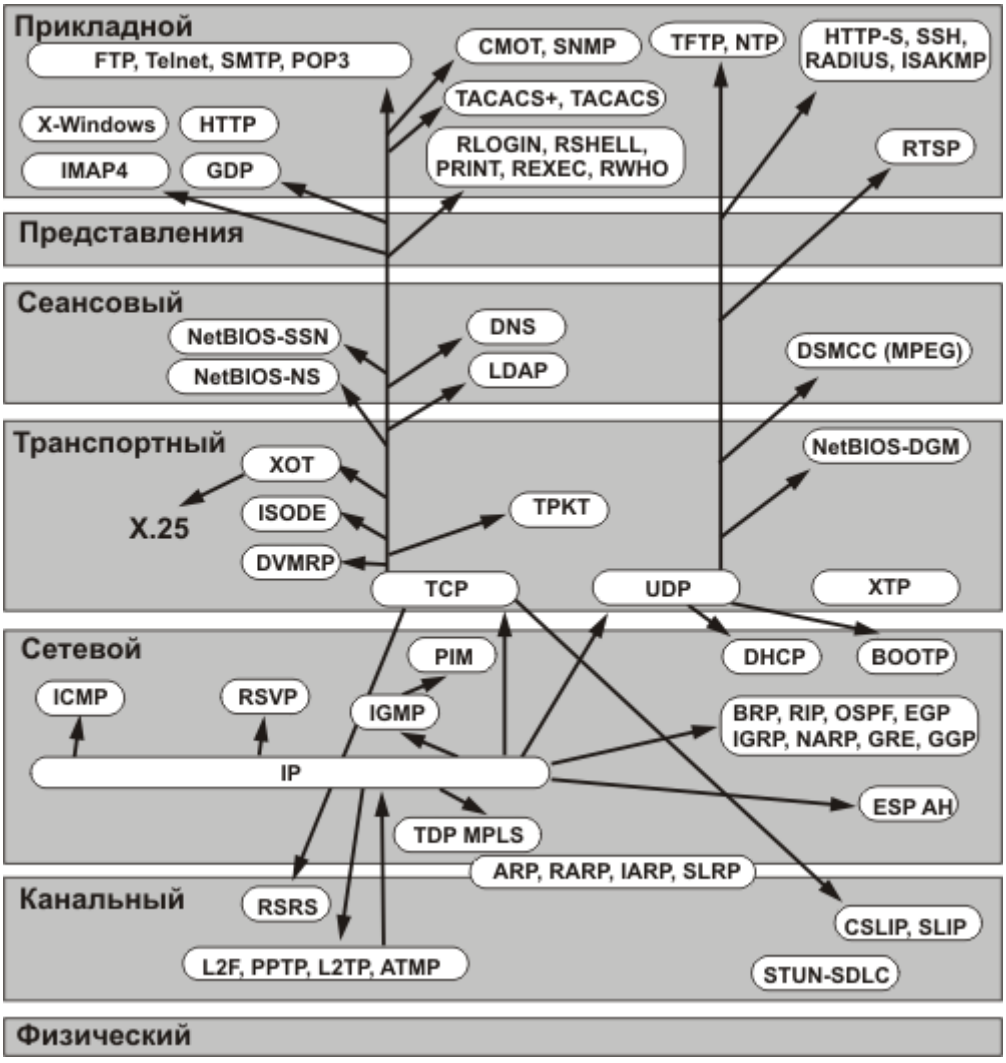

Рис. 9.8. Структура протокольных модулей сети, построенной на основе IP

В общем виде схема достаточно сложная (более того, спорная), ее подробное рассмотрение лежит далеко за рамками рассматриваемого в данной книге материала.

Тем не менее, в следующих главах постараемся рассмотреть основные принципы передачи данных на сетевом уровне.

Протокол адресации (IP)

Основными функциями протокола IP можно назвать разделение данных (передаваемых протоколами более высокого уровня) на дейтаграммы для их доставки получателю в другой сети, и сборку блоков данных из дейтаграмм при их получении от других узлов сети. Для этого к данным присоединяется специальный заголовок унифицированного формата, который для используемой в настоящее время четвертой версии IP может иметь длину до 20 байт (пять 32-х битовых слов).

Таб. 9.3. Формат дейтаграммы IP

<table>
<tr><td>Версия</td><td>Длина</td><td>Тип сервиса</td><td colspan="2">Общий размер</td></tr>
<tr><td colspan="3">Идентификация</td><td>Флаги</td><td>Смещение фрагмента</td></tr>
<tr><td colspan="2">Время жизни</td><td>Протокол</td><td colspan="2">Контрольная сумма заголовка</td></tr>
<tr><td colspan="5">Адрес отправителя</td></tr>
<tr><td colspan="5">Адрес получателя</td></tr>
<tr><td colspan="5">Опции и заполнение</td></tr>
<tr><td colspan="5">Данные</td></tr>
</table>

Заголовок дейтаграммы IP имеет следующие поля:

- Номер версии (Vers) протокола IP.
- Длина заголовка (Hlen), измеренная в 32-битовых словах. Как правило, заголовок составляет 20 байт (пять 32-битовых слов). Но в теории, он может быть увеличен за счет использования поля Резерва (IP OPTIONS).
- Тип сервиса (Servise type) задает приоритетность дейтаграммы, и критерий выбора способа доставки. Маршрутизаторы могут использовать это поле (вернее, его первые три бита) для установления очередности обработки сообщений. Для обычного пакета данных значение поля устанавливается равным "0", а для управляющей информации (максимальный приоритет) - "7". Следующие три бита определяют способ доставки. Так, значение "D" (delay) предписывает использовать путь с минимальной задержкой доставки, "T" - для достижения максимальной пропускной способности, "R" - с использованием пути, имеющего максимальную надежность доставки.
- Общая длина (Total length) с учетом заголовка и поля данных. Надо заметить, что максимальный размер дейтаграммы IP определяется для каждого типа сетей по максимальной единице транспортировки (Maximum Transfer Unit, MTU). Для сети Ethernet она имеет значение, равное 1500 байт, а сеть X.25 используют MTU в 128 байт.
- Идентификатор (Identification) используется для определения дейтаграмм, до фрагментации являющихся частями одного блока данных.
- Флаги (Flags) позволяют управлять фрагментацией данных. Так, установленный бит DF (Do not Fragment) запрещает маршрутизатору разделять данную дейтаграмму, а бит MF (More Fragments) - признак того, что дейтаграмма содержит промежуточный фрагмент.
- Смещение фрагмента (Fragment offset) используется сборке/разборке частей пакетов при передачах их между сетями с различными величинами максимальной длины дейтаграммы. Для этого указывается в байтах смешение начала фрагмента, вошедшего в дейтаграмму, от начала общего блока данных, подвергнутого фрагментации.
- Время жизни (Time to live) определяет предельный срок, в течение которого дейтаграмма может перемещаться по сети. При значении этого поля, равном "0",

дейтаграмма уничтожается. Время измеряется в секундах, и вычитается на транзитных узлах при передаче (единица вычитается даже в том случае, если передача заняла меньшее время). При современных скоростях передачи, можно считать, что время жизни задается числом транзитных узлов.
- Идентификатор протокола верхнего уровня (Protocol) указывает на протокол верхнего уровня, которому принадлежит дейтаграмма.
- Контрольная сумма (Header Checksum), которая рассчитывается по всему заголовку на каждой точке обработки дейтаграммы.
- Адрес источника (Source IP address) и Адрес назначения (Destination IP address) служат для доставки дейтаграммы, и получения ответа.
- Резерв (IP options) является необязательным и, как правило, используется на стадии при отладке сети.

Остановимся подробнее на IP-адресах, по которым происходит доставка дейтаграмм. На практике существует достаточно сложный механизм, позволяющий эффективно организовывать этот процесс.

IP-адрес состоит из 4 байт (одно 32-битное слово), которое принято записывать в десятичном виде. Например, 192.168.0.2 - адрес одного из сетевых адаптеров моего компьютера в маленькой изолированной "квартирной" сети. Если записать этот же адрес в двоичном виде, получится 11000000-10101000-00000000-00000010. Биты, входящие в адрес, часто называют октетами.

Как уже говорилось выше, IP-адрес состоит из двух частей: номера сети и номера узла. Если устройство является частью сети Интерент, то адрес сети назначается согласно рекомендациям одного из подразделений Сетевого Информационного Центра (Network Information Center, NIC). Для независимой (закрытой) сети администратор может назначить адреса самостоятельно.

На практике сложилось, что Интернет-провайдеры сначала получают диапазоны адресов (подсети) в NIC для себя, а далее предоставляют их своим клиентам на тех, или иных условиях.

Особо надо отметить, что не только каждый узел сети может иметь несколько адресов. Одному сетевому адаптеру (интерфейсу) могут быть назначены различные адреса, или, наоборот, нескольким интерфейсам - один адрес. Система управления достаточно гибкая, описать все ее возможности сложно.

В начале развития сети Интеренет для удобства управления адресным пространством введено деление сетей на классы "**Классовая модель**", но впоследствии была повсеместно принята "**Безклассовая модель**" (CIDR).

Рассмотрим классовую модель. В ней граница между сетевой частью IP-адреса, и части, предназначенной для идентификации хостов, всегда проходит по границе октета. Т.е. возможно четыре и только четыре типа сети.

Таб. 9.4. Деление IP сетей на классы

Класс <сети	Диапазон значений первого октета	Значения адреса в десятичной записи	Возможное кол-во сетей	Возможное кол-во узлов
A <сети	от 00000001-… до 01111110-…	от 1.xxx.xxx.xxx до 126.xxx.xxx.xxx	126	16777214

B <сети	от 1000000-00000000-… до 1011111-11111111-…	от 128.0.xxx.xxx до 191.255.xxx.xxx	16382	65534
C <сети	от 1100000-00000000-00000000… до 1101111-11111111-11111111…	от 192.0.0.xxx до 223.255.255.xxx	2097150	254
D <сети	от 1110000-… до 1110111-…	от 224.xxx.xxx.xxx до 239.xxx.xxx.xxx	-	268435456
E <сети	от 1111000-… до 1111111-…	от 240.xxx.xxx.xxx до 255.xxx.xxx.xxx	-	134217728

Понятно, что адреса класса A предназначены для использования в очень больших сетях общего пользования (например, национальных). Класс B может найти применение в сетях крупных провайдеров или компаний (при американском толковании масштабов). Небольшим провайдерам, или сетям, приходится иметь дело в основном с сетями класса C, которые позволяют адресовать 254 узла. Адреса класса D используются при обращениях к группам машин, а адреса класса E зарезервированы для использования в эксперементальных целях.

В любой сети первый (вернее, нулевой) адрес является номером всей сети и не может быть присвоен никому конкретно. Адрес, являющийся последним в сети, предназначен для широковещательных (broadcasting) сообщений, которые доставляются всем узлам данной сети. Соответственно, эти два адреса недоступны для узлов. Именно поэтому, в сети класса C можно адресовать не 256, а только 254 узла.

Кроме этого, зарезервировано несколько групп адресов специального назначения. Так, сеть класса A с номером 127 (loopback), предназначена для общения компьютера с собой. При посылке данных на этот адрес, они не передаются по сети, а возвращаются протоколам верхнего уровня. Поэтому, узлам запрещено присваивать адреса этой сети, и считается, что она не входит в адресное пространство Интернет.

Аналогично, адрес вида 0.0.0.0 считается локальным адресом данного узла, и из диапазона доступных сетей исключен соответствующий блок.

Есть еще одно важное соглашение (RFC 1918) о сетях, которые считаются "частными", т.е. не маршрутизируемыми в сети Интернет. Это блоки адресов от 10.0.0.0 - 10.255.255.255 (сеть класса A), 172.16.0.0-172.31.255.255 (16 сетей класса B), 192.168.0.0-192.168.255.255 (255 сетей класса C). Такие адреса часто используются для маскарадинга, транзитных, или изолированных сетей. В этом случае даже ошибки в маршрутизации не вызовут сбоев в работе других узлов Интернет.

Как ни велико адресное пространство, при таком простом способе адресации оно не может быть использовано эффективно. Тяжело представить физическую сеть, в которой количество узлов будет достаточным для IP-сети класса A. С другой стороны, невозможно использовать только небольшие сети. Каждая сеть, так или иначе, создает особое правило на транзитных маршрутизаторах. И большое количество сетей вызовет их неоправданную загрузку (или вообще, неработоспособность).

В классовой модели старшие биты IP-адреса определяли принадлежность узла к конкретному классу, и соответственно по нему маршрутизаторы определяли размер сети. Для претворения в жизнь технически привлекательного принципа произвольного разделения адресного пространства пришлось ввести 32-битовую маску (netmask) или маску подсети (subnet mask).

Сетевая маска действует по следующему простому принципу:
в позициях, соответствующих номеру сети, биты установлены в 1;
в позициях, соответствующих номеру хоста, биты сброшены в 0.

Таким образом, был разработана "безклассовая модель" адресации (CIDR, Classless Internet Direct Routing, прямая бесклассовая маршрутизация). В ней отсутствуют технические причины разделения сеть-хост в IP-адресе точно по границе октета. И вдобавок, схема может быть иерархической. При этом крупные магистральные маршрутизаторы обрабатывают проходящий трафик в соответствии с правилами для полных сетей, даже не подозревая о том, что они где-то разделены на подсети. Таким образом, нагрузка "перекладывается" на периферийные маршрутизаторы.

Рассмотрим этот вопрос на наиболее распространенном случае разделения сети класса С, например 192.168.25.0 с маской 255.255.255.0 (11111111. 11111111. 11111111.00000000), или, в компактной форме записи, 192.168.25.0/24 (24-количество значащих разрядов маски).

Таб. 9.5. Возможные варианты разделения сети класса С на подсети.

Запись маски	Последний октет маски	Количество подсетей	Количество адресов в подсети	Количество значащих разрядов
255.255.255.252	11111100	64	4	30
255.255.255.248	11111000	32	8	29
255.255.255.240	11110000	16	16	28
255.255.255.224	11100000	8	32	27
255.255.255.192	11000000	4	64	26
255.255.255.128	10000000	2	128	25

Нужно иметь в виду, что "нулевой" адрес в каждой подсети (например, 192.168.25.64/255.255.255.192) является собственно адресом сети, а последний (192.168.25.127/255.255.255.192) - бродкастовым. Использовать их для узлов нельзя, и, соответственно, теоретически возможная маска 255.255.255.254 не может быть применена. Вариант с 255.255.255.252 имеет всего 2 реальных адреса, и может быть использован в ограниченном числе случаев.

В остальном, нужно отметить, что возможны самые разные варианты разделения сетей. Так, например, сеть класса "С" можно представить как сумму из 2*4+1*8+1*16+3*32+2*64. Но при этом будет "потеряно" 16 адресов.

Роль подсетей нельзя недооценивать. Например, с точки зрения маршрутизатора адрес 192.168.25.149/255.255.255.128 (192.168.25.149/25) будет выглядеть как номер сети 192.168.25.128 и номер узла 21, что несколько отличается от привычной записи, и может породить серьезные проблемы.

Протокол преобразования адресов ARP (RARP)

Как уже было сказано выше, маршрутизаторы упаковывают дейтаграммы IP в кадры локальных сетей (обычно Ethernet). Для установления соответствия MAC по IP адресу они используют специальный протокол разрешения адреса (Address Resolution Protocol, ARP). Соответственно, для решения обратной задачи (установления IP по известному MAC-

адресу) используется реверсивный протокол разрешения адреса (Reverse Address Resolution Protocol, RARP). Классический случай применения RARP - старт рабочей станции, у которой IP-адрес не установлен в явном виде.

Алгоритм работы протокола следующий:

1. Маршрутизатор, которому необходимо доставить дейтаграмму IP-адреса узлу в локальной сети, формирует ARP-запрос, и вкладывает его в кадр широковещательной рассылки.
2. Все узлы локальной сети получают кадр с ARP-запросом, и сравнивают указанный там IP-адрес с собственным.
3. При совпадении адресов, узел формирует ARP-ответ (совпадающий по формату с ARP-запросом), в котором указывает свой IP-адрес и MAC-адрес, и отправляет его маршрутизатору.
4. После получения кадра маршрутизатор отправляет по MAC-адресу IP-дейтаграмму адресату.

Работа протокола занимает вполне определенное, и часто не малое время, за которое дейтаграмма может быть потеряна (превысит время хранения в кэше сетевого адаптера). Поэтому, маршрутизаторы и рабочие станции с сети хранят таблицу соответствия (ARP-таблицу), по которой отправка производится без посылки ARP-запроса.

Кроме IP и MAC-адреса, в таблице хранится возраст записи, что позволяет ее обновлять по определенным условиям. Далее, нужно особо отметить, что во многих операционных системах таблица может быть сформирована вручную администратором сети. Такая возможность часто используется для установления жесткого соответствия MAC и IP адреса узла для ограничения несанкционированного доступа к различным ресурсам.

Таб. 9.6. Формат пакета протокола ARP/RARP в Ethernet

<table>
<tr><td colspan="2">Тип оборудования (для Ethernet - 1)</td><td>Тип протокола (для IP-0800)</td></tr>
<tr><td>Длина MAC-адреса</td><td>Длина IP-адреса</td><td>Операция. 1-ARP (запрос), 2-ARP (ответ), 3-RARP (запрос), 4-RARP (ответ)</td></tr>
<tr><td colspan="3">Аппаратный адрес (для Ethernet MAC) отправителя (байты 9-14)</td></tr>
<tr><td colspan="3">IP-адрес отправителя (байты 15-18)</td></tr>
<tr><td colspan="3">Аппаратный адрес (для Ethernet MAC) получателя (байты 19-24)</td></tr>
<tr><td colspan="3">IP-адрес получателя (байты 25-28)</td></tr>
</table>

В общем случае, форматы локальных адресов различны для разных видов протоколов. Поэтому красивую таблицу с определенными заранее полями составить сложно. Так как длина MAC-адреса в Ethernet составляет 6 байт, а IP - 4 байта, получается, что запрос занимает 28 байт.

Мультипротокольная коммутация меток (протокол MPLS)

Одно из узких мест IP связано с низкой скоростью маршрутизации данных. Действительно, пограничные рутеры должны прочитывать все заголовки IP-кадров что бы перепрвить их на нужный интерфейс. Конечно, есть много фирменных технологий, ускоряющих процесс... Однако методов, позволяющих ускорить маршрутизацию всей

сети сразу не так и много. Наиболее популярным последнее время стал MPLS (разработка Cisco).

Принципиальной основой MPLS являются IP-туннели. Для его работы нужна поддержка протокола маршрутизации MP-BGP. Протокол MPLS может работать практически для любого маршрутизируемого транспортного протокола (не только IP).

При появлении пакета в виртуальной сети ему присваивается метка, которая не позволяет ему покинуть пределы данной виртуальной сети. Протокол MPLS предоставляет возможность обеспечения значения QoS, гарантирующего более высокую безопасность. Для обеспечения структурирования потоков в пакете создается стек меток, каждая из которых имеет свою зону действия. Формат стека меток представлен на рис. 3 (смотри RFC-3032). В норме стек меток размещается между заголовками сетевого и канального уровней (соответственно L2 и L3). Каждая запись в стеке занимает 4 октета.

MAC-заголовок	Стек меток MPLS	IP-заголовок

Место заголовка MAC может занимать заголовок PPP. В случае работы с сетями ATM метка может занимать поля VPI и VCI.

В свою очередь, стек MPLS выглядит следующим образом:

CoS

Метка	S	TTL	Стек	
20 бит	3 бита	1 бит	8 бит	-

Полю CoS соответствует приоритет поля ToS. Поле CoS имеет три бита, что достаточно для поля приоритета IP-заголовка. S - флаг-указатель дна стека меток; TTL - время жизни пакета MPLS.

MPLS представляет собой интеграцию технологий уровней L2 и L3. Управление коммутацией по меткам основывается на базе данных LIB (Label Information Base). Пограничный маршрутизатор MPLS LER (Label Edge Router) удаляет метки из пакетов, когда пакет покидает облако MPLS, у вводит их во входящие пакеты.

Управление трафиком MPLS автоматически устанавливает и поддерживает туннель через опорную сеть. Путь туннеля вычисляется, основываясь на сформулированных требованиях и имеющихся ресурсах (constraint-based routing). IGP автоматически маршрутизирует трафик через эти туннели. Обычно, пакет, проходящий через опорную сеть MPLS движется по одному туннелю от его входной точки к выходной.

Глава 9

Межсетевой протокол управляющих сообщений (ICMP).

Для успешной передачи дейтаграмм между сетями необходим механизм диагностики состояния маршрута, при необходимости сообщающий о возникающих ошибках узлу-отправителю. Этой цели служит протокол обмена управляющими сообщениями ICMP. Самостоятельной роли он не играет, исправлять ошибки (или чем-то управлять) не может, более того, взаимодействие узлов может проходить и без использования этого протокола. Хотя некоторая функциональность связи без ICMP может быть потеряна. Например при неработающем MTU-Discovery (ICMP зафильтрован полностью) могут не проходить пакеты больше какого-либо количества байт.

Тем не менее, ICMP предназначен для диагностики, и использование его возможностей является серьезной помощью для устранения неисправностей.

Сразу надо отметить, что этот протокол не участвует в процессе обмена дейтаграммами IP, и присоединяется к обычному IP-заголовку, занимая место данных. Но это не мешает ICMP (как и большинству протоколов более высоких уровней) иметь свой заголовок (до 8 байтов), и сообщение (не имеет фиксированной длинны).

В общем, все сообщения ICMP можно разделить на парные, состоящие из двух компонентов, запрос (Request) и ответ (Reply), и непарные - только ответ, возникающий из-за проблемы в передаче.

Вот пример наиболее часто встречающиеся непарного сообщения:

Цель недоступна (Destination Unreachable). Формируется в случае, если запрошенный сетевой ресурс является недоступным для запрашивающей его станции. Например, Network Unreachable, Host Unreachable, Protocol Unreachable, и другие. Причем эти сообщения могут быть сформированы не только узлом назначения, но и промежуточным роутером. Например, в случае невозможности доставить сообщение узлу, последний доступный маршрутизатор выдает сообщение типа:

Ответ от 192.168.0.2: Заданный узел недоступен (Destination Host Unreachable)

В качестве распространенного примера парного сообщения можно привести Echo (эхо). Используются они для того, что бы определить принципиальную достижимость узла, или маршрут по ответу (Echo Reply), который должен быть сформирован в ответ на ICMP запрос (Echo Request).

Именно на этом механизме построена простая и широко применяемая для диагностики утилита ping, или traceroute. Более подробно способ их использования на практике будет описан в следующих главах.

В заключение этого раздела, хотелось бы отметить, что есть еще целый ряд протоколов, работающих на сетевом уровне модели OSI. С ростом уровня, резко расширяется функциональность протоколов. Даже полное описание возможностей относительно простого ICMP может занять больше места, чем эта глава. А это очень мало по сравнению, например, с RIP (протокол маршрутизации, выполняющий широковещательную рассылку таблиц маршрутизации), или OSPF (протокол выявления маршрутов маршрутизаци по состоянию связи).

Транспортный уровень.

Как следует из названия, протоколы транспортного уровня предназначены для непосредственного взаимодействия двух пользовательских процессов. При этом для передачи информации они используют описанные выше дейтаграммы IP, помещая свои сообщения в их поле данных.

В общем виде существует два типа протоколов транспортного уровня - сегментирующие (TCP, разбивают исходное сообщение на блоки), и не сегментирующие, или дейтаграммные (UDP, отправляют сообщение "как есть", одним куском). Разумеется, второй способ намного проще, но он не гарантирует доставки.

Не будет большой ошибкой сказать, что в реальной сети Интернет используются всего два транспортных протокола:

- Протокол передачи пользовательских дейтаграмм (UDP User Datagram Protocol).
- Протокол управления передачи (TCP Transmission Control Protocol).

На практике для эффективной организации обмена информацией между процессами оказалось недостаточно сетевого адреса узла (на котором выполняется пользовательские программы). Понятно, что на одном компьютере может одновременно работать десятки приложений, и для каждого желательно иметь возможность устанавливать соединения независимо от других. Для решения задачи используется специальный виртуальный интерфейс (порт), номер которого передается в заголовке пакета TCP (или дейтаграммы UDP).

Транспортный протокол UDP

Дейтаграммы UDP имеют переменную длину и состоят из заголовка сообщения, и собственно данных.

Таб. 7.7. Формат дейтаграммы UDP

Номер порта отправителя	Номер порта получателя
Длина сообщения	Контрольная сумма
Данные	

Номер порта источника указывается только в том случае, если предполагается ответ. Минимальная длина дейтаграммы составляет 8 байт (размер заголовка).

Протокол UDP не обеспечивает гарантированной доставки сообщений. Поэтому, он может быть использован только для приложений, которые не нуждаются в этом качестве. Как пример можно привести передачу звука, или видео. Второй вариант использования UDP - приложения, которые обеспечивают доставку своими средствами. Например, всем известный Telnet и старые версии ICQ.

Транспортный протокол TCP

Этот протокол, пожалуй, более распространен, чем все остальные, вместе взятые. Он используется для гарантированной доставки сообщений (называемых пакетами) в сетях Интернет.

Таб. 7.8. Формат пакета TCP

Номер порта отправителя								Номер порта получателя
Порядковый номер								
Номер подтверждения								
Смещение	Резерв	U	A	P	R	S	F	Окно
Контрольная сумма								Указатель важности
Опции и заполнение								
Данные								

Заголовок пакета TCP состоит из нескольких (обычно 6) 32-х битных слов, и в этом похож на формат дейтаграммы IP. Поясним значение некоторых полей:

- Порядковый номер первого октета в сегменте необходим для определения места пакета для сборки блока переданных данных после сегментации (если она была проведена перед передачей).
- Номер подтверждения содержит значение следующего порядкового номера, который отправитель сегмента рассчитывает получить.
- Смещение данных - 4-х битовое поле, указывающее число 32-х битовых слов в заголовке пакета, или начало поля данных.
- Резерв - зарезервированное поле размером в 6 бит.
- Поле флагов управления. U (URG) - значимое поле указателя важности, A (ACK) - значимое поле подтверждения, P (PSH) - функция push, R (RST) - сброс соединения, F (FIN) - нет данных от отправителя.
- Окно, это 16-битовое поле, которое содержит число октетов данных, которые отправитель данного сегмента будет отправлять без немедленного подтверждения доставки. Отсчет ведется, начиная с октета, указанного в поле номер подтверждения.
- Уровень важности - значение смещения до октета, с которого начинаются важные (urgent) данные. Разумеется, поле принимается во внимание только для пакетов с установленным флагом "U".

Различия в величине заголовка пакета TCP и дейтаграммы UDP сразу обращают на себя внимание. Объяснение кроется в сложности обеспечения гарантированной и эффективной доставки (да еще и с заданным уровнем качества). Для этого можно использовать метод квитирования с повторной передачей.

Несмотря на сложное название, его суть достаточно проста. При получении пакета узел назначения посылает отправителю специальный сигнал ACK (квитанцию). Узел, передавший пакет, в свою очередь, до получения подтверждения прекращает передачу. А в случае отсутствия "квитанции" в течение определенного времени, начинает передачу пакета заново. Несмотря на простоту, такой алгоритм имеет большой недостаток - пропускная способность сети передачи данных используется очень неэффективно. Как минимум, половину времени процессы ожидают получения подтверждения.

В связи с этим применяется более эффективный алгоритм квитирования с использованием "скользящего окна", при котором передающий узел отправляет сразу несколько пакетов, не дожидаясь получения подтверждения о приеме. Для определения максимального количества передающихся таким образом пакетов TCP применяют параметр "окно" в заголовке. Соответственно, узел, принимающий пакеты так же может обработать несколько "квитанций" за один раз.

При отсутствии ошибок и задержек передачи, получается что "окно" передаваемых пакетов непрерывно скользит вдоль входящего потока данных, эффективно загружая сеть.

От размера окна очень много зависит, но его выбор - не слишком тривиальная задача. На практике алгоритм пошел немного "от противного", не от максимальной скорости передачи. Каждое сообщение подтверждения доставки пакета содержит значение размера окна, которое может быть предоставлено принимающим узлом (window advertisement). Обычно, оно определяется размером свободного в данный момент буфера принимающего адаптера.

При этом достигается еще одна цель - становятся не нужными дополнительные механизмы, которые контролируют процесс переполнения. В каком-то плане, это можно рассматривать как довольно красивый (хотя и не полный) ответ сложным методам, применяемым для тех же целей (но на канальном уровне) в технологии ATM.

Но для обеспечения передачи с заданным качеством одного механизма квитирования совершенно недостаточно. И существует еще достаточно широкий спектр способов повышения эффективности транспортных протоколов. Например, этому служит виртуальное логическое соединение, или TCP-сессия. Инициировать ее установление может один из узлов, а далее обе стороны контролируют качество, и при возникновении сложностей в информационном обмене, могут разорвать сессию с отправкой соответствующих сообщений протоколам более высокого уровня.

Кроме этого, может быть использован режим потокового обмена, механизм ускорения доставки трафика, чувствительного ко времени (push), и некоторые другие.

Чем более высокий уровень OSI используется, тем больше возможностей предоставляют протоколы для управления. Описать их все - большая, но отдельная задача. Поэтому, рассматривать сеансовый и более высокие уровни (или уровень приложений стека TCP/IP) в рамках данной главы не целесообразно. Разумеется, необходимые для работы простых сетей протоколы (такие как NetBios, DNS, FTP, Telnet, http) будут описаны в следующих главах.

С другой стороны, для функционирования простой сети становится более важно умение работать (или настраивать) вполне определенные программные комплексы, а не понимание механизма работы протоколов. Так, например, большинство специалистов предпочитает не вдаваться в протокольные подробности функционирования операционной системы, довольствуясь обычными руководствами по эксплуатации. И, разумеется, такой подход им совершенно не мешает получать хорошие результаты в работе.

Исходя из вышесказанного, на транспортном уровне описание модели OSI можно закончить, и рассматривать работу протоколов более высокого уровня на примере конкретных приложений.

Глава 10. Активные устройства.

Из всех способов межличностного общения
он предпочитал полнодуплексные

В предыдущих главах были рассмотрены вопросы построения оптимальной кабельной инфраструктуры. Но сама по себе она не может и не должна являться конечной целью работы. Сеть создается для передачи данных между рабочими станциями, серверами, и другими активными устройствами.

Активные устройства осуществляют формирование, преобразование, коммутацию, а так же прием сигнала с использованием внешнего (не передающегося в составе сигнала) источника энергии. Соответственно, они является неотъемлемым компонентами любой сети передачи данных.

Вопрос правильного выбора оборудования далеко не второстепенен. Даже в недорогих офисных сетях от этого зависит качество и скорость работы сети. Что уж говорить про условия домашних сетей, с их жесткой внешней средой и критическими нагрузками. В этом случае важны даже мелочи, приходится ориентироваться не только на тип и параметры устройства, но на опыт реальной эксплуатации разных моделей.

Активные устройства можно, с некоторой долей условности, разделить на рабочие станции, повторители (концентраторы), коммутаторы, мосты и маршрутизаторы.

Простое соединение рабочих станций было рассмотрено в главе 5, поэтому основное внимание будет уделено другим группам устройств. Кроме этого, в этой главе будут кратко рассмотрены вопросы оптимального выбора по производителю, модельному ряду, и другим факторам, влияющим на стоимость и работоспособность сети.

Использование пассивного оборудования не предусматривается стандартами Ethernet, тем не менее, в некоторых случаях применение возможно, и будет рассмотрено в одной из следующих глав, совместно с описанием альтернативных способов построения сетей.

Глава 10

Повторители и концентраторы.

Одной из первых задач, которая стоит перед любой технологией транспортировки данных, является возможность их передачи на максимально большое расстояние.

Физическая среда накладывает на этот процесс свое ограничение - рано или поздно мощность сигнала падает, и прием становится невозможным. При этом не имеет значения абсолютное значение амплитуды - для распознавания важно соотношение сигнал/шум.

Привычное для аналоговых систем усиление не годится для высокочастотных цифровых сигналов. Разумеется, при его использовании какой-то небольшой эффект может быть достигнут, но с увеличением расстояния искажения быстро нарушат целостность данных.

Проблема не нова, и в таких ситуациях применяют не усиление, а повторение сигнала. При этом устройство на входе должно принимать сигнал, далее распознавать его первоначальный вид, и генерировать на выходе его точное подобие. Такая схема в теории может передавать данные на сколь угодно большие расстояния (если не учитывать особенности разделения физической среды в Ethernet).

Первоначально в Ethernet использовался коаксиальный кабель с топологией "шина", и нужно было соединять между собой всего несколько протяженных сегментов. Для этого обычно использовались повторители (repeater), имевшие два порта. Несколько позже появились многопортовые устройства, называемые концентраторами (concentrator). Их физический смысл был точно такой же, но восстановленный сигнал транслировался на все активные порты, кроме того, с которого пришел сигнал.

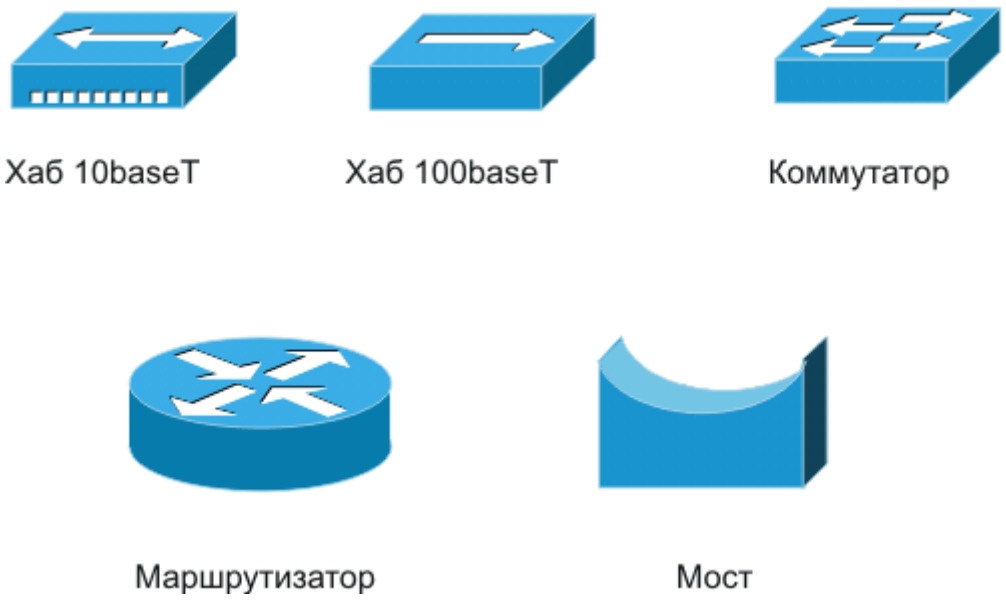

Рис. 10.1. Схематическое изображение активных устройств

С появлением протокола 10baseT (витой пары) для избежания терминологической путаницы многопортовые повторители для витой пары стали называться хабами (hub), а коаксиальные - репитерами (по крайней мере в русскоязычной литературе). Эти названия хорошо прижились, и используется в настоящее время очень широко.

Особенности работы концентраторов

Первое, что необходимо отметить - концентраторы работают на физическом уровне модели OSI. Поэтому для них совершенно безразлично, какие протоколы более высоких уровней используются в сети. Идеология проста и поэтому достаточно надежна. Все порты хаба равноправны, никакой логической обработке сигнал не подвергается, не буферизируется, коллизии не обрабатываются (только фиксируются их наличие на индикации некоторых моделей устройств).

Есть несколько простейших операций, которые делаются большинством концентраторов в автоматическом режиме.

- Автосегментация (network integrity), иначе говоря, автоматическое включение или отключение порта. Порт, к которому подсоединена неисправная линия, или не подключено какое-либо активное устройство, считается свободным и находится в неактивном режиме. При обнаружении устройства работоспособность порта восстанавливается. Для этого используются служебные сигналы проверки целостности линии (link test pulses) представляющий собой периодический импульс длительностью 100 нс, посылаемый через каждые 16 мс;
- Показывают состояние портов (или устройства в целом) на светодиодных индикаторах. Единого подхода к индикации нет, но распространены следующие:

состояние портов (Port Status), наличие коллизий (Collisions), активность канала передачи (Activity) и наличие питания (Power);
- Обнаруживают ошибку полярности (перепутаны проводники внутри пары) при использовании витопарного кабеля, и автоматически ее переключают.

Как повторители, так и концентраторы можно использовать в качестве отдельного устройства, или соединять друг с другом, увеличивая размер сети и усложняя топологию. Возможным вариантом будет шина, звезда, иерархическая звезда (дерево). Кольцевая топология недопустима.

Так как логической обработки сигнала не происходит, данные передаются с использованием всей полосы пропускания. Если не учитывать задержку на хабе (по стандарту IEEE 802.3 менее 3 микросекунд, а в реальности существенно меньше), то концентратор (или повторитель) ничем не отличается по смыслу от сегмента коаксиального кабеля.

В этом есть некоторые плюсы - полная прозрачность перед протоколами более высоких уровней и прямая доступность всех узлов. Но недостатки разделяемой среды то же видны в полной мере. Все устройства, подключенные к сети, построенной на хабах, видят весь сетевой трафик. Данные, адресованные другому узлу, принимаются, анализируются по крайней мере на уровне заголовка кадра, и только после этого отбрасываются.

По скорости можно различить хабы 10baseT и 100baseT. Часто встречаются смешанные конструкции, которые работают на полную скорость только в том случае, если соединены только с оборудованием 100baseT. Последнее легко объяснимо - при разных скоростях на разных портах неизбежно придется каким-то образом обрабатывать данные, и накапливать их в специальном буфере. А это означает резкое усложнение конструкции (вернее так было несколько лет назад).

Надо обратить внимание на следующий момент. В литературе часто встречается разделение повторителей на классы (I и II). И стандарт 802.3u действительно это предусматривает. Различие между ними следующее. Повторители I класса полностью декодируют входящий сигнал, преобразуют его в логическую форму, и передают на активные порты (задержка в районе 0,7 мс). При этом возможно использование нескольких технологий одновременно - например, 100BaseT4, 100BaseTX или 100BaseFX. Повторители II класса восстанавливают форму сигнала без его явного преобразования в логический вид. Соответственно, в этом случае задержка передачи заметно меньше (менее 0,46 мс по стандарту), но можно использовать только один протокол.

Однако в реальной практике встретить концентратор I класса почти невозможно (разве что в музее). Они стали мертворожденным раритетом совместно с 100BaseT4, и ему подобными технологиями.

Назначение и классификация концентраторов

Основное назначение концентраторов (хабов) - это объединение территориально сосредоточенных рабочих мест в рабочую группу. Но вполне возможно использование хабов в качестве ретрансляторов между удаленными сетями или связи нескольких рабочих групп.

Рис. 10.2. Схема применения хабов

Из-за отсутствия в концентраторах каких либо механизмов обеспечения безопасности, гарантированной скорости, их применение рационально только в части сети, где существуют общие требования по этим важным параметрам. Например, неправильным будет соединение при помощи хабов нескольких фирм, или бухгалтерии с отделом нелинейного видеомонтажа.

В каком-то плане хабы можно отнести к устаревшему оборудованию. Действительно, практически по всем техническим показателям они серьезно уступают коммутаторам, и очень близки по цене (дешевле всего на 30-40%). Поэтому, их применение в локальной сети предприятия не имеет смысла - при незначительном увеличении затрат можно получить в десятки (!) раз большую скорость.

Но в домашних или территориальных сетях дело обстоит несколько сложнее. Хабы более надежны в тяжелых условиях эксплуатации, и способны передавать данные на большие расстояния (или по кабелю худшего качества). Поэтому в данной нише им предстоит еще весьма долгая жизнь, окончательно их вытеснит только широкое распространение оптики.

По сложности, можно разделить коцентраторы на следующие классы:

- Начальный уровень. 5-ти или 8-ми портовые концентраторы. Часто имеют порт для подсоединения коаксиального кабеля (BNC), реже - порт AUI. При небольшой стоимости ($30-50) являются простым и дешевым решением для сети небольшого размера.
- Средний уровень. Это 12-ми, 16-ти и 24-х портовые устройства. Имеют 19-ти дюймовое исполнение, BNC или AUI порты. Такое решение позиционируют для построения средних и малых сетей. Однако, в связи с стремительным снижением цен на коммутаторы, вытеснение хабов из этой технической ниши можно считать завершившимся делом.
- Управляемые концентраторы. Их отличает наличие консольного порта RS-232 для управления или сбора статистики с использованием протоколов SNMP/IP или IPX. В настоящее время практически не применяются.
- Хабы 10/100. Обычный хаб может связывать рабочие станции только на одной скорости. Так, стоит в сети, построенной на 100-мегабитных хабах появиться всего одной 10-ти мегабитной сетевой карте, вся сеть начнет работать с этой пониженной скоростью. Это крайне неудобно. Поэтому появились хабы, содержащие коммутатор между 10 и 100 мегабитными шинами. Получилось достаточно

удобная и не дорогая конструкция. Но широкого распространения она просто не успела получить, так как была полностью вытеснена дешевыми неуправляемыми свитчами.

Глава 10

Мосты.

В предыдущем параграфе было показано, что для соединения двух соседних сегментов Ethernet можно применять повторители или концентраторы. Но что делать, если две (или более) сети уже слишком велики для объединения в один коллизионный домен, или, вдобавок, территориально удаленны друг от друга?

Для решения этой задачи применяют мосты (Bridge). Как и повторители, они принимают данные на входящий порт, и передают на исходящий с восстановленными уровнем и формой сигнала. Но на этом сходство заканчивается, и начинаются различия.

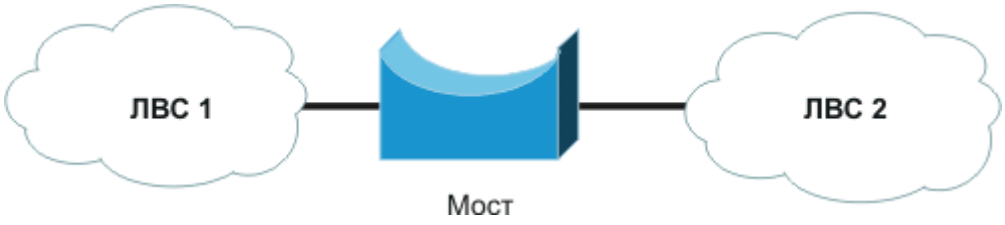

Рис. 10.3. Схема типичного варианта применения моста

Мост принимает входящий кадр в свой буфер, определяет его целостность и адрес (MAC) назначения. При этом каждая половина моста, анализируя поле адреса отправителя, ведет таблицу Ethernet-адресов узлов, находящихся на своей стороне. На другую сторону моста передаются только кадры широковещательной рассылки (Broadcast), и кадры, не имеющие получателя на своей стороне. Таким образом, коллизии не транслируются (как это происходит в повторителях).

Буферизация данных перед их отправкой (store-and-forward) приводит к возникновению большей по сравнению с концентраторами задержки, что несколько снижает скорость работы сети. С другой стороны, количество устройств, которые разделяю между собой физическую среду, снижается. В результате обычно реальная скорость передачи данных возрастает.

Первые мосты были, подобно повторителям, двухпортовыми. Но распространение получила технология 10baseT, построенная на многопортовых хабах, и следовательно, популярность получили многопортовые мосты. Последние приобрели специальное название - коммутатор (switch), которое полностью вытеснило старый термин.

Тем не менее, совсем из сетевого лексикона мосты не исчезли. Так часто стали называть устройства, предназначенные для связи ЛВС по отличной от Ethernet физической среде. Например, по радиоканалу, xDSL, модемной связи, или другими способами. При этом с одной стороны моста кадры Ethernet будут инкапсулированы в какой-либо иной протокол канального уровня, а с другой - восстановлены обратно.

В свете такого использования, надо отметить следующий момент. Мосты не могут выполнять фрагментацию и повторную сборку пакетов более высокого (сетевого) уровня. Это свойство вызывает важное, но не заметное на первый взгляд следствие. Многие модели мостов имеют ограничение по размеру передаваемого кадра, слишком большой может быть отброшен как поврежденный.

Иногда приходится искусственно снижать посредством параметра MTU (Maximum Transmission Unit) размер дейтаграммы IP перед его инкапсуляцией в кадр Ethernet, что бы не превысить допустимый итоговый размер.

Глава 10

Маршрутизаторы.

Можно сказать, что маршрутизаторы (роутеры, routers) - это следующая ступень сетевой иерархии. Упрощенного говоря, их задача - выбор маршрута передачи данных (иначе говоря, объединение разнородных сетей). Соответственно, если мосты для передачи кадров используют адреса физического уровня (MAC), то маршрутизаторы (роутеры) обычно используют IP адреса глобальной сети Интернет.

Для этого им, как минимум, нужно развернуть кадр Ethernet, извлечь из его поля данных дейтаграмму IP, и по ее заголовку направить пакет (возможно, опять упаковав дейтаграмму в кадр Ethernet). Однако, большинство маршрутизаторов работает по еще более сложному алгоритму, используя для передачи данных протоколы следующих уровней модели OSI (TCP, UDP, Novell IPX, AppleTalk II, и другие).

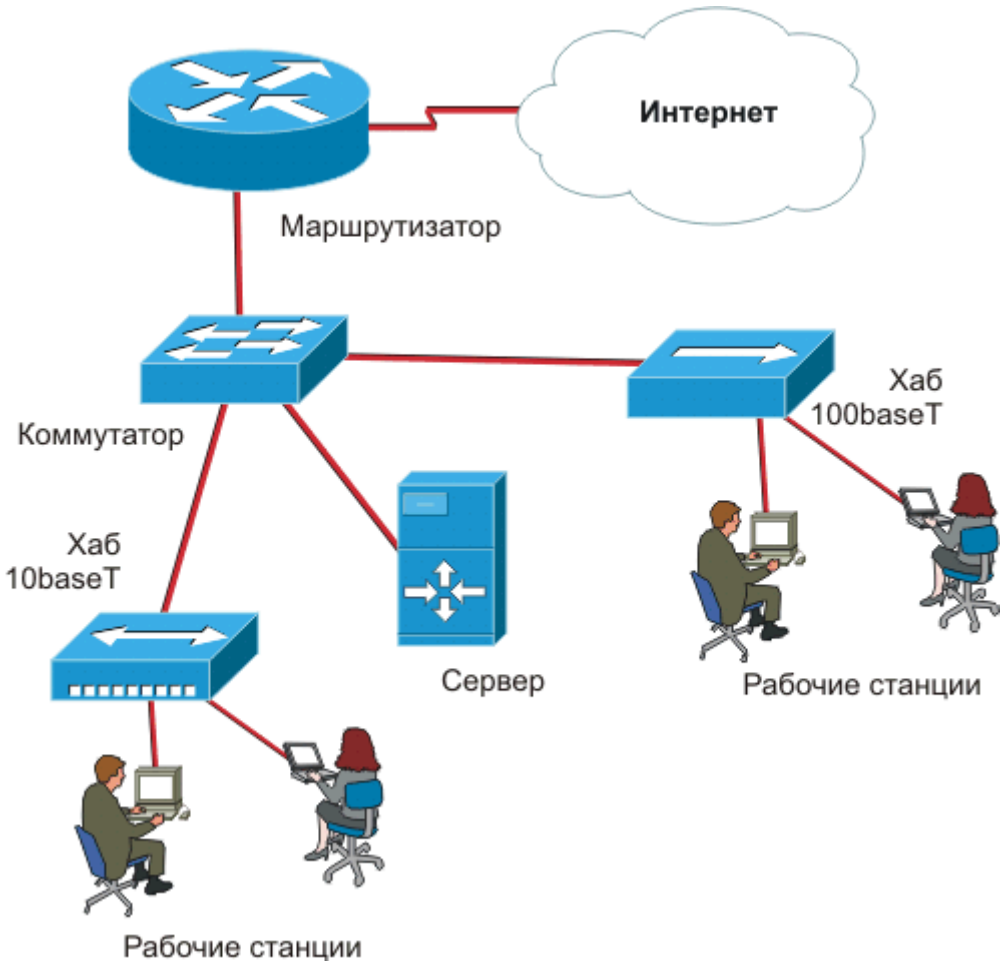

Рис. 10.4. Применение маршрутизатора в корпоративно сети

Подобно повторителям, маршрутизаторы восстанавливают уровень и форму предаваемого сигнала. Так же, как и мосты, они не передают адресату коллизии или поврежденные кадры, и из-за буферизации имеют задержку при передаче. Но в отличие от повторителей, мостов и коммутаторов, маршрутизаторы изменяют все передаваемые кадры Ethernet (вернее сказать, они их разбирают, и формируют заново по определенным правилам).

Но даже на этом функциональные возможности роутеров не заканчиваются. В зависимости от типа, программного обеспечения, они могут поддерживать очень сложные и не типовые функции. Например, подсчет трафика, авторизацию пользователей, ведение статистики, и т.п.

Так же очень сильно они могут отличаться по мощности. Наиболее простой и недорогой вариант - персональный компьютер с несколькими (или даже одной) сетевыми адаптерами. Программное обеспечение может быть любым, но наиболее распространены клоны unix - linux или FreeBSD, которым обычно достаточно даже устаревших "486" процессорных блоков.

Кроме "самосборных" маршрутизаторов на рынке представлена масса специализированных устройств - от простейших (от $100), до мощных систем (начиная с нескольких, и заканчивая многими сотнями тысяч долларов), способных определять маршруты для значительных потоков данных.

Несмотря на большие функциональные возможности, и сравнительно не большую скорость, маршрутизаторы практически не применяются в локальных сетях. В них просто нет надобности, а большие потенциальные возможности обычно оборачиваются малой надежностью и сложностью в эксплуатации. Поэтому применять маршрутизацию желательно как можно реже, только в случаях, когда от нее невозможно отказаться.

Классический пример их использования в простых провайдинговых схемах - граница между локальной сетью и Интернет. Вот незаменимые преимущества маршрутизаторов в этой технологической нише:

- обеспечивает более высокий уровень локализации трафика, чем мост, так как позволяет фильтровать широковещательные кадры, не имеющие корректных адресов назначения (нет угрозы бродкастовых штормов);
- развитые возможности защиты от несанкционированного доступа из-за возможности использования фильтрации трафика на более высоких уровнях модели OSI (сетевом и транспортном);
- сеть, части которой соединены через маршрутизаторы, не имеют ограничений на число узлов;
- обеспечивают возможность настройки параметров качества (Quality of Service, QoS), настройку системы приоритетов, ширины полосы пропускания для каждого типа трафика;
- поддерживают основные протоколы динамической маршрутизации, такие как RIP, OSPF, BGP-4, IPX RIP/SAP, могут связывать несколько IP сетей одновременно;

Последняя возможность очень важна для построения действительно больших телекоммуникационных сетей со сложной, и часто многосвязной топологией. При этом задача максимально эффективной и быстрой доставки отправленного пакета решается совсем не просто. Распространены два основных алгоритма выбора наиболее выгодного пути и способа: RIP и OSPF.

При использовании протокола RIP, основным критерием выбора является минимальное число сетевых устройств между устройством-отправителем и получателем. Технически это просто реализуется, не требует существенных вычислительных ресурсов, и достаточно часто применяется в простых сетях.

Однако, понятно, что лучше 10 ретрансляторов на оптоволокне, чем одно модемное соединение. Поэтому при использовании RIP на практике появляется много дополнительных ограничений, серьезно затрудняющих управление.

OSPF лишен этих недостатков, поскольку который кроме числа "хопов" учитывает производительности сети, задержки при передаче пакета и т.п. критерии. Оборотной стороной, как обычно, является относительно высокая сложность управления, и требовательность к аппаратным ресурсам.

Производительность маршрутизаторов принято измерять в PPS (Packets Per Second), т.е. количество маршрутизируемых пакетов в секунду. Рассчитать возможную скорость передачи данных легко по следующей формуле:

Скорость = N/(K)*8*S ,

Где:
K - Коэффициент поправки на реальные условия (примерно около 5);
S - размер пакета (для Интернет - ~500, для ЛВС - ~1500, для VOIP - ~100).

Например, для 3620 Cisco получаем 40000/5*500*8=32 Mbit/s

Однако нужно учитывать, что access листы, роутмапы, firewallы, динамический роутинг, и другие дополнительные функции способны снизить реальную скорость маршрутизации в несколько раз.

В заключение параграфа надо сказать, что к рассмотрению роутеров мы еще вернемся в следующих главах, при рассмотрении практической маршрутизации в домашних (территориальных) сетях.

Глава 10

Коммутаторы (Свитчи).

Разделяемая среда передачи данных Ethernet была и остается причиной обвинений этой технологии в недостаточной стабильности и надежности. Отчасти это действительно так - алгоритм CSMA/CD не обманешь никакими программными решениями. И для преодоления этих недостатков фирма Kalpana (впоследствии купленная Cisco) в 1990 предложила технологию коммутации сегментов Ethernet. Таким образом, разделяемая среда (домен коллизий) не ограничивалась (с помощью мостов или маршрутизаторов), а полностью исчезала.

Сказать, что это было принципиальное логическое изобретение, нельзя. Работа основывалось на простом, но в то время труднодостижимом технологическом фундаменте - параллельной обработке поступающих кадров на разных портах (мосты обрабатывают кадры последовательно, кадр за кадром). Это особенность позволила коммутаторам Kalpana передавать кадры независимо между каждой парой портов, и реализовать на практике привлекательную идею отказа от разделяемой среды.

Технологии Ethernet очень повезло, что коммутаторы появились раньше, чем начала применяться технология ATM. У пользователей вовремя оказалась в наличии достойная альтернатива, позволяющая получить существенный рост качества сети с небольшими затратами. Для этого требовалось лишь заменить концентраторы на коммутаторы, или просто добавить последние в растущую сеть для разделения сегментов. Огромное количество уже установленного оборудования конечных узлов, кабельных систем, повторителей и концентраторов сохранялось, что давало колоссальную экономию по сравнению с переходом на какую-либо новую технологию (например, ATM).

Коммутаторы (подобно мостам) прозрачны для протоколов сетевого уровня, маршрутизаторы их "не видят". Это позволило не менять основную схему работы сетей между собой.

Более того, в стремительном распространении коммутаторов не последнюю роль сыграла простота их настройки и установки. По умолчанию (без использования дополнительных возможностей) это самообучающееся устройство, его не обязательно конфигурировать. Достаточно правильно подключить кабельную систему к свитчу, а дальше он сможет

работать без вмешательства администратора сети, и при этом сравнительно эффективно выполнять поставленную задачу.

В общем, сегодня можно с полной уверенностью сказать, что коммутаторы - это самый мощный, универсальный, удобный для ЛВС класс оборудования. В простейшем случае (как было показано выше) это многопортовый мост Ethernet. Но развитие технологии внесло так много изменений в их свойства, что подчас основной принцип работы тяжело увидеть за нагромождением полезнейших технических возможностей.

Техническая реализация коммутаторов.

Техническая основа работы коммутатора достаточно проста, и может быть выражена одним длинным предложением. Кадр, которые попадает на его вход (source port), направляется не на все активные порты (как это делает концентратор), а только на тот, к которому подключено устройство с MAC-адресом, совпадающим с адресом назначения кадра (destination port).

Соответственно, первый вопрос, который приходится решать - соответствие портов коммутатора подключенным устройствам (вернее, их MAC-адресам). Для работы используется специальная таблица соответствия (content-addressable memory, CAM), которую коммутатор формирует в процессе "самообучения" по следующему принципу: стоит порту получить ответ от устройства с физическим адресом X, как в CAM таблице появляется соответствующая строчка соответствия.

Кадры с адресом назначения (source address, SA), имеющимся в таблице, направляются на соответствующий порт. При этом кадр, предназначенный всем узлам, или имеющий неизвестный коммутатору адрес назначения (destination address, DA), направляется на все активные порты. В процессе работы физические адреса подключенного оборудования могут меняться. При этом в таблице появляется новая запись. Если в ней отсутствует свободное место, стирается самая старая запись (принцип вытеснения).

Так как скорость выборки нужного адреса напрямую зависит от размера CAM таблицы, неиспользованные в течении продолжительного промежутка времени записи автоматически удаляются.

Однако такой упрощенный алгоритм жестко (без изменений) действует только в неуправляемых коммутаторах (Dumb). Это недорогие, простые устройства, которые успешно вытесняют хабы из ниши простейших сетей. Как правило они имеют небольшое количество портов, "офисное" исполнение, и не высокие технические характеристики. Возможность управления администратором отсутствует.

Следующей ступенью развития стали настраиваемые коммутаторы (Smart). В них, используя порт RS-232, обычный Ethernet, или даже простейшую микро-клавиатуру, администратор может менять многие важные конфигурационные параметры, которые считываются затем только один раз (при загрузке). Например, таким образом можно блокировать механизм "самообучения" (составлять статическую таблицу соответствия портов MAC-адресам), устанавливать фильтрацию, виртуальные сети, задавать скорость и многое другое.

Но самые большие возможности имеют управляемые коммутаторы (Intelligent). Они имеют интерфейс к полноценному процессору (точнее, компьютеру, поскольку он имеет и свою память), который позволяет контролировать работу и изменять параметры

устройства без перезагрузки. Так же появляется возможность в реальном времени наблюдать за проходящими пакетами, считать проходящий трафик, и т.п.

Однако, несмотря на огромное различие в уровне возможностей (и стоимости), общий принцип остается неизменным. Все узлы оказываются соединенными "отдельными" каналами с полной полосой пропускания (если нет одновременного обращения нескольких устройств к одному), и могут работать не подозревая о существовании друг друга. Единственную опасность для коммутируемой сети представляют "бродкастовые" штормы, т. е. случаи лавинообразно нарастающей перегрузки сети широковещательными (бродкастовыми) кадрами. Однако, во-первых, это возможно только в большох сетях (несколько сотен узлов), во-вторых, большинство управляемых коммутаторов позволяет легко решать и эту проблему за счет разделения одной большой сети на несколько виртуальных.

Соответственно, базовые свойства (и ограничения) Ethernet (как разделяемой среды передачи данных) не применимы к сети, построенной с использованием коммутаторов. Коллизии отсутствуют, нет физического обоснования понятия максимальной длины линии, и максимального количества подключенных устройств.

Например, реально могут использоваться оптоволоконные линии, передающие кадры Ethernet на сотни километров, а локальные сети могут объединять сотни рабочих станций или серверов.

Классификация коммутаторов.

Для определения порта (или портов) назначения, процессору коммутатора необходимо для анализа иметь доступ к заголовку кадра Ethernet. Соответственно, эти данные нужно принять в буфер. Отсюда вытекает различие коммутаторов по способу продвижения кадра:

- на лету (cut-through);
- с буферизаций (Store-and-Forward).

При коммутации "на лету", коммутатор может не помещать приходящие кадры в буфер целиком. Запись их целиком происходит только в случае, когда нужно согласовать скорости передачи, занята шина, или порт назначения. Таким образом, при большом объеме трафика большая часть данных будет все равно в той или иной степени буферизироваться.

Иначе говоря, коммутатор лишь анализирует адрес назначения в заголовке пакета, и в соответствии с CAM-таблицей (время задержки от 10-40 мкс) направляет кадр в соответствующий порт. Штатной является ситуация, когда кадр еще целиком не поступил на входной порт, а его заголовок уже передается через выходной.

При методе полной буферизации (Store-and-Forward) кадр записывается целиком, а лишь затем процессор порта принимает решение о передаче (или фильтрации). Такой путь имеет некоторые недостатки (большое время задержки), и существенные достоинства, например, уничтожение испорченного кадра, поддержка разнородных сетей. Большая часть современных коммутаторов поддерживает именно такой режим работы.

Наиболее сложные и дорогие модели имеют возможность автоматической смены механизма работы коммутатора (адаптацию). В зависимости от объема трафика,

количества испорченных кадров, и некоторых других параметров может быть использован один из описанных режимов.

Кроме способа продвижения кадров, коммутаторы можно разделить на группы по внутренней логической архитектуре.

- коммутационная матрица;
- многовходвая разделяемая память;
- общая шина.

Коммутационная матрица. Наиболее быстрый способ, который был реализован в первом промышленном коммутаторе. После анализа заголовка входящего кадра процессором порта, в соответствии с таблицей коммутации, в начало кадра добавляется номер порта назначения. Затем кадр (вернее сказать, номер порта назначения) попадал в двухмерную матрицу логических переключателей, каждый из которых управлялся определенным битом номера порта назначения.

Коммутационная матрица пытается установить путь до порта назначения. Если это возможно, последовательно проходя через переключатели, кадр оказывается в нужном исходящем порту.

Если нужный исходящий порт занят (например, соединен с другим входящим портом), кадр остается в буфере входного порта, а процессор ожидает возможности образования коммутационной матрицей нужного пути.

Важной особенностью является то, что коммутируются физические каналы. Таким образом, если несколько кадров должны пройти на один и тот же порт, или через один "общий" переключатель матрицы, сделать это они могут только последовательно. Кроме этого, к недостаткам можно отнести быстро нарастающую с увеличением числа портов сложность. По сути, можно сказать, что решение плохо масштабируемо, и сейчас применяется очень редко (хотя еще есть варианты использования многоступенчатых коммутаторов).

Многовходовая разделяемая память. В этом случае входные и выходные блоки соединяются через общую память, подключением которой к блокам которой управляет специальный менеджер очередей выходных портов. Он же организует в памяти несколько (обычно по числу портов) очередей данных.

Входные блоки передают менеджеру запросы на запись данных (части кадров) в очередь нужного исходящего порта.

Системы такого типа достаточно сложны, требуют дорогой быстродействующей памяти, но не обладают при этом серьезными преимуществами перед более простой шинной архитектурой. Поэтому, широкого практического применения системы с разделяемой памятью не нашли.

Архитектура с общей шиной. Название говорит само за себя - для связи процессоров портов используется одна шина. Для сохранения высокой производительности ее скорость должна быть по крайней мере в C/2 (где C - сумма скоростей всех портов) раз больше, чем скорость поступления данных в порт коммутатора.

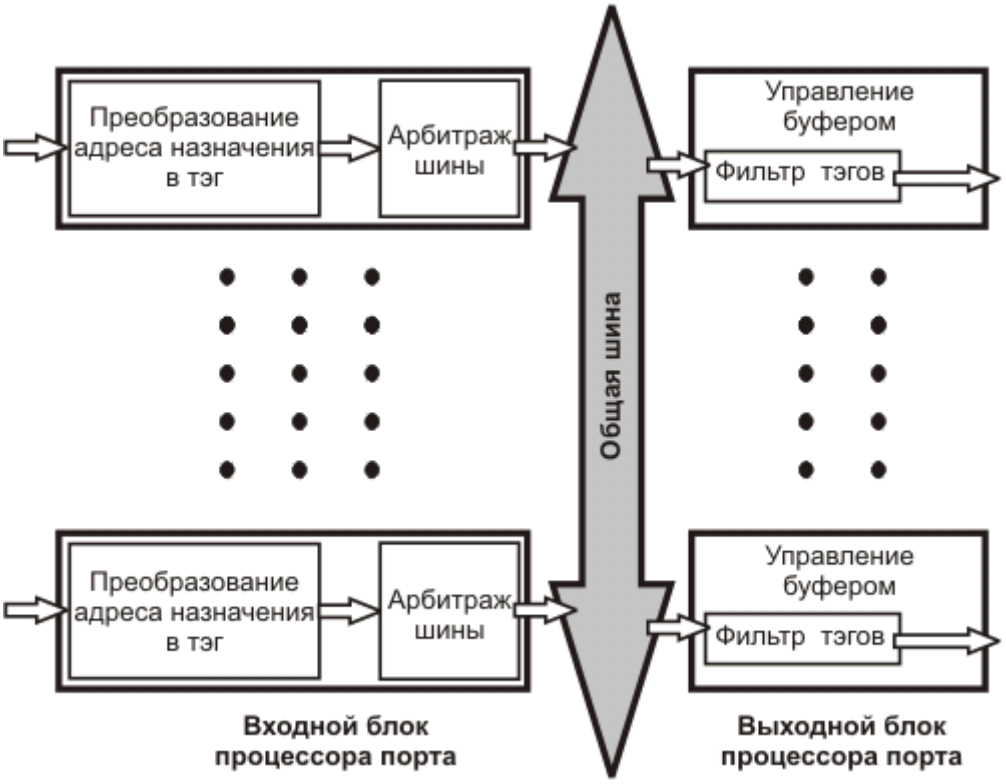

Рис. 10.5. Коммутация с использованием общей шины

Кроме этого, много зависит от способа передачи данных по шине. Понятно, что кадр целиком передавать нежелательно, так как в это время остальные порты будут простаивать. Что бы обойти это ограничение, обычно применяют метод, сильно похожий на ATM. Данные разбиваются на небольшие блоки (по несколько десятков байт), и передаются "почти" параллельно сразу между несколькими портами.

Таким образом, эта архитектура реализует метод временной коммутации… частей кадров (можно назвать их по аналогии с ATM ячейками). Решение легко масштабируется, достаточно просто, надежно, и в настоящий момент безусловно доминирует на рынке.

Еще один признак, по которому можно классифицировать коммутаторы - это область применения. С некоторой долей условности, можно выделить:

- настольные коммутаторы;
- коммутаторы для рабочих групп.
- магистральные коммутаторы;

Настольные коммутаторы. Предназначены для работы с небольшим числом пользователей, и могут служить хорошей заменой концентраторов 10/100Base-T. Обычно имеют 8-16 портов, небольшие габариты, настольное или "настенное" исполнение. Такие коммутаторы, как правило, не имеют возможности управления, поэтому просты в установке и обслуживании (хотя ценой отказа он некоторых полезных возможностей).

Стоимость на один порт составляет обычно менее $15-20, что обеспечивает их широкое применение самого широкого круга задач. Наиболее типичным образцом недорогих настольных моделей можно считать Surecom 808X или Compex 2208.

Коммутаторы для рабочих групп. Используются главным образом для объединения в единую сеть настольных коммутаторов или концентраторов 10/100Base-T, и ее соединения с магистральной СПД. Для этого используется объемная таблица маршрутизации (до нескольких десятков тысяч MAC-адресов на коммутатор), развитые средства фильтрации, построения виртуальных сетей, мониторинга трафика. Обязательно присутствует возможность управления (обычно удаленного), распространен протокол SNMP.

Такие коммутаторы часто имеют порты 1000baseT (или возможность создания транковых соединений) для подключения серверов, или нескольких свитчей между собой. Дополнительно могут применяться встроенные оптоволоконные модули, или другие конвертеры физических сред.

Стоимость колеблется в диапазоне $30-100 за порт 10/100baseT. К нижнему порогу этой группу можно отнести Surecom EP-716X, SVEC FD1310, а к верхнему такие популярные на сегодня модели, как 3com 4400 или Cisco 2950.

Магистральные коммутаторы. Служат для соединения ЛВС в сетей передачи данных. Обычно это сложные и мощные конструкции, часто модульные. Имеют массу дополнительных возможностей настройки (вплоть до маршрутизации на III уровне по модели OSI), резервные источники питания, горячую замена модулей, обязательную поддержку приоритезации, протокола Spanning Tree, 802.1q, и других функций.

Стоимость магистральных коммутаторов в расчете на один порт составляет $100 - $1000. Наиболее подходящим примером оборудования данного класса могут служить тяжелые коммутаторы серии Cisco Catalyst.

Глава 10

Технические параметры коммутаторов.

К основным техническим параметрам, которыми можно оценить коммутатор, построенный с использованием любой архитектуры, является скорость фильтрации (filtering) и скорость продвижения (forwarding).

Скорость фильтрации определяет количество кадров в секунду, с которыми коммутатор успевает проделать следующие операции:

- прием кадра в свой буфер;
- нахождения порта для адреса назначения кадра в адресной таблице;
- уничтожение кадра (порт назначения совпадает с портом-источником).

Скорость продвижения, по аналогии с предыдущим пунктом, определяет количество кадров в секунду, которые могут быть обработаны по следующему алгоритму:

- прием кадра в свой буфер,
- нахождения порта для адреса назначения кадра;
- передача кадра в сеть через найденный (по адресной таблице соответствия) порт назначения.

По умолчанию считается, что эти показатели измеряются на протоколе Ethernet для кадров минимального размера (длиной 64 байта). Так как основное время занимает анализ заголовка, то чем короче передаваемые кадры, тем более серьезную нагрузку они создают на процессор и шину коммутатора.

Следующими по значимости техническими параметрами коммутатора будут:

- пропускная способность (throughput);
- задержка передачи кадра.
- размер внутренней адресной таблицы.
- размер буфера (буферов) кадров;
- производительность коммутатора;

Пропускная способность измеряется количеством данных, переданных через порты в единицу времени. Естественно, что чем больше длина кадра (больше данных прикреплено к одному заголовку), тем больше должна быть пропускная способность. Так, при типичной для таких устройств "паспортной" скорости продвижения в 14880 кадров в секунду, пропускная способность составит 5.48 Мб/с на пакетах по 64 байта, и ограничение скорости передачи данных будет наложено коммутатором.

В то же время, при передаче кадров максимальной длины (1500 байт), скорость продвижения составит 812 кадров в секунду, а пропускная способность - 9,74 Мб/с. Фактически, ограничение на передачу данных будет определяться скоростью протокола Ethernet.

Задержка передачи кадра означает время, прошедшее с момента начала записи кадра в буфер входного порта коммутатора, до появления на его выходном порту. Можно сказать, что это время продвижения единичного кадра (буферизация, просмотр таблицы, принятие решения о фильтрации или продвижении, и получение доступа к среде выходного порта).

Величина задержки очень сильно зависит от способа продвижения кадров. Если применяется метод коммутации "на лету", то задержки невелики и составляют от 10 мкс до 40 мкс, в то время как при полной буферизации - от 50 мкс до 200 мкс (в зависимости от длины кадров).

В случае большой загруженности коммутатора (или даже одного из его портов), получается, что даже при коммутации "на лету" большая часть входящих кадров вынужденно буферизируется. Поэтому, наиболее сложные и дорогие модели имеют возможность автоматической смены механизма работы коммутатора (адаптацию) в зависимости от нагрузки и характера трафика.

Размер адресной таблицы (CAM-таблицы). Определяет максимальное количество MAC-адресов, которые содержатся в таблице соответствия портов и MAC-адресов. В технической документации обычно приводится на один порт, как число адресов, но иногда бывает, что указывается размер памяти под таблицу в килобайтах (одна запись занимает не менее 8 кб, и "подменить" число весьма выгодно недобросовестному производителю).

Для каждого порта CAM-таблица соответствия может быть разной, и при ее переполнении наиболее старая запись стирается, а новая - заносится в таблицу. Поэтому при превышении количества адресов сеть может продолжить работу, но при этом сильно

замедлиться работа самого коммутатора, а подключенные к нему сегменты будут загружены избыточным трафиком.

Раньше встречались модели (например, 3com SuperStack II 1000 Desktop), в которых размер таблицы позволял хранить один или несколько адресов, из-за чего приходилось относиться очень внимательно к дизайну сети. Однако, сейчас даже самые дешевые настольные коммутаторы имеют таблицу из 2-3К адресов (а магистральные еще больше), и этот параметр перестал быть узким местом технологии.

Объем буфера. Он необходим коммутатору для временного хранения кадров данных в тех случаях, когда нет возможности сразу их передать на порт назначения. Понятно, что трафик неравномерен, всегда есть пульсации, которые нужно сглаживать. И чем больше объем буфера, тем большую нагрузку он может "принять на себя".

Простые модели коммутаторов имеют буферную память в несколько сотен килобайт на порт, в более дорогих моделях это значение достигает нескольких мегабайт.

Производительность коммутаторов. Прежде всего, надо отметить, что коммутатор - сложное многопортовое устройство, и просто так, по каждому параметру в отдельности, нельзя оценить его пригодность к решению поставленной задачи. Существует большое количество вариантов трафика, с разной интенсивностью, размерами кадров, распределением по портам, и т.п. Общей методики оценки (эталонного трафика) до сих пор нет, и используются разнообразные "корпоративные тесты". Они достаточно сложны, и в данной книге придется ограничиться только общими рекомендациями.

Идеальный коммутатор должен передавать кадры между портами с той же самой скоростью, с которой их генерируют подключенный узлы, без потерь, и не вносить дополнительных задержек. Для этого внутренние элементы коммутатора (процессоры портов, межмодульная шина, центральный процессор и т.п.) должны справляться с обработкой поступающего трафика.

В то же время, на практике есть много вполне объективных ограничений на возможности свитчей. Классический случай, когда несколько узлов сети интенсивно взаимодействуют с одним сервером, неизбежно вызовет уменьшение реальной производительности из-за фиксированной скорости протокола.

На сегодня производители вполне освоили производство коммутаторов (10/100baseT), даже очень дешевые модели имеют достаточную пропускную способность, и достаточно быстрые процессоры. Проблемы начинаются, когда нужно применять более сложные методы ограничений скорости подключенных узлов (обратного давления), фильтрации, и других протоколов, рассмотренных ниже.

В заключение, нужно сказать, что лучшим критерием по-прежнему остается практика, когда коммутатор показывает свои возможности в реальной сети.

Дополнительные возможности коммутаторов.

Как уже говорилось выше, современные коммутаторы имеют настолько много возможностей, что обычная коммутация (казавшаяся технологическим чудом десять лет назад) уходит на второй план. Действительно, быстро, и относительно качественно, коммутировать кадры умеют модели стоимостью от $50 до $5000. Различие идет именно по дополнительным возможностям.

Понятно, что наибольшее количество дополнительных возможностей имеют управляемые коммутаторы. Далее в описании будут специально выделены опции, которые обычно нельзя корректно реализовать на настраиваемых коммутаторах.

Соединение коммутаторов в стек. Эта дополнительная опция одна из наиболее простых, и широко используемых в больших сетях. Ее смысл - соединить несколько устройств скоростной общей шиной для повышения производительности узла связи. При этом иногда могут быть использованы опции единого управления, мониторинга и диагностики.

Надо заметить, что не все вендоры используют технологию соединения коммутаторов при помощи специальных портов (стекирование). В этой области все большее распространение получают линии Gigabit Ethernet, или при помощи группировки нескольких (до 8) портов в один канал связи.

Протокол покрывающего дерева (Spanning Tree Protocol, STP). Для простых ЛВС соблюдать в процессе эксплуатации правильную топологию Ethernet (иерархическая звезда) не сложно. Но при большой инфраструктуре это становится серьезной проблемой - неправильная кроссировка (замыкание сегмента в кольцо) может привести к остановке функционирования всей сети или ее части. Причем найти место аварии может быть совсем не просто.

С другой стороны, подобные избыточные связи часто удобны (многие транспортные сети передачи данных построены именно по кольцевой архитектуре), и могут сильно повысить надежность - при наличии корректного механизма обработки петель.

Для решения этой задачи используется Spanning Tree Protocol (STP), при котором коммутаторы автоматически создают активную древовидную конфигурацию связей, находя ее с помощью обмена служебными пакетами (Bridge Protocol Data Unit, BPDU), которые помещаются в поле данных кадра Ethernet. В результате, порты, на которых замыкаются петли, блокируются, но могут быть автоматически включены в случае разрыва основного канала.

Таким образом, технология STA обеспечивает поддержку резервных связей в сети сложной топологии, и возможность ее автоматическую изменения без участия администратора. Такая возможность более чем полезна в больших (или распределенных) сетях, но в силу своей сложности редко используется в настраиваемых коммутаторах.

Способы управления входящим потоком. Как уже отмечалось выше, при неравномерной загрузке коммутатора он просто физически не сможет пропустить через себя поток данных на полной скорости. Но просто отбрасывать лишние кадры по понятным причинам (например разрыв TCP сессий) крайне не желательно. Поэтому приходится использовать механизм ограничения интенсивности передаваемого узлом трафика.

Возможно два способа - агрессивный захват среды передачи (например, коммутатор может не соблюдать стандартные временные интервалы). Но этот способ годится только для "общей" среды передачи, редко используемой в коммутируемом Ethernet. Этим же недостатком обладает метод обратного давления (backpressure), при котором узлу передаются фиктивные кадры.

Поэтому на практике востребована технология Advanced Flow Control (описанна в стандарте IEEE 802.3x), смысл которой в передаче коммутатором узлу специальных кадров "пауза".

Фильтрация трафика. Часто бывает очень полезно задавать на портах коммутатора дополнительных условий фильтрации кадров входящих или исходящих кадров. Таким образом можно ограничивать доступ определенных групп пользователей к определенным сервисам сети, используя MAC-адрес, или тэг виртуальной сети.

Как правило, условия фильтрации записываются в виде булевских выражений, формируемых с помощью логических операций AND и OR.

Сложная фильтрация требует от коммутатора дополнительной вычислительной мощности, и при ее нехватке может существенно снизить производительность устройства.

Возможность фильтрации очень важна для сетей, в которых конечными пользователями выступают "коммерческие" абоненты, поведение которых невозможно регулировать административными мерами. Так как они могут предпринимать несанкционированные деструктивные действия (например, подделывать IP или MAC адрес своего компютера), желательно предоставить для этого минимум возможностей.

Коммутация третьего уровня (Layer 3). Из-за быстрого роста скоростей, и широкого применения коммутаторов, на сегодня образовался видимый разрыв между возможностями коммутации и классической маршрутизацией при помощи универсальных компьютеров. Наиболее логично в этой ситуации дать управляемому коммутатору возможность анализировать кадры на третьем уровне (по 7-ми уровневой модели OSI). Такая упрощенная маршрутизация дает возможность значительно поднять скорость, более гибко управлять трафиком большой ЛВС.

Однако в транспортных сетях передачи данных применение коммутаторов пока очень ограничено, хотя тенденция к стиранию их отличий от маршрутизаторов по возможностям прослеживается достаточно явно.

Управление и возможности мониторинга. Обширные дополнительные возможности подразумевают развитые и удобные средства управления. Ранее простые устройства могли управляться несколькими кнопками через небольшой цифровой индикатор, или через консольный порт. Но это уже в прошлом - последнее время выпускаются коммутаторы с управлением через обычный порт 10/100baseT при помощи Telnet'a, Веб-браузера, или по протоколу SNMP. Если первые два способа по большому счету являются лишь удобным продолжением обычных стартовых настроек, то SNMP позволяет использовать коммутатор как поистине универсальный инструмент.

Для Etherenet интересны только его расширения - RMON и SMON. Ниже описан RMON-I, кроме него существует RMON-II (затрагивающий более высокие уровни OSI). Более того, в свитчах "среднего уровня" как правило, реализованы только группы RMON 1-4 и 9.

Принцип работы следующий: RMON-агенты на свитчах шлют информацию на центральный сервер, где специальное программное обеспечение (например, HP OpenView) обрабатывает информацию, представляя ее в удобном для администрирования виде.

Причем процессом можно управлять - удаленным изменением настроек привести работу сети в норму. Кроме мониторинга и управления, при помощи SNMP можно строить систему биллинга. Пока это выглядит несколько экзотично, но примеры реального использования данного механизма уже есть.

Стандарт RMON-I MIB описывает 9 групп объектов:

1. Statistics - текущие накопленные статистические данные о характеристиках кадров, количестве коллизий, ошибочных кадров (с детализацией по типам ошибок) и т.п.
2. History - статистические данные, сохраненные через определенные промежутки времени для последующего анализа тенденций их изменений.
3. Alarms - пороговые значения статистических показателей, при превышении которых агент RMON генерирует определенное событие. Реализация этой группы требует реализации группы Events - события.
4. Host - данные о хостах сети, обнаруженных в результате анализа MAC-адресов кадров, циркулирующих в сети.
5. Host TopN - таблица N хостов сети, имеющих наивысшие значения заданных статистических параметров.
6. Traffic Matrix - статистика о интенсивности трафика между каждой парой хостов сети, упорядоченная в виде матрицы.
7. Filter - условия фильтрации пакетов; пакеты, удовлетворяющие заданному условию, могут быть либо захвачены, либо могут генерировать события.
8. Packet Capture - группа пакетов, захваченных по заданным условиям фильтрации.
9. Event - условия регистрации событий и оповещения о событиях.

Более подробное рассмотрение возможностей SNMP потребует не меньшего объема, чем данная книга, поэтому будет целесообразно остановиться на этом, весьма общем описании этого сложного, но мощного инструмента .

Виртуальные сети (Virtual Local-Area Network, VLAN). Пожалуй, это наиболее важная (особенно для домашних сетей), и широко используемая возможность современных коммутаторов. Надо отметить, что существует несколько принципиально отличных способов построения виртуальных сетей с помощью коммутаторов. В связи с большим значением для Ethernet-провайдинга, ее развернутое описание технологии будет сделано в одной из следующих глав.

Краткий же смысл - средствами коммутаторов (2 уровня модели OSI) сделать несколько виртуальных (независимых друг от друга сетей) на одной физической ЛВС Ethernet, предоставив возможность центральному маршрутизатору управлять портами (или группами портов) на отдаленных коммутаторах. Что собственно и делает VLAN очень удобным средством для оказания услуг передачи данных (провайдинга).

Глава 10

Коммутаторы 3-го уровня.

Технический прогресс двух последних лет не разочаровал поклонников коммутируемого Fast Ethernet. После того, как производители Китая освоили массовый выпуск свитч-чипов стоимость коммутаторов упала почти до уровня упаковки. Действительно, сносный

неуправляемый 8-ми портовый коммутатор можно купить дешевле $40. С хорошей упаковкой, документацией, и годовой гарантией.

Поползли вниз и цены на профессиональные управляемые модели. Все, что положено делать "классическому" коммутатору уже имеют модели дешевле $400 за 24 порта. Поэтому можно сказать, что производители коммутаторов в последние несколько лет начали своеобразную "гонку уровней" - ведь не только производителям процессоров нужны четкие и простые ориентиры (типа гигагерцев) для привлечения покупателей. (попытка сыграть на мощности матрицы коммутации провалилась с массовым выходом неблокируемых моделей).

Прогресс пошел по вполне очевидным путем - ведущие производители не захотели соревноваться ценой с устройствами "made in china", и перевели острие технологической моды на усложнение коммутаторов в области расширения их функций за счет возможностей следующих уровней по модели OSI.

И сейчас можно видеть в продаже сравнительно недорогие модели 3-го и 4-го уровней. В них видят что-то вроде универсального средства решения всех проблем сетей - от существенного увеличения производительности до обеспечения конфиденциальности трафика.

В принципе, такую постановку вопроса нельзя считать совсем неверной - хороший коммутатор L3 действительно способен кардинально изменить возможности управления сетью. Но применение теории к реальности (да еще Российской) никогда не было простым. Поэтому вопросов с уровнями выходит много…

Немного теории для тех, кто ее подзабыл. Если сузить поле применения стандартов до конкретной реальности современных бюджетных сетей (не использующих что-либо типа SDH или ATM), то уровень 2 (по семиуровневой модели OSI) соответствует кадрам Ethernet. Соответственно их передвижение происходит согласно MAC-адресам, известных CAM-таблицам коммутаторов. Свитчи, которые "не знают" ничего выше по стеку протоколов называются коммутаторами 2-го уровня.

При этом они могут производить весьма сложные операции. Например, ставить и убирать метки VLAN, распознавать приоритеты (QoS), устанавливать кадры в очереди, определять атаки, считать Ethernet-трафик, шейпить его, фильтровать по номерам портов, и т.п. Классическим типом "продвинутого" L2 можно считать несколько устаревшие на сегодня 3com SuperStack 3300 или Catalyst 2924. Следующие модели этих брендов (например 3com SuperStack 4400 или Catalyst 2950) уже имеют те или иные возможности следующих уровней.

Соединять разные сети Ethernet (т.е. реальные и виртуальные сети 2-го уровня) должны маршрутизаторы, которые обрабатывают данные на 3-м уровне (IP пакетов). При этом заголовки IP идут по сети Ethernet в поле данных, и обычным коммутаторам 2-го уровня недоступны.

Такая технология сложилась из-за того, что традиционно сети Ethernet соединялись друг с другом при помощи иной (не Ethernet) канальной средой передачи данных (WAN). Например Frame Relay, X.25, ATM, G.703, и т.п. Для преобразования данных была нужна гибкость, универсальность, сложный софт, и... хватало небольшой скорости.

Когда сети Ethernet "выросли", внедрились в "магистральные" ниши, то необходимость в таком подходе отпала, и даже более того, стала мешать (как и любая избыточность возможностей). Можно сказать, что очень к месту появились коммутаторы 3-го уровня, способные в добавление к обычным функциям маршрутизировать трафик между портами на IP-уровне. Быстро, но с весьма ограниченными возможностями (как правило нельзя подсчитать трафик, построить сложные фильтры, добавить скрипты, NAT, и т.п.). Хотя конечно есть и монстры типа Catalyst 6509...

Вроде бы почти финал длинной истории L3… Но она еще не совсем закончена. Так, сначала различали маршрутизирующую коммутацию, коммутация потоков и коммутирующую маршрутизацию. Эти термины сейчас можно считать в некотором роде анахронизмом, но корни той же MPLS растут из них, и в дальнейшем смогут сильно изменить дизайн сетей. Но это уже лежит далеко за рамками рассматриваемой темы.

Конечно, о серьезных операторских или корпоративных сетях речь не идет. Можно сказать, что там коммутаторы 3-го и последующих уровней уже прошлый день, и речь идет скорее о внедрении технологий типа MPLS. Но посмотрим, как можно применить коммутаторы 3-го уровня в небольшой или средней бюджетной сети?

Возьмем условную схему сети.

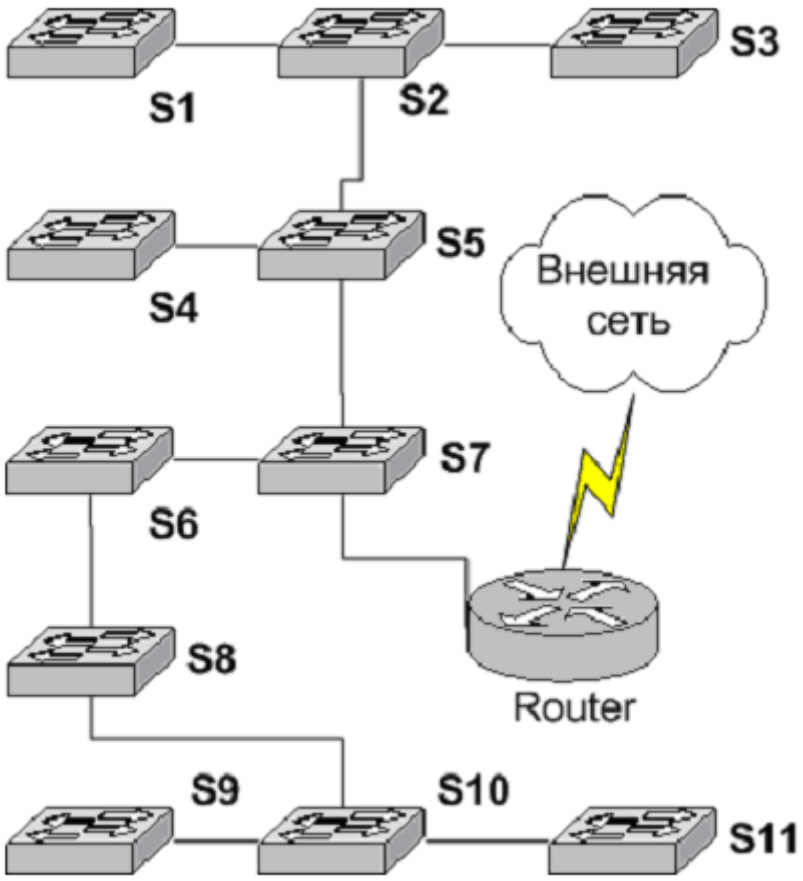

Рис. 10.6. Условная схема сети.

Собственно, большинство небольших сетей так или иначе сводятся к такой простой иллюстрации. А из нескольких подобных сегментов можно построить уже вполне крупную инфраструктуру.

Перечислим варианты установки оборудования.

1. Полностью неуправляемые коммутаторы. Вариант, разумеется, вполне реальный, но для рассмотрения не интересный. Да и перспективность его в общем сомнительна - слишком много неудобств. Достоинство только одно - сверхнизкая стоимость.
2. S7, S5, S10 - управляемые свитчи 2-го уровня, остальные неуправляемые. Такое построение не даст заметного выигрыша. Если два управляемых коммутатора 2-го уровня разделены неуправляемым (с подключенными пользователями) то не все, но большинство функций (VLAN, QoS) будет потеряно. Поэтому имеет смысл поставить мощные устройства только в точках S7 и S5 - тогда их можно будет использовать эффективно.
3. S7, S5, S10 - управляемые 3-го уровня, остальные неуправляемые. Вполне эффективное использование для разделения сегментов в точках S5, S10, но в S7, рядом с маршрутизатором, функции 3-го уровня могут быть излишни. Ну а в остальных точках контроль над сетью будет неполным.
4. Все коммутаторы управляемые 2-го уровня. Этот вариант дает возможность полностью контролировать и при необходимости маршрутизировать каждый порт сети. Для мультисервисного использования возможно соблюдение QoS, мультикастинг, и прочие функции. Как недостаток - необходим отдельный мощный маршрутизатор, через который пойдет весь междусегментный трафик.
5. S7, S5, S10 - управляемые 3-го уровня, остальные - управляемые 2-го уровня. Этот вариант на сегодня фактически стандарт для серьезных корпоративных и операторских структур, но для небольших сетей рекомендовать его несколько рано.
6. Все коммутаторы управляемые 3-го уровня. Подход возможно и неплох, но на сегодня избыточен даже для корпоративных решений. Про остальные и говорить нечего.

Из краткого перечисления вариантов видно, что при выборе стратегического направления развития можно использовать варианты 3 и 4. Кстати сказать, производители оборудования пришли (судя по продаваемым линейкам) к похожим выводам, но к этому придется вернуть после небольшого отступления.

Сначала надо ответить на вопрос - "зачем нужно разделять трафик на уровне IP?".

Когда сети строились на хабах, ответ был тривиален - нужно разделять коллизионные домены, поэтому маршрутизаторы (коммутаторы L3 обычно были непозволительной роскошью) ставились между каждыми 4 хабами (или 30-40 пользователями). Если этого не делать, то наступала быстрая деградация производительности сети.

Однако, в коммутируемой сети такого ограничения нет. И ее размер ограничивается только бродкастовым трафиком, который постепенно заполняет полосу пропускания. Считается, что "бродкастовый шторм" может наступить около 300-500 одновременно работающих пользователей. И это не предел, если в центре сети использовать оборудование с фильтрацией на 4-м уровне (т.е. по протоколам).

Много ли найдется в России сетей, в которых возможно собрать столько пользователей в помещении, не разделенными каналами WAN? Только единичные случаи, наиболее

типичным размером можно считать решения в 100-200 портов. Таким образом, можно сказать что технологическая причина применения L3 в "гладкой" сети Ethernet по сути отсутствует. А традиционно узкие места типа коммутатор-сервер дешевле "расшить" недорогим гигабитом.

Для чего может быть нужно разделение на отдельные сегменты в случае 4? Подсчет локального трафика, ограничение скорости отдельных сегментов, фильтрация, построение закрытых VLAN. В остальном сеть и так полностью управляемая, в ней отдельно можно маршрутизировать каждый отдельный порт. Да и с мультисервисными сервисами проблем не возникнет.

Минусов два. Приличная стоимость управляемого железа (оно понадобится на все порты) и проведение межсегментного трафика через центральный узел, что плохо сказывается на пропускной способности основной магистрали. Собственно последнее и ограничивает размеры плоской сети Ethernet на управляемых коммутаторах 2-го уровня.

Для варианта 3 вероятные причины сегментирования иные. Подсчет трафика на недорогих коммутаторах 3-го уровня делать затруднительно (а при отсутствии финансовых проблем см. вариант 5). Закрытые VLAN то же сделать не удастся - разве что ставить управляемые свитчи во всех точках подключения "отдельных" пользователей. Так что единственный смысл решения - повысить производительность и управляемость сети в некоторых "узких" точках, локализовать неисправности, ограничить доступ пользователей друг до друга хотя бы на уровне нескольких узлов.

Наиболее полно достоинства можно видеть на примере корпоративной сети, распределенной по нескольким отдаленным территориям, которые связаны бриджами xDSL. Коммутаторы L3 позволят строить сети без установки маршрутизаторов на каждый сегмент таким образом, что низкоскоростные xDSL линии будут загружены минимально (только данными, адресованными непосредственно на другую территорию).

Можно сказать, что достоинство данного решения - не нужен выделенный маршрутизатор, нет лишнего трафика через центральные магистрали. Недостаток - из-за многократной маршрутизации на IP-уровне сильно повышается сложность сети - лишние подсети, лишние проблемы. Если сегментов будет более десятка, по неволе придется поднимать OSPF, RIP-2 или что-то подобное из арсенала операторов связи.

Сравним некоторые коммутаторы L3, например D-Link DES-3326S ($800) и Catalyst 3550-24 ($4500). Конечно не на уровне технических параметров, а по парадигме их использования. На мой взгляд, они наиболее полно характеризуют ориентацию производителя оборудования на решение по вариантам 3 и 4 соответственно.

Первый, вероятно, предназначен к использованию по варианту 3, и именно в расчете на небольшие офисные сети, не имеющие разветвленной структуры и требований по ограничению доступа между пользователями. Хорошо вписываются в подобную схему коммутаторы от с портовыми, нетегированными виланами, для которых L3 на ближайшей по топологии развилке - хорошее решение проблемы как скорости, так и безопасности.

Однако большую сеть построить таким образом будет достаточно сложно.

Ну а Cisco 3550 конечно "заточена" под варианта 5, и проходит в связке с Catalyst 2950 через пособия по дизайну сетей. Как раз один 3550 или 3550-12G, и к нему звездой - десяток-другой 2950 (2950T). Это позволяет достичь максимальной скорости передачи

данных. Кстати, нет в линейке этого производителя свитчей с портовыми виланами, а вот поддержка тегированных 802.1q на маршрутизирующих портах становится принципиально необходимой...

Подведем краткие итоги.

Решений много, выбирать или комбинировать нужно в каждом конкретном случае по разному. Но на мой взгляд, даже широкое применение устройств L3 с неуправляемыми или частично управляемыми коммутаторами (без поддержки полных возможностей L2) не позволяет получить значительных преимуществ в управлении сетью (нельзя произвольно контролировать каждый отдельный порт). Но с их помощью можно добиться повышения скорости передачи данных на структуре со сложной топологией или большим "горизонтальным" трафиком.

В остальных случаях их применение будет не слишком эффективным из-за наличия недорогой альтернативы гигабитных магистралей. Т.е. пока пользователи включены на 100 мегабит, они не смогут (конечно до определенного количества) перегрузить магистраль до центрального маршрутизатора.

Возможно именно по этой причине сейчас более широкое распространение получили устройства с "возможностями" 3-го, 4-го, или даже более высоких уровней. При этом из полного спектра свойств IP-заголовка берется всего несколько наиболее полезных (например фильтрация по IP адресу). Это не слишком дорого, но уже в некотором роде позволяет принять участие в "гонке уровней".

Дальнейшее развитие ситуации спрогнозировать сложно. Если пользователи массово перейдут на гигабит, а 10-ти гигабитные магистральные линии останутся слишком дорогим удовольствием, то L3 станет более чем востребован (нельзя будет построить даже минимальную "пирамиду скорости" магистраль-пользователь).

Однако, на мой взгляд более реален другой путь. Десятигигабитные сетевые адаптеры уже существуют, и при появлении недорогой возможности перевода основных каналов на 10 гигабит сегодняшняя ситуация повторится - только уже на более высоких скоростях, и с большими "дополнительными" возможностями.

В заключение, остается добавить что есть большое количество локальных вариантов использования коммутаторов 3-го уровня, при которых L3 будет удобен, или даже незаменим. Поэтому о их наличии стоит помнить при проектировании сети. Но так же надо учитывать, что "третий уровень" совсем не волшебное средство решения всех проблем, а лишь инструмент. Который имеет смысл применять к месту и в нужных количествах. Как лекарство.

Глава 10

Приоритезация в Ethernet.

Продолжение пишется.

Часть 2.

Глава 1. Введение в правосвязие.

Два юриста - три мнения.
Профессиональная поговорка

В борьбе обретешь ты право свое.

Долгое время рынок услуг связи считался недоступным для работы небольших операторов - слишком большие ресурсы требовались для строительства АТС, магистральных и распределительных сетей, центров абонентского обслуживания и т.д.

Однако появление Интернет разрушило этот стереотип до самого основания, иногда даже с лихвой. Выяснилось, что соответствующие технологии позволяют развернуть сети связи при ограниченных или вовсе ничтожных по объему инвестициях.… Разумеется, "малобюджетные" сети по своей структуре напоминали "соковыжималку, сделанную радиолюбителем" - много проводков, изоленты, магически помаргивающих светодиодов и ненадежного, зато трехгрошового каналообразующего оборудования.

Первоначально операторы домашних сетей, будучи исключительно инженерами, вовсе не задумывались о степени легальности своей деятельности, продавая свои услуги по образу обычных лоточников. Однако масштабы сетей росли, привлекая внимание органов государственного контроля, чему способствовала невысокая надежность сетей и соответствующие рекламации со стороны абонентов.

В отличие от крупных операторов, большинство владельцев домашних сетей не могли себе позволить содержать юридические службы, а сами обладали близкими к нулю знаниями в области юриспруденции. Учитывая юридическую малограмотность самих контролирующих органов, получалась своеобразная химера, построенная на туманных и часто меняющихся договоренностях операторов с различными надзорными инстанциями. Привлекать внешние инвестиции в таких условиях невозможно, да и риск лишиться своего бизнеса весьма высок.

Эта статья предназначена для руководителей небольших операторов связи, инженеров и инспекторов ФСНСС - технических специалистов, не имеющих юридического образования и специальных знаний в этой области. Предметом работы является лишь краткое рассмотрение основные принципы юридической науки, знание которых позволит научиться толковать различные законодательные акты. Эти знания пригодятся не только в операторской деятельности, но и в жизни - от общения с гаишниками до общения с ЖКХ и государственными органами.

Разумеется, на нескольких страницах принципиально невозможно исчерпывающим образом рассмотреть юридическую науку - для этого необходимы годы упорного труда и практической деятельности. Однако незнание основ права почти исключает саму возможность грамотно поставить задачу перед юристом-профессионалом, что очень часто приводит к проигрышам весьма несложных судебных процессов, невозможностью разрешения конфликтов с правоохранительными органами и другими неприятностями. Слишком трудно оказывается инженеру понять юриста, а юристу - понять инженера.

Юридическая литература зачастую оказывается слишком скучной и трудной для чтения техническими специалистами - такова уж специфика юриспруденции, требующей педантичности. Однако, продравшись сквозь тяжеловесные конструкции юридического языка, человек неожиданно обнаруживает простор для фантазии и творчества в жестких, на первый взгляд, рамках закона. Именно "фантазия педантизма" отличает хорошего юриста от плохого и для этого вовсе не обязательно вызубрить наизусть толстенные фолианты законодательства. Главное - понять внутреннюю логику правоприменения, а своды лучше всех знает компьютер с юридической базой данных. Которую, кстати, можно смело рекомендовать приобрести любому оператору связи, да и не только оператору.

К сожалению, случившееся весеннее обострение реформаторского зуда государственной службы не позволит комментировать подзаконные акты за отсутствием таковых, но общие принципы организации государственного регулирования отрасли "Связь", по всей видимости, изменятся незначительно, если вообще изменятся. А жаль….

Часть 2. Глава 1

Законы, субъекты и объекты права

Введение в право несомненно покажется наиболее скучной и трудной частью всего цикла статей. Слишком абстрактны рассматриваемые вопросы, слишком сух и тяжеловесен язык изложения. К сожалению, альтернативы нет - всякий начинающий специалист сначала учится терминологии и профессиональному языку. Сначала все кажется непонятной "китайской грамотой", однако со временем язык становится привычным и понятным, и вы не замечаете, как начинаете свободно им пользоваться...

Избежать изучения этой вводной части невозможно - в противном случае все дальнейшие статьи окажутся попросту непонятными, а всякий раз использовать общедоступную терминологию, с одной стороны - невозможно, а с другой стороны - не хватит никакого дискового пространства. Так что если Вы не юрист - попробуйте хотя бы дочитать введение до конца, невзирая на скуку. Зато, щегольнув знанием юридической терминологии, вы иной раз поставите на место зарвавшегося чиновника или даже партнера.

Всем известно, что физическая наука изучает законы природы, это настолько очевидно, что мало кто задумывается над сущностью понятия "закон", по привычке полагая физические и юридические законы чем-то совершенно разным, не подлежащим прямой аналогии. Между тем, понятие "закон" означает всего лишь правило, обязательно выполняющееся субъектами этого правила, при выполнении заранее сформулированных уточнений и ограничений. В качестве пример закона приведем второй закон Ньютона - "ускорение тела прямо пропорционально внешней силе, действующей на тело и обратно пропорционально массе соответствующего тела&quot.

Второй закон Ньютона, таким образом, регулирует взаимные отношения механической силы, действующей на тело, и свойств самого тела - ускорения и массы. Пользуясь юридическим языком, упомянутые отношения являются объектом второго закона Ньютона. С другой стороны, само тело и внешняя сила являются субъектами данного физического закона. (При этом, разумеется, сам закон по определению является предикатом, откуда, собственно, и следуют приведенные выше выводы).

Однако заметим, что второй закон Ньютона выполняется не всегда, а только при скоростях, существенно меньших скорости света, иначе надо учитывать релятивистские эффекты. Иными словами, любой закон действителен только с учетом его относимости к рассматриваемым отношениям. (Не путать с принципом относительности - это совсем другая история…)

Основным качеством субъектов физических законов является отсутствие у них свободы воли, что делает их неспособными к самостоятельному волеизъявлению. В самом деле, кирпич, падающий с крыши, никоим образом не решает, с какой скоростью и на кого именно ему падать и в одинаковых ситуациях всегда ведет себя одинаково. Говоря юридическим языком, субъекты физических законов всегда правоспособны, дееспособны и добросовестны с учетом принципа относимости.

Правоспособностью называют способность нести права и обязанности по закону, дееспособностью - способность самостоятельно исполнять этим права и обязанности, а под добросовестностью юристы понимают волеизъявление к надлежащему исполнению прав и обязанностей. Отсутствие у субъектов физических законов собственной субъективной воли приводит к априорной их добросовестности - даже если субъект ведет себя не так, как предписывает ему физический закон, проблема очевидно заключается в неотносимости закона к возникшей ситуации. (Например, уже упоминавшийся второй закон Ньютона неотносим к телам, скорость которых близка к световой в инерциальной системе отсчета)

В отличие от физики, объектом юриспруденции являются взаимные отношения людей, способных к самостоятельному волеизъявлению, что сразу исключает постулат добросовестности. Юридическая добросовестность субъектов права предполагается (конституционная презумпция невиновности и презумпция гражданской добросовестности согласно п. 3 ст. 10 ГК РФ), однако никак не является бесспорной, имманентной субъектам права, которые в силу свободы воли могут по своему усмотрению выполнить или не выполнить требования закона.

Несмотря на то, что любой физический или юридический закон есть всего лишь продукт мышления, способ формализации мироощущения человека, свойства, да и сущность закона коренным образом изменяются от наличия или отсутствия свободы воли у субъектов соответствующих отношений. Так, физические законы существуют вне зависимости от воли человека, а юридические законы, напротив, определяются людьми по своему усмотрению и лишь после придания им юридической силы в строго установленном порядке, становятся обязательными для исполнения участниками правоотношений.

Юридические законы, устанавливаемые людьми, не могут быть относимы к субъектам физических законов. Даже если принять закон об округлении числа "пи" до трех или об установлении скорости света равной 500 000 км/сек, эти физические константы не изменятся, поскольку сами не являются продуктами волеизъявления людей. Поэтому область нормативно-технического регулирования составляет отдельную область юридической науки, практически трудноотделимую от естественнонаучных знаний и представляет собой связующее звено между правом и физикой. Но это уже отдельная тема, которая будет рассмотрена более подробно в связи с ее важностью для любой инженерной деятельности.

Правоспособные субъекты права принято называть "лицами&quot. Гражданский кодекс выделяет два класса лиц - физические лица (глава 3 ГК) и юридические лица (глава 4 ГК).

Физические лица приобретают правоспособность в момент рождения и прекращается смертью. Дееспособность физических лиц в полном объеме возникает, как правило, с достижением совершеннолетия (в некоторых случаях полная дееспособность может возникнуть и до совершеннолетия).

Статья 23 ГК гарантирует право физических лиц заниматься предпринимательской деятельностью без образования юридического лица, при условии государственной регистрации гражданина в качестве индивидуального предпринимателя. Пункт 3 ст. 23 ГК распространяет на индивидуальных предпринимателей действие гражданского законодательства, регулирующего деятельность коммерческих предприятий - юридических лиц. Надо особо отметить, что индивидуальный предприниматель отвечает по своим обязательствам всем принадлежащим ему имуществом (квартира, машина, загородный дом и т. п.), а не только активами, непосредственно используемыми для предпринимательской деятельности.

Гражданский кодекс (ст. 48) определяет юридическое лицо как организацию, которая имеет в собственности, хозяйственном ведении или оперативном управлении обособленное имущество и отвечает по своим обязательствам этим имуществом, осуществляет личные имущественные и неимущественные права, может являться истцом или ответчиком в суде, а также имеет самостоятельный баланс или смету.

Юридическое лицо учреждается как физическими, так и другими юридическими лицами. Статус юридического лица возникает только после государственной регистрации юрлица в едином государственном реестре юридических лиц (ЕГРЮЛ) через органы налоговой службы. Не следует путать с постановкой на налоговый учет, которая, хоть и обязательна, но производится после регистрации организации в ЕГРЮЛ. Юридическое лицо определяется наименованием и местом нахождения, которые указываются в учредительных документах (ст. 54 ГК).

В этой связи необходимо предостеречь от использования фиктивных "юридических адресов", которые фактически не являются местом нахождения организаций. В частности, существует практика бывшего Госстроя России по судебному прекращению лицензий организаций, не указавших своего фактического места нахождения. Кроме того, все официальные уведомления, судебные повестки и другие документы могут высылаться на "юридический адрес" без выяснения фактического места нахождения организации. Таким образом, вполне можно проиграть судебное дело даже не узнав о его возбуждении…

Правоспособность лиц может быть ограничена законом. Например, видами предпринимательской деятельности субъекты могут заниматься только при наличии лицензии, то есть специального условного разрешения (права) на осуществление соответствующей предпринимательской деятельности (ст. 49 ГК РФ). Специальность лицензии подразумевает, что ее действие распространяется исключительно на лицо, указанное в лицензии. Условность лицензии подразумевает обязательность для держателя лицензии (лицензиата) соблюдения требований лицензирующего органа (лицензиара), указанных в приложении к лицензии. Здесь надо отметить, что гражданское законодательство понимает под предпринимательской деятельностью систематическую деятельность, направленную на извлечение прибыли. Лицензиар вправе отказать в выдаче лицензии не по собственному усмотрению, а только в случаях, предусмотренных законом.

Правовые акты

Физическая природа, будучи к счастью (или к сожалению) единственно доступной людям реальностью, хотя бы в силу своей единственности не оставляет места для вопроса о "норме" поведения физических объектов - проблема только в адекватности научного познания. Человек же, обладая свободой воли и, в определенной степени, волеизъявления, вполне способен придумать великое множество различных норм поведения. Нормы, естественные для первобытного человека, коренным образом отличаются от естественных правил интеллигентного бюргера… и каждый искренне полагает свое мироощущение правильным и адекватным.

Юридические законы как раз и устанавливают норму поведения, характерную для данного общества. Именно поэтому столь важна процедура принятия нормативного правового акта, в случае несоблюдения которой данный акт не приобретает юридической силы, то есть не становится обязательной нормой поведения субъекта права.

Итак, нормативные правовые акты (не только сами законы) составляют законодательство страны и отличаются следующими признаками:

- действуют в отношении неопределенного круга лиц;
- действуют неоднократно;
- опубликованы для всеобщего сведения (п. 3 ст. 15 Конституции РФ).

Ненормативные (индивидуальные) правовые акты действуют в отношении конкретного лица или нескольких лиц, но могут быть как однократного применения (разрешение на строительство), так и многократного применения (лицензия, водительское удостоверение, гражданский договор). Судебные решения также можно отнести к ненормативным правовым актам.

Нормативные и индивидуальные правовые акты являются источниками права, то есть формируют права и обязанности субъекта права - правоспособного лица. Не следует сравнивать степень обязательности индивидуальных и нормативных правовых актов для исполнения конкретным лицом - они одинаково обязательны. Но только при условии соблюдения установленной процедуры принятия правовых актов и отсутствию противоречия правовым актам, имеющим большую юридическую силу.

Надо различать нормы прямого и непрямого действия, то есть содержащие ссылку на иной правовой акт. Обилием отсылочных норм, в частности, весьма богат Федеральный закон "О связи" № 126-ФЗ (далее именуемый "ЗоС"), который предусматривает регулирование важнейших отношений в области связи не прямыми указаниями закона, а постановлениями Правительства.

Система законодательства различных стран построена по-разному. Например, англо-саксонское право признает судебное решение по конкретному делу источником права для разрешения аналогичных дел (прецедентное право). В России принято так называемое кодифицированное право, а судебный прецедент имеет крайне ограниченное значение и применяется только при арбитражном обжаловании нормативных правовых актов (п. 7 ст. 194 АПК РФ).

Система законодательства строго иерархична - нормативные акты более низкого уровня иерархии не должны противоречить нормативным актам, более высокой ступени иерархии. Индивидуальные правовые акты вообще не должны противоречить актам

нормативным, если только иное специально не оговорено соответствующим нормативным актом.

Иерархия российского федерального законодательства построена следующим образом:

1. Конституция России - основной закон. Никакой правовой акт не может противоречить Конституции, имеющей высшую юридическую силу и прямое действие;
2. Федеральные конституционные законы, принимаемые в случаях, предусмотренных Конституцией;
3. Кодексы;
4. Федеральные законы;
5. Постановления Правительства РФ;
6. Нормативные акты федеральных органов исполнительной власти.

Субъекты Российской Федерации также наделены правом издания законов, постановлений и нормативных актов соответствующих органов исполнительной власти. Однако законы субъектов РФ не должны противоречить федеральным законам, а также могут издаваться только по вопросам, отнесенным Конституцией к предметам совместного или исключительного ведения субъектов федерации.

В частности, законодательство в области связи отнесено к исключительному ведению федерации, и региональные власти не вправе регулировать деятельность в области связи. (Зато регионы вправе регулировать строительную деятельность, в том числе и строительство сетей и сооружений связи).

В случае, если нормативный акт противоречит нормативному акту, имеющему большую юридическую силу, он может быть признан недействующим судом или арбитражным судом. Суд также может признать недействительным индивидуальный акт, противоречащий нормативному акту. Логика совершенно очевидна: подобно тому, как распоряжение нижестоящего начальника не должно противоречить распоряжению вышестоящего руководителя, иерархия нормативных актов требует их непротиворечивости.

Часто возникает вопрос, следует ли исполнять требования нормативного или индивидуального акта, которые явно противоречат правовым актам, имеющим большую юридическую силу? К сожалению, однозначного ответа на этот вопрос дать невозможно. С одной стороны, до признания недействующим в установленном порядке, правовой акт сохраняет юридическую силу и обязателен для исполнения. С другой стороны, действующее законодательство предусматривает самозащиту прав субъектов, такая норма есть и в Гражданском кодексе (ст. 14), Кодексе РФ об административных правонарушениях (ст. 38) и в Уголовном кодексе (ст. ст. 37, 39, 41). В этой связи придется рассмотреть некоторые фундаментальные вопросы правоустройства.

Конституция РФ гарантирует равенство всех субъектов перед законом и судом (ст. 19). Однако, эта норма вовсе не означает равенство всех субъектов друг перед другом. В любом человеческом обществе существуют начальники и подчиненные, отношения между которыми основаны не на равенстве их правового статуса, а на принципе власти, или, как говорят юристы, на властеотношениях.

Иерархия власти ни в коем случае не отменяет равенство субъектов перед законом или судом, поскольку споры между начальником и подчиненным могут быть переданы на

рассмотрение в суд, который уполномочен принять окончательное решение. Тем не менее, совершенно очевидно, что правоотношения равных субъектов и властеотношения имеют различные свойства и должны рассматриваться отдельно. Еще во времена императора Юстинина было принято разделение права на публичное (jus publicum) и гражданское (jus civile).

Публичные правоотношения, которые часто называют "административными", вытекают не из договора сторон, а из требований закона, нормативного акта, либо индивидуального правового акта, изданного в соответствии с нормами законодательства. "Классический" пример публичной нормы права - закон об ОСАГО, согласно которому каждый автомобиль должен быть застрахован вне зависимости от желания сторон. Еще один пример - обязанность операторов заключить договор о присоединении сетей электросвязи при организации такого присоединения согласно ст. 18 ЗоС.

Источником публичного права являются и условия действия лицензий, поскольку они не являются следствием соглашения сторон, а властным распоряжением лицензирующего органа (лицензиара). Нормы гражданского права вообще и Гражданского кодекса в частности за исключением случаев, специально установленных законодательством, не могут применяться к публичным правоотношениям, что прямо указывается в ст. 2 ГК РФ.

Анализируя любой нормативный правовой акт необходимо четко отделять публичные и гражданские нормы, хотя зачастую это не так просто. Гражданские правоотношения регулируются гражданским законодательством, но возникают только в результате заключения договора. Иначе говоря, любая сделка должна соответствовать требованиям гражданского законодательства, но само заключение сделки совершается сторонами свободно и без всякого принуждения. Нормы публичного права действуют и в отсутствие соглашения сторон.

Толкование публичных норм, а именно это и составляет основные сложности операторов связи, основывается на так называемом принципе субъективной позитивности: "разрешено все, что явно не запрещено&quot. Статья 2 Конституции РФ постулирует, что "Признание, соблюдение и защита прав и свобод человека и гражданина - обязанность государства", а статья 3 Конституции устанавливает единственным источником власти в России не органы власти, а "многонациональный народ&quot. В то же время ст. 55 допускает ограничение прав и свобод исключительно федеральным законом и только в той степени, "в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства&quot. При этом статья 34 Конституции гарантирует право на "свободное использование своих способностей и имущества для предпринимательской и иной не запрещенной законом экономической деятельности&quot. Из вышеперечисленного делается три очень важных вывода:

1. Никакой орган власти не имеет права действовать полностью по своему собственному усмотрению. Полномочия органа власти определены законодательством, а превышение полномочий преследуется в административном и уголовном порядке. В частности, условия действия лицензии, произвольно и необоснованно ограничивающие права лицензиата, могут быть признаны судом недействительными.
2. Все правоотношения, которые прямо не урегулированы законом, оставляются на усмотрение субъектов права и ни в коем случае не считаются запрещенными.
3. Право на использование имущества для предпринимательской деятельности, имущества, может быть ограничено только законом. Таким образом, специальные

разрешения на эксплуатацию имущества могут быть введены только федеральным законом.

Любой оператор связи немедленно задаст вопрос о законности разрешений на эксплуатацию, оформляемых согласно приказу Минсвязи от 09.09.02 № 113. К сожалению, приходится признать сомнительность требований условий действия лицензий в этой части, поскольку не существует федерального закона, который уполномочивал бы федеральный орган исполнительной власти в области связи осуществлять выдачу таких разрешений. Впрочем, оспаривание условий действия лицензии в судебном порядке - занятие непростое, весьма длительное и, зачастую, требующее куда больше сил, времени и денег, нежели формальное соблюдение требований лицензии.

Часть 2. Глава 1

Участники правоотношений: лица

Следует различать материальные и процессуальные аспекты правоотношений. Под материальной нормой понимается установление прав и обязанностей субъектов права, а процессуальная норма определяет порядок установления и осуществления прав и обязанностей.

Например, требования к лицензиатам, выполнение которых является обязательным для получения лицензии, относятся к материальным нормам, а порядок представления и рассмотрения заявлений на выдачу лицензий - к процессуальным нормам.

Несоблюдение как материальных, так и процессуальных норм влечет недействительность соответствующих решений. С другой стороны, суд может признать нарушение процессуальных требований несущественным и не имеющим правовых последствий. Впрочем, суд вправе принять аналогичное решение и в отношении материальных вопросов, поскольку именно суд в России осуществляет толкование законодательства, как по форме, так и по существу логики законодателя.

Теперь вернемся к вопросу о классификации и особенностях юридических лиц различной организационно-правовой формы. (Напомним, что статус юридического лица возникает после государственной регистрации организации в органах налоговой службы России) Гражданское законодательство выделяет два класса юрлиц - коммерческие и некоммерческие организации (ст. 50 ГК РФ) в зависимости от основной цели деятельности, зафиксированной в уставе.

Коммерческие организации создаются с целью извлечения прибыли, то есть предпринимательской деятельности и распределения полученной прибыли между учредителями. Коммерческие организации, за исключением унитарных предприятий обладают общей правоспособностью, то есть вправе осуществлять любой вид предпринимательской деятельности, даже если устав организации специально не предусматривает какого - либо вида деятельности (п. 1 ст. 49 ГК РФ)

В отличие от коммерческих, некоммерческие организации не имеют извлечение прибыли в качестве основной цели и не распределяют полученную прибыль между учредителями (ст. 50 ГК РФ). Некоммерческие организации вправе заниматься предпринимательской деятельностью лишь поскольку это служит достижению целей, ради которых они созданы

и только, если эти виды деятельности прямо указаны в учредительных документах организации. Юристы называют такой статус некоммерческих организаций "специальной правоспособностью", в отличие от общей правоспособности коммерческих организаций.

Собственно, различие правового положения некоммерческих и коммерческих организаций этим и исчерпывается - никаких специальных льгот некоммерческие организации не имеют, разве кроме возможности не относить членские взносы и пожертвования на прибыль и не уплачивать с них налог на прибыль и НДС. Если некоммерческая организация занимается предпринимательской деятельностью, например - оказывает услуги связи, то такая деятельность регулируется в том же порядке, что и деятельность коммерческих организаций, включая требования лицензирования, специального порядка приемки в эксплуатацию объектов связи и так далее.

Коммерческие организации создаются в различных организационно-правовых формах (приведем только наиболее распространенные)

- **Общество с ограниченной ответственностью** (см. ст. 87 - 94 ГК, Федеральный закон "Об обществах с ограниченной ответственностью" от 08.02.1998 № 14-ФЗ). ООО учреждается одним или несколькими лицами, уставный капитал разделен на доли, пропорциональные вкладу каждого из учредителей, которые не несут ответственности по обязательствам общества и несут риск убытков, связанных с деятельностью общества в пределах стоимости внесенных ими вкладов в уставный капитал. Заметим, что ООО не может иметь в качестве единственного участника другое хозяйственное общество, состоящее из одного лица (п. 2 ст. 88 ГК), то есть единственный учредитель не может создать бесконечную цепочку последовательно учрежденных ООО. Учредительными документами ООО являются Учредительный договор или Решение учредителя о создании общества, а также Устав. Прибыль общества распределяется между участниками пропорционально вкладу каждого из них в уставный капитал. Порядок наследования долей в уставном капитале ООО определяется его Уставом.
- **Акционерное общество** (см. ст. 96-104 ГК, Федеральный закон "Об акционерных обществах" от 26.12.1995 № 208-ФЗ). Акционерным обществом (АО) признается хозяйственное общество, уставный капитал которого разделен на определенное число акций, при этом акционеры (участники) акционерного общества не отвечают по его обязательствам и несут риск убытков, связанных с деятельностью общества в пределах стоимости принадлежащих им акций. Акционерные общества создаются в двух формах (ст. 97 ГК): АО, акционеры которого вправе в любой момент продавать принадлежащие им акции, называется "открытым" (ОАО), если же акции распределяются исключительно среди заранее определенного круга лиц, такое АО называется "закрытым" (ЗАО). Надо заметить, что при продаже (но не при дарении) акций ЗАО, другие акционеры пользуются преимущественным правом выкупа акций по той же цене.
- **Государственные унитарные предприятия** (см. ст. 113 - 115 ГК). Унитарным предприятием признается коммерческая организация, не наделенная правом собственности на закрепленное за ней собственником имущество. В форме унитарных предприятий могут создаваться только государственные и муниципальные предприятия, поэтому мы упоминаем о них только в связи с распространенными заблуждениями о статусе ГУПов. В частности, ФГУП "Главный радиочастотный центр" является коммерческой организацией, то есть по своему уставу обязуется извлекать прибыль из своей деятельности, которая сводится к оформлению различного рода разрешений и согласований. Кстати, Закон Российской Федерации "О Конкуренции и ограничении монополистической

деятельности на товарных рынках" запрещает наделение хозяйствующих субъектов административными полномочиями органов исполнительной власти (п.3 ст. 7 Закона). Таким образом, различного рода разрешительная деятельность ГУПов с юридической точки зрения весьма сомнительна именно в силу статуса ГУПа как коммерческой организации.

Некоммерческие организации, не имеющие своей уставной целью извлечение прибыли, также создаются в различных формах (см. ст. 116-123 ГК, Федеральный закон "О некоммерческих организациях" от 12.01.1996 г. № 7-ФЗ), в том числе:

- **Некоммерческое партнерство** (см. ст. 8 закона "О некоммерческих организациях". Некоммерческим партнерством является основанная на членстве некоммерческая организация, учрежденная гражданами и (или) юридическими лицами для содействия ее членам в достижении различных общественных благ и не распределяющая прибыль между членами. В этой связи представляется довольно сомнительным создание НП с целью коллективного потребления услуг связи, поскольку для этой цели создается потребительский кооператив (см. ниже). Кроме того, управление НП существенно затрудняется необходимостью собирать общее собрание членов по различным поводам - собрать кворум общего собрания из нескольких тысяч членов - весьма сложная организационная задача. НП вправе осуществлять предпринимательскую деятельность, соответствующую целям партнерства и прямо указанную в его уставе, однако в таком случае НП является обычным участником гражданских правоотношений и на него распространяются все нормы, регулирующие предпринимательскую деятельность. Включая необходимость получения лицензий в предусмотренных законом случаях - в том числе при оказании возмездных услуг связи. Заметим также, что продать сеть связи, принадлежащую НП, очень сложно, если не невозможно, поскольку для этого потребуется решение общего собрания членов данного НП.
- **Потребительский кооператив** (ст. 116 ГК, Закон РФ "О потребительской кооперации (потребительских обществах, их союзах) в Российской Федерации" в редакции ФЗ от 11.07. 1997 г. № 97-ФЗ). Потребительским кооперативом признается добровольное объединение граждан и юридических лиц (пайщиков) на основе членства с целью удовлетворения материальных и иных потребностей участников, осуществляемое путем объединения его членами имущественных паевых взносов. В отличие от других форм некоммерческих организаций, при выходе пайщика из кооператива, ему возвращается паевой взнос, а также и кооперативные выплаты как часть доходов от предпринимательской деятельности кооператива.
- **Автономная некоммерческая организация** (см. ст. 10 закона "О некоммерческих организациях" от 12.01.1996 г. № 7-ФЗ). Автономной некоммерческой организацией признается не имеющая членства некоммерческая организация, учрежденная гражданами или юридическими лицами на основе добровольных взносов в целях предоставления различных услуг. Учредители АНО теряют право на имущество (включая денежные средства), переданное ими в собственность организации, однако осуществляют надзор за деятельностью учрежденной ими АНО. При этом закон специально оговаривает, что учредители АНО вправе пользоваться ее услугами только на равных условиях с другими лицами. Надо сказать, что форма АНО наиболее подходит к оказанию различных услуг связи, если по каким-то соображениям создание операторской компании в форме коммерческой организации невозможно или нецелесообразно. При осуществлении предпринимательской деятельности АНО обязана соблюдать действующее законодательство, в том числе оформлять необходимые лицензии.

- **Учреждение** (ст. 120 ГК, ст. 9 закона "О некоммерческих организациях" от 12.01.1996 г. № 7-ФЗ). Учреждением признается некоммерческая организация, созданная собственником для осуществления управленческих, социально-культурных или иных функций некоммерческого характера и финансируемая собственником полностью или частично. Например, служба госсвязьнадзора до недавнего времени существовала в виде Государственных учреждений, осуществляющих функции государственного управления в области связи и информатизации на подведомственных территориях. Не следует путать ГУП и ГУ - их правовое положение существенно различается, ведь ГУП предназначено для коммерческой деятельности, а ГУ - для управленческой. При этом возложение административных полномочий на ГУ, в отличие от ГУПа, не противоречит законодательству о конкуренции. Учредительным документом учреждения является Положение о данной организации.

Вышеперечисленные организационно-правовые формы отнюдь не исчерпывают перечень форм некоммерческих организаций и включают лишь те, с которыми чаще всего приходится сталкиваться операторам связи в процессе своей деятельности.

Надо сказать, что существует весьма распространенная практика создания некоммерческих организаций для ведения фактически коммерческой деятельности по оказанию услуг связи. Кроме очевидной противоправности, такую форму организации оператора связи можно смело признать бессмысленной и не приносящей никаких преимуществ организаторам, более того, затрудняющей развитие бизнеса.

Полноценная операторская деятельность, наряду с возможностью привлечения инвестиций, возможна только при условии организации полноценного оператора связи в форме коммерческой организации и получения необходимого комплекта лицензий и специальных разрешений. Несмотря на всю трудоемкость и дороговизну легализации операторского бизнеса, этот путь, к сожалению, единственный, в той или иной степени гарантирующий неприкосновенность активов и самого предприятия.

Говоря о юридических лицах, нельзя не сказать об особых субъектах права, имя которым - органы власти, которые не относятся как к коммерческим, так и некоммерческим предприятиям. Правовое положение органов власти как субъектов гражданских правоотношений базируется на 5-й главе ГК РФ. Органы власти являются юридическими лицами и действуют на основании Положений о соответствующем органе, порядок утверждения которого определяется вышестоящим органом власти.

В частности, положения о федеральных министерствах, федеральных службах и федеральных агентствах утверждаются Правительством или Президентом России в зависимости от подчиненности соответствующего органа власти. Разумеется, органы власти ни в коем случае не являются субъектами предпринимательской деятельности, что прямо запрещается ст. 7 закона "О Конкуренции и ограничении монополистической деятельности на товарных рынках".

Как гражданская, так и административная правоспособность органов власти жестко ограничивается положением о данном органе и не может толковаться расширительно. В частности, органы власти могут выступать в качестве заказчика услуг связи от имени государства, однако не могут быть исполнителями по соответствующим государственным контрактам.

Государственная власть

Конституция России (ст. 10) предусматривает разделение государственной власти на три формально независимых ветви – законодательная, исполнительная и судебная. Исполнительная власть называется так именно потому, что призвана обеспечивать надлежащее исполнение законов, принятых властью законодательной, а судебная и только власть осуществляет правосудие, то есть является арбитром для всех субъектов права по вопросам, связанным с толкованием законов. При этом сам суд не имеет полномочий по принуждению к исполнению своих решений – это дело исполнительной власти, к которой относится Правительство, министерства, федеральные службы и агентства, а также органы власти регионов федерации.

Судебная власть осуществляет правосудие не произвольно, а в порядке, определенном процессуальным законодательством – Арбитражным процессуальными кодексом, Гражданским процессуальным кодексом, процессуальной частью Кодекса об административных правонарушениях, Уголовно-процессуальным кодексом, а также целым рядом других законодательных актов. Несоблюдение судом процессуального порядка является основанием для отмены решения суда вышестоящим судом (однако процессуальные нарушения оцениваются судом высшей инстанции и сами по себе не влекут автоматической недействительности принятого решения).

Любое правоспособное лицо вправе обратиться в суд за защитой своих законных прав, если полагает, что эти права были нарушены. Заметим, что дела юридических лиц и индивидуальных предпринимателей по вопросам, связанным с осуществлением предпринимательской деятельности разрешает Арбитражный суд, а дела физических лиц подведомственны суду общей юрисдикции. Однако дела об оспаривании нормативных правовых актов разрешаются судом общей юрисдикции, если законом не установлена их подведомственность арбитражному суду. Разумеется, при этом суд общей юрисдикции сталкивается с большими сложностями, поскольку судьи часто не обладают опытом рассмотрения дел в области предпринимательской деятельности, но так уж решил законодатель (п. 1 ст. 29 АПК).

Подготовка исковых заявлений и других судебных документов требует от юриста не только знания процессуальных и материальных аспектов дела, но и практического опыта. Поэтому после принятия решения об обращении в суд желательно привлечь для консультации юриста, имеющего опыт судебной практики, при этом способного понять технологические аспекты спора, если, разумеется, таковые имеются.

Отметим, что представителем лица в суде общей юрисдикции может быть любое лицо, имеющее соответствующую доверенность, а представителем лица в арбитражном суде может быть либо штатный сотрудник юридического л ица – участника дела, либо адвокат по ордеру юридической консультации или коллегии. Поэтому зачастую приходится принимать в штат юристов, занятых разрешением конкретного спора… но тут уж ничего поделаешь – таково требование закона.

Правовая природа государства, зафиксированная ст. 1 Конституции, означает, как уже говорилось, обязанность органов исполнительной власти принимать решения не по собственному усмотрению, а в соответствии с требованиями законодательства и в пределах соответствующих полномочий. При этом ст. 2 Конституции утверждает, что обязанностью государства является не ограничение, а признание субъективных прав и

свобод, тем самым формулируется знаменитый принцип «все, что прямо не запрещено законом является разрешенным».

К сожалению, многие, очень многие сотрудники федеральных органов исполнительной власти вообще и Минсвязи - в частности, полагают, что они вправе по своему усмотрению ограничивать права и свободы при условии соблюдения только лишь процедуры принятия соответствующих решений… Увы, только судебные споры способны образумить бюрократов, потерявших чувство всякой меры и ответственности. С юридической точки зрения, органы исполнительной власти выполняют три основные функции:

- правоустанавливающую (издание нормативных и индивидуальных правовых актов в пределах компетенции соответствующего органа);
- надзорную (осуществление мероприятий по проверке соблюдения различными лицами действующего законодательства в пределах компетенции соответствующего органа власти, а также понуждение поднадзорных лиц к соблюдению требований закона);
- контрольную – то есть управление деятельностью различного рода подведомственных предприятий и организаций. Примером контрольной деятельности является взаимодействие упраздненного Минсвязи с подведомственными ГУ УГНСИ. Контрольную деятельность часто путают с надзорной деятельностью, что совершенно неверно. В частности, мероприятия по «контролю лицензируемой деятельности», выполняемые органами надзора за связью и информатизацией, на самом деле являются сугубо надзорными по своей природе, поскольку госсвязьнадзор не вправе вмешиваться в повседневную деятельность операторов связи, если эта деятельность соответствует требованиям законодательства.

Часть 2. Глава 1

Государственное принуждение и ответственность субъектов права

Любое суверенное государство обеспечивает исполнение законодательства на своей территории. Разумеется, дело не обходится без властного принуждения к соблюдению законов и других правовых актов, которые приняты государством в качестве обязательных для исполнения. Государственное принуждение охватывает не только административную сферу взаимоотношений различных лиц с самим государством, но и сферу гражданских правоотношений. Например, ст. 168 Гражданского кодекса устанавливает недействительность сделки, не соответствующей закону или иным правовым актам. Но любой законодательный акт остается пустой декларацией, если государство не примет эффективных мер к принуждению субъектов к исполнению законодательства.

Существует особый класс органов исполнительной власти, основной задачей которых является принуждение субъектов права к соблюдению требований действующего законодательства. К таким специальным органам власти, которые часто называют «правоохранительные органы», относятся:

- прокуратура, выполняющая функцию общего надзора за соблюдением законодательства, а также функцию следственного органа по уголовным делам и ряд других функций. Именно в прокуратуру следует обращаться с жалобами на неправомерные действия должностных лиц органов власти, нарушающие законные права лиц, при этом жалоба составляется в произвольной форме – прокурорские работники сами разберутся с юридической подоплекой дела. Хотя, разумеется, помощь юриста будет нелишней, учитывая нежелание прокуратуры конфликтовать с другими органами власти;
- Министерство внутренних дел;
- Федеральная служба безопасности;
- Служба судебных приставов-исполнителей;
- Целый ряд других служб и органов власти.

Разумеется, любой орган власти является в той или иной степени «правоохранительным», поскольку обязан соблюдать и защищать законные права и интересы лиц. Фактически же, общим критерием отнесения органа власти к семейству правоохранительных органов является предоставленное законом право осуществления оперативно-розыскной деятельности (ОРД). Надо заметить, что самовольное и (или) незаконное осуществление ОРД запрещается и влечет уголовную ответственность.

Далеко не все надзорные инстанции относятся к правоохранительным органам, хотя и осуществляют государственное принуждение. В качестве примера можно привести все тот же Госсвязьнадзор, который вправе привлекать лиц к административной ответственности за различные правонарушения в области связи и информатизации, однако не наделен правом осуществления ОРД. В этом смысле полномочия правоохранительных органов качественно превосходят полномочия «обычных» надзоров. Штраф несколько тысяч рублей за нарушение условий действия лицензий Минсвязи, наложенный УГНСИ – это одно, а даже одна ночь в изоляторе временного содержания – это совсем другое.

Вывод прост: не стоит оказывать прямое сопротивление даже заведомо незаконному действию сотрудника правоохранительного органа, поскольку полномочия сотрудников чрезвычайно широки. Гораздо безопасней и эффективней тщательное протоколирование или хотя бы запоминание всех подробностей проверки, проводимой сотрудниками, например, милиции, с последующим обжалованием в прокуратуру или суд. Грамотный адвокат всегда найдет массу нарушений…

Нарушение закона всегда является нарушением права, которое устанавливает или охраняет соответствующий нормативный правовой акт, поэтому нарушение законодательства обычно называют «правонарушением» или, на юридическом языке, «деликтом». Вместе с тем, нет правонарушения, если оно не предусмотрено законом, даже если деяние однозначно осуждается общественным мнением. Надо четко отделять гражданско-правовые деликты от административных правонарушений и уголовных преступлений.

Дело в том, что гражданско-правовая ответственность может наступать и при отсутствии вины нарушителя. В частности, п.1 ст. 1064 ГК РФ устанавливает: «Вред, причиненный личности или имуществу гражданина, а также вред, причиненный имуществу юридического лица, подлежит возмещению в полном объеме лицом, причинившим вред. Законом обязанность возмещения вреда может быть возложена на лицо, не являющееся причинителем вреда…». Таким образом, для наступления гражданско-правовой ответственности достаточно факта причинения вреда вне зависимости от наличия или отсутствия вины.

Ответственность за административные или уголовные деликты, в отличие от гражданско-правовой ответственности, наступает только при наличии полного состава правонарушения, который состоит из четырех элементов:

1. **Объект деликта** – охраняемые законом общественные отношения. В качестве примера можно привести обязанность получения лицензии на право осуществления некоторых видов предпринимательской деятельности. Ст. 171 УК РФ предусматривает санкцию за осуществление предпринимательской деятельности без лицензии, если такая лицензия обязательна.
2. **Объективная сторона** – сознательное деяние (действие или бездействие), нарушающее охраняемые законом общественные отношения. Например, поскольку ст. 29 Федерального закона «О связи» установлено лицензирование деятельности по возмездному оказанию услуг связи, то сознательное и волящее осуществление этой деятельности без соответствующей лицензии нарушает охраняемые ст. 171 УК РФ общественные отношения.
3. **Субъект правонарушения** – лицо, способное сознавать вредные последствия своих действий. Административной ответственности подлежат как юридические так и физические лица, уголовной ответственности подлежат только физические лица, что накладывает особую ответственность на руководителей предприятий и организаций.
4. **Субъективная сторона правонарушения** – вина, которая может существовать в двух формах – умышленная и неосторожная. Однако ключевым моментом является наличие у субъекта возможности не совершать деликт. Например, если оператор связи в установленном законом порядке подал документы на продление срока действия лицензии в уполномоченный орган власти, а лицензиар по любым причинам не успел рассмотреть документы и принять соответствующее решение, то оператор полностью освобождается от уголовной или административной ответственности за незаконное предпринимательство за отсутствием вины. Особо отметим так называемый принцип «недопустимости объективного вменения», действующий в уголовном и административном праве – отсутствие вины означает отсутствие правонарушения даже при наличии первых трех элементов состава деликта.

Еще раз надо подчеркнуть, что условием привлечения лица к административной или уголовной ответственности является наличие полного состава правонарушения, то есть всех его четырех элементов. Уголовные деликты – преступления, преследуются в порядке, установленном УПК РФ и отличаются от административных правонарушений повышенной степенью общественной опасности. Разумеется, определение меры этой самой общественной опасности есть прерогатива законодательной власти…

Привлечение к административной ответственности производится в порядке, установленном Кодексом РФ об административных правонарушениях. Несоблюдение процессуальных норм КоАП влечет недействительность административного взыскания.

Привлечение к административной ответственности обычно состоит из двух этапов – составление протокола об административном правонарушении и рассмотрение материалов дела с принятием решения о наложении взыскания. И возбуждение дела (составление протокола) и рассмотрение дела могут осуществлять только лица, специально уполномоченные КоАП (ст. 28.3 и гл. 23). Подробное рассмотрение вопросов административной ответственности операторов связи будет предметом отдельной публикации – слишком много возникает при этом вопросов, неточностей, а то и просто мифов.

Часть 2. Глава 1

Мифология переходного периода

Недостаток правовых знаний породил множество мифов, бытующих в среде предпринимателей, и операторы связи – отнюдь не исключение. Разумеется, большая часть этой мифологии относится к специальным вопросам операторской деятельности, и будет рассматриваться отдельно. Однако есть ряд распространенных заблуждений, о которых просто невозможно не сказать:

- Миф 1: «Любая проблема решается взяткой». Решается. Но не любая и только на некоторое время. Потому что чиновники приходят и уходят, причем каждый последующий чиновник обычно творчески пересматривает договоренности своего предшественника. Кроме того, чиновники очень любят «доить» тех, кто жаждет давать взятки по любому поводу.
- Миф 2: «Обращаться в суд бесполезно». Очень вредное заблуждение, развращающее чиновников и монополистов. На самом деле, обращаться в суд очень полезно – просто надо уметь это делать. Точно так же, как надо уметь строить сети. Ярчайший пример – победа, одержанная сетью «Сонет» над Минсвязи России в споре о признании CDMA сотовой связью…
- Миф 3: «Легальная деятельность в области связи невозможна в принципе». Этот миф, как не прискорбно, не лишен материальной основы. Действительно, никакая полностью легальная предпринимательская деятельность в России пока невозможна. Однако, из этого вовсе не следует само собой полная нелегальность самого бизнеса. Истина, как всегда, находится посередине – единственный способ избежать неизбежного закрытия бизнеса это соблюдать как можно больше различных норм и правил, за исключением разве что совершенно неисполнимых. Иначе аппетит контролирующих органов достигнет таких зияющих высот, что продолжать какую-либо деятельность станет совершенно бессмысленно. Поиск компромиссных решений и составляет искусство руководителя предприятия в условиях переходного периода государства Российского.

Глава 2. Операторы и государство.

Облик современной цивилизации неразрывно связан с уровнем развития отрасли связи и информатизации. Именно поэтому практически каждое государство достаточно жестко регулирует все, что связано с предоставлением услуг связи.

А случившаяся активизация всеобщей борьбы с терроризмом еще больше усилила повсеместный государственный пригляд за операторами связи. Разумеется, Россия – не исключение, более того, Россия принадлежит к странам с наиболее детализированной регламентацией операторской деятельности. Конечно, до Китая или Ирана нам еще далеко… пока далеко.

Как уже отмечалось, общая правоспособность коммерческих организаций может быть ограничена законом необходимостью получения специального разрешения уполномоченного органа исполнительной власти на осуществление некоторых видов

деятельности. Статья 29 Федерального закона «О связи» № 126-ФЗ (который по традиции именуется «ЗоС»), устанавливает, что возмездное оказание услуг связи на допускается при наличии лицензии, выданной федеральным органом исполнительной власти в области связи.

До недавнего времени таким органом являлось Минсвязи России, а в настоящее время лицензирование передано в новообразованную Федеральную службу по надзору в сфере связи (ФСНСС). К сожалению, пакет нормативных правовых актов, который должно было принять правительство России во исполнение ЗоС, так и не был принят (на 01.07.04), поэтому оформление новых лицензий отложено как минимум до осени 2004 года, когда, возможно, будут приняты необходимые подзаконные акты. А пока таких актов не существует, так что и комментировать нечего.

До вступления в силу новой редакции ЗоС, то есть до первого января 2004 года, получить лицензию Минсвязи было относительно несложно, поэтому большинство операторов такими лицензиями обзавелись. Увы, проблемы легального осуществления деятельности в области связи получением лицензии отнюдь не исчерпываются, но наоборот, все только начинается…

Часть 2. Глава 2

Легализация: выживание или развитие

Вообще, термин «легализация» в юридическом смысле подразумевает приведение деятельности некоторого субъекта права в соответствие с законодательством. В условиях противоречивости и неопределенности действующего законодательства задача легализации выглядит весьма сложной, если не вовсе неразрешимой. Однако, строгость российского законодательства, как известно, компенсируется ограниченностью его исполнения. Проблема состоит в осознанном и адекватном выборе границы исполнения и неисполнения законодательства… но эту проблему каждый оператор решает для себя сам.

Легальная операторская деятельность – занятие не из дешевых, впрочем, телекоммуникации вообще довольно дорогой бизнес, требующий значительных инвестиций как в инфраструктуру, так и в персонал. Однако ни один здравомыслящий инвестор не станет вкладывать средства в нелегальную деятельность, да еще и чреватую уголовным преследованием.

Нелегально построенные сети не являются объектом права собственности и сделки с ними ничтожны (ст. 168, 169 ГК РФ). Более того, эксплуатант или собственник здания вправе ликвидировать сеть за счет ее фактического владельца (ст. 222 ГК РФ), иными словами, оператора могут обязать оплатить услуги подрядных организаций по уничтожению взращенной нелегкими трудами сети. Обидно, сурово – но таков закон. Разумеется, привлечь инвестиции, да и просто получить кредит под залог такой нелегальной сети в принципе невозможно.

А если добавить еще и риск стать обвиняемым по уголовному делу (ст. 171 УК РФ) – необходимость легализации станет очевидной. Разумеется, можно надеяться всякий раз откупиться малой мздой чиновнику, однако купить всех чиновников обойдется дороже любой легализации, во-вторых, чиновники часто меняются, да и в случае жалобы, например, конкурента – никакой чиновник не рискнет своим креслом ради

незначительной взятки. Можно, попытаться дать большую взятку, вот только размер взяток, умноженный на их частоту следования, быстро превысит любые расходы на легализацию бизнеса.

Издержки на легализацию деятельности оператора связи зависят, в числе прочего, и от того, когда решается данная задача – на этапе создания новой сети или после начала эксплуатации сети, построенной без оглядки на требования регулирующих органов. Чудес в природе не бывает – если второй способ чреват существенно меньшими издержками на этапе строительства, то первый способ позволит сэкономить на приведении сети в соответствие с требованиями государства. Как будет показано далее, издержки на создание сети в обоих способах примерно одинаковы и, увы, весьма значительны.

Легальное осуществление деятельности в области связи подразумевает, помимо соблюдения законодательства, выполнение условий действия лицензий Минсвязи России. Основные проблемы у операторов, строящих сети или легализующих уже построенные сети, создает пункт о необходимости оформления разрешения органов государственного надзора за связью и информатизацией на эксплуатацию всех без исключения объектов связи, используемых для предоставления услуг связи. Оформление такого разрешения влечет необходимость выполнения множества других требований государственных органов, и, поэтому, является наиболее сложной задачей при легализации сетей связи.

Часть 2. Глава 2

Лицензирование.

До начала работ по строительству объекта связи, лицензия оператора должна быть зарегистрирована в территориальном органе Госсвязьнадзора. Единых правил регистрации лицензий не существует. На практике вполне достаточно представить копии учредительных документов оператора связи, заверенных соответствующей ИМНС; нотариально заверенной копии лицензии и простой копии условий ее действия, схему организации связи и справку о состоянии сети. Если оператор оформляет первое разрешение за период своей деятельности, целесообразно в справке указать, что услуги связи по лицензии не предоставляются, поскольку оператор не имеет разрешения на эксплуатацию.

В настоящее время (июнь 2004 г.) разрешения на эксплуатацию объектов связи оформляется как итоговый документ, фактически подтверждающий приемку в эксплуатацию соответствующего объекта связи приемочной комиссией. Порядок приемки в эксплуатацию объектов связи определяется приказом Минсвязи России от 09.09.2002 г. № 113 «Об утверждении правил ввода в эксплуатацию сооружений связи» - далее «приказ 113».

Надо заметить, что не существует нормативного правового акта, уполномочивающего Минсвязи, МИТС, ФСНСС или иные органы власти выдавать эти самые разрешения. Дело в том, что Постановление правительства № 380 от 26.04.2000 г., уполномочивает органы госсвязьнадзора приостанавливать или аннулировать разрешения на эксплуатацию (пп. 9(и) Положения о ГСН, утвержденного указанным постановлением). При этом приказ № 113 ссылается именно на это постановление правительства.

Увы, сомнительность правовых оснований для издания нормативного акта сама по себе не прекращает его действие. Разумеется, операторы связи могут обращаться в суд с заявлением о признании недействительным приказа Минсвязи № 113, однако до сих пор никто из операторов такого мужества не проявил. Так что приказ №113 действует, как действуют и положения условий действия операторских лицензий, требующие оформления соответствующих разрешений на эксплуатацию объектов связи.

Приказ 113 подразумевает, что разрешение на эксплуатацию объекта связи официально подтверждает два юридически значимых факта:

- **Техническую готовность объекта связи** - соответствие построенного объекта утвержденной проектной документации, прошедшей государственную экспертизу, надлежащее качество строительства и пусконаладочных работ, подтвержденное результатами измерений и проведенных испытаний. Техническую готовность подтверждает акт приемки рабочей комиссией законченного строительством объекта по форме КС-14. Заметим, что данная форма акта распространяется на приемку любых объектов строительства, вплоть до жилых домов, заводов, плотин и кабельной канализации;
- **Организационную готовность оператора связи** к оказанию услуг с использованием принимаемого в эксплуатацию объекта. Организационную готовность оператора связи подтверждает заключение госсвязьнадзора (п. 5.5 приказа).

Разрешение на эксплуатацию содержит перечень оборудования с адресами его размещения (места нахождения), наименование оператора, наименование услуг связи, которые допускается оказывать с использованием оборудования, указанного в разрешении. Обычно на оборудование узлов телематических служб и передачи данных выдается одно разрешение. Отдельное разрешение оформляется на узлы телефонной связи и прочие услуги связи, за исключением случаев, когда одно и то же оборудование используется для предоставления нескольких видов услуг (определяется проектом).

Оператор связи, который будет эксплуатировать создаваемый объект связи, не всегда является заказчиком создания соответствующего объекта. По общему правилу, заказчиком строительства является инвестор, либо лицо, специально уполномоченное инвестором при наличии лицензии Госстроя РФ на право осуществления деятельности заказчика-застройщика. Инвестору, одновременно являющемуся заказчиком, лицензия Госстроя не требуется. Оператор связи может являться инвестором, заказчиком или эксплуатантом, а также совмещать любые из этих функций. Разумеется, если оператор связи исполняет функции еще и заказчика по договору с инвестором, оператору потребуется соответствующая лицензия Госстроя.

Приказ 113 определяет две процедуры приемки в эксплуатацию объектов связи – общую и упрощенную, которая применяется только для некоторых видов объектов, исчерпывающий перечень которых приводится в приложении «А» к указанному приказу.

Часть 2. Глава 2

Приемка в эксплуатацию объектов связи

Анализ приказа 113 позволяет выделить семь основных этапов оформления разрешения на эксплуатацию объекта связи по общей процедуре (ряд этапов можно осуществлять одновременно):

1. Подготовительные мероприятия – регистрация лицензий, разработка, государственная экспертиза и утверждение проектной документации, согласование плана мероприятий по СОРМ с территориальным управлением ФСБ РФ, обучение сотрудников в области охраны труда и техники безопасности и т.д.
2. Направление в территориальный орган госсвязьнадзора уведомления о начале работ по созданию или реконструкции объекта связи.
3. Строительные и монтажные работы по созданию сети согласно утвержденной ранее проектной документации.
4. Проведение мероприятий, обеспечивающих организационную готовность оператора связи к оказанию услуг связи.
5. Создание и организация работы рабочей комиссии по приемке объекта связи. Приемочная комиссия назначается приказом заказчика создания объекта. Рассмотрение рабочей комиссией документов, подтверждающих техническую готовность объекта к коммерческой эксплуатации, подписание всеми членами комиссии и утверждение заказчиком акта КС-14.
6. Подготовка инспектором госсвязьнадзора заключения по организационно-технической готовности оператора к оказанию услуг связи и отсутствию нарушений, препятствующих этой деятельности (п. 5.5 приказа 113).
7. Оформление территориальным органом госсвязьнадзора разрешения на эксплуатацию соответствующего объекта связи соответствующим оператором связи в течение 10 дней после получения утвержденного акта КС-14 и положительного заключения инспектора.

1. Подготовительные мероприятия

До начала разработки проектной документации на создание сети, необходимо решить вопрос, который часто является ключевым для оформления разрешения на эксплуатацию. А именно, определить оператора присоединяющей сети связи, через которую будет осуществляться взаимодействие создаваемой сети с другими сетями общего пользования. Дело в том, что в разрешениях на эксплуатацию всегда указывается адрес размещения соответствующего оборудования связи. Таким образом, разрешения присоединяемой и присоединяющей сети должны «стыковаться» по адресам, то есть не должно существовать участков сети, на которые разрешения на эксплуатацию не оформлены.

Здесь возникает очень много споров ввиду нежелания оператора присоединяющей сети тратить время на приемку в эксплуатацию оборудования, используемого исключительно для межсетевого взаимодействия, например – кабеля связи между узлом присоединяющей и присоединяемой сети. Между тем, отсутствие «стыковки» по почтовым адресам разрешений на эксплуатацию присоединяющей и присоединяемой сети полностью исключает возможность оформления разрешения на эксплуатацию присоединяемой сети.

Вопросы организации и эксплуатации межсетевого взаимодействия определяются договором присоединения сетей электросвязи, который должен быть заключен согласно требованиям главы 4 ЗоС. Для заключения такого договора достаточно наличие у обоих операторов лицензий на осуществление деятельности в области связи, поэтому договор присоединения должен заключаться до начала проектирования.

Технические условия, выдаваемые оператором присоединяющей сети, являются основанием для проектирования сетевых стыков и оформления соответствующих разрешений. Но оператор присоединяемой сети должен тщательно изучить границы раздела зон ответственности операторов, поскольку каждый их операторов обязан оформить разрешение на эксплуатацию оборудования в пределах своей зоны ответственности.

Также необходимо запросить у оператора присоединяющей сети копию разрешения на эксплуатацию его сети в точке раздела зон ответственности и предъявить этот документ инспектору в процессе подготовки заключения госсвязьнадзора после подписания акта КС-14.

Остальные подготовительные мероприятия обычно проводятся одновременно с разработкой проектной документации на создание объектов связи. Общие требования к проектной документации будут рассмотрены отдельно, однако оператор должен располагать не только проектной документацией, но и заключением государственной экспертизы, в котором должна содержаться ключевая фраза «… рекомендуется к утверждению…». На основании заключения государственной экспертизы руководитель заказчика издает приказ об утверждении проектной документации. Копию приказа желательно впоследствии приложить к акту КС-14.

Основные подготовительные мероприятия указаны в таблице и могут незначительно изменяться в зависимости от требований конкретных территориальных органов госсвязьнадзора и конкретных инспекторов:

п/п	Наименование подготовительного мероприятия	Результат мероприятия (документ)	Примечание
1.	Регистрация лицензии о территориальном органе госсвязьнадзора	1. Свидетельство о регистрации лицензиата.	Срок регистрации не определен, однако дата регистрации не может быть позже даты начала оказания услуг по лицензии.
2.	Заключение договоров о присоединении сетей электросвязи и договоров аренды каналов связи (при необходимости).	1. Договор о присоединении; 2. Технические условия; 3. Копия разрешения на эксплуатацию присоединяющей сети в точке присоединения согласно ТУ.	Требования к договору о присоединении см. главу 4 ЗоС. Аренда каналов связи не является объектом договора о присоединении.
3.	Обучение персонала правилам техники безопасности и охраны труда	1. Удостоверения о проверке знаний по технике электробезопасности, квалификационная группа персонала не ниже III до 1000 В; лиц, имеющих право выдавать наряды (руководители) – не ниже IV до 1000 В. 2. Удостоверения о проверке знаний по охране труда. 3. Журналы инструктажей сотрудников. 4. Инструкции по охране труда и технике безопасности на предприятии.	Обучение проводится в специализированных учебных комбинатах. Удостоверения п.1 действительны в течение одного года, п. 2 в течение трех лет.

4.	Оформление частотно-разрешительной документации	 1. Решение ГКРЧ о выделение полос частот для эксплуатации РЭС 2. Частотные назначения для эксплуатации РЭС в установленном порядке	Порядок оформления частотных назначений для эксплуатации РЭС будет определен Федеральным агентством связи.
5.	Разработка проектной документации, согласование, государственная экспертиза и утверждение проектной документации	1. Задание на проектирование; 2. Согласованная проектная документация; 3. Заключение государственной экспертизы с рекомендацией об утверждении проектной документации; 4. Приказ заказчика об утверждении проектной документации.	
6.	Разработка и согласование плана мероприятий по СОРМ	Письмо из территориального УФСБ о разрешении оказания услуг связи до согласования плана СОРМ либо согласованный план мероприятий по СОРМ.	
7.	Заключение договоров аренды технологических помещений (площадок) по выданным ТУ, аренды оборудования и т. д.	Договоры с соответствующими лицами.	

Некоторые замечания по подготовительным мероприятиям:

1. Свидетельство о регистрации лицензиата содержит ФИО и контактный телефон инспектора госсвязьнадзора, которому поручено «курировать» данного оператора-лицензиата.

2. Договор аренды каналов связи, заключенный с оператором, имеющим соответствующую лицензию, не является договором присоединения сетей электросвязи, поскольку аренда каналов связи «точка-точка» не предоставляет возможности установления соединения и передачи информации между другими пользователями сети оператора каналов связи (см. определение услуги присоединения ст. 2 ЗоС).

В условиях действия лицензий операторов сетей, предназначенных для предоставление в аренду каналов связи, прямо указывается на возможность предоставления данной услуги как абонентам, так и операторам связи. Иначе говоря, договор аренды каналов связи всегда заключается как абонентский. К сожалению, не все сотрудники госсвязьнадзора это понимают.

Нередко возникают сложности с определением статуса договоров, заключаемых между операторами передачи данных и (или) телематических служб и операторами местных телефонных сетей общего пользования о предоставлении коммутаторной емкости ТфОП для служб dial-up и IP-телефонии, которая в нормативных документах Минсвязи именуется «служба передачи речевой информации» (см. РД 45.129-2000). Условия действия лицензий на услуги телематических служб, а также РД 45.129-2000 допускают

присоединение оборудования ТМС к телефонной сети общего пользования исключительно на уровне абонентских установок.

С другой стороны, оборудование телематических служб вообще и СПРИ - в частности, позволяет организовать соединение между абонентами ПД и ТфОП, а также абонентами ТфОП через СПРИ. С третьей стороны, организация межстанционных соединений через сети ПД не допускается РД 45.129-2000 и РД 45.129-2000. С четвертой стороны, указанные руководящие документы не прошли государственной регистрации в Минюсте и не обладают юридической силой нормативного правового акта…

Неопределенность законодательства приводит к невозможности однозначного юридического обоснования правомерности договоров присоединения между операторами ТфОП и операторами ТМС/ПД и, соответственно, о применимости положений 4-й главы ЗоС к данным правоотношениям. Самым простым и надежным способом избежать проблем при оформлении разрешений на эксплуатацию в данном случае является консультация у инспектора госсвязьнадзора, курирующего данного оператора. И провести такие консультации лучше в самом начале работ по созданию сети, до разработки проектной документации.

3. Мероприятия в области охраны труда и техники безопасности традиционно вызывают сильное раздражение руководителей операторов связи. Многие, и не без основания, говорят, что соблюдение всех правил ТБ и работа предприятия есть вещи несовместные. Однако, во-первых, небрежение элементарными правилами безопасности нередко влечет поражения электрическим током, падение с высоты, отравление метаном в подземных сооружениях и другие крайне неприятные последствия.

Более того, если на предприятии не организована работа в области охраны труда, сотрудники не прошли соответствующего обучения и инструктажа, то любой случай гибели или увечья сотрудника предприятия может повлечь уголовную ответственность руководителя предприятия. Таким образом, сравнительно небольшие затраты, необходимые для обучения персонала (или, зачастую, просто оформления «корочек») можно считать инвестициями в спокойный сон руководителей предприятий.

Зачастую операторы затрудняются предоставить Госсвязьнадзору документы, подтверждающие профессиональную квалификацию сотрудников. Для подтверждения профессиональных знаний и навыков сотрудников целесообразно организовать внутреннюю аттестационную комиссию, которая назначается приказом руководителя оператора связи. Председателем комиссии обычно назначается главный инженер или технический директор оператора.

Наличие внутренней аттестационной комиссии полностью устраняет проблему допуска сотрудников к самостоятельной работе и позволяет обойтись без всякого рода «сертификатов», юридический статус которых более чем сомнителен. (Например, производители оборудования не имеют лицензий на осуществление образовательной деятельности и выдаваемые ими сертификаты юридически не являются документами об образовании).

4. Оформление частотно-разрешительной документации должно осуществляться до начала проектных работ, поскольку разрешения на использование полос частот для эксплуатации РЭС в конкретных географических точках содержат важнейшие исходные данные для проектирования. Вопреки расхожему мнению, в России практически нет диапазонов, в которых допускается эксплуатация РЭС без специального разрешения или

регистрации. Исключения составляют РЭС радиоуправления моделями, сотовые телефоны федеральных стандартов (только абонентские терминалы), некоторые бытовые радиотелефоны.

В столь популярном диапазоне 2400 – 2483 МГц (IEEE 802.11b) эксплуатация РЭС допускается без оформления оператором специального решения ГКРЧ, но при наличии разрешения Государственной радиочастотной службы. Причем разрешение ГРЧС требуется независимо от мощности передатчика. Состав частотно-разрешительной документации будет рассмотрен отдельно по мере издания соответствующих нормативных правовых актов.

Следует различать разрешение на эксплуатацию объекта связи, оформляемое согласно приказу 113 и разрешение на эксплуатацию РЭС, оформляемое органами ГРЧС. Несмотря на схожесть названия данных документов, эти документы имеют различную природу. Разрешение на эксплуатацию объекта связи, если в состав объекта входят РЭС с излучением, выдается госсвязьнадзором только при наличии частотно-разрешительной документации, предусматривающей право данного оператора на использование полос частот для эксплуатации РЭС и на эксплуатацию данного РЭС, а также санитарных паспортов и иных документов, оформление которых предусмотрено действующим законодательством.

В частотно-разрешительная документации должна предоставлять право на эксплуатацию РЭС именно для предоставления услуг связи, поскольку требования ЭМС для операторов связи более жесткие, чем для владельцев внутрипроизводственных сетей. Оформление частотно-разрешительной документации есть процесс долгий и дорогостоящий.

Необходимо получить решение ГКРЧ (до полугода, за исключением случаев наличия общего решения ГКРЧ или использования оборудования отечественного производства), заключение об электромагнитной совместимости (ЭМС) с РЭС гражданского и негражданского назначения (может занять несколько лет!) и лишь затем ГРЧС оформляет разрешение на эксплуатацию РЭС. Стоимость и длительность этих процедур такова, что в городских условиях экономически выгоднее строить волоконно-оптические линии связи.

5. Градостроительный кодекс определяет проектную документацию как «графические и текстовые материалы, определяющие объемно-планировочные, конструктивные и технические решения». Различают одностадийное и многостадийное проектирование (СнИП 11.01.95). Многостадийное проектирование подразумевает последовательную разработку:

- Обоснования инвестиций (стадия ОИ) с последующей государственной экспертизой в установленном порядке. ОИ утверждаются заказчиком после госэкспертизы;
- Технико-экономического обоснования создания объекта (стадия «П»). Заметим, что ТЭО и является проектом объекта согласно официально принятой терминологии. ТЭО подлежит госэкспертизе и утверждению заказчиком. ТЭО (проект) относится к так называемой «утверждаемой части» проектной документации;
- Рабочей документации (стадия «Р»), то есть рабочих чертежей, схем, спецификаций и других документов, необходимых для производства строительно-монтажных работ.

Отдельным томом выпускается сметная документация, которая разрабатывается на основании проекта и рабочей документации в соответствии с технологическими картами и утвержденными Госстроем единичными расценками.

Одностадийное проектирование осуществляется по решению заказчика при разработке проектной документации на создание технически несложных объектов (что практически означает – почти любых объектов связи, поскольку одностадийное проектирование выполняется гораздо быстрее и дешевле). Результатом одностадийного проектирования является «Рабочий проект» в состав которого входит общая пояснительная записка (ОПЗ) и рабочая документация (РД).

Разработка проектной документации должна осуществляться проектными организациями, имеющими соответствующие лицензии. Копия лицензии прикладывается к проектной документации. Необходимо также заключение государственной экспертизы проектной документации, которую, в соответствии с приказом Минсвязи от 22.07.2003 № 96 проводит ФГУ «ЦНИЭС» (Москва, Тверская ул., дом 7, тел. (095)-292 12-13, директор Филюшин Юрий Иванович).

Институт государственной экспертизы проектной документации введен постановлением Правительства от 27.12.2000г. №1008, которым определено разграничение полномочий между федеральными органами исполнительной власти в данной области. Государственную экспертизу проектной документации на создание любых объектов, строительство которых финансируется за счет средств федерального бюджета, вправе проводить исключительно ГУ Главгосэкспертиза при Госстрое РФ, заключение которой вполне приемлемо для Госсвязьнадзора, если показать инспектору указанное постановление Правительства.

Приказом Минсвязи от 22.07.2003 г. № 96 утверждено Положение о государственной экспертизе предпроектной и проектной документации Министерства РФ по связи и информатизации. Пункт 2.3 положения предусматривает, что «Государственной экспертизе Минсвязи России подлежит предпроектная и проектная документация на строительство объектов информатизации, почтовой и электрической связи сети связи общего пользования, независимо от источников финансирования, за исключением объектов, отнесенных к компетенции Главгосэкспертизы России…».

Таким образом, государственной экспертизе подлежит вся без исключения проектная документация на создание объектов в области связи. Это, в свою очередь, означает, что руководитель оператора связи или заказчика объекта связи не имеет права утверждать проектную документацию до получения заключения госэкспертизы с рекомендацией об утверждении проекта.

Надо заметить, что пунктом 2.3 приказа 96 фактически установлена обязательность госэкспертизы объектов информатизации. Это означает, что ввод в эксплуатацию удостоверяющих центров электронной цифровой подписи (ЭЦП) потребует оформления заключения ФГУ ЦНИЭС, что, в свою очередь, приводит к обязательности разработки проектной документации на создание УЦ ЭЦП.

Особую сложность для небольших операторов представляет оформление и согласование проектной документации на узлы связи в части электроустановок (обеспечения электроснабжения). Данный раздел проекта разрабатывается на основании технических условий и разрешения на присоединение электрической мощности, выдаваемого энергоснабжающей организацией и подлежит согласованию с энергосбытовой

организацией в части приборов учет электроэнергии и территориальным органом Государственного энергетического надзора.

Последнее является непростым делом, требующим квалификации проектировщика, а также затрат разного рода, включая мотивацию сотрудников Энергонадзора. Как показывает практика, без «мотивационных мероприятий» согласование проекта электроустановки может затягиваться на многие месяцы…. Более подробно процедура разработки и согласования проектов электроустановок будет рассмотрена в следующих разделах.

Одновременно с разработкой проектной документации желательно разработать эксплуатационную документацию. Не следует путать эксплуатационную документацию (ЭД) на оборудование, входящее в состав объекта связи и эксплуатационную документацию на весь объект связи в целом, которая как раз и требуется для последующей приемки объекта в эксплуатацию. Существует два разных подхода к разработке ЭД – производственный и строительный.

Производственный подход подразумевает разработку четырех документов – технического описания, инструкции по монтажу, инструкции по эксплуатации и формуляра, в котором отражаются эксплуатационно-технические и регламентные работы (ГОСТ 2.601). Совершенно очевидно, что для сетей связи, являющихся объектом строительно-монтажных работ, данный подход абсолютно неприемлем – ну какая, например, может быть инструкция по монтажу уже построенной ВОЛС.

Строительный подход к разработке эксплуатационной документации подразумевает подготовку комплекта инструкций по эксплуатации объекта связи, в который входят инструкции изготовителей оборудования, а также инструкция по эксплуатации объекта в целом. Эту работу целесообразно поручить проектной организации и специально указать в задании на проектирование. Тогда, как прошедшая государственную экспертизу в составе проекта, подготовленная ЭД не может вызвать претензий со стороны Госсвязьнадзора. Другая часть ЭД включает так называемые аппаратные и кабельные журналы, в которых указываются все контрольные замеры и проведенные испытания, а также журнал регистрации повреждений.

В состав комплекта ЭД входят инструкции по эксплуатации оборудования, входящего в состав объекта связи. Однако поставщики аппаратуры далеко не всегда прилагают документацию на русском языке, этим грешат даже гиганты, например, Cisco Systems, Allied Telesyn, да и большинство других производителей, ссылаясь на отсутствие таких документов. В этом есть большая доля лукавства – наличие эксплуатационной документации на русском языке является обязательным условием сертификации в ССС, поэтому, коль скоро на данное оборудование выдан сертификат, – комплект ЭД был разработан и предоставлен соответствующей испытательной лаборатории (ИЛ).

Причина «засекречивания» ЭД на оборудование прозаична и проста: документы, переданные ИЛ, имеют самое отдаленное отношение к эксплуатации соответствующего оборудования, ограничиваясь в основном перепечаткой Технических условий на соответствующую аппаратуру. Вот производители и не хотят позориться…

Операторы выходят из положения по-разному. Некоторые просто «прогоняют» англоязычные описания через автопереводчик. Получается очень забавно, но, поскольку инспектор не вдается в детали текста, такой метод частенько приводит к успеху. Вот

только использовать изготовленную таким способом инструкцию можно только для предъявления инспектору….

Весьма желательно в проектной или эксплуатационной документации привести перечень средств измерений, необходимых для метрологического обеспечения эксплуатации объекта связи. Однако надо иметь в виду, что Госсвязьнадзор не выдаст разрешение на эксплуатацию объекта связи без предъявления соответствующих измерительных приборов. Поскольку это оборудование зачастую стоит немалые деньги, можно просто заключить договор на метрологическое обеспечение объекта с каким-нибудь предприятием и предъявить его инспектору. Данный вид деятельности лицензированию не подлежит….

Некоторые территориальные органы Госсвязьнадзора по-прежнему требуют от операторов положение о метрологической службе, согласованное с главным метрологом Минсвязи ссылаясь не требование приказа Минсвязи от 17.06.96 № 159 «О метрологической службе Минсвязи России». Если ЭД предусматривает метрологический контроль, то разработка положения о метрологической службе действительно обязательна согласно закону «О единстве средств измерений».

Что же касается согласования с главным метрологом Минсвязи, то не существует нормативного правового акта, зарегистрированного Минюстом РФ, и обязывающего операторов заниматься этими согласованиями. Соответственно, незаконно и требование о согласовании положения о метрологической службе оператора связи с любыми органами государственной власти. Более того, пункт 7 приказа 159 прямо возлагает финансирование работ по организации метрологической службы на само Минсвязи. Так что до поступления целевого финансирования, оператор вправе игнорировать требования приказа

Вообще, «измерением» называют сравнение некоторой физической величины с эталоном ее единицы измерения. Эталон всегда, по определению, существует в единственном экземпляре во всем мире, а его признание обеспечивается международными соглашениями, которые, кстати, подлежат ратификации и являются объектом международного права.

Разумеется, при проведении каждого измерения невозможно сравнивать физическую величину непосредственно с единственным эталоном, поэтому каждое государство обеспечивает единую систему средств измерений, единство и системная целостность которой регулируется национальным законодательством. В результате в любой стране метр, вольт, ампер и т. д. одинаковы и обозначают одно и то же, что, собственно, и является следствием единства средств измерений.

В Российской Федерации принят специальный федеральный закон «Об обеспечении единства измерений» от 27.04.1993г. №4871-I, который регулирует отношения в области метрологии и определяет основные правила организации метрологического обеспечения. Согласно этому закону, аппаратура, предназначенная для измерения физических величин подлежит обязательной сертификации в качестве средства измерения, результатом которой является включение соответствующего прибора в государственный реестр средств измерений, о чем выдается соответствующий сертификат.

При этом каждое средство измерений подлежит периодической государственной поверке, то есть метрологическому контролю и калибровке, которая выполняется организациями, имеющими аккредитацию федерального органа исполнительной власти по

стандартизации и метрологии (в настоящее время – Федеральное агентство по техническому регулированию и метрологии).

Каждое сравнение с эталоном, то есть «измерение» физической величины, производится с некоторой, точностью, которая определяется погрешностью средства измерения. Разумеется, погрешность эталонных приборов должна быть существенно, обычно – на порядки, меньше точности калибруемых средств измерений, поскольку итоговая погрешность равна суперпозиции погрешностей всех средств измерений в цепочке от международного эталона.

Для обеспечения единства средств измерений служит их государственная поверка, то есть калибровка измерительной аппаратуры специально уполномоченными органами. Порядок обеспечения единства измерений в пределах одного предприятия и устанавливается соответствующим положением о метрологической службе.

Надо различать «измерение» и «учет». Учет, в отличие от измерения, представляет собой не сравнение с эталоном, а прямой пересчет объектов. Например, количество слитков золота подлежит учету, а масса каждого слитка – измерению. Разумеется, учет производится с абсолютной точностью и метрологическому контролю не подлежит. В самом деле, бухгалтерия любого предприятия учитывает количество денег на расчетном счете без всякой погрешности, да и зарплату в кассе желательно выдавать точно по ведомости…

Заметим, что единица информации – байт, не является физической величиной и не может подлежать метрологическому контролю. Определение объема трафика в байтах не требует проведения измерений, то есть сравнения с «эталоном байта» поскольку такого эталона не существует и существовать не может. Байты можно «пересчитать», а не «измерить». Поэтому средства учета объема информации не подлежат внесению в реестр средств измерений и государственной поверке. При этом, например, аппаратура учета времени соединения, напротив, подлежит внесению в госреестр и государственной поверке, поскольку фактически предназначено не для учета, а для измерения времени как физической величины.

6. Обеспечение системы оперативно-розыскных мероприятий осуществляется совместно с территориальным управлением Федеральной службы безопасности. Требования к системе ОРМ определяются соответствующими нормативными правовыми актами, конкретная их реализация производится согласно плану мероприятий, согласованному оператором связи и УФСБ.

Наличие согласованного плана мероприятий по СОРМ либо письма из УФСБ об отсутствии возражений против начала предоставления услуг связи до завершения разработки указанного плана, является обязательным условием оформления разрешения на эксплуатацию. В настоящее время практически на всех объектах связи должна устанавливаться СОРМ, включая узлы передачи данных и телематических служб сети Интернет.

2. Уведомление о начале работ

Уведомление о начале работ по созданию (реконструкции, расширению, техническому перевооружению) объекта связи составляется по форме, указанной в приложении «Б» к приказу 113 и оформляется оператором связи, который будет получать соответствующее разрешение на эксплуатацию. На основании полученных уведомлений орган

госсвязьнадзора формирует план своей работы. Заполнение бланка уведомления обычно не представляет никаких сложностей.

Никаких дополнительных документов к Уведомлению прикладывать не требуется.

3. Строительно-монтажные работы

Строительные и монтажные работы (СМР) по созданию сети должны выполняться в соответствии с проектной документацией, утвержденной ранее заказчиком объекта связи. В случае, если в процессе выполнения СМР обнаружится невозможность точного соблюдения рабочей документации, допускается незначительные отклонения от проекта, если такие отклонения ограничены рабочей документацией и не требуют внесения изменений в утверждаемую часть проекта (Общую пояснительную записку, ТЭО, сметную часть). Все отступления от рабочих чертежей проекта указываются в так называемой исполнительной документации.

СМР должны выполняться организацией, имеющей лицензию Госстроя России на право производства соответствующих видов работ. В принципе, действующее законодательство не запрещает выполнение СМР своими силами (хозяйственным способом). Строго говоря, создание одного объекта не является «деятельностью», поскольку термин «деятельность» подразумевает систематическое выполнение соответствующих работ в интересах различных лиц. Однако четкого определения термина «деятельность» действующее законодательство не содержит, что позволяет органам госсвязьнадзора отказывать в выдаче разрешения на эксплуатацию объектов, построенных лицами, не имеющими лицензий Госстроя России, даже если создание сети осуществлялось самим оператором хозяйственным способом.

В процессе проведения пуско-наладочных работ производятся необходимые измерения и испытания законченного строительством объекта. Результаты измерений и испытаний оформляются соответствующими протоколами и подшиваются в исполнительную документацию. Надо особо отметить, что инспектор госсвязьнадзора обязательно затребует на проверку протоколы измерений. Обязательному метрологическому контролю при приемо-сдаточных испытаниях подлежат все физические цепи, включая волоконно-оптические линии.

Для ВОЛС необходимо иметь протоколы рефлектометрических измерений в части затухания оптического сигнала на длине волны эксплуатации. Измерения производятся оператором самостоятельно, либо строительно-монтажной организацией с использованием аппаратуры, прошедшей государственную поверку и внесенной в реестр средств измерений. Неофициально допускается использование неповеренной аппаратуры, поверка которой почти невозможна в условиях испытательных лабораторий Госстандарта, например – оптических рефлектометров. Но, разумеется, официально уведомлять об этом инспектора госсвязьнадзора не стоит….

Вообще, все измерения производятся в целях установления соответствия построенных сооружений требованиям нормативно-технических документов отрасли. Однако, если для телефонных сетей такие нормативные документы разработаны и введены (например, Эксплуатационные нормы на электрические параметры каналов сети ТфОП, утвержденные Приказом Госкомсвязи России от 05.04.99 № 54), то для сетей и систем передачи данных таких документов практически нет. Что, с одной стороны – плохо, потому что оставляет место для произвола надзорных органов, а с другой стороны – хорошо, потому что не требуются многочисленные и не всегда простые измерения.

4. Организационная готовность оператора к оказанию услуг связи

Понятие «организационная готовность» подразумевает выполнение оператором связи определенных требований, установленных как отраслевыми, так и общими нормами. Обеспечение организационной готовности оператора связи не связано прямо с вводом в эксплуатацию конкретного объекта связи и распространяется на всю производственную деятельность предприятия. Многие из требований к операторам связи одинаковы для всех субъектов экономической деятельности, связанной с эксплуатацией технических средств.

Ряд организационных требований, предъявляются специально к операторам связи и соблюдение их проверяется органами Госсвязьнадзора как при вводе в эксплуатацию отдельных сооружения связи, так и при осуществлении общего контроля лицензируемой деятельности (КЛД). При этом Госсвязьнадзор вправе выдать предписание об устранении недостатков и (или) запретить ввод в эксплуатацию объекта связи до устранения недостатков, указанных в соответствующем предписании. Более того, неисполнение предписания в установленный срок влечет административную ответственность согласно ст. 19.5 КоАП РФ.

Рассмотрим отдельно общие и специальные организационные требования к операторам связи, соблюдение которых проверяется органами Госсвязьнадзора:

А. Общие организационные требования

1. Соблюдение норм и правил охраны труда и техники безопасности. Наличие инструкций по технике безопасности в местах, доступных для ознакомления персоналом. Наличие заполненных журналов инструктажа сотрудников, средств индивидуальной защиты, специальной одежды и обуви. Прохождение сотрудниками обучения в области охраны труда и техники безопасности в специализированных учебных организациях, наличие соответствующих удостоверений, в том числе о присвоении квалификационных групп по технике электробезопасности.
2. Соблюдение правил эксплуатации электроустановок. (Проверяется как Госсвязьнадзором, так и Госэнергонадзором, при этом заключение Госэнергонадзора имеет большую юридическую силу). Требуется наличие проектной документации на электроустановку, согласованной с энергоснабжающей организацией и Госэнергонадзором, а также Акта допуска электроустановки к эксплуатации, протоколов измерений параметров заземления, изоляции и потерь мощности. Квалификационные группы по электробезопасности, присвоенные персоналу, должны соответствовать служебным обязанностям. Лицо, ответственное за электрохозяйство предприятия должно назначаться специальным приказом руководителя оператора связи. Полный перечень требований к организации эксплуатации электроустановок содержится в действующей редакции «Правил технической эксплуатации электроустановок потребителей», введенных в действие нормативными документами Государственного энергетического надзора России.
3. Соблюдение правил пожарной безопасности. Требования к обеспечению противопожарных мероприятий определяются нормативными документами Государственной противопожарной службы МЧС России (НПБ, ППБ и т.д.). Выполнение указанных требований зачастую весьма затруднительно как по экономическим, так и по техническим причинам. В частности, установка автоматической системы газового пожаротушения в помещениях узлов связи формально обязательна… поэтому обычно операторы связи ограничиваются

установкой самосрабатывающих огнетушителей. Проектная документация на устройство охранно-пожарной сигнализации и иных противопожарных систем должна быть выполнена организацией, имеющей специальную лицензию МЧС РФ и согласована с территориальным органом Государственной противопожарной службы (ГПН). Монтаж средств огнезащиты также осуществляется при наличии соответствующей лицензии МЧС. К сожалению, лицензии Госстроя России в данном случае не применимы, поскольку закон «О лицензировании отдельных видов деятельности» прямо относит лицензирование деятельности в области противопожарных мероприятий к компетенции ГПН. Итоговым документом, подтверждающим надлежащее соблюдение противопожарных требований, является Заключение Государственной противопожарной службы, которого более чем достаточно для предъявления Госсвязьнадзору. Практика показывает, что оформление заключений ГПН есть в основном продукт договоренности с уполномоченными сотрудниками Государственной противопожарной службы….

4. Соблюдение санитарных норм и правил. Основной задачей является аттестация рабочих мест по уровню освещенности, шума, достаточности площади и т.д. Аттестация производится органами Государственного санитарно-эпидемиологического надзора (ЦГСЭН) и представляет собой трудоемкий процесс, требующий довольно значительных инвестиций. На первом этапе можно ограничиться оформлением заключения ЦГСЭН о пригодности помещений для эксплуатации узлов связи.
5. Соблюдение единства средств измерений. Использование измерительного оборудования, включенного в государственный реестр средств измерений, наличие действующих свидетельств о государственной поверке, период проведения которых определяется технической документацией на соответствующую аппаратуру. Необходимо утвержденное руководителем предприятия положение о метрологической службе, приказа о назначении главного метролога. (При отсутствии на предприятии средств измерений либо наличии договора на метрологическое обеспечения сторонней организацией не требуется положение о метрологической службе и предоставлении документов на метрологическое оборудование.)
6. Формализация работы персонала. Наличие штатного расписания, трудовых договоров (контрактов) и должностных инструкций, утвержденных руководителем предприятия. Одновременно с подписанием трудового договора, сотрудник знакомится с должностной инструкцией и подписывает ее в графе «ознакомлен». Вообще, проверка соблюдения трудового законодательства не входит в компетенцию Госсвязьнадзора (это функция Гострудинспекции), однако проще выполнить данный пункт, чем спорить с инспектором. Допуск сотрудника к самостоятельной работе осуществляется распоряжением руководителя оператора на основании сведений о прохождении инструктажей по технике безопасности и охране труда, а также решения внутренней аттестационной комиссии о соответствии знаний и навыков сотрудника производственно-техническим нуждам предприятия. Все инструктажи и аттестацию желательно проводить в течение испытательного срока сотрудника.
7. Организация делопроизводства и документального оборота. Бюрократию можно любить или ненавидеть, но правильная организация делопроизводства есть непременное условие легализации деятельности любой компании.

Б. Специальные организационные требования

1. Договорные отношения с операторами взаимодействующих сетей. Согласно ст. 18 ЗоС, присоединение сетей электросвязи общего пользования осуществляется на

основании договоров о присоединении. Заключение договоров о присоединении обычно производится операторами на основании Технических условий (Условий присоединения), которые выдаются оператором присоединяющей сети. Условия присоединения должны содержать все существенные условия договора о присоединении сетей связи согласно п. 3 ст 18 ЗоС и п. 3 ст. 19 ЗоС. Операторы, занимающие существенное положение в сети связи общего пользования (согласно ст. 2 ЗоС - располагающие 25% от ресурса нумерации, монтированной емкости или пропущенного трафика на территории данного региона), обязаны в семидневный срок опубликовать условия присоединения в качестве публичной оферты. Условия присоединения должны соответствовать правилам присоединения, которые утверждаются Правительством России.

2. Договорные отношения с абонентами (пользователями) услуг связи оператора. Следует отличать договоры с абонентами – юридическими лицами и абонентами – физическими лицами. Согласно ст. 45 ЗоС, договор с абонентом - физическим лицом является публичным договором, то есть оператор не вправе вводить особые условия предоставления услуг связи для конкретного абонента. Тарифы оператора для физических лиц должны быть утверждены приказом руководителя оператора связи. Правила оказания услуг связи утверждаются Правительством России. Кроме того, приказом руководителя оператора должен быть утвержден порядок предоставления бесплатной связи для вызова экстренных служб и порядок предоставления льгот, предусмотренных действующим законодательством.
3. Законные права пользования помещениями, зданиями и сооружениями. Документы, подтверждающие право оператора на пользование офисными и технологическими помещениями. Такими документами являются свидетельство о государственной регистрации права собственности либо договор аренды помещений. Надо заметить, что договор аренды недвижимого имущества, заключаемый на срок более одного года, подлежит обязательной государственной регистрации (ст. 651 ГК РФ).
4. Статистическая отчетность. Операторы связи обязаны предоставлять специальную статистическую отчетность. Отчетность представляется в местные органы статистики, а также в МИТС.
5. Отчисления операторов связи. Согласно п. 2 ст. 27 ЗоС, все без исключения операторы связи, имеющие соответствующие лицензии, обязаны отчислять в пользу федерального бюджета часть доходов, полученных от реализации возмездных услуг связи. Соответствующие денежные средства используются для финансирования Госсвязьнадзора. Ставка отчислений установлена в размере 0,3% от объема реализации услуг связи без НДС. Реквизиты бюджетных счетов и код бюджетной классификации для перевода отчислений можно узнать в территориальной налоговой инспекции.
6. Организация технической эксплуатации сети связи. Общее требование к организации эксплуатации сети связи – обеспечение надежности и оперативного устранения неисправностей, учет жалоб абонентов и контроль устранения причин жалоб и претензий. Для некоторых объектов и технических средств связи установлен особый порядок эксплуатации, например – таксофоны, РЭС и т.п.

Выполнение всех организационных и организационно-технических мероприятий потребует от оператора связи проведения серьезной работы по разработке множества внутренних правовых актов, инструкций, журналов и реестров, а также довольно значительных инвестиций в организационную структуру предприятия, приобретение средств индивидуальной защиты и спецодежды, создание противопожарных, организацию метрологической службы.

Тем не менее, аккуратное выполнение организационных требований позволит с одной стороны избежать претензий и штрафов со стороны различных надзорных органов, а с другой стороны избежать затрат времени и сил на судебные разбирательства. Кроме того, в случае чрезвычайных происшествий или несчастных случаев (что, увы, случается), аккуратное следование правилам организации производственной деятельности поможет сократить или значительно уменьшить глубину взаимоотношений с органами прокуратуры и милиции.

Разумеется, не каждый небольшой оператор физически способен выполнить все организационные требования. Есть несколько простых, но, увы, юридически не бесспорных, способов уменьшить расходы на обеспечение организационной готовности. Конечно, видимость проведения мероприятий и действительное их осуществление есть вещи разные и в случае серьезной проверки оператора все тайное вполне может стать явным… после чего тайной уже станет сама деятельность оператора.

Сократить затраты на организацию технической эксплуатации можно путем заключения договора со сторонней организацией. При этом не требуется создание метрологической службы, приобретение средств измерений, создание бригад по техническому обслуживанию и оперативному ремонту линейных сооружений и, соответственно, приобретение средств индивидуальной защиты и спецодежды.

Сократить затраты на санитарное и противопожарное оснащение можно путем непредоставления соответствующих заключений инспектору Госсвязьнадзора, благо приказ 113 не предусматривает проведение проверки наличия этих документов. В то же время, инспектор обязан проверить пункт лицензии Минсвязи, обязывающий оператора к соблюдению действующего законодательства, так что формально инспектор имеет право затребовать у оператора соответствующие документы, а в случае их отсутствия выдать соответствующее предписание. Срочное оформление заключений ГПН и ЦГЭСН потребует больших усилий и еще больших затрат…

Впрочем, использование личных договоренностей с сотрудниками надзорных органов делает бессмысленной затраты на легализацию деятельности. Половинчатые решения частенько обесцениваются полностью.

5. Создание и организация работы рабочей комиссии по приемке в эксплуатацию законченного строительством объекта связи

До создания рабочей комиссии необходимо завершить все строительно-монтажные работы и провести предварительные испытания. Лучше всего, если методика приемосдаточных испытаний войдет в состав проектной документации, что исключит любые споры с представителями госсвязьнадзора по данному поводу. Если же методика испытаний разрабатывается индивидуально, то ее следует заранее согласовать с курирующим инспектором, хотя бы в устной форме.

Состав рабочей комиссии определяется заказчиком создания соответствующего объекта связи (п. 3.7 приказа 113). На самом деле, этот вопрос куда сложнее, чем кажется, ввиду наличия письма Минстроя РФ от 13.02.1996 г. № БЕ-19-4/9 «Об упорядочении процесса согласования проектов строительства», согласно которому полномочия по определению перечня согласующих организаций принадлежат органу субъекта Российской Федерации, уполномоченному в области архитектуры и строительства (различные АПУ, АПО и т.п.).

С другой стороны, нормы законодательства в области связи являются специальными по отношению к общим нормам строительства. Да и статус письма Минстроя как нормативного правового акта весьма сомнителен (не зарегистрирован Минюстом РФ). Таким образом, с юридической точки зрения право определения состава рабочей комиссии принадлежит заказчику создания объекта, который должен издать соответствующий приказ.

В состав приемочной комиссии входит представитель госсвязьнадзора (п. 3.7 приказа 113). За две-три недели до начала работы приемочной комиссии, а вообще – чем раньше, тем лучше, надо направить в территориальный орган госсвязьнадзора письмо с запросом об участии их представителя в работе комиссии. К письму желательно приложить схему организации связи, краткую пояснительную записку и перечень оборудования из спецификации проекта. Перечень оборудования особенно важен, поскольку именно это оборудование будет указано на обороте разрешения на эксплуатацию. На «бытовом» жаргоне госсвязьнадзора пояснительную записку с приложениями часто называют «предъявительской запиской».

В состав рабочей комиссии целесообразно включать представителей проектной организации, разработавшей проектную документацию, и всех подрядных организаций, выполнивших строительно-монтажные и пусконаладочные работы. Включение в состав приемочной комиссии представителей санэпиднадзора и госпожнадзора целесообразно только в тех случаях, когда необходимо согласование проектной документации с данными органами.

В частности, если проектом предусмотрена строительная подготовка помещений, особенно с их перепланировкой. К сожалению, уровень коррупции в органах СЭС и ОГПН очень высок, что зачастую не дает возможности принять в эксплуатацию объекты связи. Лучшим способом оформления взаимоотношений с СЭС и ОГПН является оформление отдельных заключений о допуске помещений к эксплуатации в качестве узлов связи до начала работы приемочной комиссии. Что касается необслуживаемых узлов связи, то оформление заключений ОГПН желательно, но мало кто из операторов реально способен получить такие заключения…

Если на объекте связи используются РЭС, необходимо письменно уведомить территориальный орган ГРЧС о предстоящем первом включении РЭС не позднее, чем за 10 дней (п. 5.3 приказа 113). При этом все необходимые измерения на РЭС производятся самим оператором, участие представителей ГРЧС в проведении измерений определяется самим территориальным органом ГРЧС на основании полученного уведомления о первом включении РЭС. Пункт 5.2 приказа 113 предоставляет соответствующему органу ГРЧС направить своего представителя для участия в работе приемочной комиссии.

Таким образом, уведомление о первом включении РЭС должно содержать запрос об участии представителей ГРЧС в проведении измерений и запрос на участие представителей ГРЧС в работе приемочной комиссии. Практика показывает, что в большинстве случаев ГРЧС отказывается от непосредственного участия в работе по наладке и приемке РЭС в составе объектов связи, однако по возможности надо постараться получить отказ в письменном виде.

До включения электропитания на оборудование узлов связи необходимо провести ряд контрольных измерений параметров электроустановки (сопротивление цепи заземления, цепи фаза-нуль и т. п.) В настоящее время лицензирование деятельности по проведению измерений электроустановок отменено вместе с изъятием у Энергонадзора полномочий

лицензиара. Тем не менее, Энергонадзор осуществляет обязательную аккредитацию электроизмерительных лабораторий, и приложение соответствующим протоколам измерений аттестата аккредитации является обязательным.

Результатом работы приемочной комиссии является акт приемки рабочей комиссией законченного строительством объекта (форма КС-14), утвержденный руководителем заказчика объекта. Акт приемки утверждается руководителем заказчика при наличии подписей всех членов комиссии (п. 3.8 приказа 113). Утвержденный акт удостоверяет соответствие созданного объекта связи и утвержденной проектной документации, а также положительный результат проведенных приемосдаточных испытаний. Таким образом, акт удостоверяет техническую готовность объекта связи к использованию для предоставления услуг согласно имеющимся у оператора лицензиям.

К акту приемки должны быть приложены все протоколы измерений, испытаний (полный комплект исполнительной документации), копии лицензий оператора связи, заказчика, проектировщиков, а также всех подрядных организаций.

6. Заключение Госсвязьнадзора

Помимо участия в работе приемочной комиссии, инспектор Госсвязьнадзора проверяет выполнение оператором различных требований в области организации производственной деятельности (организационная готовность). Результатом проверки является Заключение, которое прилагается к акту приемочной комиссии (п. 5.5 приказа 113). Акт рабочей комиссии вместе с Заключением являются безусловным основанием для оформления разрешения на эксплуатацию объекта связи. Таким образом, одновременно с проверкой объекта связи, фактически проверяется и деятельность оператора связи, который этот объект будет эксплуатировать.

Вообще, приказ 113 пунктом 5.5 ограничивает предмет заключения только двумя вопросами:

- соответствие принимаемого в эксплуатацию объекта утвержденной проектной документации;
- соответствие услуг связи, для предоставления которых предназначен объект, имеющимся у оператора лицензиям.

Однако законодатель не принял во внимание, что проверить соответствие объекта проектной документации может только проектировщик, а вопросы соответствия функционального назначения объекта имеющимся у оператора лицензиям решаются в процессе государственной экспертизы проектной документации. Таким образом, подготовка заключения согласно формальным требованиям п. 5.5 приказа 113 становится бессмысленной формальностью.

Однако Госсвязьнадзор нашел выход из положения – при приемке объекта связи осуществляется полный или частичный контроль лицензируемой деятельности (КЛД) оператора. Если оператор впервые вводит в эксплуатацию объект связи, КЛД производится всегда в полном объеме. Таким образом, заключение Госсвязьнадзора, предусмотренное п. 5.5 приказа 113 полностью или почти полностью совпадает с заключением по результатам проведения планового или внепланового КЛД.

Подготовка заключения производится по документам, представленным оператором связи, за исключением жалоб и обращений, поступивших непосредственно в Госсвязьнадзор

помимо воли оператора. Оператор представляет инспектору Госсвязьнадзора два основных документа – справку о выполнении условий действия лицензии и предъявительскую записку.

Справка о выполнении условий действия лицензии представляет собой сведения о выполнении каждого из условий действия лицензии. По каждому из пунктов лицензионных условий оператор самостоятельно делает вывод – «выполняется», «выполняется частично» или «не выполняется». К справке прилагаются копии документов из приведенного ниже перечня (пункты помечены «звездочкой»). Прилагаемые документы передаются инспектору Госсвязьнадзора в отдельной папке с оглавлением.

Предъявительская записка содержит наименование, местонахождение и банковские реквизиты оператора, номера лицензий и свидетельств о регистрации лицензиата, сведения о вводимом в эксплуатацию объектов связи – наименование местонахождение, схема организации связи и техническое описание объекта, титул проектной документации и наименование проектировщика, сведения о государственной экспертизе и утверждении проектной документации, монтированной абонентской емкости и иных параметрах вводимого в эксплуатации объекта.

Для подготовки заключения инспектору Госсвязьнадзора предоставляются следующие документы (прилагаются к справке о выполнении условий действия лицензий):

1. *Лицензии оператора связи;
2. *Свидетельства о регистрации лицензиата;
3. *Акт (акты) рабочей комиссии по вводу в эксплуатацию (оригинал для подписания представителем Госсвязьнадзора – при проведении КЛД в связи с приемкой в эксплуатацию законченного строительством объекта связи);
4. *Справка о выполнении условий лицензии – оригинал;
5. *Предъявительская записка - оригинал;
6. *Копии сертификатов соответствия системы сертификации «Связь» на все технические средства вводимых в эксплуатацию объектов связи;
7. *Схема организации связи с указанием присоединяющих и присоединяемых сетей, схемы линейных сооружений;
8. *Справка о применяемых автоматизированных системах расчетов (АСР) либо справка об отсутствии АСР (оригинал);
9. Проектная документация и приказ (приказы) об утверждении проектной документации;
10. *Заключения государственной экспертизы проектной документации;
11. Оформленные ранее разрешения на эксплуатацию объектов связи данного оператора;
12. *Перечень взаимодействующих сетей с указанием адресов точек присоединения, номеров лицензий и номеров разрешений на эксплуатацию взаимодействующих сетей в точках присоединения;
13. Договоры присоединения сетей связи;
14. *Копии лицензий и разрешений на эксплуатацию присоединяющих и присоединяемых сетей связи;
15. *Технические условия на присоединение, выданные оператором присоединяющих сетей связи;
16. Эксплуатационная документация на объекты связи;
17. *Решения Государственной комиссии по радиочастотам и разрешения на использование полос частот для эксплуатации радиоэлектронных средств,

свидетельства о регистрации РЭС. (При наличии РЭС в составе сети связи оператора или принимаемого в эксплуатацию объекта связи);
18. *Должностные инструкции персонала;
19. *Приказы: о назначении лиц, ответственных за электрохозяйство, о назначении рабочей комиссии по приемке законченного строительством объекта связи, об утверждении тарифов (для абонентов – физических лиц), порядке предоставления льгот, о создании аттестационной комиссии.
20. *Заключения центра санитарно-эпидемиологического надзора;
21. Аттестаты рабочих мест;
22. Паспорт на заземляющее устройство, протоколы испытаний заземляющих устройств, протоколы измерений параметров электроустановок;
23. Инструкции ТБ и охране труда;
24. Журнал учета и содержания средств защиты (укомплектованность средствами защиты);
25. Журналы инструктажа и проверке знаний по ТБ и охране труда (наличие у персонала удостоверений по охране труда и ТБ).
26. *Сведения о противопожарных мероприятиях либо заключение Государственной противопожарной службы;
27. Укомплектованность средствами оказания первой помощи (аптечки).
28. Протоколы внутренней аттестационной комиссии;
29. Журнал учета повреждений;
30. Документация по метрологическому обеспечению (положение о метрологической службе, перечень и журнал и свидетельства государственной поверки приборов, договоры по метрологическому обслуживанию);
31. *Схема энергоснабжения, однолинейная схема, акт разграничения балансовой принадлежности и эксплуатационной ответственности между энергоснабжающей организацией и потребителем (если не выполнено в составе проектной документации на создание объекта связи);
32. Содержание и эксплуатация помещения аккумуляторной и аккумуляторных батарей (батарейные журналы) – если такие помещения имеются;
33. Работа с письмами, обращениями и жалобами пользователей услугами связи.
34. *Статистическая отчетность;
35. *Документы по СОРМ – согласованный с УФСБ план мероприятий по внедрению СОРМ, акт ввода ТСС СОРМ в эксплуатацию либо письмо УФСБ об отсутствии возражений против начала эксплуатации объекта связи до реализации СОРМ;
36. *Копия платежных поручений на перевод отчислений (0,3%), если оператор оказывал услуги связи.

Примечание:

копии документов, помеченные «*» предоставляются инспектору приложением к справке о выполнении условий действия лицензии.

Все указанные выше документы необходимо хранить и постоянно обновлять, не ограничиваясь периодом приемки в эксплуатацию очередного объекта связи, поскольку Госсвязьнадзор и другие надзорные органы вправе проверить деятельность оператора в любое время.

Упрощенная процедура приемки в эксплуатацию объектов связи

Упрощенная процедура приемки в эксплуатацию и оформления разрешения на эксплуатацию применяется исключительно к объектам связи, перечень типов которых

приведен в приложении «А» к приказу 113. С юридической точки зрения, упрощенная процедура является специальной, то есть имеющей большую юридическую силу, нежели общая, однако может применяться только в отношении объектов, прямо указанных в приложении А. Поэтому никакое расширительное толкование перечня не допускается.

Анализ приложения «А» к приказу 113 не позволяет выявить внятную логику в формировании перечня объектов связи, приемка в эксплуатацию которых производится в упрощенном порядке. Складывается впечатление, что сам перечень есть плод беспорядочных усилий лоббистов. Например, радиорелейные линии полосой пропускания до 8 Мбит/с и почему-то только на местных, следовательно – телефонных сетях подлежат упрощенной процедуре. Получается, что РРЛ производительностью 10 Мбит/с или используемые в сетях передачи данных упрощенной процедуре приемки в эксплуатацию не подлежат.

Удивительно, что все виды телематических служб подлежат упрощенной процедуре, а сети передачи данных, организованные на том же самом оборудовании, на которое оформляется то же самое разрешение на эксплуатацию, упрощенной процедуре не подлежат. Зато в упрощенном порядке принимаются в эксплуатацию все виды пунктов коллективного доступа к услугам связи, включая компьютерные клубы и интернет-кафе.

Упрощенная процедура формально предусматривает три послабления операторской жизни:

1. Не требуется предъявление представителю Госсвязьнадзора проектной документации и заключения государственной экспертизы, а также проведение измерений и приемосдаточных испытаний;
2. Представитель Госсвязьнадзора принимает участие в работе приемочной комиссии не по определению, а по усмотрению самого Госсвязьнадзора.
3. Не требуется подготовка заключения Госсвязьнадзора по соответствию объекта связи проектной документации и лицензиям оператора.

Между тем, заключение Госсвязьнадзора фактически представляет собой результат КЛД, то есть оформляется практически всегда в процессе работы приемочной комиссии. Разумеется, если Госсвязьнадзор не направляет своего представителя для участия в работе приемочной комиссии, то КЛД не проводится. Однако это случается крайне редко, а в случае ввода первого сооружения – не случается никогда, поскольку надзор просто обязан провести КЛД по истечении срока, отведенного лицензией для начала оказания услуг связи. Госсвязьнадзор справедливо предпочитает «совмещать приятное с полезным» и производит КЛД одновременно с приемкой в эксплуатацию объекта связи.

Таким образом, остается одно, зато весьма существенное упрощение – отсутствие необходимости разработки и государственной экспертизы проектной документации. Действительно серьезное упрощение, учитывая стоимость проекта, экспертизы, а также затрат времени на их оформление. Создание объектов связи из перечня приложения А разрешается осуществлять не только по проектной документации, но и по спецификации и схеме соединений, утвержденной заказчиком, а также заводским инструкциям производителей оборудования, либо типовым проектам. К сожалению, первое, самое важное, упрощение в юридическом смысле более чем сомнительно:

1. Статья 61 Градостроительного Кодекса Российской Федерации (ГСК РФ) прямо указывает, что «Строительство, реконструкция, капитальный ремонт зданий, строений и сооружений, их частей, осуществляются на основе проектной

документации – графических и текстовых материалов, определяющих объемно-планировочные, конструктивные и технические решения…» (п. 1 ст. 61 ГСК). Таким образом, строительство объекта связи без разработки проектной документации запрещено законом вне зависимости от содержания приказа 113. Иначе говоря, проектную документацию на создание объектов связи разрабатывать надо всегда.

2. Статья XX Конституции Российской Федерации вообще не относит регулирование строительной деятельности к компетенции федерации или к предметам совместного ведения федерации и субъектов федерации. Федеральные органы исполнительной власти не вправе регулировать деятельность по строительству объектов связи, за исключением особенностей их функционального устройства.

Таким образом, основное упрощение, предоставленное операторам при приемке объектов из перечня приложения А к приказу 113, сводится к отсутствию необходимости государственной экспертизы проектной документации, поскольку разработка проектной документации обязательна по закону. Все остальные требования к операторам связи, предъявляемые при приемке в эксплуатацию объектов связи, остаются неизменными.

Разумеется, при использовании упрощенной процедуры, не требуется предъявлять инспектору Госсвязьнадзора утвержденную проектную документацию – проверка ее наличия в этом случае в компетенцию инспектора не входит. В то же время, проверка, проводимая налоговой службой или иными надзорными органами, вполне может привести к плачевным для оператора результатам, вроде доначисления налогов (по выбору ИМНС – на имущество, НДС или налога на прибыль), проблем с Госархстройнадзором, Энергонадзором, Госсанэпиднадзором и т.п. Проблемы также возникнут в случае необходимости установления собственника сооружений связи для судебных или следственных органов.

Впрочем, если оператор решает только текущую задачу оформления разрешения на эксплуатацию объекта связи, то приложение «А» - неплохое подспорье. Приемка в эксплуатацию таких объектов потребует от оператора предъявить инспектору Госсвязьнадзора один из следующих документов взамен проектной документации:

- типовой проект с привязкой к конкретному объекту. К сожалению, до настоящего времени не выпущено ни одного нормативного документа, регламентирующего порядок типового проектирования. Формально действуют еще советские нормы, согласно которым заказчиком типового проекта может являться … министерство или ведомство. Ясно одно, постановление Правительства от 27.12.2000 г. №1008 пунктом 10(г) устанавливает обязательную государственную экспертизу в ГУ Главгосэкспертиза типовых (базовых) проектов, предназначенных для массового применения;
- заводские инструкции производителя оборудования, а также утвержденные руководителем оператора схему соединений и спецификацию объекта. В спецификации указывается назначение объекта, основные технические характеристики объекта (монтированная емкость, пропускная способность и т.п.), перечень оборудования, входящего в состав объекта, условия эксплуатации аппаратуры. По сути, спецификация представляет собой общую пояснительную записку из рабочего проекта.

Все остальные документы, за исключением проектной документации и заключения государственной экспертизы должны соответствовать общей процедуре.

7. Инженерная бюрократия

Легальное предоставление услуг связи, легальная операторская деятельность представляет собой ни что иное, как документарное обеспечение всех направлений работы оператора. Государство в лице надзорных и контрольных инстанций, имя которым – даже не легион, а целая армия, требует одно: на каждый вопрос инспектора оператор должен предоставить документ.

Желательно, чтобы этот документ соответствовал каким-нибудь нормативным актам, однако поскольку полностью выполнить предписания законодателя невозможно, надо представить документ, хотя бы внешне похожий на искомое. Если оператор оказывается не в состоянии предоставить никакого документа, решение надзорного органа практически предрешено: повинен наказанию. Причем строгость наказания определяется количеством имеющихся в распоряжении оператора бумаг.

Наивно полагать, будто главные сложности ожидают легального оператора в области взаимоотношений с Госсвязьнадзором. При всей трудоемкости процедуры приемки в эксплуатацию объектов связи, Госсвязьнадзор часто идет навстречу операторам, понимая специфику деятельности в области связи.

Общаться с местными монополистами, ЖКХ, ТСЖ и ГУП ДЕЗ, пожарниками, СЭС, муниципальными и региональными властями еще сложнее, учитывая постоянный характер взаимодействия. Но общий принцип всегда один и тот же: ее величество Бумага. И каждый оператор, который решил несмотря на все тернии, легализоваться и попытаться привлечь инвестиции в свою деятельность должен позаботиться о создании документальной основы своего бизнеса.

Часть 2. Глава 2

Административная и уголовная ответственность в отрасли.

Перефразируя Ленина, можно смело утверждать, что всякое государство лишь тогда чего-нибудь стоит, если оно умеет защитить себя от «деструктивных антигосударственных элементов». Тех, кото-рые не желают исполнять установленные государством обязательные требования.

Как уже говорилось во вводной части Правосвязия, суверенитет означает право государства устанавливать на своей терри-тории нормы права, в том числе и императивные – то есть обязательные для исполнения без всяких условий, нравятся они субъектам права или нет. Впрочем, и условные нормы права также нуждаются в охране – практика показывает стойкое нежелание несознательных субъектов исполнять действующее законодательство, если это противоречит их интересам. Что, впрочем, по-человечески вполне понят-но…

Правонарушения и наказания

Государственное принуждение базируется на трех основных «китах» - исполнительное производ-ство, уголовная ответственность и административная ответственность.

Исполнительное производство не является наказанием – это лишь средство исполнения конкретного решения государственного ор-гана. Чаще всего исполнительное производство возбуждается по решению суда, например, о принуди-тельном взыскании долга.

При этом должника не подвергают наказанию как таковому – судебный пристав просто принудительно изымает средства у должника и передает их кредитору. Но судебный пристав облечен властью от имени государства и противодействие исполнению его обязанностей вле-чет административную, а то и уголовную ответственность непокорного субъекта права.

Уголовная и административная ответственность, в отличие от исполнительного производства, подразумевает именно наказание виновного лица за совершенное им правонарушение (деликт). Зако-нодательство, в частности п. 1 ст. 3.1 КоАП, изящно определяет наказание как установленную госу-дарством меру ответственности за совершенные деликты, причем основной целью наказания деклари-руется именно предупреждение совершения подобных проступков в будущем. То есть опасение, а в случае уголовной ответственности – так и просто банальный страх. Именно поэтому так часто юристы говорят о необходимости обеспечения «неотвратимости наказания»…

Как уже отмечалось во Введении, различают разные деликты – уголовные преступления и адми-нистративные правонарушения. Уголовная ответственность является очень серьезной мерой, даже са-ма судимость влечет неприятные последствия для преступника, поэтому если речь зашла о привлече-нии к уголовной ответственности, то без квалифицированного адвоката не обойтись, самозащита в та-ких делах чревата большими проблемами. По этой причине в этой статье вопросы уголовной ответст-венности принципиально не рассматриваются – если такая неприятность случилась, то надо немедлен-но обращаться к профессионалам. Пока не поздно….

Разумеется, изложить в краткой статье все аспекты привлечения к административной ответствен-ности невозможно, поэтому ограничимся лишь основными понятиями, которые часто встречаются в практике операторской деятельности в области связи в отдельно взятой России. К сожалению, админи-стративная практика в других странах СНГ все сильнее отличается от российской, поэтому этой ча-стью Правосвязия не стоит руководствоваться при осуществлении деятельности за пределами границ РФ.

Основные отличия преступления от административного правонарушения показаны в таблице:

ПРАВОНАРУШЕНИЯ (ДЕЛИКТЫ)	
Уголовное преступление	Административное правонарушение
Общественно опасное виновное деяние (то есть действие или бездействие), запрещенное и нака-зуемое исключительно Уголовным кодексом Рос-сии (ст. 14 УК РФ).	Виновное противоправное деяние, запрещенное и наказуемое согласно федеральному КоАП, либо законами субъектов Российской Федерации
Субъектом преступления могут являться только физические лица (ст. 19 УК).	Субъектом преступления могут быть признаны как физические, так и юридические лица (ст. 2.1 КоАП).
При назначении наказания учитывается	По общему правилу, неоднократность

неодно-кратность преступлений (ст. 16 УК).	совершения административного правонарушения не учитыва-ется.
Различают категории преступлений: особо тяж-кие, средней тяжести, тяжкие и небольшой тяже-сти (ст. 15 УК).	Административные правонарушения не разделя-ются на категории по степени тяжести.
Учитывается совокупность и рецидив преступле-ний (ст. 16, 17 УК).	Совокупность и рецидив административных пра-вонарушений не учитываются и не имеют юриди-ческого значения.
Минимальный возраст субъекта преступления (в некоторых случаях) – 14 лет.	Минимальный возраст субъекта административ-ной ответственности – 16 лет (ст. 2.3 КоАП).
Различают оконченное и неоконченное преступ-ление (ст. 29 – 31 УК).	Административные правонарушения не различа-ются на оконченные и неоконченные.
Не могут быть признаны преступлением деяния, совершенные в состоянии необходимой обороны, крайней необходимости, обоснованного риска, исполнении приказа и т.п. (ст. 37 – 42 УК).	Административное правонарушение исключается только состоянием крайней необходимости (ст. 2.7 КоАП). При этом само понятие крайней необ-ходимости, используемое КоАП, существенно от-личается от определения УК.

Необходимо различать административные правонарушения и дисциплинарные проступки, то есть нарушения норм трудового права (ст. 192 – 195 ТК РФ). Дисциплинарный проступок представляет со-бой виновное неисполнение или ненадлежащее исполнение работником своих трудовых обязанностей. При этом работника привлекает к ответственности работодатель, а не уполномоченный орган государ-ственной власти, да и наказание определяется не только Трудовым кодексом, но и нормами внутренне-го распорядка данной организации. При этом не могут применяться административные наказания – штраф, административный арест, конфискация и т.д.

К административной, так же, как и к уголовной ответственности привлекаются только виновные лица. Более подробно об этом говорилось во вводной части Правосвязия, заметим только, что отсутст-вие вины полностью исключает ответственность субъекта, даже если объективная сторона правонару-шения наличествует в полном объеме. КоАП различает две формы вины – умышленную и неосторож-ную (ст. 2.2). Заметим, что к умышленной форме относится и косвенный умысел, то есть правонару-шитель прямо не желает наступления вредных последствий своего деяния, однако сознательно допус-кает такие последствия или относится к ним безразлично. Косвенный умысел следует отличать от не-осторожной формы вины.

Например, выезжая на встречную полосу, водитель предвидит возможность наступления больших неприятностей в виде лобового столкновения, однако не желает совершения ДТП (разумеется, о самоубийцах речь не идет). Это классический пример неосторожной формы вины. А вот лицо, сознательно похищающее кабель электроснабжения или связи, желает похитить кабель (прямой умысел), но не желает, хотя и безразлично допускает, перерывы в электропитании или связи (косвенный умысел).

Новацией КоАП является привлечение к административной ответственности юридических лиц (п.2 ст. 2.1 и ст. 2.10 КоАП). Разумеется, этих субъектов нельзя посадить под арест, однако вполне можно оштрафовать, применить конфискацию или возмездное изъятие. Кроме того, п. 2 той же ст. 2.1 КоАП устанавливает, что назначение

административного наказания юридическому лицу не освобож-дает от административной ответственности за то же правонарушение виновное физическое лицо.

Наоборот, привлечение к ответственности физического лица точно так же не исключает ответственности за то же правонарушение соответствующего юридического лица. Разумеется, обычно речь идет об от-ветственности должностных лиц – чаще всего руководителей и менеджеров предприятий и организа-ций Особенностью наказаний юридических лиц является существенно более жесткие санкции, в част-ности размер штрафов для юрлиц может десятикратно превышать максимальный размер штрафов для физических лиц.

Вообще, перечень видов административных наказаний четко и однозначно определен КоАП. Ни-какие иные виды наказаний, кроме восьми, указанных в ст. 3.2 КоАП, не могут применяться в качестве меры ответственности за административные правонарушения. Различают основные и дополнительные наказания, которые могут применяться только вместе с основными наказаниями (ст. 3.3 КоАП). При этом п. 3 ст. 3.3 устанавливает, что за одно правонарушение может быть назначено одно основное ли-бо одно основное и одно дополнительное наказание. Дополнительные наказания не могут применяться отдельно от основных наказаний.

Виды административных наказаний (санкций)					
№	Вид наказания	Определение	Основное или дополнит.	Субъекты (ЮЛ, ФЛ)	Примечание
1	Предупреждение	Письменное официальное порицание винов-ного лица	Основное	ЮЛ, ФЛ	
2	Административный штраф	Денежное взыскание, налагаемое на винов-ное лицо: • граждане (и лица без гражданства)- до 25 МРОТ; • должностные лица – до 50 МРОТ; • юридические лица – до 1000 МРОТ. Штраф также может быть назначен в сумме, кратной стоимости предмета правонаруше-ния.	Основное	ЮЛ, ФЛ	Диапазон штрафов оп-ределяется в конкрет-ных статьях раздела II КоАП (особенная часть). За совершение отдель-ных правонарушени й установлены повышен-ные размеры штрафов
3	Возмездное изъятие орудия или предме-та правонарушения	Принудительное изъятие и последующая продажа с передачей бывшему собственнику вырученной суммы за вычетом расходов на реализацию	Основное Дополнит.	ЮЛ, ФЛ	Назначается только судьей
4	Конфискация ору-дия или предмета правонарушения	Принудительное безвозмездное обращение в федеральную	Основное Дополнит.	ЮЛ, ФЛ	Назначается только судьей

		собственность или в собствен-ность субъекта федерации не запрещенных к гражданскому обороту вещей.			
5	Лишение специаль-ного права, предос-тавленного физиче-скому лицу	Лишение физического лица специального права (то есть предоставленного специально этому лицу) за грубое или систематическое нарушение порядка пользования этим правом.	Основное	Только ФЛ	Назначается только судьей на срок не менее 1 месяца, но не более 2-х лет. Пример – лишение во-дительских прав. Лишение юридиче-ского лица предостав-ленной ему лицензии не является админи-стративным наказа-нием.
6	Административный арест	Содержание нарушителя в условиях изоля-ции от общества в течение до 15 суток. За нарушение требований режима чрезвы-чайного положения или режима в зоне про-ведения контртеррористической операции до 30 суток.	Основное Дополнит.	Только ФЛ	Назначается только судьей. Знаменитые «15 су-ток»…
7	Административное выдворение за пре-делы РФ	Принудительное и контролируемое переме-щение иностранных граждан и лиц без граж-данства через Государственную границу РФ, либо контролируемый самостоятельный вы-езд таких лиц за пределы РФ.	Основное Дополнит.	Только ФЛ	Не может применять-ся в отношении граж-дан России. В операторской дея-тельности случается редко…
8	Дисквалификация	Лишение физического лица права занимать руководящие должности в исполнительном органе юридического лица, управлять юри-дическим лицом либо осуществлять пред-принимательскую деятельность по управле-нию юридическим лицом.	Основное	Только ФЛ	Назначается только судьей на срок не менее 6 месяцев, но не более трех лет.

Важнейшим условием законности привлечения любого лица к административной ответственно-сти является соблюдение уполномоченным органом власти установленной процедуры, то есть процес-суально-правовых требований КоАП. Собственно, именно процессуальные требования защищают подвластных лиц от произвольного применения различных санкций со стороны бесчисленного сонма надзорных и контрольных органов. Несоблюдение процессуальных требований влечет недействитель-ность самого постановления о привлечении к ответственности (ст. 1.6 КоАП).

Административный процесс

Процедура привлечения к административной ответственности состоит, по общему правилу, из следующих этапов: возбуждение дела, производство по делу и рассмотрение дела об административном правонарушении. Дело об административном правонарушении считается возбужденным с момента составления уполномоченным лицом протокола об административном правонарушении либо с момента принятия мер обеспечения производства по делу (изъятие вещей и документов и другие меры, указанные в ст. 27.1 КоАП), а также в иных случаях, предусмотренных ст. 28.1. При этом право возбуждения дела имеют только должностные лица органов, уполномоченных в области соответствующего правонарушения, иначе дело считается невозбужденным.

Надо специально отметить, что по общему правилу срок давности, по истечении которого лицо не может быть подвергнуто административному наказанию, составляет по общему правилу 2 месяца, а в некоторых случаях - один год (ст. 4.5). (Таможенные и налоговые правонарушения, а также защита прав потребителя и ряд других специальных случаев).

Если речь идет о длящемся правонарушении, например – эксплуатации узла связи с нарушением условий действия лицензии, то срок давности исчисляется с момента обнаружения соответствующего правонарушения уполномоченным органом. Грубо говоря, у Россвязьнадзора есть ровно два месяца на рассмотрение протокола, составленного инспектором. По истечении этого срока рассмотрение дела автоматически исключается.

Рассмотрение дела об административном правонарушении осуществляется должностным лицом (обычно, но не всегда, руководителем или заместителем руководителя) органа, специально уполномоченного КоАП рассматривать соответствующие дела. Надо заметить, что далеко не всегда орган власти, должностное лицо которого оформило протокол, имеет право рассматривать соответствующие дела.

Тот же Россвязьнадзор имеет право составить протокол по ст. 14.1 ч. 2, 3 (деятельность без лицензии или с нарушением условия действия лицензии), однако не вправе самостоятельно рассмотреть дело и привлечь виновного к ответственности, поскольку КоАП предоставляет это право только судье. Поэтому всякий раз целесообразно проверять полномочия надзорного органа, пользуясь приведенной ниже таблицей.

Надо заметить, что не все органы, должностные лица которых имеют право возбуждать дела об административных правонарушениях, имеют право рассматривать эти дела и выносить соответствующие постановления о наложении взысканий и иные решения, предусмотренные КоАП. А вот обратное утверждение верно всегда, то есть если орган власти уполномочен рассматривать дела о соответствующих административных правонарушениях, то его должностные лица вправе возбуждать дела.

Очень распространенным нарушением административных органов, влекущим недействительность постановлений о привлечении к ответственности, является превышение полномочий (компетенции). Тем самым должностное лицо, рассматривающее дело, нарушает требования части 2 ст. 1.6 КоАП и уже само подлежит привлечению к ответственности – как к дисциплинарной, так и, в некоторых случаях и уголовной.

В любом случае постановление о привлечении к административной ответственности, вынесенное неуполномоченным лицом, недействительно. В самом деле, не может же пожарник штрафовать за нарушение ПДД, а инспектор Россвязьнадзора или Энергонадзора оштрафовать кого-нибудь за «самовольное оставление места административного ареста»…

Привлечение к административной и уголовной ответственности возможно только при наличии полного состава правонарушения в деянии (действии или бездействии) субъекта деликта (см. Введение в Правосвязие). Формулировка состава правонарушения, вообще говоря, подразумевает наличие юридических знаний у должностного лица, рассматривающего дело.

А поскольку далеко не все должностные лица различных технических надзоров такими знаниями обладают, то грамотный адвокат обычно может оспорить постановление по отсутствию состава правонарушения либо по несоблюдению установленной процедуры. Напомним, что состав правонарушения обязательно должен состоять из четырех аспектов, которые должны быть упомянуты в постановлении по делу об административном правонарушении:

I. Объект правонарушения, которым могут являться, в зависимости от правонарушения:

- охраняемые законом права физических и юридических лиц;
- имущество физических и юридических лиц;
- общественные отношения в различных областях.

II. Объективная сторона правонарушения:

- процесс и способ совершения правонарушения;
- время, место и условия совершения правонарушения;
- вредные последствия правонарушения, если соответствующей статьей КоАП наличие вреда предусматривается как условие привлечения к ответственности. Но вообще, большинство статей КоАП предусматривает «формальные составы», то есть сам факт деяния влечет ответственность вне зависимости от наличия или отсутствия фактического вреда, как, например, «выезд на полосу встречного движения»;
- наличие причинно-следственной связи между деяниями правонарушителя и объектом правонарушения (например, небрежное хранение паспорта повлекло его утрату).

III. Субъект правонарушения:

- Физическое (и) или юридическое лицо (лица), совершившие деяние, составляющее административное правонарушение.

IV. Субъективная сторона правонарушения, то есть отношение нарушителя к совершенному правонарушению:

- вина субъекта правонарушения должна быть установлена исчерпывающим образом. Неустранимые сомнения толкуются в пользу субъекта (ст. 1.5 КоАП);
- недостижение субъектом – физическим лицом минимального возраста деликтоспособности (см. ст. 2.3 КоАП);
- совершение субъектом деяния в состоянии крайней необходимости (ст. 2.7 КоАП);
- совершение субъектом деяния в состоянии невменяемости (ст. 2.8 КоАП).

На самом деле, КоАП обеспечивает неплохие гарантии соблюдения субъективных прав. Проблема заключается в том, что суды зачастую действуют в полном единодушии с административно-уполномоченными органами, безоглядно соглашаясь с чиновниками в самых диких случаях. Некоторый оптимизм внушает только то, что в отсутствие надлежащего правосудия никакое экономическое развитие страны попросту невозможно, поэтому федеральной власти придется, несмотря на все нежелание, наводить порядок в этой сфере. Иначе настанет не «удвоение», а «уполовинивание» ВВП…

Конкретные колобки

КоАП, следуя общепринятой и разумной практике законотворчества, редко упоминает наименования конкретных органы власти, уполномоченных в соответствующих областях. Поэтому непросвещенному субъекту бывает непросто разобраться, является ли должностное лицо, привлекающее его к административной ответственности, компетентным в соответствующей области. С другой стороны, упоминание конкретных наименований органов власти приводит к неопределенности в случае их упразднения. Например, налоговая полиция несколько раз упоминается в КоАП…

Административная реформа весеннее-летнего сезона 2004 года привела к путанице в компетенциях административных органов, разобраться в которой непросто даже опытному юристу. Далее приводится таблица компетенции соответствующих органов, составленная по результатам анализа положений об органах власти по состоянию на август 2004 года. Однако при применении сведений из таблицы не следует забывать слова классика философии о том, что все течет и все изменяется…

Некоторые административные органы власти, уполномоченные КоАП РФ				
Компетенция	**Наименование**	**Контакты (центральный аппарат)**	**Вышестоящий орган**	**Основание**
Органы, осуще-ствляющие государственный надзор за связью и информатизацией	Федеральная служба по над-зору в сфере связи	Москва, Тверская ул., д. 7	Министерство информа-ционных технологий и связи	ППРФ от 30 июня 2004 г. № 318
Органы внутренних дел (милиция)	Министерство внутренних дел РФ	117049, Москва, ул. Житная, д. 16 (095) 237 7585 www.mvdinform.ru	Президент РФ	Указ Президента РФ от 18 июля 1996 г. N 1039 (в ред. Указов Прези-дента РФ от 06.09.97 N 993, от 24.04.98 N 433, от 27.05.98 N 598, от 20.10.98 N 1269)
Органы,	Министерство	103012, Москва,	Президент РФ	Указ Президента

осуществляющие государственный пожарный надзор	Российской Федерации по делам граждан-ской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий (МЧС России)	Театральный пр, 3. Главное управ-ление Государственной противопожарной службы МЧС РФ. Справочная МЧС: (095) 926-3901		РФ от 11 июля 2004 г. N 868
Органы государственного энергетического надзора	Федеральная служба экологи-ческого, техноло-гического и атомного надзора	Москва, Таганская, д.34, стр. 1, ул. А.Лукьянова, д. 4, корп. 8, ул. Кедрова, д. 8, корп. 1, проезд Китайго-родский, д. 7	Правительство РФ	ППРФ от 30.07.2004 г. № 401 «О федеральной службе по экологиче-скому, техноло-гическому и атомному надзору»
Органы государственной санитарно-эпидеми-ологической службы	Федеральная служба по над-зору в сфере защиты прав потребителей и благополучия человека	Москва, Вадковский пере-улок, дом 18/20	Министерство здраво-охранения и социального развития РФ	ППРФ от от 6 апреля 2004 г. # 154, Положе-ние о службе утв. ППРФ от 30 июня 2004 г. № 322
Органы государственного архитектурно-строительного надзора	Уполномоченные органы власти или государственные учреждения субъектов Российской федерации. Регулирование строительной деятельности относится к компетенции субъектов Федерации (ст. 72, 73 Конституции РФ).			
Органы, осуществляющие контроль за обеспечением защиты государственной тайны	Федеральная служба безопасности Российской Федерации	101000, Москва, приемная ФСБ РФ, ул.Кузнецкий мост, дом 22. www.fsb.ru справочный телефон (095) 921-07-62	Президент РФ	Указ Президента РФ от 11 августа 2003 г. N 960 в ред. Указа от 11 июля 2004 года N 870
Органы, осуществляющие государственный контроль в области обращения и защиты информации	Федеральная служба по тех-ническому и экспортному контролю	Нет данных. Адрес Минобороны РФ: 105175, Москва, Мясницкая ул., д. 37 тел. (095) 293-38-54	Президент РФ, Минобороны России	Указ Президента РФ от 16 августа 2004 г. №1085
Органы государственной инспекции по торговле, качеству товаров и защите прав потребителей	Федеральная служба по надзору в сфере защиты прав потребителей и благополучия человека	Москва, Вадковский пере-улок, дом 18/20	Министерство здраво-охранения и социального развития РФ	Распоряжение Правительства РФ от 30 июля 2004 г. № 1024р.
Федеральный антимонопольный орган	Федеральная антимоно-польная служба	Москва, ул. Садовая-Кудринская, д. 11.	Правительство РФ	ППРФ от 7 апреля 2004 г. № 189 «Вопро-сы Федеральной анти-монопольной службы» Положение утверждено ППРФ от 30 июня 2004 г. № 331.
Примечание: аббревиатура ППРФ – постановление Правительства Российской Федерации				

Заметки для адвоката

Защита субъектов инфокоммуникаций обычно сталкивается с серьезными проблемами при толковании объективной стороны деликтов в силу их специальной технологической природы. Аналогичные проблемы возникают и у судей, которые, разумеется, не владеют соответствующими специальными знаниями в области связи. При этом, в силу еще советской привычки, презумпция невиновности часто толкуется судом как презумпция добросовестности и компетентности государственных надзорных органов.

Фактически презумпция невиновности правонарушителя не действует. Поэтому очень важно использовать ряд процессуальных несовершенств законодательства в области связи – практика показывает, что некоторые неточности законодательства оказывают сильное психологическое воздействие на судей.

Разумеется, защита субъектов экономической деятельности в рамках административного или уголовного процесса по составам деликтов в области пожарной безопасности, охраны труда и иных подобных составов, характерных для предпринимательской деятельности, осуществляется в обычном порядке. Остановимся только не двух составах, характерных только для отрасли связи.

1. Компетенция органов, уполномоченных в области связи.

Федеральный закон «О связи» от 07.07.2003 г. № 126-ФЗ, частью 1 ст. 27 императивно предусматривает, что государственный надзор в области связи осуществляется специально создаваемыми государственными учреждениями в субъектах РФ. Правовой статус государственных учреждений вытекает из ст.120 главы 4 ГК РФ и законодательства о некоммерческих организациях.

Между тем, в настоящее время (август 2004 г.) постановлением Правительства РФ от 30 июня 2004 г. № 318, указанные полномочия переданы Федеральной службе по надзору в сфере связи, которая является федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере информационных технологий и связи.

Юридический статус органов власти как юридических лиц определяется главой 5 ГК РФ, в частности – ст. 125 ч. 1 ГК РФ и принципиально отличается от правового положения некоммерческих организаций вообще и государственных учреждений в частности. Таким образом, наделение подразделений ФСНСС функциями административно уполномоченного органа противоречит ст. 27 ЗоС и дает основания, предусмотренные ч. 4 ст. 200 АПК РФ, для обжалования любого постановления или предписания ФСНСС как ненадлежащего органа, уполномоченного в области связи и информации.

2. Разрешения на эксплуатацию.

Условия действия лицензии в области связи требуют от оператора оформления специального разрешения на эксплуатацию технических средств (РЭ). Фактически РЭ является лицензией на осуществление деятельности по коммерческой эксплуатации объектов связи, поскольку:

- является субъективным специальным правом;
- объективно разрешает длительное и неоднократное использование объекта связи для оказания услуг связи неопределенному кругу лиц. При этом состав услуг связи

определяется оператором самостоятельно в пределах класса услуг, указанных в операторской лицензии.

Таким образом, требование наличия РЭ ограничивает конституционное право оператора связи на свободное использование своего имущества (объекта связи) для предпринимательской деятельности (ст. 34 Конституции РФ). Такое ограничение допускается Конституцией (ч. 3 ст. 55), при условии:

- если установлено федеральным законом, а не любым другим нормативным правовым актом;
- если и в той степени, в какой это необходимо для защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Однако, до настоящего времени не существует федерального закона, устанавливающего обязательность оформления РЭ. Федеральный ЗоС не содержит соответствующей нормы. Единственным нормативным актом, на основании которого вводятся разрешения на эксплуатацию, является п. 5.6.2 Положения о ФСНСС, утвержденного постановлением Правительства РФ от 30 июня 2004 г. № 318. Поскольку постановление Правительства не является федеральным законом, обязательное требование РЭ не основано на законе и противоречит Конституции.

Необходимо отметить, что эксплуатация сетей связи для безвозмездного предоставления услуг связи не подлежит обязательному лицензированию согласно ст. 29 ЗоС. Поэтому эксплуатация объектов связи для безвозмездного предоставления услуг связи не требует оформления специального разрешения на эксплуатацию. Таким образом, объектом ограничения конституционного права свободного использования имущества для предпринимательской деятельности в области связи фактически является не техническая эксплуатация вообще, а косвенное извлечение предпринимательского дохода. Едва ли такой объект можно считать соответствующим ч. 3 ст. 55 Конституции РФ…

Некоторые административные правонарушения в различных областях, а так же размеры штрафов можно посмотреть здесь

Глава 3. Операторы и подрядчики или правила бега по минному полю.

Пожалуй, немного найдется областей предпринимательской деятельности, столь же подверженных разнообразным слухам и домыслам, как деятельность проектировщиков. Причин тому несколько, причем как объективных, так и вполне субъективных.

В советское время сложилась целая традиция разработки проектной документации, частично зафиксированная в ГОСТ и СНиП, а частично в "священном предании" проектировщиков. Проектная документация разрабатывалась целыми институтами, довольно тесно связанными друг с другом, что обусловило появление устойчивых и фактически обязательных правил, хоть и не введенных какими-либо официальными нормативными актами. Впрочем, установленная ГОСТом "Единая система проектной документации" унифицировала требования к оформлению проектов, их составу и, частично, к их содержанию.

Первые сложности возникли с приходом на рынок системных интеграторов, ориентированных на внедрение технических решений зарубежных производителей оборудования и программного обеспечения. Сразу выяснилось, что проектная документация, подготовленная по западным стандартам, не пригодна для использования в России – хотя бы по причине оформления, не соответствующего ЕСПД.

До принятия ФЗ "О техническом регулировании" вопросы оформления проектной документации вообще не решались никаким образом, поскольку выполнение ГОСТов являлось обязательным для всех. Но дело не только и не столько в оформлении – сама структура проектов западного образца не соответствует принятой в России, совершенно по-другому составляются сметы, совсем иные требования к рабочей документации.

Закон "О техническом регулировании" разрешил игнорировать стандарты, которые не затрагивают вопросы безопасности продукции. Однако действие этого закона не распространяется на правоотношения в области связи, то есть возникло своеобразное "многозаконие": во всех областях, кроме некоторых (связь, ВПК и т.д.) соблюдать функциональные стандарты необязательно. Но в специальных областях ГОСТы по-прежнему действуют в полном объеме. Конечно, так недалеко и до параллельной промышленности, но…. Lex dura sed Lex.

В результате, западные модели и требования к проектированию коренным образом отличаются от российских, соответственно и проектная документация, разработанная крупными интеграторами, зачастую не может пройти государственную экспертизу. А созданные по ним объекты по сути своей являются объектами незаконного строительства. Если обычные строители довольно быстро адаптировались к российским реалиям, то интеграторы зачастую "гордо" настаивали на своей правоте, ссылаясь на стандарты, хоть и европейские, но не действующие в России. В частности, всякие "красивости" из Visio не соответствуют ЕСПД и формально не должны использоваться в проектной документации на объекты связи. К счастью, эксперты органов государственной экспертизы обычно "смотрят сквозь пальцы" на отступления подобного рода.

Часть 2. Глава 2

Сертификация: мифы и право.

Что такое "строительство"

Многие юридические проблемы строительной индустрии возникли по причине парадоксальной ситуации: российское законодательство не содержит четкого определения понятия "строительство". Основополагающая статья 740 ГК РФ (ч. 1) определяет правоотношения заказчика и подрядчика по договору строительного подряда, однако не содержит определения самого объекта правоотношений: "По договору строительного подряда, подрядчик обязуется в установленный договором срок построить по заданию заказчика определенный объект либо выполнить иные строительные работы…". По всей видимости, законодатель полагал, что термин "строительство" является общеизвестным. Если это действительно так, то законодатель, увы, заблуждался…

В самом деле, если создание жилого дома на пустом месте безусловно является строительством, то является ли строительством подключение телевизора к абонентской розетке 220В? Или к коллективной антенне? Является ли строительством замена

смесителя? А замена унитаза? Единственное косвенное указание, которое содержит ст. 740 ГК заключается в том, что к строительству относится и капитальный ремонт… следовательно текущий ремонт строительством не является.

Однако с точки зрения смесителя, его замена является капитальным ремонтом "системы смешивания горячего и холодного водоснабжения". При этом, разумеется, капитальный ремонт смесителя не является капитальным ремонтом здания. Да и вообще, законодатель не определил отличие капитального ремонта от ремонта текущего.

Субъекты строительной деятельности

Действующее законодательство относит создание объектов связи к строительной деятельности с особенностями, установленными федеральным законодательством в области связи. Таким образом, субъектный состав участников правоотношений и статусы соответствующих субъектов определяются строительным законодательством. Да и "обычаями делового оборота" тоже.

Перечень субъектов правоотношений в области строительства приведен в таблице:

Наименование статуса		**Функция**
Общий	**Специальный**	
Инвестор	-	Лицо, осуществляющее финансирование создания объекта из собственных или привлеченных средств. Является фактическим собственником построенного объекта. В качестве инвестора обычно выступают операторы связи, инвестиционные институты (в том числе банки), а также иные лица.
	Соинвестор	Участник простого товарищества, образованного группой инвесторов для совместного финансирования создания объекта. Права и обязанности соинвесторов определяются договором соинвестирования.
Заказчик (Заказчик-застройщик)	-	Лицо, уполномоченное договором с Инвестором на выполнение функций технического заказчика создания объекта. Заказчик должен иметь лицензию Госстроя, а также компетенцией в соответствующей предметной области, позволяющей квалифицированно оценивать деятельность других участников строительства.
Проектировщик	-	Лицо, осуществляющее разработку проектной или предпроектной документации на основании договора с Заказчиком и в соответствии с Заданием на проектирование, утвержденным Заказчиком. Часто, но отнюдь не всегда, проектировщики выполняют и изыскательские работы.
	Генеральный проектировщик	Лицо, непосредственно заключившее договор с Заказчиком на выполнение всего комплекса проектных работ.

	(Суб) Проектировщик	Лицо, выполняющее часть проектных работ на основании договора с Генеральным проектировщиком. Иногда субпроектные организации заключают договоры непосредственно с Заказчиком строительства, что с юридической точки зрения некорректно.
Подрядчик	-	Лицо, выполняющее строительно-монтажные работы, либо предпроектные изыскания по договору с Заказчиком и в соответствии с утвержденной проектной документацией.
	Генеральный подрядчик	Лицо, на которое договором с Заказчиком возложена ответственность за строительство объекта в целом. Генеральный подрядчик вправе выполнить все работы самостоятельно или поручить их выполнение Субподрядчику. Возможность и порядок привлечения субподрядных организаций определяются договором генерального подряда.
	Субподрядчик	Лицо, по договору с Генеральным подрядчиком выполняющее часть работ по созданию объекта.

Законодательство никак не ограничивает возможность совмещения одним лицом функций, указанных в таблице, разумеется, при условии наличия необходимых лицензий. В следующей таблице приведены основные лицензии, необходимые для выполнения функций в области строительства **объектов связи**:

Статус	Работы (функции)	Лицензии		Примечания
		Госстрой РФ	ФСНСС	
Инвестор	Владение акциями, паями или долями в уставном капитале операторской компании	Не требуется	Не требуется	Если инвестор не является оператором связи
	Операторская деятельность в области связи	Не требуется	Требуется по соответству-ющим видам деятельности	Инвестор сам является оператором связи.
	Исполнение функций заказчика создания объекта связи	Не требуется	Не требуется	Инвестор заказывает объект для собственных нужд.
Заказчик	Исполнение функций заказчика по договору с Инвестором	Лицензия на проектирование зданий и сооружений с указанием "исполнение функций заказчика – застройщика"	Не требуется	Заказчик не является оператором связи, который будет эксплуатировать создаваемый объект
Проекти-ровщик	Генеральный проектировщик: Разработка или координация разработки проектной документации на объект в целом)	Лицензия на проектирование зданий и сооружений с указанием "исполнение функций генерального проектировщика	Не требуется	По договору с Заказчиком
	Разработка отдельных разделов проектной документацию	Лицензия на проектирование зданий и сооружений	Не требуется	По договору с Заказчиком.

	(субпроектировщик)			
Подрядчик	Генеральный подрядчик. Осуществление и координация всего комплекса работ по созданию объекта	Лицензия на строительство зданий и сооружений с указанием "исполнение функций генерального подрядчика"	Не требуется	По договору с Заказчиком
	Субподрядчик	Непосредственное осуществление строительно-монтажных работ Лицензия на строительство зданий и сооружений	Не требуется	По договору с Генеральным подрядчиком
Предпроектные изыскания (съемка геоподосновы, нивелировка и привязка к местности, определение географических координат, исследование грунтов и т.д.) осуществляется организациями, имеющими лицензии Госстроя на право осуществления инженерных изысканий для строительства. В качестве изыскателей могут привлекаться участники строительства, а также специально привлеченные подрядчики по договору с Заказчиком или Генеральным проектировщиком.				

Примечания:

1. ФСНСС – Федеральная служба по надзору в сфере связи;
2. Госстрой РФ – Федеральное агентство по строительству и жилищно-коммунальному хозяйству.
3. Проектирование и строительство отдельных видов инженерного оборудования объектов требует наличия лицензий специально уполномоченных органов власти. В частности, проектирование и устройство оборудования огнезащиты, пожарной безопасности и противопожарного оборудования допускается при наличии лицензии Главного управления противопожарной службы МЧС России. В настоящее время Госстрой не лицензирует указанные виды работ. Ранее выданные Госстроем лицензии на производство этих видов работ формально сохраняют юридическую силу, однако не признаются органами специализированных надзоров.

В отличие от общегражданского строительства, каждый объект связи создается согласно условиям действия лицензий конкретного оператора. Поэтому до начала проектных работ, инвестор должен определить оператора связи, который будет эксплуатировать создаваемый объект, и заключить с ним соответствующие договоры.

Надо сказать, что обычно в качестве инвестора и заказчика объектов связи выступают сам оператор, что упрощает процедуру. Однако далеко не всегда оператор оказывается компетентным заказчиком строительства. Слишком далека область строительная деятельность от операторской, слишком много используется в строительстве специальных документов и стандартизованных форм. Самые распространенные проблемы, вызванные некомпетентностью заказчика – неправильно оформленная исполнительная документация, сметы, акты сдачи-приемки работ. Все это чревато не только проблемами с Россвязьнадзором, но и с налоговой службой, а это чревато куда более серьезными неприятностями.

Основы в проектирование сетей.

Проектная документация с точки зрения юриста

Определение понятия

Гражданский кодекс РФ статьей 743 устанавливает, что подрядчик осуществляет строительство в соответствии с технической документацией, определяющей объем, содержание работ и иные, предъявляемые к ним требования, а также сметой, определяющей цену работ. В свою очередь, ст. 759 ГК указывает, что техническая документация, упомянутая ст. 743, является результатом выполнения проектных и изыскательских работ. При этом ч. 2 ст. 760 ГК РФ обязывает проектировщика гарантировать заказчику отсутствие у третьих лиц права воспрепятствовать выполнению работ или ограничивать их выполнение на основании разработанной проектировщиком технической документации.

Проектная документация разрабатывается на основании и в соответствии с заданием на проектирование (ЗП) и иными исходными данными, которые заказчик обязан передать проектировщику до начала проектных работ. Однако заказчик имеет право поручить разработку ЗП самой проектной организации, при этом ЗП приобретает юридическую силу с момента его утверждения заказчиком.

Градостроительный кодекс статьей 61 определяет проектную документацию как "графические и текстовые материалы, определяющие объемно - планировочные, конструктивные и технические решения для строительства, реконструкции и капитального ремонта объектов, а также благоустройства их земельных участков"

Таким образом, наличие утвержденной ПСД является обязательным условием начала строительства любого объекта. При этом та же статья 743 ГК не возлагает на заказчика императивную обязанность предоставления подрядчику ПСД, оставляя этот вопрос на усмотрение сторон как существенное условие договора на производство строительно-монтажных работ (СМР). Тем самым допускается совмещение функций проектировщика и подрядчика, что, разумеется, никоим образом не прекращает раздельное лицензирование этих видов деятельности.

С учетом вышеизложенного, можно сформулировать определение проектной документации следующим образом: "Техническая документация, включающая графические и текстовые материалы, разработанная проектной организацией, на основании специального задания на проектирование и определяющая стоимость, объем и содержание работ, а также иные мероприятия по созданию объекта, гарантирующие беспрепятственное выполнение строительно-монтажных работ и беспрепятственную эксплуатацию законченного строительством объекта".

Заметим, что фраза "проект объекта" некорректна по своей сути. Проектная документация разрабатывается в связи с созданием или реконструкцией объекта и не содержит всю полноту сведений о его устройстве. Проект на АТС не содержит принципиальных схем устройства применяемой телефонной станции и рассматривает ее как "черный ящик" с заранее заданной функциональностью.

Правоотношения в области выполнения проектных и изыскательских работ определены статьями 758 – 762 ГК РФ, определяющие основные права и обязанности заказчика и проектировщика, в частности:

- Заказчик обязан передать проектировщику задание на проектирование, либо поручить проектировщику подготовить такое задание с последующим утверждением уполномоченным лицом заказчика;
- Заказчик обязан передать проектировщику иные исходные данные, необходимые для разработки проектной документации;
- Проектировщик обязан соблюдать требования задания на проектирование, а также иных исходных данных и вправе отступить от них только с согласия заказчика;
- Проектировщик обязан согласовать разработанную ПСД с заказчиком и передать заказчику согласованную документацию в полном объеме;
- Заказчик и проектировщик совместно осуществляют согласование ПСД с компетентными органами государственной власти и местного самоуправления;
- Проектировщик не вправе передавать ПСД третьим лицам без согласия заказчика;
- Заказчик также не вправе передавать ПСД третьим лицам или разглашать данные технической документации без согласия проектировщика;
- Проектировщик несет гражданско-правовую ответственность за недостатки проектной документации, в том числе и за недостатки, обнаружившиеся в процессе эксплуатации законченного строительством объекта;
- Заказчик обязан оплатить проектировщику договорную цену разработки ПСД.

При этом не стоит забывать, что права и обязанности сторон по договору на разработку проектной документации следуют из самого текста договора, а ГК лишь устанавливает некоторые обязательные требования к правоотношениям сторон (ст. 422 ГК). Статья 421 ГК гарантирует право свободы договора всем участникам экономических отношений.

Только не надо забывать, что публично-правовые обязанности вытекают не из договора, а из закона и гражданским кодексом не регулируются. Поэтому приходится, иногда затрачивая немало сил, выделять публично-правовые (административно-правовые) нормы из действующего законодательства…

Стадийность проектирования

Стадии разработки проектной документации являются частью "священного предания" проектировщиков. Вообще-то эти стадии определены СНиП 11.01.95, однако Госстрой РФ так и не сумел зарегистрировать этот документ в Минюсте РФ, который с завидной регулярностью отказывал в регистрации этой инструкции о порядке разработки и согласования проектной документации. С другой стороны, "нетрадиционная" ориентация проектировщика вызывает столь пристальное внимание государственной экспертизы, да и других надзорных органов, что согласовать "нетрадиционный" проект оказывается почти невозможно.

С советских времен проектная документация разрабатывалась в три или в одну стадию. Трехстадийная схема проектирования в отрасли связи почти не применяется в силу сложности, длительности, высокой стоимости – да и просто в силу отсутствия необходимости в этом. Трехстадийная схема подразумевает последовательную разработку:

1. Обоснования инвестиций (стадия "ОИ"). Этот документ рассматривает различные технические и экономические аспекты создания объекта в данных условиях и в данном месте нахождения. ОИ на особо сложные или опасные объекты подлежат обязательной государственной экспертизе как предпроектная документация.
2. Технико-экономическое обоснование (стадия "П"). Другое название ТЭО – "Проект", поэтому, строго говоря, не надо путать термины "проект" и "проектная

документация". Этот документ разрабатывается на основании утвержденных и прошедших экспертизу ОИ и представляет собой подробное изложение принятых технических решений, описание функционирования объекта с учетом внешних условий, требования к эксплуатации и т.д. ТЭО подлежит отдельной государственной экспертизе.

3. Рабочая документация (Стадия "Р"). Комплект рабочей документации (РД) содержит все чертежи и технологические пояснения, необходимые строительства объекта. РД – основной документ для производителя работ, бригадиров, монтажников.

Одновременно с РД разрабатывается сметная часть проекта, содержащая подробный расчет стоимости объекта с учетом всех технологических мероприятий строительства - стоимости материалов, амортизации машин и механизмов, зарплаты рабочих, рентабельности строительно-монтажной организации.

Одностадийное проектирование применяется в отношении "технически несложных" объектов. Однако поскольку степень "технической сложности" фактически определяет заказчик, то такая схема применяется при создании подавляющего большинства объектов связи – это позволяет сэкономить много времени и денег по сравнению с трехстадийной схемой проектирования.

Одностадийное проектирование обычно называют "рабочее проектирование", поскольку его результатом является так называемый "Рабочий проект", который содержит три части:

1. Общая пояснительная записка (ОПЗ) с изложением основных технологических решений, и мероприятий, условий функционирования объекта и обоснования выбранных решений, если такие обоснования необходимы;
2. Рабочая документация (РД) – все рабочие чертежи, необходимые для производства всех строительно-монтажных работ и пояснения к ним;
3. Сметная часть комплекта проектной документации.

Проектная документация и авторское право

Согласно ст. 1 Градостроительного кодекса РФ, проектная документация является объектом градостроительной деятельности и разрабатывается в соответствии с градостроительной документацией (ст. 61 ГСК). С другой стороны, ст. 7 Федерального закона "Об авторском праве и смежных правах" от 09.07.1993 г. № 5351-1 прямо относит произведения градостроительства к объектам авторского права. Проектная документация существует в объективной форме (документ) и не указана в закрытом перечне произведений, которые не могут являться объектом авторского права (ст. 8 ФЗ "Об авторском праве и смежных правах").

Таким образом, проектная документация является объектом авторского права и смежных прав, что накладывает некоторые ограничения на ее использование. Соавторами проектной документации является соответствующая группа инженеров проектной организации под руководством главного инженера проекта (ГИП). Интересы авторов представляет проектная организация.

С другой стороны, законодатель не дал прямых указаний на отнесение проектной документации к градостроительной и архитектурной документации, поэтому отнесение проектной документации к объектам авторских прав нельзя признать бесспорным.

Однако, как показывает судебная практика, суды склонны в подавляющем большинстве случаем поддерживать требования авторов…

Нормы, правила, стандарты

Обязанность проектировщика обеспечить беспрепятственное строительство эксплуатацию проектируемого объекта влечет обязанность учета требований действующих нормативно-технических актов (НТА). В то же время, нормативно-технические акты не могут являться источниками прав и обязанностей субъектов права, если они не опубликованы и не зарегистрированы Минюстом России.

С другой стороны, лицензии, в том числе и лицензии операторов связи, требуют соблюдения требований нормативно-технических документов. Проблема состоит в том, что НТА сами по себе не ограничивают права субъектов права, поскольку устанавливают требования только к техническим объектам. По этой причине Минюст признает такие акты не требующими государственной регистрации, да и обязательному опубликованию они не подлежат.

Строго говоря, НТА являются как бы приложением к лицензиям операторов, проектировщиков и строителей и действуют не сами по себе, а в связи с соответствующими ненормативными или нормативными правовыми актами. Именно поэтому чрезвычайно сложно обжаловать НТА – суд просто не признает такой акт правовым и признает дело неподведомственным суду, даже если НТА установит, что скорость света в России равна нулю.

Впрочем, можно обжаловать акт государственного органа о введении в действие НТА, однако это потребует дорогостоящих и длительных экспертиз, времени…. В общем, можно дать очень простую рекомендацию: соблюдать НТА, а в случае технической невозможности их соблюдения обосновать в ОПЗ соответствующие отступления. Есть такое право у проектировщика, причем источником этого права как раз и является обязанность проектной организации обеспечить беспрепятственное во всех смыслах использование объекта строительства.

Выбор оборудования и технических средств

Федеральный закон «О связи» предусматривает обязательную сертификацию средств связи. Специально для сертификации телекоммуникационного оборудования создана отдельная система сертификации «Связь» (ССС). Таким образом, все применяемое активное оборудование, кабели и кабельные изделия, оборудование гарантированного электропитания, серверы телематических служб и автоматизированные системы расчетов, даже люки кабельных колодцев могут применяться исключительно при наличии сертификатов соответствия ССС. Экспертиза очень внимательно изучает наличие сертификатов ССС на все оборудование. Кроме того, на оборудование должен быть нанесен знак соответствия ССС (прямоугольник с буквами «ССС»). При отсутствии знака соответствия придется приобретать голографические наклейки, которые продает ОАО ССКТБ-ТОМАСС (www.ssktb.ru). Но для приобретения этих наклеек придется ехать в Москву, получать доверенность держателя сертификата, ехать в ТОМАСС… в общем, надо требовать у поставщика оборудования наличие знака соответствия.

При использовании того или иного оборудования необходимо учитывать его назначение и условия применения, изложенные в сертификате ССС. Разумеется, экспертиза, да и проектировщик не станут подробно изучать технические условия на аппаратуру, но вот

краткие условия применения соблюдать необходимо. Например, некоторые серверы телематических служб по сертификату могут применяться в качестве маршрутизаторов сетей передачи данных, а некоторые – не могут. Соответственно, если необходимо применить роутер на основе СТС, надо применять только тот СТС, условиями применения которого предусматривается такое предназначение.

Большие проблемы иногда возникают с установочными изделиями, включая компоненты структурированных кабельных систем, поскольку их производители зачастую не удосуживаются получить сертификат ССС. С патч-кордами вопрос решается довольно просто – в спецификации указывается, что они входят в комплект поставки сертифицированного активного оборудования. С патч-панелями, розетками и другими компонентами СКС все гораздо сложнее и применять их надо весьма осмотрительно.

Рабочий проект

Подавляющее большинство объектов связи проектируется в одну стадию. Результатом выполнения одностадийных проектных работ является рабочий проект создания объекта (далее – РП). В состав РП, как уже отмечалось, входят следующие части: общая пояснительная записка (ОПЗ), рабочая документация (РД) и сметная часть.

Рассмотрим содержание рабочего проекта на примере узла передачи данных и телематических служб с учетом рекомендаций СНиП 11.01.95:

Примечание: все рекомендации, приведенные в дальнейшем, основаны на личном опыте деятельности автора в качестве ГИП и не являются обязательными или исчерпывающими. Не следует превращать рекомендации в фетиш и следовать им неукоснительно как законодательному акту. Как говорил Дэн Сяо-пин, «Пусть расцветут сто цветов»….

Задание на проектирование

Строго говоря, ЗП не является частью рабочего проекта, однако всегда подшивается к тому ОПЗ, поскольку иначе невозможно оценить соответствие проектной документации требованиям заказчика.

Форма ЗП законодательством не установлена, однако ее вполне можно отнести к «священному преданию» проектировщиков и несоблюдение этой формы обычно воспринимается экспертами как свидетельство отсутствия опыта работы у проектной организации.

Образец:

ЗАДАНИЕ НА ПРОЕКТИРОВАНИЕ ОБЪЕКТА
Создание узла передачи данных и телематических служб УПДТС «Пример»

1.	Наименование объекта	Создание узла передачи данных и телематических служб «УПДТС «Пример». Далее – УПДТС.
2.	Основание	Договор создания и передачи проектной продукции №XXXXX от «___»_____ 200x
3.	Источник финансирования	Собственные средства заказчика строительства

4.	Проектная организация	Наименование проектной организации Лицензия Госстроя РФ № ГС-XXXXXXXXXX
5.	Подрядная организация	Наименование подрядной организации Лицензия Госстроя РФ № ГС-XXXXXXXXXX (необязательный пункт)
6.	Стадийность проектирования	Рабочий проект в одну стадию
7.	Заказчик проектирования и строительства объекта	Наименование заказчика
8.	Сроки строительства	Указывается «квартал – год» или просто «год»
9.	Объект строительства	Место нахождения объекта и функциональное назначение объекта строительства.
10.	Технологическая схема	Самая объемная часть ЗП. Указываются общие принципы функционирования, объекта строительства, которые обеспечивают его совместимость с взаимодействующими объектами, требования к составу оборудования, иные технологические требования, которым должен удовлетворять рабочий проект. Технологические вопросы, которые не указаны в данной части ЗП разрешаются усмотрением проектной организации с учетом действующих норм, правил и стандартов.
11.	Требования по строительству	Требования к подготовке строительных площадок, режиму доступа в технические помещения и т.п.
12.	Требования по строительной подготовке и приспособлению помещений	Указываются специальные требования по проведению общестроительных работ, либо указывается на отсутствие необходимости в них.
13.	Требования к комплекту документации	Приводятся специальные требования к оформлению и согласованию РП.
14.	Количество экземпляров выпускаемой проектной документации	Указывается количество экземпляров РП.

Задание на проектирование подписывается уполномоченными представителями заказчика и проектировщика. В случае размещения объекта на территории третьих лиц ЗП желательно согласовать и с ними в целях исключения споров в дальнейшем.

Исходные данные для проектирования

Кроме задания на проектирование к исходным данным относятся:

- условия действия лицензий оператора связи, которому заказчик поручает коммерческую эксплуатацию создаваемого объекта связи;
- технические условия на размещение оборудования;
- технические условия на присоединение сети электроснабжения;
- технические условия на присоединение к другим инженерным сетям;

- решение ГКРЧ и разрешение на использование полос частот, выданное Федеральным агентством связи (для объектов, содержащих РЭС), согласованный частотный план для сетей КТВ;
- документы, подтверждающие отвод земельного участка для строительства (если требуется);
- иные документы, предоставленные заказчиком;
- материалы предпроектных изысканий, выполненных заказчиком, проектировщиком или третьими лицами.

Исходные данные должны обеспечивать возможность составления сметной документации, то есть рассчитать объем работ, расходных материалов, оборудования и технических средств связи. Поэтому можно использовать только те планировочные и градостроительные чертежи, которые позволяют точно и однозначно определить привязку объекта к местности или проектируемых систем связи к существующему зданию. Привязка систем связи к несущим конструкциям существующего зданию производится путем указания расстояний на выкопировке планов БТИ (экспликация БТИ). С наружными сетями все оказывается гораздо сложнее.

Совершенно ясно, что бессмысленно производить дорогостоящую топографическую съемку района развертывания сети, тем более, что для этого нужно получать специальное разрешение, располагать лицензией УФСБ на право использования сведений, составляющих государственную тайну и т.п. Гораздо проще заплатить территориальному Геотресту за предоставление такой карты (обычно в масштабе 1:2000 или 1:5000). При этом на карту будут нанесены контуры зданий. Очень желательно, чтобы на карте имелись и отметки высот по коньку зданий. На такую картографическую геоподоснову можно легко нанести воздушные линии, точки размещения транзитных узлов сети, размещаемых в зданиях населенного пункта и, при этом, достаточно точно рассчитать объем работ, пользуясь точным масштабом геоподосновы.

Приходится не без сожаления констатировать, что действующее законодательство вообще не регулирует вопросы оформления исходно-разрешительной документации (ИРД) на строительство сетей связи, для создания которых не требуется отвод земельного участка. Очевидно, что устройство воздушных линий связи не препятствует использованию земель, расположенных под ВЛ, а ограничение минимальной высоты подвеса ВЛ никоим образом не является выбором земельного участка.

Между тем, с точки зрения законодателя именно правоустанавливающие документы на землеотвод являются основными исходными данными для проектной организации. Несоблюдение формального порядка оформления ИРД влечет незаконность строительства со всеми последствиями, предусмотренными гражданским законодательством включая снос незаконно построенного объекта за счет заказчика строительства. Существует несколько относительно легальных способов решения проблемы ИРД для создания таких сетей связи.

Структура проектной документации

Рабочий проект состоит из томов, разделов и книг. Структуру разбиения выбирает проектная организация по своему усмотрению. Титул проектной документации может быть, например, таким: Номер_договора_проектирования-РП (0312/23-РП). Части проектной документации могут нумероваться так: номер_договора-марка.том.раздел.книга.-РП (0312/23-СС.1.2.1-РП).

В советское время нормоконтроль проектной документации не пропускал неправильные наименования марок (типов) документов. В настоящее время марки употребляются довольно беспорядочно. Тем не менее, основные марки, применяемые в процессе проектирования объектов связи (сокращенный перечень):

Марка	Наименование
РП	Рабочий проект
РД	Рабочая документация
РЧ	Рабочие чертежи
СС	Сети связи
НСС	Наружные сети связи
ЭМ	Схемы электрические (монтажные)
СП	Спецификации

Практика показывает, что этих марок вполне достаточно для оформления проектной документации. Кстати, об оформлении. По традиции, закрепленной ЕСПД, проектная документация оформляется на форматированных бланках, оформление которых несколько отличается от принятого в ЕСКД для конструкторской документации. В частности, вместо поля «масса» используется поле «Стадия». При одностадийном проектировании в поле «Стадия» ставится марка «РП». (Трехстадийное проектирование – стадии «О», «П», «Р»).

В каждую отдельно переплетенную часть проектной документации вкладывается лист «состав проекта», на котором указываются наименования всех частей рабочего проекта, что позволяет проверить полноту представленных документов.

Часть 2. Глава 3

Строительство сетей связи.

Общая пояснительная записка (ОПЗ)

ОПЗ, так же, как и сметная часть, относится к так называемой "утверждаемой части" проектной документации, то есть определяет и уточняет принятые технические и технологические решения, технико-экономические параметры объекта наряду с его внутренней и внешней функциональностью.

ОПЗ должна содержать обязательство, заверенное подписью ГИП: "Настоящий проект соответствует заданию на проектирование, действующим нормам и правилам и отвечает современному техническому уровню". Подпись ГИП часто заверяют печатью проектной организации.

Также в ОПЗ вкладывают "лист согласований", на котором ставят согласующие подписи и печати организации, согласующие проектную документацию в целом. В частности, рабочий проект должен быть согласован с заказчиком строительства. Организации, согласующие отдельные технологические решения (трассы кабелей, электропитание, узлы межсетевого взаимодействия и т.п.) ставят согласующие отметки непосредственно на рабочих чертежах.

В состав ОПЗ входит общая схема организации связи, а также ситуационный план размещения сети, выполненный либо на геоподоснове, либо без точной привязки к местности, если сеть создается в существующих кабельно-канализационных сооружениях по техническим условиям их владельцев.

Технические условия и прочие исходные данные, а также копии сертификатов соответствия обычно подшивают в ОПЗ либо оформляют отдельной книгой "Прилагаемые документы". ОПЗ обычно выполняется отдельным томом или книгой и состоит из следующих разделов:

1. Общие данные

Приводятся сведения о назначении объекта строительства, его месте нахождения, наименование заказчика объекта и основание для проектирования (реквизиты договора).

Также указываются основные технико-экономические параметры объекта. Необходимо указывать абонентскую емкость, которая впоследствии будет приведена в разрешении на эксплуатацию. Далее перечисляются исходные данные, на основании которых осуществлена разработка РП. В состав исходных данных входят лицензии оператора связи, технические условия от присоединяющих сетей связи и технические условия на размещение линейных сооружений, а также активного оборудования.

Указывается, что разработка осуществлялась в одну стадию согласно заданию на проектирование (в противном случае экспертиза может потребовать трехстадийное проектирование, поскольку решение об одностадийном проектировании вправе принять только заказчик). Далее перечисляются нормативно-технические и нормативно-правовые акты, с учетом требования которых разработана проектная документация. Желательно указать, что все применяемое оборудование и технические средства сертифицированы в системе сертификации "Связь".

2. Основные технологические решения

Данный раздел является наиболее объемным и важным разделом ОПЗ. Традиционно состоит из следующих подразделов:

2.1 Технологические принципы и технические характеристики; В этом подразделе подробно описывается функционирование объекта в целом, а также назначение и взаимодействие его структурных элементов. Указываются применяемые протоколы взаимодействия всех уровней со ссылкой на IETF RFC, а также способы и протоколы взаимодействия с абонентскими терминалами.

2.2 Адресация, маршрутизация и межсетевое взаимодействие; Здесь надо обязательно указать на использование динамической маршрутизации с автоматической генерацией маршрутных таблиц. В противном случае государственная экспертиза потребует привести текст маршрутных таблиц… сети Интернет. Это не шутка.

2.3 Синхронизация и сигнализация; Здесь надо учитывать, что системы, построенные на основе Ethernet IEEE802.3 являются асинхронными и не требуют использования сигнализации. Основание – РД 45.176-2001. Все стыки с синхронными сетями (потоковые интерфейсы типа G.703, STM и т.п.) работают в режиме принудительной сигнализации от присоединяющей сети. Проверьте, чтобы указание на принудительную синхронизацию содержалось в технических условиях операторов соответствующих сетей связи. Вопрос о

применяемой сигнализации является как минимум дискуссионным. Можно указать, что в соответствии с техническими регламентами сети Интернет применяется сигнализация по протоколу ICMP. С другой стороны, эксперты госэкспертизы и Россвязьнадзора привычно понимают под системой сигнализации специальные протоколы, принятые в ТфОП – EDSS1, ОКС №7, 2ВСК и так далее. Поэтому, дабы не привлекать излишнего внимания, можно указать, что "общеканальная и внутриканальная системы сигнализации не используются".

2.4 Использование радиоэлектронных средств с излучением Если на объекте предусматривается использование РЭС, необходимо указать реквизиты решений ГКРЧ и частотных назначений Федерального агентства связи (ФАС), на основании которых проектируются РЭС. Указывается также энергетические параметры радиоканала, зона покрытия для сетей беспроводного доступа, а при использовании радиорелейных линий – особенности и длина трассы РРЛ и степень (коэффициент) доступности с учетом климатических особенностей данного региона и параметров РЭС.

2.5 Идентификация и аутентификация абонентов. Автоматизированная система расчетов Раскрываются способы идентификации, аутентификации абонентов и защиты от несанкционированного доступа к проектируемой сети связи. В данном разделе описывается применение VLAN и (или) VPN, протоколов типа RADIUS II, парольная защита и т.п. Следует иметь в виду, что применение криптографических средств допускается при наличии сертификата бывшего ФАПСИ. Поскольку подавляющее большинство программных средств для организации VPN таких сертификатов не имеет, вопрос криптозащиты желательно деликатно опустить и в проектной документации об этом не писать. Тем более, что НТА не требуют обязательной криптозащиты на сетях связи. Все АСР подлежат обязательной сертификации в системе сертификации "Связь". При этом отдельный сертификат ССС на соответствующий сервер не требуется. С точки зрения сертификации, АСР представляет собой аппаратно-программный комплекс, требования к аппаратуре которого установлены приложением к сертификату (параметры компьютера, операционная система и т.д).

2.6 Обеспечение СОРМ Данный пункт, пожалуй, является одним из наиболее болезненных для операторов. Однако с точки зрения проектировщика СОРМ не составляет никаких особенных проблем, поскольку технические и организационные мероприятия по обеспечению СОРМ осуществляются согласно плану мероприятий, который разрабатывается рабочей группой по согласованию с УФСБ. План мероприятий разрабатывается уже после ввода объекта в эксплуатацию и к проектировщику отношения не имеет. Поэтому в данном подразделе РП необходимо указать на необходимость разработки в реализации плана мероприятий по обеспечению СОРМ совместно с территориальным УФСБ без внесения изменений в разработанный РП. Практика показывает, что экспертиза вполне благожелательна к такому способу описания решений СОРМ. Но наличие данного подраздела является совершенно обязательным в любых РП создания объектов связи. Таковы условия действия операторских лицензий.

2.7 Метрологическое обеспечение Приводятся требования к метрологическому обеспечению функционирования проектируемого объекта связи, рекомендуемые типы средств измерений, а также параметры, подлежащие обязательному метрологическому контролю. Следует различать измерение и учет. Всякое измерение представляет собой сравнение физической величины с некоторым эталоном, например эталоном вольта, метра, килограмма и т.п. Метрологический контроль, предусмотренный федеральным законодательством о единстве измерений, как раз и призван обеспечить "одинаковость" эталонных физических величин на всей территории России, чтобы 1 Вольт в

Калининграде был равен 1 Вольту во Владивостоке. Этой же цели служит государственная поверка средств измерений.

Учетные операции не являются измерениями, поскольку не предусматривают сравнения с эталонным значениям и являются абсолютно точными. В качестве примера объекта учета можно привести денежные средства в кассе или на расчетном счете, а также трафик в байтах по сети передачи данных. Измерить трафик невозможно, трафик можно только учитывать. Поэтому коллекторы данных пропущенного трафика АСР не являются средствами измерений и не подлежат поверки или иному метрологическому контролю в отличие от измерения времени соединения. Время – физическая величина, объект измерений, а не учета.

2.8. Требования к эксплуатационному персоналу Данный пункт позволяет избежать дорогостоящей и в целом бесполезной сертификации сотрудников в учебных центрах производителей оборудования. Достаточно предусмотреть аттестацию персонала внутренней аттестационной комиссией предприятия. Положительное заключение государственной экспертизы избавит оператора от претензий Россвязьнадзора в части представления документов, подтверждающих право сотрудников предприятия эксплуатировать соответствующее оборудование (см. приказ Минсвязи РФ от 09.09.02 № 113).

3. Архитектурно-строительные решения

Если предполагается строить отдельное здание или сооружение на выделенном земельном участке, то данный раздел просто содержит ссылку на соответствующие тома проектной документации. В случае необходимости строительной подготовки существующих помещений, приводится ссылка на соответствующий раздел рабочей документации, а также требования по размещению оборудования с учетом максимально допустимой нагрузки на несущие конструкции здания. В случае, если прочность здания заведомо позволяет размещать оборудование, желательно прямо указать, что дополнительных мероприятий по упрочнению несущих конструкций здания не требуется (иногда государственная экспертиза начинает выдвигать весьма экзотические требования).

В самых простых случаях указывают "Объект создается в специально существующих специально предназначенных помещениях. Дополнительных мероприятий не требуется"…

4. Инженерное оборудование, сети и системы

Данный раздел обычно содержит следующие подразделы:

4.1 Отопление. При создании узлов сетей связи в существующих помещениях обычно указывают, что предусматривается использование существующих систем отопления и дополнительных мероприятий не требуется. При организации необслуживаемых узлов сетей связи в технических помещениях зданий желательно указать мероприятия по поддержанию температуры в пределах, установленных ТУ на оборудование.

4.2 Вентиляция и кондиционирование. Системы вентиляции и кондиционирования должны быть рассчитаны на отвод тепла, рассеиваемого активным оборудованием.

4.3 Электропитание и заземление Наибольшие сложности у начинающих проектировщиков вызывает именно данный подраздел, поскольку приходится применять

нормативно-технические акты, которые сильно отличаются от НТА отрасли "Связь" и, зачастую, плохо известны связистам. Проектирование электроснабжения целесообразно поручить специалистам, знакомым со спецификой таких объектов. Далее приводятся лишь самые краткие замечания к данному подразделу.

Устройство электроснабжения и заземления объектов связи производится согласно Правилам устройства электроустановок потребителей (ПУЭ) с учетом отраслевых требований. Надо иметь в виду, что существует немало редакций как самих ПУЭ, так и отдельных частей этих Правил. В настоящее время (сентябрь 2004 г.) действует седьмая редакция большинства глав ПУЭ.

Проектирование электроснабжения начинают с получения технических условий электроснабжающей организации. В ТУ должна быть указана граница зоны ответственности потребителя, а также номер распределительного устройства и точка подключения фидера (обычно указывается либо номер автомата либо номер установочного места для автомата РУ). Обязательным условием ТУ является указание максимальной разрешенной либо установочной мощности. В случае использования существующих электрифицированных помещений ТУ должны содержать указания на использования контура заземления.

Условиями действия операторских лицензий предусматривается обязанность оператора предоставлять услуги связи круглосуточно семь дней в неделю. Поэтому проект электроснабжения должен предусматривать первую повышенную категорию надежности электропитания проектируемого оборудования связи. Первая повышенная категория подразумевает использование устройств резервного гарантированного электроснабжения, то есть либо ИБП либо дизельных генераторов в зависимости от потребляемой мощности.

В состав рабочей документации должна входить расчетная схема электропитания с расчетом потерь, а также расчет тока срабатывания автоматов защиты. Сечение кабеля выбирается исходя из электрической мощности, потребляемой активным оборудованием узла связи, электроосвещением и системой кондиционирования. В рабочей документации обязательно должен быть план трассы кабеля электропитания.

Вопросы защитного заземления должны быть проработаны максимально тщательно, поскольку проектировщик несет ответственность (вплоть до уголовной) за безопасность жизнедеятельности на проектируемом объекте. Надо обеспечить не только заземление активного оборудования, но и экранов кабелей. Особо отметим необходимость защитного заземления бронезащиты волоконно-оптических кабелей, поскольку наведенные в ней токи и напряжения вполне могут представлять опасность для человека. В частности, серьезную опасность представляет бронепокров ВОК, проложенного в кабельных коллекторах, поскольку в тех же сооружениях проходят высоковольтные кабели электроснабжения и наведенное напряжение может превышать 600 В. Помимо защитного заземления рекомендуется использовать устройства защитного отключения (дифференциальные реле).

Существует до сих пор не отмененный ГОСТ 464-79, согласно которому заземление любых узлов связи должно быть организовано тремя контурами – двумя измерительными и одним рабочее-защитным. Разумеется, данный стандарт вполне оправдан при создании АТСДШ или АТСКУ, однако техническая возможность реализации данного требования в условиях неспециализированных зданий либо отсутствует вовсе либо крайне проблематично. Проектировщик должен обосновать эти отступления.

4.4 Электрическое освещение Проектирование электроосвещения рабочих мест осуществляется в соответствии с санитарно-гигиеническими нормативами с учетом требований СНиП 11.23.05-95. Расчет основан на требованиях к уровню освещенности рабочих мест. Не требуется проектирование электроосвещения в случае размещения проектируемого оборудования в существующих приспособленных помещениях, либо проектирования необслуживаемых объектов связи, на которых не предполагается постоянное присутствие персонала.

4.5 Связь и сигнализация В данном подразделе проекта рассматриваются вопросы обеспечения объекта строительства услугами связи для собственных нужд, а также вопросы организации охранной сигнализации, автоматизированных систем ограничения и контроля доступа в помещения объекта.

4.6 Противопожарные мероприятия Проектирование средств огнезащиты, охранно-пожарной сигнализации, автоматизированных установок пожаротушения (АУПС) и дымоудаления, а также иных противопожарных средств должно осуществляться организациями, имеющими соответствующие лицензии Государственной противопожарной службы (ГПС) МЧС России. Госстрой РФ, осуществляющий лицензирование деятельности по проектированию зданий и сооружений, не лицензирует деятельность проектных организаций в области противопожарных мероприятий.

Проектные решения в области противопожарных мероприятий должны быть согласованы с территориальным подразделением ГПС включая устройство охранно-пожарной сигнализации и АУПС. Заметим, что противопожарные нормы обязывают устанавливать на объектах связи дорогостоящие АУПС порошкового типа. Большинству небольших операторов такие решения недоступны по экономическим соображениям, поэтому проектной организации приходится изобретать основания для отступления от действующих НТА.

Владельцы некоторых кабельно-канализационных сооружений требуют проведения работ по огнезащите кабелей связи, даже если соответствующая кабельная продукция прошла сертификацию на соответствие требованиям пожарной безопасности. В случае создания узлов связи в существующих подготовленных помещениях дополнительных мероприятий не требуется.

5. Мероприятия по охране труда и технике безопасности

Данный раздел проектной документации весьма важен для успешного прохождения государственной экспертизы, опять же в силу обязанности проектировщика обеспечить возможность беспрепятственной надлежащей эксплуатации построенного объекта. Проектировщик должен предусмотреть мероприятия по охране труда и ТБ с учетом специфики проектируемого объекта.

До настоящего времени не разработаны специальные правила охраны труда на узлах передачи данных, поэтому приходится руководствоваться "Правилами охраны труда на телефонных станциях и телеграфах" (ПОТ РО 45.007-96), "Инструкцией по санитарному содержанию предприятий связи" (ОМДР 45.003-94), а также иными нормативами в области охраны труда.

Действующие НТА и НПА предъявляют особые требования к уровню знаний персонала операторов связи в области техники безопасности при работе в электроустановках. В частности, сотрудники оператора, занятые работами по техническому обслуживанию

оборудования, должны иметь квалификационную группу по электробезопасности не ниже IV. Заметим, что ПТЭ электроустановок общего назначения считает достаточной наличие группы III, а группа IV требуется только для лиц, имеющих право оформлять наряды-допуски на работы в электроустановках.

Желательно предусмотреть проектом периодическое обучение персонала правилам и навыкам охраны труда и техники безопасности в специализированных учебных заведениях, вводный и периодический инструктаж по технике безопасности на рабочих местах, а также аттестацию рабочих мест с участием органов санитарно-эпидемиологического надзора. (Кстати, конструкция фразы "предусмотреть проектом" является классическим примером профессионального сленга проектировщиков)

6. Воздействие на окружающую среду

Сооружения связи редко оказывают вредное воздействие на окружающую среду. Исключениями являются разве что радиоэлектронные средства с излучением (РЭС) и дизельные электростанции системы аварийного электропитания с хранилищами запасов топлива.

При проектировании объектов связи, в состав которых входят РЭС, проект должен содержать расчет зоны отчуждения (зоны санитарной охраны) вокруг антенных постов в соответствии с санитарными нормативами. Впрочем, зачастую в проекте только указывают на необходимость расчета санитарных зон, а сам расчет осуществляется едва ли не после утверждения рабочего проекта.

Дизельные электростанции не оказывают существенного воздействия на окружающую среду, учитывая их относительно небольшую тепловую мощность и непродолжительность работы в аварийном режиме. Однако с формальной точки зрения применение дизелей может потребовать недешевой экологической экспертизы… впрочем, если такие требования и выдвигаются, то только в каких-то исключительных случаях

Часть 2. Глава 3

Немного о метрологии.

Рабочая документация (рабочие чертежи)

Рабочая документация (РД) обычно переплетается отдельно от ОПЗ. При разработке РД следует учитывать, что этими документами будут руководствоваться рабочие при выполнении строительно-монтажных работ. Поэтому не следует включать в РД неоднозначные или вариантные решения – рабочий, в отличие от инженера, не должен принимать самостоятельных решений по существу устройства объекта.

Каждая книга РД предваряется разделом "Общие данные" (ОД) или "Общие указания", в котором проектировщик поясняет порядок, способ и технологию производства работ, выполнение которых предусмотрено в данной книге РД. По сути своей, ОД является инструкцией по монтажу. Кстати, ОД иногда так и называют: "Указания по монтажу".

Основные документы, входящие в состав РД, это рабочие чертежи и спецификации к ним, то есть перечни оборудования и материалов, необходимых для выполнения строительно-

монтажных работ. Нет никакого смысла "раздувать" объем РД за счет копий сертификатов соответствия, ИРД и прочих документов, которые не содержат информацию, необходимую для непосредственного выполнения работ.

Важнейшим условием приемлемости рабочего чертежа является указание так называемых "привязок", то есть расстояний от проектируемых элементов объекта до существующих конструкций либо географических координат, что позволяет однозначно и точно определить места установки оборудования, прокладки кабелей и т.п., а также объем соответствующих работ. При этом не допускается использование в качестве точек привязки различного рода временных конструкций, которые могут быть перенесены в другое место или вовсе демонтированы. Например, на плане трассы прокладки кабеля в существующем здании должны быть нанесены расстояния до несущих конструкций данного здания (колонн, несущих стен и т.п.). Все расстояния на строительных чертежах указываются в метрах (а не в миллиметрах, как это принято в единой системе конструкторской документации).

В качестве привязки также может указываться номер и расположение кабельного канала или консоли, а также ссылочный номер аппаратной стойки (стойкоместа), номер юнита в аппаратном шкафу и т.д. Главное, чтобы место нахождения проектируемого оборудования было определено однозначным образом.

Рабочие чертежи электроснабжения проектируемого оборудования выполняются согласно ПУЭ. Как правило, в состав этого раздела РД входит однолинейная схема с расчетом токов и потерь в проводах и кабелях, токов срабатывания и уставок автоматов защиты, а также планы трасс прокладки кабелей электропитания и заземления. Рабочие чертежи электрического освещения выполняются на основании расчетов освещенности рабочих мест.

Оформление рабочей документации традиционно выполняется в соответствии с требованиями ЕСПД (единая система проектной документации). Разумеется, с принятием ФЗ "О техническом регулировании", требования ЕСПД утратили обязательный характер, однако "явно нестандартное" оформление привлекает столь пристальное внимание контролирующих государственных органов, что затрудняет, или делает невозможным согласование и утверждение проектной документации.

Итак, в состав РД обычно включаются следующие документы:

- лист "состав проекта";
- Общие данные (Указания по монтажу);
- Рабочие чертежи (схемы, планы, конструкции);
- Спецификации оборудования и материалов.

Сметная документация (сметная часть)

Сметная часть комплекта проектной документации определяет подробный состав, количество и стоимость оборудования, расходных материалов и строительно-монтажных работ, необходимых для создания объекта. Сметная часть состоит из локальных и сводных (объектовых) смет, форма которых определяется СНиП. Надо отметить, что данные сметной части используются при составлении отчетной документации в процессе строительства: актов сдачи-приемки работ по ф. КС-2 ("процентовки"), справок КС-3, актов КС-14 и КС-11. При этом акты по форме КС-2 почти полностью повторяют формы

локальных смет, а остальные формы содержат итоговые данные сводного сметного расчета в части стоимости работ, расходных материалов и оборудования.

Для разработки сметной части используются следующие данные:

- текущая стоимость оборудования, расценки на которое не утверждены СНиП (активное каналообразующее и коммутационное оборудование и т.д.). Для оценки текущих цен используются прайс-листы поставщиков или опросные листы, заполненные поставщиками соответствующей аппаратуры;
- перечень и объем строительно-монтажных работ по данным рабочей документации;
- технологические карты строительно-монтажных работ, нормы потребности в расходных материалах, амортизации машин и механизмов, трудозатраты;
- единичные расценки на производство работ с учетом стоимости расходных материалов и трудозатрат;

Технологические карты и единичные расценки утверждаются Госстроем РФ в форме СНиП и обладают статусом нормативно-технического документа, а в случае их государственной регистрации в Минюсте, то и юридической силой нормативного правового акта, обязательного для исполнения всеми участниками правоотношений в области строительства. В настоящее время разработка сметной документации осуществляется в соответствии с Государственными элементными сметными нормами (ГЭСН), сборники которых постепенно издает Госстрой России. ГЭСН включает в себя всю информацию, необходимую для разработки сметной документации. Основная проблема состоит в том, что Госстрой пока не принял ГЭСН в полном объеме, поэтому некоторые виды работ приходится "осмечивать" по устаревшим сборникам, в том числе 1984 г. издания. Достоверность сметных расчетов, разумеется, оказывается весьма относительной…

Результатом разработки сметной документации является расчет себестоимости создания объекта в условных ценах, а также соотношения между стоимостями отдельных работ с учетом расходных материалов, трудозатрат, амортизации строительных машин и механизмов. Иначе говоря, образуется "экономически обоснованная база для определения договорной цены строительных работ, оборудования и расходных материалов. При этом цены в сметах так и указываются в условных ценах с пометкой, например "в ценах 1991 г.". Фактическая договорная цена определяется исходя из текущего коэффициента пересчета цен (устанавливается Госстроем РФ), а также различных коэффициентов, устанавливаемых по соглашению с строительной организацией. При этом основным коэффициентом, определение которого часто осуществляется на конкурсной основе, является коэффициент рентабельности строительно-монтажной организации.

В заключение заметим, что наличие сметной части вовсе не является непременным условием положительного заключения государственной экспертизы и приемлемости проектной документации в целом для создания объекта. Заказчик вправе не поручать проектной организации разработку сметной документации (это может сделать и строительно-монтажная организация), однако в таком случае в задании на проектирование необходимо прямо указать: "сметную часть не разрабатывать".

Согласование проектной документации

Согласование проектной документации часто оказывается более сложной задачей, нежели сам процесс разработки и оформления проекта. Хитросплетения политических и

экономических интересов, законодательная неопределенность, а часто и просто неприкрытая коррупция – все это самым негативным образом сказывается на процессе согласования ПСД. К сожалению, никаких позитивных тенденций пока даже не просматривается…

Согласно отмененному, но по-прежнему актуальному СНиП 11.01-95, проектная документация подлежит согласованию с "заинтересованными организациями". К сожалению, законодательство не определяет критерий этой самой "заинтересованности", однако едва ли имеет смысл запрашивать, в общем случае, согласования таких организаций, как ООН, НАТО или государство Ватикан… а также Президента Российской Федерации.

Необходимость согласования проектной документации следует из предусмотренной Гражданским кодексом обязанности проектировщика обеспечить беспрепятственное выполнение работ по созданию и эксплуатации проектируемого объекта. Сущность согласования состоит в письменном подтверждении согласующей организацией следующих юридических фактов:

1. Соответствие проектируемого объекта правилам и требованиям, установленным данной организацией либо надзор за соблюдением которых поручен данной организации;
2. Согласие на предоставление заказчику проектной документации права использования имущества, принадлежащего согласующей организации, для создания и эксплуатации создаваемого объекта. При этом, разумеется, ограничиваются права согласующей организации на свободное использование соответствующего имущества в части обеспечения интересов владельцев создаваемого объекта.

Таким образом, согласующие организации можно разделить на два класса:

- **публично-правовые** (организации, обязательность согласования с которыми напрямую вытекает из законодательных актов);
- **гражданско-правовые** (организации, обязательность согласования с которыми следует из их гражданского права свободного владения, пользования и распоряжения имуществом включая принадлежащие им объекты недвижимости).

В качестве примера публично-правовых согласований можно привести обязательность согласования проекта электроустановок с органами государственного энергетического надзора, проекта охранно-пожарной сигнализации и (или) огнезащиты – с органами государственной противопожарной службы и т.д. Основной целью публично-правового согласования является подтверждение соответствия проектируемого объекта установленным нормативным правовым и нормативным техническим актам. Фактически публично-правовое согласование защищает общественные права и интересы, которые могут быть затронуты в процессе строительства и эксплуатации проектируемого объекта, что, собственно, и является главнейшей задачей государства.

Особенностью публично-правового согласования является недопустимость отказа в согласовании по собственному усмотрению, то есть уполномоченный государственный орган имеет право отказать в согласовании только по мотивам нарушения требований обязательных нормативных или ненормативных актов, никоим образом не вдаваясь в вопросы целесообразности самого создания объекта или предложенных технических решений. Другой особенностью публично-правового согласования является

специальность компетенции согласующего органа, иными словами, пожарник не вправе выдвигать функциональные требования по использованию радиочастотного спектра, а Энергонадзор не вправе требовать покрытия кабелей огнезащитной пастой.

Примером гражданско-правовых согласований могут служить согласования проектов размещения узлов связи с владельцами соответствующих зданий, проектов прокладки кабелей с владельцами кабельно-канализационных сооружений, проектов устройства кабельно-канализационных сооружений с владельцами соответствующих земельных участков и т.д. С юридической точки зрения гражданско-правовое согласование можно рассматривать как своеобразную форму одностороннего договора, условиями которого являются условия согласования, а также оплата услуг согласующей организации.

В отличие от публично-правового согласования, гражданско-правовое согласование может предусматривать выполнение различных технических и организационных мероприятий по усмотрению согласующей организации. Кроме того, принцип свободы договора, зафиксированный Гражданским кодексом, по общему правилу предоставляет согласующей организации право отказать в согласовании проектной документации без объяснения причин. Разумеется, закон может предусматривать и обычно предусматривает специальное ограничение свободы усмотрения согласующих организаций в области согласования проектной документации.

В частности, ст. 6 ЗоС предоставляет организациям связи право создания линейных сооружений на территории различных объектов независимо от форм собственности. Однако, в части, прямо не урегулированной действующим законодательством, свобода усмотрения гражданско-правовых согласующих организаций сохраняется как в части права отказа в согласовании, так и в части условий согласования включая возложение на заказчика объекта обязанности по оплате услуг по согласованию и (или) установлению условий договоров на размещение проектируемого объекта на соответствующей территории.

Необходимость согласования проектной документации также ограничена п. 4 Положения о проведении государственной экспертизы и утверждении градостроительной, предпроектной и проектной документации в Российской Федерации (утверждено Постановлением Правительства РФ от 27.12.2000 г. № 1008). Согласно данному документу, проектная документация, разработанная в соответствии с техническими условиями и иными исходными данными, не подлежит согласованию с организациями, выдавшими их, за исключением случаев, прямо предусмотренных законодательством Российской Федерации. Заметим, что исключения могут быть предусмотрены только федеральным законодательством, а не законодательством субъектов РФ. Таким образом, следует по возможности избегать включения в технические условия пунктов о необходимости специального согласования проектной документации после ее разработки, поскольку отсутствие этого требования означает, что проектную документацию с данной организацией согласовывать не обязательно.

Согласование проектной документации осуществляется тремя способами:

1. Проставлением штампа или надписи с текстом условий согласования на листе согласований рабочего проекта. При этом проектная документация считается согласованной в полном объеме в пределах компетенции соответствующей согласующей инстанции;
2. Проставлением штампа или надписи с текстом согласования на листе рабочей документации. При этом согласованной считается часть рабочей документации,

относящаяся к листу, на котором проставлено согласование. Например, согласование проектов устройства кабельных линий обычно производится на первом чертеже рабочего проекта.

3. Согласование письмом согласующей организации в адрес заказчика объекта или проектной организации. Проектная документация считается согласованной в пределах компетенции соответствующей согласующей организации на условиях, указанных в письме.

Часть 2. Глава 3

Свобода и надзор (кто и как нас проверяет).

Государственная экспертиза и утверждение проектной документации

После согласования со всеми заинтересованными инстанциями, проектная документация подлежит государственной экспертизе в порядке, установленном положением о проведении государственной экспертизы и утверждении градостроительной, предпроектной и проектной документации в Российской Федерации которое утверждено Постановлением Правительства РФ от 27.12.2000 г. № 1008 (далее по тексту – "Постановление 1008"). Если проектная документация подлежит обязательной государственной экспертизе, то положительное заключение экспертного органа является основным условием утверждения заказчиком разработанной ПСД.

По общему правилу государственной экспертизе подлежит любая проектная документация, за исключением документации на объекты, строительные работы на которых не затрагивают их характеристик надежности и безопасности и для строительства которых не требуется оформлять специальное разрешение. (Перечень объектов, на строительство которых не требуется оформлять специальное разрешение, устанавливается органом местного самоуправления или субъектом Российской Федерации). Государственной вневедомственной экспертизе, в частности, подлежит любая проектная документация на создание объектов, финансируемое за счет средств федерального бюджета.

Различают вневедомственную и ведомственную (отраслевую) государственную экспертизу. Не является исключением и отрасль связи – функцию ведомственной экспертизы в телекоммуникационной отрасли выполняет ФГУ "ЦНИЭС", созданное при Министерстве информационных технологий и связи. Порядок производства государственной ведомственной экспертизы в отрасли "связь" установлен приказом Минсвязи РФ от 22.07.2003 г. № 96 (далее по тексту – "приказ 96").

В отличие от Постановления 1008, Приказ 96 не содержит вообще никаких исключений из общего правила обязательной государственной экспертизы проектной документации. Таким образом, **вся без исключения проектная документация на создание объектов связи подлежит государственной экспертизе в ФГУ "ЦНИЭС". Не допускается утверждение проектной документации на создание объектов связи до получения заключения государственной экспертизы с рекомендацией об утверждении ПСД.** Надо заметить, корреспондирующая норма содержится и в приказе Минсвязи от

09.09.2002 г. № 113, который требует предоставления в органы Россвязьнадзора копии заключения государственной ведомственной экспертизы во всех случаях, когда создание объектов связи производилось по проектной документации.

Государственная экспертиза производится за счет заказчика ПСД. Стоимость работ обычно составляет порядка 15% от стоимости проектных работ, длительность процедуры составляет порядка 1,5 – 2 месяца после заключения договора с ФГУ "ЦНИЭС". Проектную документацию на экспертизу представляет либо заказчик либо проектная организация, выполнившая соответствующие работы.

Государственная экспертиза рассматривает соответствие проектной документации требованиям ИРД (технические условия на размещение оборудования, технические условия на присоединение сетей связи, технические условия на присоединение к сетям электроснабжения и другим инженерным системам, генеральный план и землеотводы, частотно-разрешительные документы и т.д.). Также проверяется соответствие ПСД требованиям нормативно-технических актов и действующему законодательству, а также условиям действия лицензий оператора связи, который будет эксплуатировать соответствующий объект.

По результатам рассмотрения проектной документации, экспертный орган готовит заключение, в котором отражаются основные параметры проектируемого объекта, а также замечания эксперта. В случае, если замечания эксперта не препятствуют созданию проектируемого объекта в заключении делается вывод о рекомендации представленного проекта к утверждению заказчиком с учетом замечаний органа государственной экспертизы. Проектная организация либо соглашается с замечаниями эксперта и вносит изменения в ПСД, либо может не согласиться с доводами эксперта и направить заказчику отзыв на заключение экспертизы, в котором дает обоснование отказа от внесения изменений в проектную документацию. В последнем случае вся полнота ответственности за возможные последствия возлагается на проектировщика.

Если эксперт сделает вывод о наличии в проектной документации существенных недостатков, препятствующих ее утверждению, то в заключение обязывает заказчика или проектную организацию повторно представить соответствующую ПСД на государственную экспертизу с учетом замечаний эксперта. В данном случае утверждение проектной документации заказчиком не допускается даже при наличии отзыва проектной организации. Иными словами, заказчик вправе утвердить ПСД только при наличии рекомендации об утверждении проектной документации, указанной явным образом в экспертном заключении органа государственной экспертизы.

Утверждение проектной документации производится приказом руководителя организации – заказчика при наличии заключения государственной экспертизы. При этом на титульном листе ОПЗ делается отметка о дате и номере приказа об утверждении проекта, а также номер и дата заключения государственной экспертизы. Утвержденный проект является основанием для оформления разрешения на строительство и производство строительно-монтажных работ.

Этапы большого пути

Итак, в результате завершения рабочего проектирования объекта связи, заказчик приобретает следующие документы:

1. **Рабочий проект объекта:**

- Общая пояснительная записка с приложениями (задание на проектирование, исходные данные и исходно-разрешительная документация, согласования, сертификаты соответствия и т.п.);
- Рабочая документация (чертежи, планы, схемы, спецификации, согласования);
- Сметная часть (кроме случаев отказа заказчика проекта от разработки данного раздела проекта, о чем делается отметка в задании на проектирование);
- Инструкции по эксплуатации объекта (если их разработка предусмотрена заданием на проектирование).

2. **Заключение государственной экспертизы** проектной документации (с рекомендацией об утверждении проекта);
3. **Приказ руководителя заказчика об утверждении проектной документации.**

Комплект проектной документации на "домашнюю сеть" масштаба 150-200 домов весит немало килограмм и стоит тоже отнюдь не мало. В крупных городах России стоимость такого проекта со всеми согласованиями может достигать 30 000 долларов с учетом различного рода согласований, экспертиз, да и просто "коррупционного налога". Телекоммуникации – действительно дорогой бизнес и даже самоотверженный труд сетеустроителей может оказаться тщетным по одному росчерку чиновного пера….

Часть 3.

Глава 1. Прокладки "воздушек".

Война план покажет.

Довольно часто задается вопрос - "как кабеля подвешиваются между домами"? Ответ прост - любую работу делают люди. И в строительстве "воздушек" (подвесных кабельных линий) то же нет никаких особых сложностях, все будет понятно из примеров.

Поэтому материал, изложенный ниже, является скорее списком практических работ, а не законченным руководством. Тем не менее, некоторые попытки обобщения опыта прокладок все же сделаны - вам судить о успехе этого начинания.

Нужно сказать заранее, что не все способы одобрит инспектор по технике безопасности, и прочие официальные органы. Однако, похожим способом в России уже несколько десятилетий монтируются сети кабельного телевидения, радиофикации, и Ethernet не будет исключением. Слишком далеки правила от реальности.

Однако, это не значит, что нормы не надо знать, совсем наоборот. Поэтому вопросам согласования целиком посвящена одна из следующих глав. Кратко - прокладка подвесных кабельных линий - это строительство. На него требуется сначала получить согласование места (скажем, в районной администрации, управе, ДЕЗе, РЕМПе). Затем заказать проект. Потом можно строить (формально должна выполнять лицензированная организация). Если сеть коммерческого назначения - то предстоит сдача с участием УГНСИ (по приказу № 113).

Но в данной части перейдем сразу к примерам.

И последнее, главное. **Работать на крыше можно только застрахованным (привязанным).** По крайней мере, если крыша не плоская, и не окружена высоким капитальным бордюром (хотя некоторые специалисты рекомендуют страховаться и в этом случае, что бы не расслабляться). Страховочная система стоит от 300 рублей, монтажный пояс можно найти даже бесплатно. Конечно, это несколько неудобно, но быстро привыкаешь. **Жизнь - в любом случае дороже**.

Часть 3. Глава 1

Протяжка кабеля через несколько домов.

Описанная протяжка была сделана весной 1999 года. Линия нормально работает без ремонтов до сих пор, т.е. уже более 4-х лет. В то уже несколько далекое время сети были не столь популярны, как сейчас, и приходилось бороться за всех, даже весьма отдаленных пользователей.

После осмотра предстоящей трассы прокладки (чуть менее 500-от метров) выяснилась следующая картина (конец трассы на первой фотографии виден плохо, поэтому приходится показывать вид с обеих сторон):

Рис. 1.1. Вид трассы, по которой нужно проложить линию (с обоих сторон).

На трассе 5 домов. В №1 (красной 14-этажке) уже был поставлен хаб, и подключено несколько пользователей. №2 (длинная, около 200 метров, 9-этажка). Несмотря на активную рекламу, желающих подключиться в ней не нашлось. №3 и №4 (5-этажные "хрущевки"). В доме №5 (5-этажная брежневка) нужно было подключить заказчика.

Работу предстояло выполнить силами 2-х человек.

Из материалов и оборудования присутствовала бухта кабеля П-296 и 100 метровая веревка. Надо отметить, что это была первая прокладка с использованием П-296, и никто точно не знал, как он себя поведет в реальных условиях.

За день до начала работ был найден в лифтовой ключ от дома №2, проверен на совпадение с замком реальной двери. Дом №1 был уже освоен и не вызывал особых трудностей. Выход на хрущевки и брежневку был свободен, если не считать железных и вечно закрытых подъездных дверей. На этом подготовка "плацдарма" была закончена.

С утра раскачивались как обычно долго. Сначала текучка, потом взяли ключи, пока собрались... Работа началась после обеда, часов в 13.

Напарник поднялся на крышу дома №2, спустил вниз веревку, к которой мной был привязан конец кабеля. Далее пришлось долго катать по двору железную бухту П-296 для разматывания кабеля (полезные приспособления для этой операции и многих других ниже по тексту). По мере этого процесса напарник поднимал его на крышу.

Рис. 1.2. Стена, вдоль которой поднимался кабель. Его настоящее состояние показано красной стрелкой.

После того, как большая часть тяжеленного кабеля была худо-бедно разложена на крыше (поднять бухту сразу не слишком хороший вариант, ее размеры и вес не позволят сделать это просто). Остаток кабеля, предназначенный для затяжки на дом №3 и далее, был подвязан к дереву "внатяг", чтобы не мешал проезду машин. При этом конец кабеля длиной около 50-ти метров оставался свободным для дальнейших манипуляций.

Рис. 1.3. Стена дома, куда был поднят конец, оставленный свободным на земле. Красная вертикальная стрелка показывает место, где была спущена вревка с крыши.

Далее напарник поднялся на крышу дома №3, и, как обычно, спустил веревку вниз. Поднимаемый кабель сразу опускался с другой стороны двухскатной крыши на землю. При этом пришлось внимательно провести конец через растяжки крепления антенн и провода радиофикации, что бы после натяжки они не мешали линии.

Веревку даже не пришлось отвязывать от кабеля, сразу после спуска в другой стороны она была перекинута через дорогу и провода между домами №№3 и 4.

Рис. 1.4. Простая улица. Провода висят низко, машины проезжают относительно редко. Деревьев почти нет.

В результате операции, кабель был сразу вытянут к подножью дома №4. Подвязывать к очередному дереву его не пришлось, т.к. напарник успел спустить веревку с очередной крыши (№4). Далее операция была повторена в комбинации №№4-5

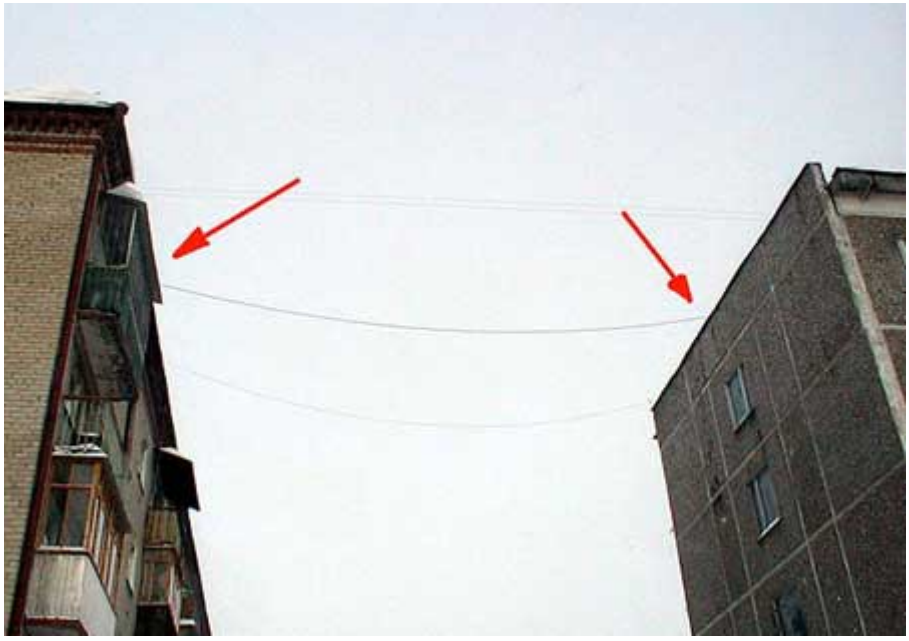

Рис. 1.5. Это совсем простой участок. Кабель, как обычно, показан красными стрелочками.

Такой небольшой пролет можно просто перекинуть, но есть риск. Веревка запутается, рука дрогнет - и груз окажется в чьем-то окне. Есть правило - не кидать на крыше веревку с грузом. Долетит просто веревка - хорошо. Не долетит - опускать на землю. Изыски а-ля Робин Гуд или Давид до добра людей без соответствующей подготовки не доводят. Что, кстати, было не раз доказано печальным опытом.

Так кабель был доведен до цели, закреплен, и работа пошла в обратную сторону. Для натяжки мы поднимались на крыши вдвоем, т.к. в одиночку натянуть и привязать кабель почти невозможно. Нельзя сказать, что это было просто, но открытий тут нет. Один человек натягивает, второй в это время закрепляет кабель на стойке.

Перед натяжкой пролета между домами №№2-3 кабель был отвязан от дерева. Далее, много хлопот причинила протяжка по крышам лифтовых 10 подъездов, с закреплением и натяжкой на каждой. Кабель тяжелый, тянуть его тяжело.

После закрепления на крыше дома №2, остаток был спущен вниз.

Рис. 1.6. Относительно широкая дорога с интенсивным движением. Но нет ни высоких проводов, ни деревьев.

Далее переход между домами №№1-2 был проведен по обычному методу. Только крыши были повыше, да машин побольше. Всего протяжка заняла часа 3-4 тяжелой работы. Это надо признать вполне удовлетворительным достижением.

В завершение, интересное дополнение. Так как кабель такого типа (П-296, описан в конце данной главы) был использован впервые, было решено провести эксперимент. Для начала, не стали отрезать конец (метров 50 из 500 метровой бухты), и подсоединили витопарный "хвостик" длиной 3 метра прямо к оконечному разъему. На стороне абонента витая пара была спущена с чердака и проведена по квартире. Всего ушло около 40 метров UTP.

К сожалению, "такого" линия не перенесла. Хотя "линки" на устройствах загорелись, и скорее всего, более приличное железо заработало бы (позже был успешно сделан линк в "полную бухту"). Но в данном случае пришлось идти и отрезать "запас". После этого все пришло в норму.

Часть 3. Глава 1

Протяжка кабеля через оживленную улицу. Подготовка.

После описания относительно простой протяжки можно перейти к более сложным случаям. Например, к преодолению оживленной дороги с проводами освещения и троллейбусными линиями.

Вот панорама улицы, через которую надо протянуть кабель.

Нужно специально отметить следующее. По правилам, подобные работы надо делать силами профессиональной бригады, с участием ГАИ, перекрывать дорогу, останавливать движение, и т.п. Однако на практике ни разу не удалось быть свидетелем подобных действий (в том числе работников радиофикации или кабельного телевидения).

Стоимость полностью "правильных" работ можно представить. Сумма будет немалой, а количество согласований еще большим. Поэтому фактически, остается прокладывать кабеля на свой страх и риск.

И речь может идти только о минимизации этого риска.

Рис. 1.7. Страшноватый вид. Но тянуть надо.

Инструмент.

- Потребуется мягкая веревка средней толщины, примерно 4 миллиметра в диаметре. Нитку использовать не желательно, она путается, и кидать ее неудобно. Так же неудобна жесткий синтетический канат.
- Веревка толстая 8-10 мм, не менее 100 метров. Она потребуется для перетяжки кабеля. Можно обойтись без нее, но стоимость обрыва в данном случае может оказаться непомерно большой.
- Груз весом около 700-800 грамм, который можно хорошо привязать к концу веревки. Хорошо подходит толстостенная трубка длиной сантиметров 10 (лучше, если на нее одет резиновый шланг).
  Однако, идеальный вариант - специальный мешочек с песком, или мелкой дробью. На крайний случай подойдет камень, но лучше позаботиться заранее.
- Очень желательны рации, они значительно удобнее сотовых телефонов (связь мгновенна, это может быть важно в подобных работах).

Люди.
Потребуется не менее четырех человек, лучше пять. Расстановка сил будет показана на схеме далее по тексту. Обязательно один работников должен уметь хорошо перекидывать веревку через провода. Если опыта нет, стоит потренироваться заранее. Оживленная улица не место для экспериментов.

Вообще говоря, известно много способов "перекидывания" веревки. Промышленная рогатка, арбалет, спиннинг, даже теннисный мячик. Если в бригаде есть большие специалисты в подобном спорте, можно считать повезло.

В противном случае применение технологических новинок может принести больше неприятностей. Запутанные на трубостойках лески, выбитые окна, и тому подобные следствия ошибочных бросков волне реальны.

На мой взгляд, самый стабильный результат дает перебрасывания веревки "с земли". Кидать веревку с грузом нужно по типу пращи, только не раскручивать, а просто "с замаха". Т.е. держать за веревку на расстоянии 20-30 см. от груза, пару раз качнуть, и кинуть. При некоторой сноровке, провода на уровне 3-4 этажа проблемой не будут.

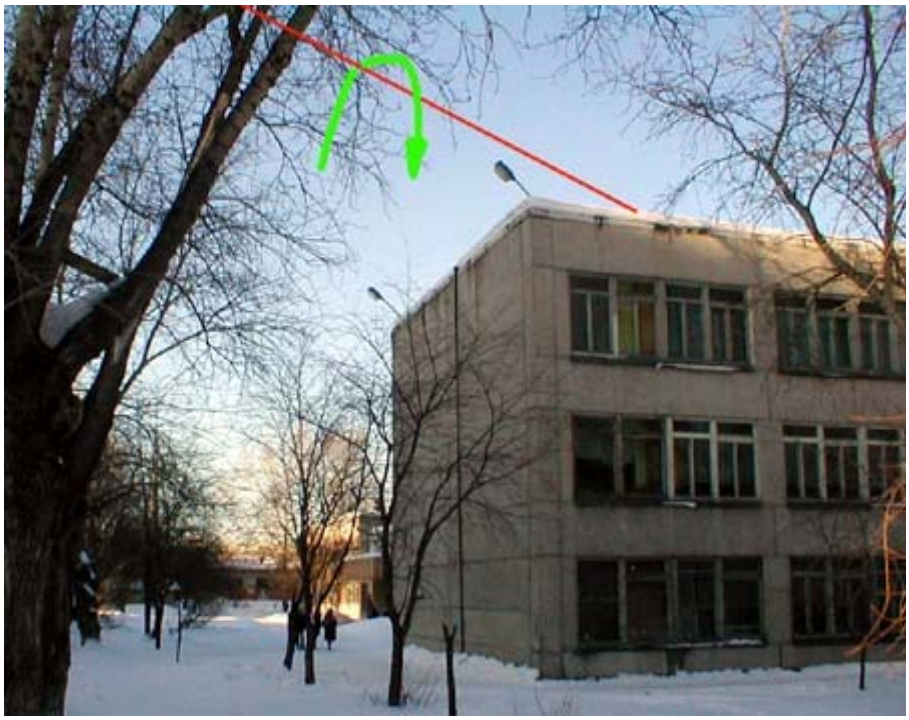

Рис. 1.8. Этот провод соответствует примерно 4-5 этажу обычного дома.

Вот, пожалуй, самый высокий провод, который мне пришлось перебрасывать (выделен красной линией). С середины крыши 3-х этажной школы, провод уходит через дорогу на крышу 12-этажки.

Но вернемся к прокладке. Посмотрим, как выглядит будущая трасса с земли.

Рис. 1.9. Трасса прокладки, вид с земли.

Можно сказать, ничего хорошего. С обеих сторон улицы "освещенка". Провода высокие, и, самое неприятное, стоят очень близко к дорогим окнам кафе и ресторана. Да еще масса припаркованых автомобилей. На проезжей части - троллейбусные провода, и мощный поток машин.

Поэтому, действовать желательно рано утром (насколько это возможно). Согласовать выходы на крыши, подготовиться.

Работа ночью без "прикрытия" - верный способ попасть в отделение милиции. Если улица днем совершенно непроходима, желательно озаботиться присутствием знакомого из какого-либо силового ведомства.

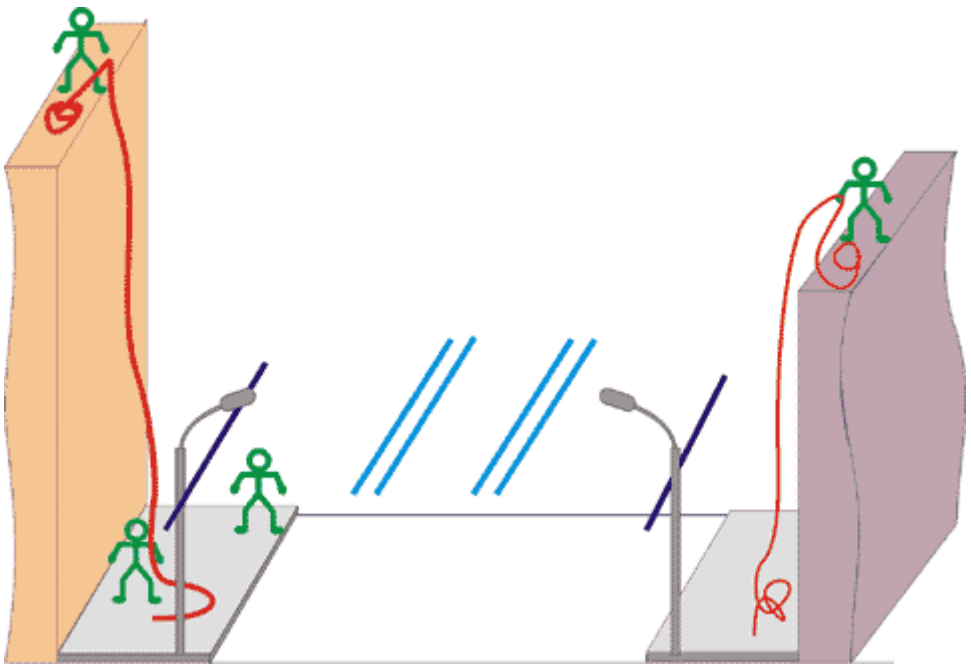

Рис. 1.10. Исходная позиция перед протяжкой.

На рисунке - исходная позиция. На нее можно выходить не торопясь, помех это никому не создаст. Но дальше нужно действовать быстро и аккуратно.

Человек сверху справа - пока статист. Сверху слева - управляет веревкой. Это совсем не синекура - в один момент нужно ослабить, в другой - натянуть, в третий - перейти вдоль крыши, что бы было удобно обойти припятствие. Двое внизу - основной "перекидающий" и помошник.

Первая задача помошника - постоянно держать веревку натянутой (не туго, но без слабины). Иначе она запутается, ее затопчут прохожие, а на проезжей части - и того хуже. Вторая - выдавать "перекидывающему" конец удобной длины, помогать укладывать веревку перед броском.

Метать груз удобно, стоя почти под проводами, в полоборота. Важно хорошо уложить веревку - кольцами на ровном месте. Витки обязательно должны идти сверху вниз, если смотреть от груза.

Остается выбрать удобное место, дождаться "окна" в потоке машин. И - перекинуть веревку. Если вам кажется, что это просто - посмотрите, как это выглядит в реальности. Провода - высоко, стекла - близко. Кругом люди и машины.

Рис. 1.11. Вид на провода.

Опастных факторов два. Во-первых, можно запутать конец на высоте. Старайтесь не вытягивать груз обратно при неудачном броске. При подъеме (быстром уменьшении плеча маятника) груз может начать раскачиваться, и веревка перекрутится несколько раз вокруг провода. Это очень неприятно. Поэтому опускайте неудачно перекинутый груз, отвязывайте его, вытягивайте веревку, привязывайте опять.

Если все же веревка запуталась - можно либо вызывать автовышку, платить, или (очень вредный совет) потихоньку покинуть место работ. Как говорится, на выбор.

Вторая опастность - недокинуть груз до провода так, что он упадет на машину (прохожего, стекло). Тут не помешает пара помошников, которые смогут "подстраховать" место падения.

Протяжка кабеля через оживленную улицу. Дорога.

Удачный бросок. Груз аккуратно перелетел через провода, и плавно спустился до земли.

Далее нужно перетянуть всю веревку через провода. Если на ней нет узлов, то это не сложно. Бояться напряжения не надо - "освещенка" днем отключена (в случае силовых проводов придется действовать втройне аккуратно).

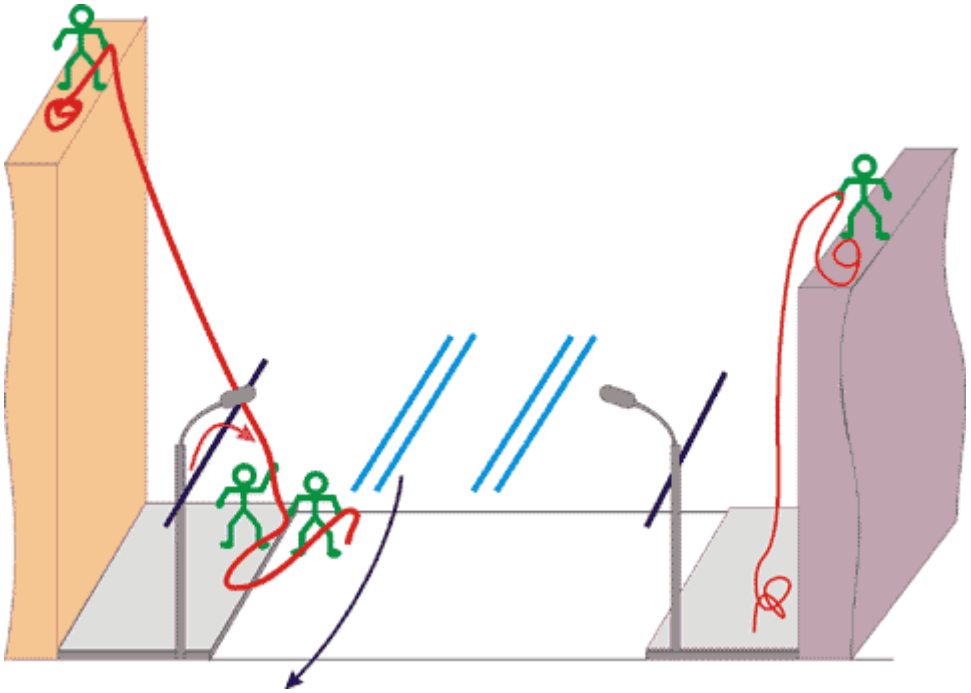

Рис. 1.12. После перекидывания "освещенки".

В таком положении нужно оказаться после перекидывания веревки через первую "освещенку". Черной стрелочкой обозначено движение машин, которым придется так или иначе вас обьезжать. Главное при этом не нервничать, действовать спокойно и предсказуемо.

Перекидывание троллейбусных проводов по сути ничем не отличается от предыдущей операции. Только придется действовать быстро - все происходит посередине оживленной дороги.

Очень много будет зависить от расторопности помощника - придержать, подать, подтянуть, ослабить. Даже задержать на минуту поток автомобилей (в конце концов, все люди, и можно договориться).

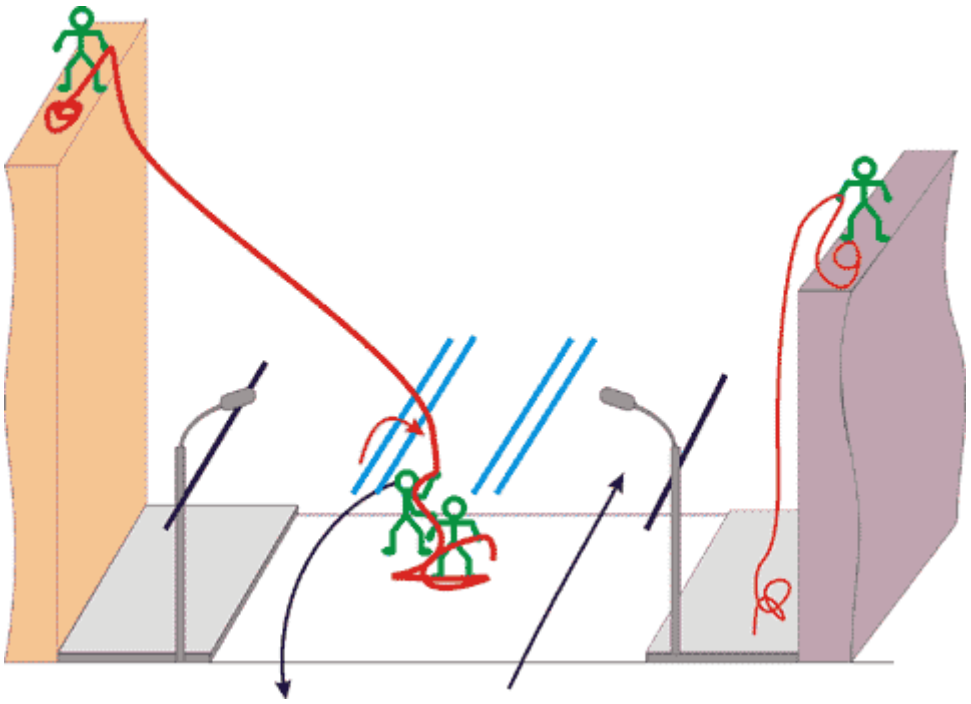

Рис. 1.13. Перекидывание троллейбусных проводов.

Следующая позиция. Ничего нового, главное, что бы вы добрались до нее (от предыдущей) быстро, за 2-3 минуты. Троллейбусные токонесущие провода (как и трамвайные) сверху защищены проволокой. Поэтому, нет ничего страшного в том, что на них лежит веревка.

Помошник при этом должен держать веревку "внятяг", что бы она не мешала проезду машин.

Действуя по описанному выше алгоритму (веревку уложить кольцами, кинуть, перетянуть, уложить), попадаем в следующую ситуацию:

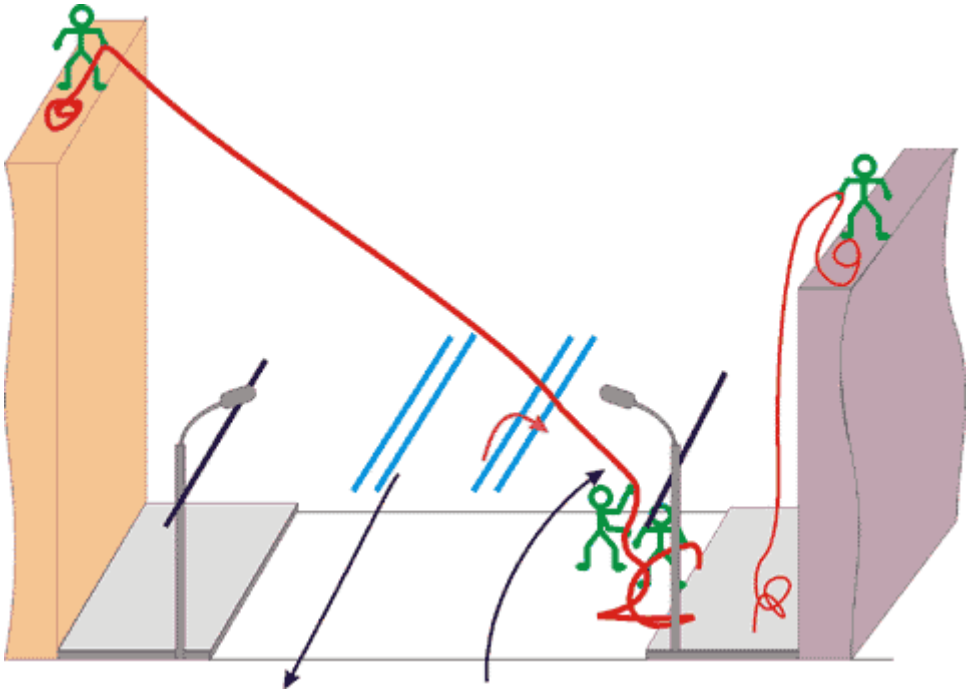

Рис. 1.14. Вторая троллейбусная линия.

Можно сказать, что дорога пройдена. Можно не торопиться, передохнуть перед последним этапом.

Все выглядит очень просто на рисунке, в реальности гораздо сложнее. Провода идут близко от дома, всего метрах в 2-2,5. Плюс к этому, козырек кафе и магазина, огромные стекла. Кидать в сторону витрин и окон нельзя. Слишком велик шанс промахнуться, и будет "не рассчитаться".

Рис. 1.15. Главное не промахнуться...

Поэтому, перекидывается конец другой веревки, как показано стрелочкой, "от дома" к дороге.

Задача помошника - держать веревку максимально высоко, в натяг с крыши дома, что бы ничего не мешало проезду машин и троллейбусов, до тех пор, пока не будет перекинута через "освещенку" вторая веревка.

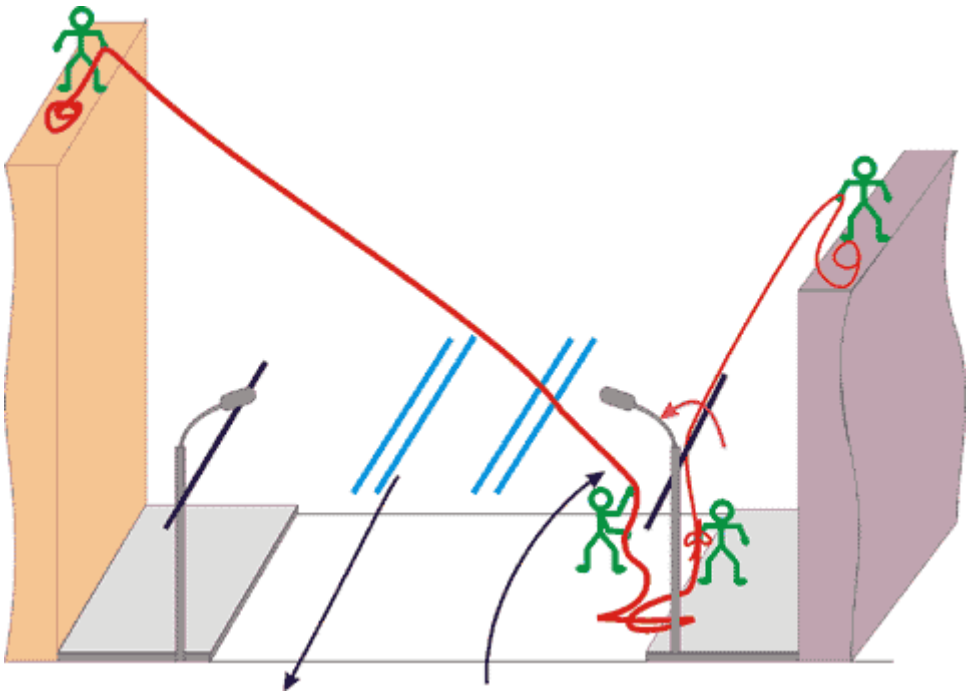

Рис. 1.16. Вторая "освещенка".

Надо сказать, что в реальности описанной протяжки пришлось перекидывать именно не правильно. Как обычно, хотел как лучше, а получилось как обычно. Сделать "правильно" помешали припаркованные на обочине машины. Между ними не было достаточного для броска просвета. А отступать поздно.

Для таких клинических случаев есть прием, типа подсечки. Когда груз, привязанный к веревке, взлетает немного выше проводов, нужно его резко остановить. Например, наступить на кучку-бухту, с которой разматывается веревка. Тогда груз резко изменит направление и будет падать по крутой траектории. Что, собственно, и нужно в данном случае. Операция деликатная, и рекомендовать ее к обычному применению никак нельзя.

Дальше все просто и понятно. Веревки связываются, и вытягиваются на крыши. Придерживать их с земли надо "до последнего", что бы ничего не запуталось.

Особенно внимательно надо следить за протяжку через провода узла, желательно делать это "с волной". Резкое движение конца веревки, с целью пустить "бегущую волну", делать умеют наверно все. Тут это надо сделать в нужный момент.

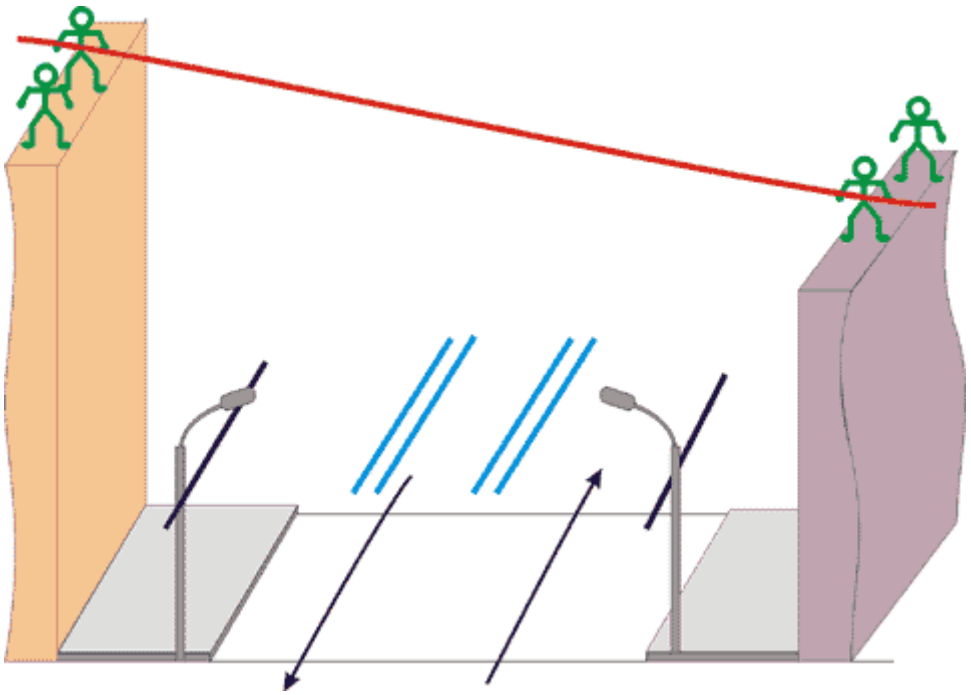

Рис. 1.17. Окончание протяжки.

Затем все поднимаются на крышу, и помогают коллегам перетянуть кабель, закрепить его, развести по крыше.

Заодно, разумеется, порадоваться сделанной работе.

Рис. 1.18. Вид сверху.

Такой вид открывается, если еще раз взглянуть на улицу с крыши. Как говорится, глаза боятся, а руки делают.

Борьба с деревьями.

Можно смело сказать, что больше всего протягивать кабеля мешают не широкие дороги с большим потоком машин, а обычные деревья. Потому что встречаются в работе гораздо чаще, а преодолевать их иногда даже сложнее, чем автострады.

Самый неприятный случай - когда деревья выше крыш домов. При этом строительство линии может превратиться в акробатику, требующую не только "отработанного" броска веревки с камнем, но и навыков древолазания.

Но для начала рассмотрим пример достаточно простой протяжки, с минимальным количеством деревьев. Для выполнения работы понадобилось две веревки средней толщины длиной около 40 метров, и 3 человека.

Пояснять тут особенно нечего (лучше один раз увидеть), поэтому ограничусь самыми краткими замечаниями.

Рис. 1.19. Спуск веревки с первого дома.

Выбрано место, где спуску веревки не помешают балконы, трубы, и прочие элементы советской градостроительной архитектуры.

Рис. 1.20. Веревка закреплена перед дальнейшей работой.

Далее, выбрано место, где на линии предполагаемой протяжки растет минимальное количество деревьев. Спущенная ранее веревка обведена между невысоких деревьев (скорее кустарников), и закреплена перед дальнейшей работой таким образом, что бы ничего не мешало ее подъему вверх.

Рис. 1.21. Спуск веревки со второго дома.

То же самое повторяется с другой стороны протяжки. Вторая веревка спущена с крыши, и "обведена" вокруг дерева так, что бы оказаться над ним (в данном случае частично).

Рис. 1.22. Связывание веревок.

Затем веревки сводятся вместе, и связываются прочным узлом (ведь с их помощью будет перетянут кабель).

Рис. 1.23. Начало подъема.

При подъеме необходимо постараться до последнего придерживать веревку, что бы она аккуратно миновала все ветви деревьев. Бывало, что качание при резком подъеме так

запутывало веревку, что приходилось начинать сначала не только работу, но и покупать новую оснастку.

Рис. 1.24. Перетяжка кабеля.

Дальше все просто - можно сказать, дело техники. К концу поднятой и слегка натянутой веревки привязывается кабель (в данном случае оптоволокно), и не торопясь перетягивается на другую сторону.

Вся работа заняла примерно 20-30 минут.

Следующая протяжка намного сложнее. Только посмотрите на эти "уральские джунгли":

Рис. 1.25. "уральские джунгли".

Протянутый кабель (показан красными стрелками) практически не виден за ветками даже зимой. Летом все выглядит вообще как сплошная зеленая стена.

Первый снимок сделан примерно с середины 200-от метровой протяжки. Второй - с места, где стоят люди (обозначено красной стрелкой). Это немного не доходя до стены 5-ти этажки, на которой крепится один конец кабеля.

Рис. 1.26. "уральские джунгли".

Сколько я не пытался найти между деревьев "окошечко" с прямой видимостью до дома, на который уходит линия, не смог.

Надо отметить, что данная протяжка делалась спешно, в условиях цейтнота. Нужно было срочно подключить дом, где жил коммунальный начальник районного масштаба, хотя бы временно, и не считаясь со сложностями. Дешевого оборудования радио-Ethernet тогда (в 1999/2000 году) не было.

Обойти - практически невозможно. С одной стороны военный госпиталь (а за ним вообще большой парк), с другой - целый комплекс зданий нескольких Екатеринбургских институтов с совершенно непонятными зонами ответственности.

В общем, при всей сложности ситуации, отступать было некуда.

Рис. 1.27. Деревья средней сложности.

Немного вдали виден дом (серая хрущевка), куда приходит провод (обозначен красными стрелками). Слева - недоступное здание, имеющее отношение к министерству образования.

Этот участок протяжки был относительно не сложен. Веревка была спущена с крыши, и "обведена" между ветками (насколько это было возможно в данной ситуации). Делается это следующим образом:

Один человек внизу, и один на крыше держат веревку "внатяг". Передвигаясь по земле нужно постараться обойти деревья (или наиболее мешающие ветки) одну за другой. Т.е. пройдя за дерево, отойти как можно дальше в сторону (насколько позволят соседние деревья), далее натянуть (поднять по диагонали с крыши) веревку как можно выше, и завести ее уже сверху на дерево. После этого можно "положить" веревку на верхние, тонкие ветви кроны. Затем операцию повторить со следующим деревом.

На словах процесс выглядит несложным, однако реально часто бывает, что ветви соседних деревьев переплетаются, и нужно их перебрасывать подобно проводам освещения. Так же, порой приходится преодолевать небольшие, но плотно сросшиеся деревья или кустарники.

Кстати, можно использовать разный подход к разным видам деревьев. Прочность ветвей (она всегда будет казаться слишком большой), их направления (вверх или вниз), гладкость коры - все можно учитывать для максимально эффективной работы.

В общем, в данной протяжке с большим трудом, но удалось миновать деревья, растущие близко к зданиям. Однако, в середине протяжки встретилась следующая проблема:

Рис. 1.28. Деревья посередине протяжки.

Такие деревья нельзя "обойти" с натянутой веревкой. Их кроны просто выше крыш домов, и завести сверху ничего не получится. Остается только вариант подъема с использованием

перекидвания, срубания веток. Могут помочь дополнительные направляющие веревки (с помощью которых основной канат можно в некоторой степени отводить в сторону).

Однако на рисунке почти безвыходная ситуация - кабель нужно было заранее провести между двух деревьев. Т.е. небольшая ошибка в первоначальном плане, и нужно по крайней мере половину работы начинать сначала.

Так как в данном случае строилась по сути времянка, было решено положиться на уникальные свойства П-296. И расчет оправдался - через два года линия была спокойно заменена на постоянную (разумеется, проложенную по другому маршруту).

И последнее. Деревья мешают не только во время протяжки. Высокие тополя довольно чато ломаются. Небольшой шквалистый ветер, и можно наблюдать следующую картину:

Рис. 1.29. Упавшее дерево.

Если на пути ствола или ветки встретится кабель - обрыв обеспечен. И хорошо, если не пострадают конструкции, где кабель был закреплен.

Это нужно учитывать, и по возможности избегать улиц, засаженных старыми тополями.

Часть 2. Глава 1

Использование существующих коммуникаций.

В современном городе с трудом можно найти крышу, через которую уже не проложены линии радиофикации, кабельного телевидения, или даже телефонии. Разумеется, не всегда они по направлению совпадают со строящейся сетью Ethernet, но такое бывает очень часто. В конце концов, цели строителей этих весьма разных сетей во многом совпадают.

Можно ли использовать уже имеющиеся коммуникации? Безусловно.

Самый простой способ - разъединить имеющийся кабель, перетянуть его на одну сторону с двойной веревкой, после чего вытянуть обратно (и привести соединение в прежнее состояние). К сожалению, рекомендовать подобное (мягко говоря) нельзя.

Трогать чужое имущество - далеко не лучший вариант проведения работ. В то же время, есть два пути - часто кабельное хозяйство бывает брошенным (особенно этим грешат ранние сети кабельного телевидения), и его можно использовать практически без опасений. Второе - договориться с собственником на кратковременное рассоединение линии. Если услуга некритична - это вполне реально.

Еще одна возможность - часто монтажники при предыдущих прокладках оставляют своеобразные "закладки" на будущее. Например, таким можно смело считать кусок полевки, который проходит над сложной улицей, и не ведет к какому-либо оборудованию. После использования такой закладки очень желательно все привести в исходное состояние - взаимная вежливость на крыше просто необходима.

Но есть способ, который за счет технической сложности позволяет решить организационные вопросы. Это механизм можно назвать "веревкоходом", или, вернее, проволокоходом.

Конструкций существует множество, вот только некоторые из них:

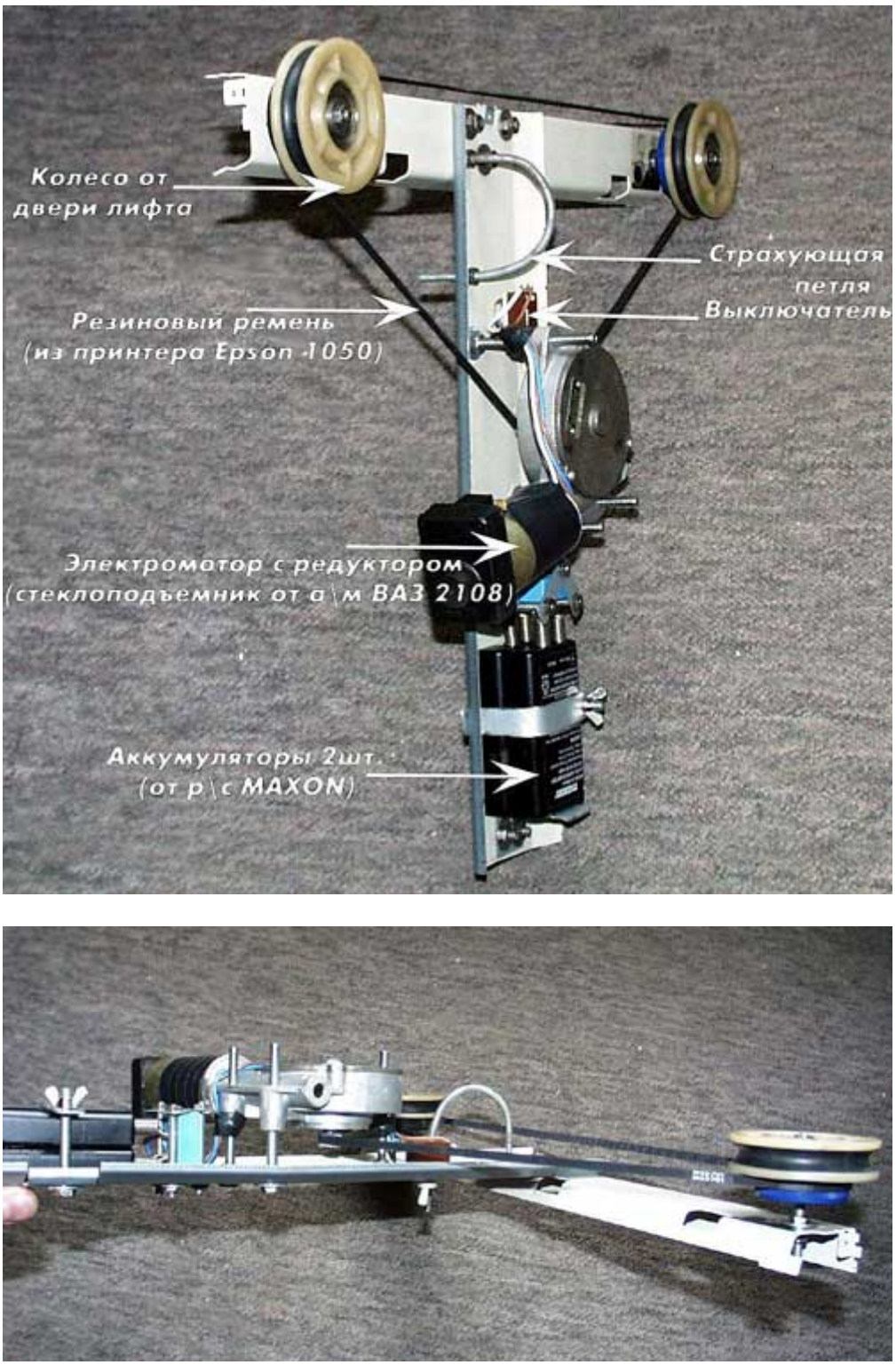

Рис. 1.30. Конструкция веревкохода.

Подробно описывать устройство не имеет смысла. Полагаю, все хорошо видно из фотографий.

Потребительские свойства следующие: веревкоход заезжает по кабелю с углом в 40-45 град. Потом начинают пробуксовывать колеса. Когда был подвешен груз 3 килограмма - проблем не возникало, скорость движения составила 5 м/мин.

Питание - два аккумулятора от радиостанций Maxon (10.8 В, 0.8 А/ч каждая), их хватает на 1 час работы. Хочется особо отметить "автомобильную" составляющую. Действительно, это источник целой кучи серийных (и не дорогих) устройств с 12-ти вольтовым питанием. Остается только их использовать "по назначению".

Если приспособить к этому автомобильную сигнализацию, то можно получить весьма "умное" приспособление с дистанционным управлением. Которое будет способно передвигаться в обе стороны, и даже выполнять простейшие действия (например, "довезти" веревку до определенной точки, и затем отпустить конец).

Доработка не такая и большая, но достаточно одной "хитрой" протяжки, что бы все затраты окупились, что называется, с лихвой.

Ниже показан еще один "веревкоход":

Рис. 1.31. Веревкоход mnetwork.ru.

Этот образец сделан на основе двигателя стеклоочистителя (12V BOSH) от "народного" автомобиля. Используются два направляющих пластиковых ролика и один "ведущий" резиновый, плюс аккумулятор (6А 12V) от UPS.

Тянет очень хорошо, и может заезжать по проволоке, натянутой под 30-45 градусами, и завозить за собой груз в 2-3 килограмма.

И еще один вариант:

Рис. 1.32. Веревкоход.

Колеса использованы от роликовых коньков, цепь от велосипеда. Двигатель опять автомобильный.

Понятно, что при наличии заметной разницы в высоте между домами (большом наклоне существующего кабеля) можно обойтись без электропривода.

Рис. 1.33. Переезд улицы на ролике.

Длина пролета, который был пройден в данном случае - около 300 метров. Простейшее устройство, всего несколько минут - и пролет пройден.

Однако, надо осознавать риск применения подобных приспособлений. Может произойти серьезная трагедия, если что-то пойдет не так, как рассчитано. Поэтому применять самоделки надо очень осмотрительно, по возможности максимально страхуясь от несчастных случаев разного рода - от отказа системы до обрыва несущего кабеля.

И главное, нельзя применять в качестве груза случайные металлические конструкции. Мешочек с песком или мелкой дробью на порядок безопаснее. В этом плане фотография демонстрирует то, как делать ни надо ни в коем случае.

А следующий материал вообще можно отнести к разряду экстремальных. К повторению его можно рекомендовать только в самых редких случаях, когда при большом наклоне несущего кабеля ролик не требуется.

Перейдем к описанию протяжки.

...Линия "предшественников" упрощала задачу - при большом перепаде высот хотелось просто опустить петлю с новым кабелем "по направляющей" П-296. Однако, попытка была неудачной. Петля из оптоволокна с несущим тросом не достигнув и половины пути остановилась и дальше не пошла. Сильный боковой ветер и малый вес оптоволокна свел на нет все усилия.

По хорошему, надо остановиться, и начать заново с лучшей технической подготовкой. Применить ролик, или более сложный самодвижущийся аппарат. Но действует обычная штурмовщина, сильна вера в "авось"... И бригада решается на опасный трюк. По другому, в общем, это назвать нельзя.

Рис. 1.34. Изготовление петли.

Если мал вес - его можно легко добавить. Причем, не стесняясь, тяжелым подшипником. А внизу, надо заметить, оживленная улица. Люди ходят толпами, машины ездят...

В общем, примотали, не жалея стальной проволоки. Если рухнет, то только вместе с опорным П-296, никак не иначе. Перетереться ничего не может - петля с 5-ти миллиметровым тросом выдержит многое. П-296 то же не гнилая нитка.

Рис. 1.35. Переезд улицы на скольжении петли.

Груз отпущен вниз, и быстро удаляется по направлению к соседней крыше.

Рис. 1.36. Кабель перекинут.

...И вполне благополучно приходит в руки ожидающих монтажников. Вернее, почти приходит. Скольжение было настолько плохое, что пришлось немного потрясти опорный П-296 на последних метрах дистанции - петля застряла не доходя 8-10 метров.

Впрочем, несколько рывков, и груз достигает цели. Кабель закрепляется, работа завершена...

Повторюсь, что несмотря на вполне невинное окончание операции, повторять ее крайне не рекомендуется. Вера в "авось" может и культурная традиция России, но и о технике безопасности надо подумать. :-)

Часть 3. Глава 1

Столбы освещения и стены домов.

Когда говорят о прокладке оптоволокна, всплывает традиционная картина - открытые люки, кабель, уходящий под землю, бригада работников ГТС в спецовках и кирзовых сапогах... Проволока на два квартала, и грузовичок-техничка.

Для, тех, кто сталкивался с домашними сетями - это крыши, проволока, веревки. Перекидывание через провода, деревья, крепление за мрачные качающиеся конструкции...

Но есть третий путь. Что делать, когда на трассе кабеля нет домов (и соответственно крыш)? Либо они недоступны или даже неудобны? В этом случае возможна прокладка по столбам освещения (элестроснабжения, трамвайно-троллейбусным опорам) или по стенам домов. Так как они часто дополняют друг-друга (ввод в здание со столба обычно идет по стене), то данные методы объединены под общим заголовком.

Более того. Прокладка по столбам освещения очень удобна для строительства магистралей. Как правило, ее проще легализовать, так как приходится договариваться с меньшим количеством инстанций (обычно достаточно согласия собственника столбов и управления архитектуры).

Еще одно несомненное достоинство - хорошая защита от вандалов. Если провод размещен на столбе, или на стене, до него значительно сложнее добраться, чем до крыши. Или, по крайней мере, злоумышленник значительно более заметен в процессе своего "дела".

Но есть и отрицательные стороны. Во-первых, прокладка требует разрешений, проекта, что стоит немалых денег. Во-вторых, работа эта более дорогостоящая, трудоемкая, требует специальных навыков и оснастки (лестниц, автовышки). В-третьих (это касается в основном столбов), более чем вероятна арендная плата за использование имущества.

Разумеется, не исключена плата и за прокладку кабелей по крышам. Но в Российских реалиях она обычно меньше, или вообще отсутствует.

Но, тем не менее, использование столбов и стен - мощный и эффективный инструмент Ethernet-провайдера. О нем надо знать, и по возможности использовать. Например, в Екатеринбурге так проложено несколько десятков (если не сотен) километров провайдерских магистралей. Хорошая альтернатива грабительским расценкам прокладок по канализации Электросвязи.

Кстати, рассматриваемый способ в мире не нов:

Рис. 1.37. Коммуникации в Японии.

В Японии такие коммуникации используют не от хорошей жизни - в условиях частых землетрясений прокладывать трассы под землей почти невозможно.

Ниже приведены несколько примеров, которые иллюстрируют данный метод применительно к Российскому Ethernet-провайдингу.

Рис. 1.38. Классический подвес на столбе освещения.

Тут подвешен не один, а сразу три кабеля (бывает и больше). Проблем с такими линиями не много, были бы в порядке столбы. Использовано оптоволокно с внешним несущим тросом (восьмеркой), его можно крепить к самым недорогим подвесным системам.

Прокладки начинаются с установки крепежа на столбы. Обычно это делается с самой простой раздвижной лестницы, только в исключительных случаях применяется автовышка. Так проходится вся трасса, заодно определяется план работ и сложные участки.

Затем по тому же самому сценарию подвешивается кабель. Сначала (в черновую) это делается без натяга, столб за столбом проходится монтажниками с кабелем. Часто его для удобства сматывают восьмеркой, так и переносят по всей трассе (и даже оставляют бухту на ночь привязанным повыше на столбе).

Но возможна и работа "с барабана". Технически последний способ сложнее, но считается, что при этом риск повреждения кабеля минимален. Впрочем на практике, вдали от инструкций и начальников, разница отсутствует - кабель перед крепежом все равно разматывается по земле, так как тяжелая тележка с барабаном неповоротлива и неудобна.

Сложные места (деревья, оживленные улицы) преодолеваются с автовышкой. Ведь перебросить кабель тут мало - нужно его еще правильно закрепить на большой высоте.

Вторая часть - натяжение. Проводится оно от середины линии к краям. Так же последовательно, столб за столбом трасса приводится в надлежащий вид. Однако, автовышку второй раз стараются не вызывать, и часто в результате процесса можно видеть следующие "артефакты":

Рис. 1.39. Остатки кабеля после натяжения.

Внешне хорошего в такой картине мало, однако разварка в муфту стоит дорого, снижает надежность, и по сути не добавляет изящества линии. В то же время, такой "остаток" можно использовать в будущем для ремонта или разветвления. Так и висит бухточка кабеля до лучших времен.

Всем хороша магистраль по столбам. Однако, при таком способе прокладки самым непростым делом становится ввод кабеля в точку назначения. Сложно попасть в здание

удаленное более чем несколько десятков метров от линии столбов. Порой приходится проложить кабель по нескольким домам, что бы наконец попасть в нужный.

Линия при этом может выглядеть следующим образом:

Рис. 1.40. Прокладка кабеля по стене.

Хорошо заметно, что тонкий кабель идет параллельно с более толстым телефонным. Надо сказать, что такая прокладка значительно безопаснее в плане гроз (и вандалов), поэтому телефонисты уже несколько десятилетий обходят стороной крыши в пользу стен (хотя из этого правила хватает исключений).

Тут даже не надо придумывать ничего особенного - достаточно копировать опыт более "старших" коллег. К сожалению, в настоящий момент провайдеры используют прокладку по стене очень редко. Вернее сказать - незаслуженно редко.

Остается добавить иллюстрацию ввода кабелей в здание практически на уровне земли.

Рис. 1.41. Спуск кабеля по стене.

Простейший металлический желоб является достаточно надежной защитой - показанные на фотографии линии нормально работают в течении более чем десяти лет.

Почему такие (внешне более чем удобные) способы прокладки редко используются в домашних сетях? Ответ лежит в предыстории - многие современные Ethernet-провайдеры "выросли" из полулегальных любительских структур, им просто непривычно прокладывать кабеля легально.

Второй довод - сроки. Согласования проектов проводятся не быстро, порой на это могут уйти месяцы. Для такой быстрорастущей отрасли как провайдинг это слишком долго. Клиент обычно столько не ждет, уходит к конкуренту. А работать "на опережение" для небольших фирм слишком дорого и сложно.

Но девиз - "повыше на крышу подальше от надзора" не будет являться выигрышной стратегией долго. Легализация неизбежна - и с ней придет опыт использования как стен, так и столбов освещения.

Крепление и подвес кабеля.

История подвешивания кабеля в воздухе насчитывает уже несколько веков. За это время было выработано великое множество приспособлений и технологий. Если посетить специализированную фирму, то можно увидеть каталоги, содержащие сотни позиций разнообразного крепежа...

Но стоимость специализированного оборудования весьма велика, тратить несколько десятков долларов на точку большинству домашних сетей не по карману. Поэтому, в нижеследующем материале будут рассмотрены способы сделать надежную линию без больших затрат.

Начать протяжку нужно с выбора точки крепления кабеля на крыше дома. Хороших мест не так и много. А законных, к сожалению, того меньше. Строго говоря, крепить можно только в место, согласованное с владельцем дома или эксплуатирующей организацией. Либо к трубостойке (анкеру), специально предназначенной для крепления воздушных линий по проекту.

Таким образом, первая возможность - это стойки радиофикации и телевизионные антенны. Крепить к ним просто и удобно - единственная проблема - могут возникнуть вопросы от собственников стоек. При их урегулировании кабельная инфраструктура буквально обретает "землю под ногами". Поэтому данный способ безусловно наиболее предпочтительный.

Что делать, если трубостоек нет, или их владельцы категорически против? Если идти полностью законным путем остается один выход - согласовывать место крепления, возможно ставить свою трубостойку. Это реально, но не дешево.

Если исходить из здравого смысла, требование к точке крепление простое - в случае форс-мажорных обчтоятельств кабельная линия должна разрушиться заведомо раньше, чем точка крепления. Поэтому ни в коем случае нельзя использовать для крепежа ограждения крыш (это опаснейший вариант), и прочие недостаточно прочные элементы.

Хорошо подойдут арматурные крюки капитальных стен, перекрытий, стропила деревянных крыш, и т.п. При их отсутствии можно, например, установить анкер в стену.

Следующее, на что нужно обратить внимание в точке крепежа - долговечность узла. Проволока, трос, стяжки - все используемые материалы не должны иметь люфта, седущего к постепенному перетиранию элементов. Так же нельзя использовать материалы "на излом", или другим свособом ведущим к преждевременному разрушению.

Но перейдем непосредственно к подвесу - эта тема проще в организационном плане (согдасования не требуются), но зато значительно более сложна в техническом.

Можно разделить протяжки на два принципиально разных способа -

- С использованием троса (проволоки).
- Самонесущий кабель.

Выбор допустимого натяжения как кабеля, так и троса (проволоки) можно рассчитать по специальной формуле:
T=PL/8F.

Где P - вес кабеля в кг/метр, T - натяжение кабеля в кг, L - длинна пролета в метрах, F - стрела провиса в метрах. На самом деле вместо кг используют N (Ньютоны). P - N/m, T - N
Далее, взяв значение допустимого напряжения для проволоки, можно получить ее минимальный диаметр.

Однако на практике расчетами никто себя не утруждает. Тем более, допустимые величины получаются очень небольшими. Так, по одной из моих прикидок получилось, что для двухсот метрового пролета достаточно проволоки диаметров 0,8 мм. И это с двукратным кратным запасом прочности.

В результате была применена оцинкованная 3-х миллиметровая проволока, недорогая и удобная в работе. Полагаю, что 4-5 мм. хватит с огромным запасом на самые длинные и сложные линии. Так как стоимость проволоки невелика, экономить на ней нет смысла.

Еще одну рекомендацию можно получить из СНиП 3.05.06-85.
3.81. Диаметр и марка каната, а также расстояние между анкерными и промежуточными креплениями каната определяются в рабочих чертежах. Стрела провеса каната после подвески кабелей должна быть в пределах 1/40 — 1/60 длины пролета. Расстояния между подвесками кабелей должны быть не более 800 - 1000 мм.

То есть при протяжке в 200 метров нормальная величина стрелы провеса (отклонение вниз от идеальной прямой) должен составлять порядка 5-ти метров (а это целых 2 этажа). Из этого можно вывести два важных вывода.
Во-первых, если линия проходит над какими-либо инженерными коммуникациями, нельзя рассчитывать, что кабель пройдет по прямой линии между точками.
Во вторых, не надо и пытаться натянуть трос "как струну". Пользы это не принесет, только лишняя нагрузка на материалы. Поэтому нет смысла массово применять тали и лебедки - подавляющее большинство линий можно натянуть силами 2-3 человек.

Протяжка с использованием троса (проволоки)

Принцип строительства линии понятен из названия. Кабель любого типа по всей длине крепится к несущей проволоке (тросу), которая берет на себя все механические нагрузки.

И первый же вопрос - что использовать, проволоку или трос? Очевидно, что последнее лучше - трос пластичней и прочнее при том же диаметре. Но при этом заметно дороже, и более подвержена коррозии. С другой стороны, кабель все же не лифт - нагрузка намного меньше, да и ущерб при падении не так велик. Поэтому, трос (желательно в пластиковой изоляции или с гальваническим покрытием) обычно используется только в самых сложных, исключительных случаях. В остальных достаточно проволоки.

Работа с проволокой немного сложнее, чем кажется на первый взгляд. Самое сложно - разматывать ее так, что бы не допустить образование "барашков".

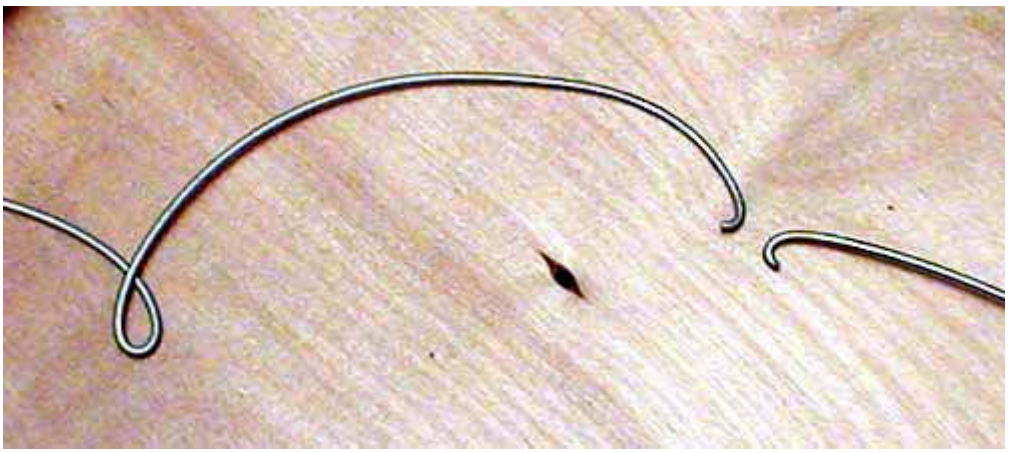

Рис. 1.42. Образование "барашков".

Особенно часто они возникают если проволока разматывается не со специального вращающегося держателя, а через край, виток за витком. Только чуть-чуть расслабиться, недоглядеть - проволока перекрутится, и в линию уйдет маленький и незаметный "барашек". При всей внешней безобидности это почти 100% разрыв. Последствия которого могут быть весьма тяжелыми.

Самое неприятное, проволока может сломаться не сразу. Иногда через час, иногда через неделю. А иногда и через год. Самый тяжелый случай был у нас при протяжке 350 метрового пролета тяжелой бронированной оптикой.

Проволока была 4-х миллиметровая, вполне достойного качества. Но - через несколько недель переломилась. Кабель оказался прочным, выбрал слабину и провис над ремонтной базой. Раскачиваясь на ветру, сломал антенну на одном из строений... Обозленное руководство базы дало команду крановщику порвать кабель.

История дальше была длинная, но закончилась тривиально. Муфта, сварка, и повторно сделанная работа. Все за свой счет. А виноват был всего-то "барашек" на проволоке.

Второй навык, который совершенно необходим для работы с проволокой - это умение ее соединять. На практике данный процесс не слишком прост - вязать сталь как веревку нельзя. Усталость материала рано или поздно сделает свое кристаллическое дело. Поэтому разработано несколько способов, один из которых описан ниже:

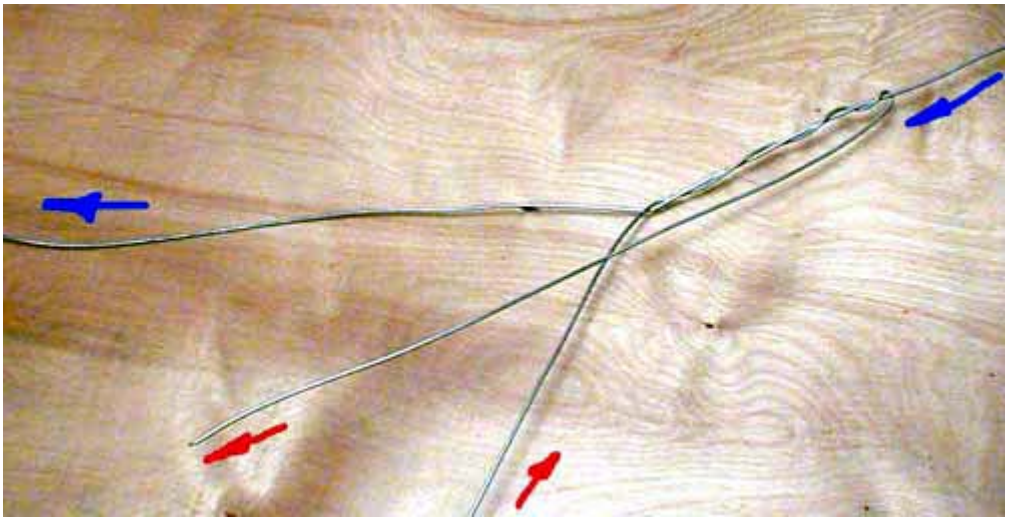

Рис. 1.43. Начало сращивания проволоки.

Концы проволоки берутся немного "накрест" навстречу друг-другу с приличным запасом (около 60-70 см). Затем один конец обвивается вокруг другой проволоки примерно на 1/3-1/4 оставленного "запаса".

Затем то же самое проделывается со вторым концом. Следующим действием концы проволоки загибаются и навиваются в обратном направлении уже навстречу друг другу.

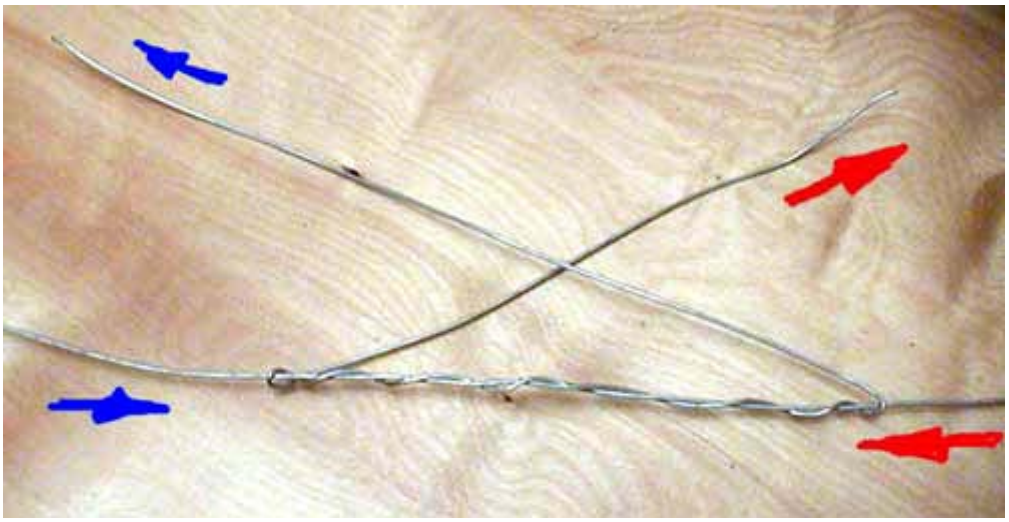

Рис. 1.44. Навивка в обратную сторону.

Чем плотнее навита проволока, тем лучше.

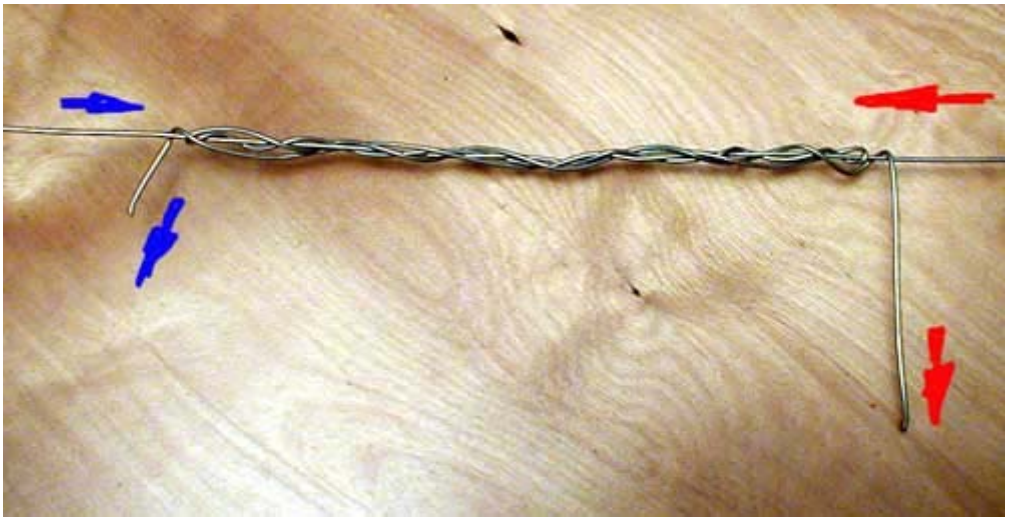

Рис. 1.45. Скрутка перед закреплением концов.

Далее нужно закрепить оставшиеся концы проволоки.

Можно завести оставшийся конец "под петлю", как показано слева. Но на мой взгляд, красивее смотрится плотная намотка на проволоку, как видно справа. Можно и сочетать оба метода - хуже от этого не будет.

Последним действием будет "обкуска" оставшихся кончиков. Желательно это сделать таким образом, что бы при необходимости через получившуюся скрутку можно было относительно безболезненно "протащить" арматуру подвеса кабеля в обе стороны.

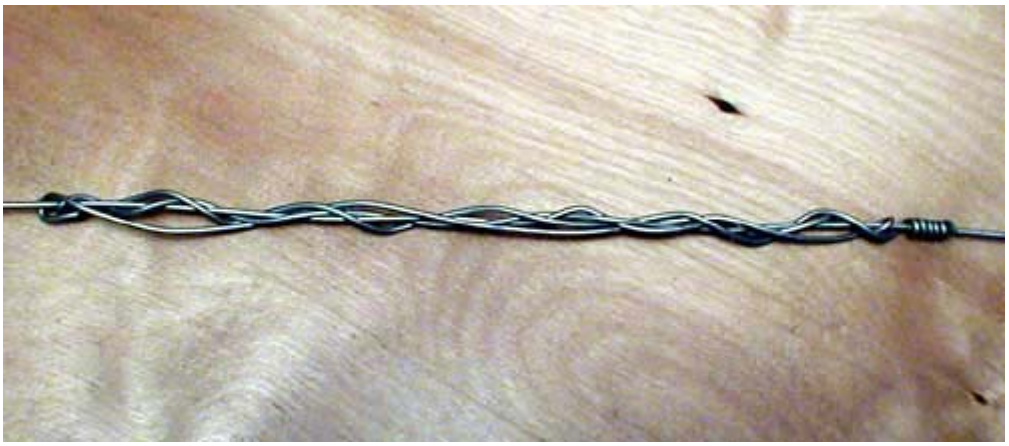

Рис. 1.46. Окончательный вид.

Вот и окончательный результат. При самом минимальном навыке, работа по соединению занимает несколько минут. Выполнить его вполне по силам одному человеку, хотя с помощником значительно удобнее.

Остается только отметить, что как ни надежна скрутка - без нее все же намного лучше. Поэтому проволоку нужно разматывать очень аккуратно.

Крепеж кабеля к проволоке

Способы крепежа кабеля к тросу (проволоке) можно разделить на на два типа.

Первый - соединение перед протяжкой (капроновые стяжки, проволока, жестяные или металлические скобы). В этом случае кабель растягивается рядом с тросом и прикрепляется (с небольшим запасом) через 0,6-0,8 метра кусочками проволоки или жестяными скобами. Иногда используют капроновые стяжки, но они могут разрушаться под действием ультрафиолета или морозов, поэтому применять их все же не желательно.

В стесненных условиях можно осуществлять крепеж такого типа и по мере протяжки линии. Для этого понадобится несколько дополнительных монтажников, или работа приобретет циклический характер - протяжка 5-х метров - остановка для крепления - и т.д.

После протяжки кабель жестко прикреплен к проволоке, и может смещаться лишь незначительно, в пределах одной-двух точек крепления. Это позволит немного выправить неравномерность крепежа, но не более того. Как монтаж, так и демонтаж проволоки придется проводить только вместе с кабелем.

Минусы данного способа очевидны - с кабелем линию сложнее натягивать, его нельзя оперативно заменить без полного демонтажа, да и повреждение (особенно если это оптика) в ходе работ более вероятно. Тем не менее, данная технология весьма удобна для коротких линий с легким кабелем. Навыки требуются минимальные, и работа производится быстро.

Однако, для сложных длинных протяжек, особенно с тяжелым кабелем, рационально сначала натянуть проволоку, а затем по ней провесить кабель. Самое простое - использовать скользящие зажимы из проволоки (хотя фабричные металлические скобы более надежны).

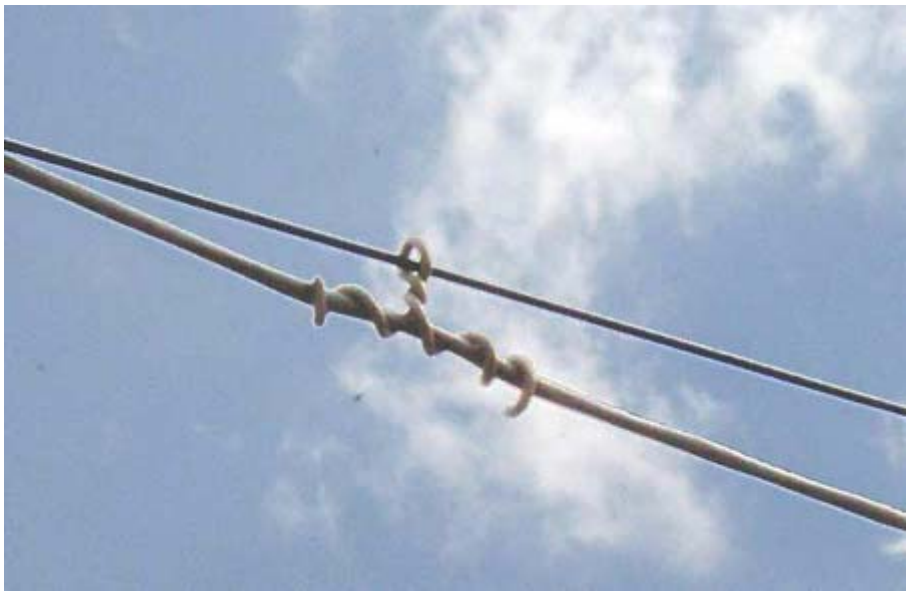

Рис. 1.47. Самодельный скользящий крепеж.

Перед началом работ следует позаботиться о том, что бы после протяжки проволоки осталась еще одна веревка (иначе работу по ее перекидывании на другую крышу придется повторить). Затем кабель неторопясь, по одной петле, надевается на проволоку, и перетягивается веревкой на соседнюю крышу.

Рис. 1.48. Вид линии после перетяжки кабеля.

По завершению протяжки нужно "не в натяг" зафиксировать концы кабеля.

Следующий способ (подвес на "спирали") более прогрессивен. Он быстрее, менее трудоемок, и вместе с тем обеспечивает значительно лучшую защиту кабеля. Минус - не слишком симпатичный вид линии после протяжки.

Спираль представляет из себя плотную пружину из проволоки толщиной около 1,5-2 мм, с диаметром витков около 100 мм. Наматывают ее, как правило, на обычном токарном станке с самым минимальным набором приспособлений. Соотношение длины спирали в начальном состоянии и после растяжения задать сложно, но легко можно регулировать в процессе протяжки добавляя или убирая витки с линии.

В своей основе технология подвеса кабеля "на спираль" очень проста. Во первых, протягивается проволока (или трос). Причем сразу натягивается, и хорошо закрепляется. Особенно это удобно на больших пролетах, где вес имеет большое значение. Желательно только до этого надеть на проволоку "спираль". Но можно легко это сделать и после - последовательной навивкой.

Во вторых, внутрь "спирали" пропускается кабель, конец которого вместе с концом "спирали" привязывается к ранее протянутой веревке. Все готово для протяжки кабеля - как это и отражено на первой части рисунка.

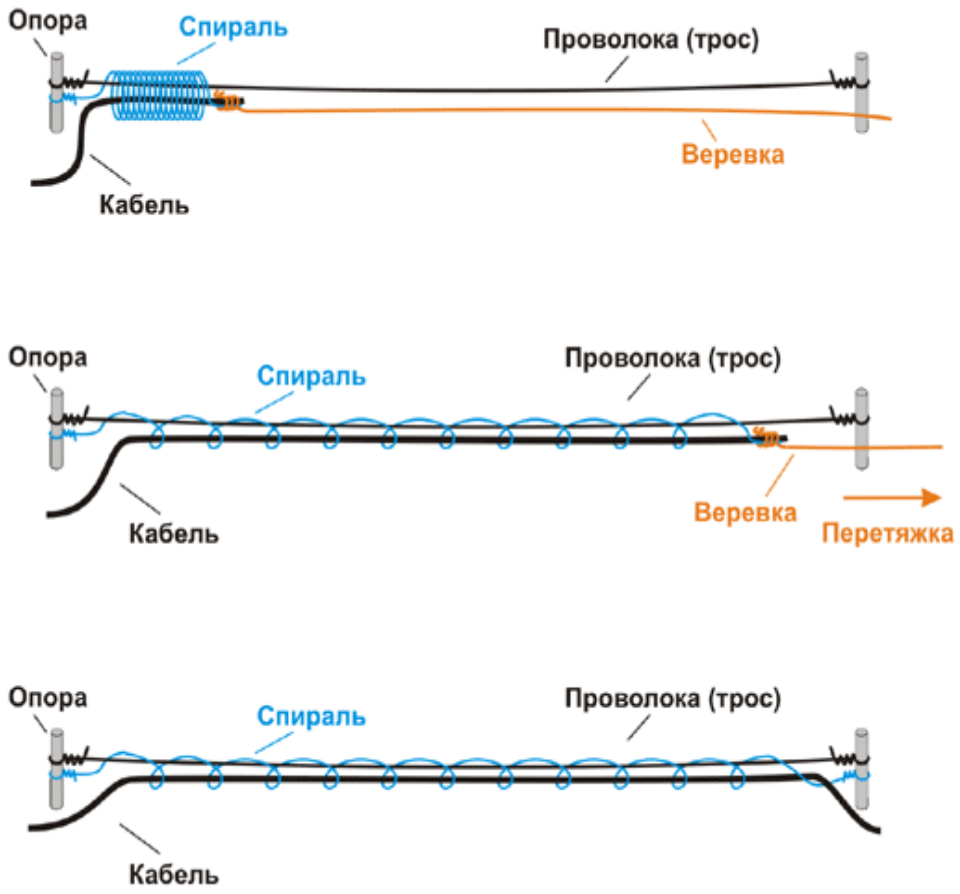

Рис. 1.49. Протяжка с использованием спирали.

Дальнейшие действия достаточно очевидны. При помощи веревки кабель и конец спирали перетягиваются на другую стороны. При этом первоначально плотная пружина растягивается по трассе протяжки, образуя надежный канал с кабелем и проволокой (тросом) внутри.

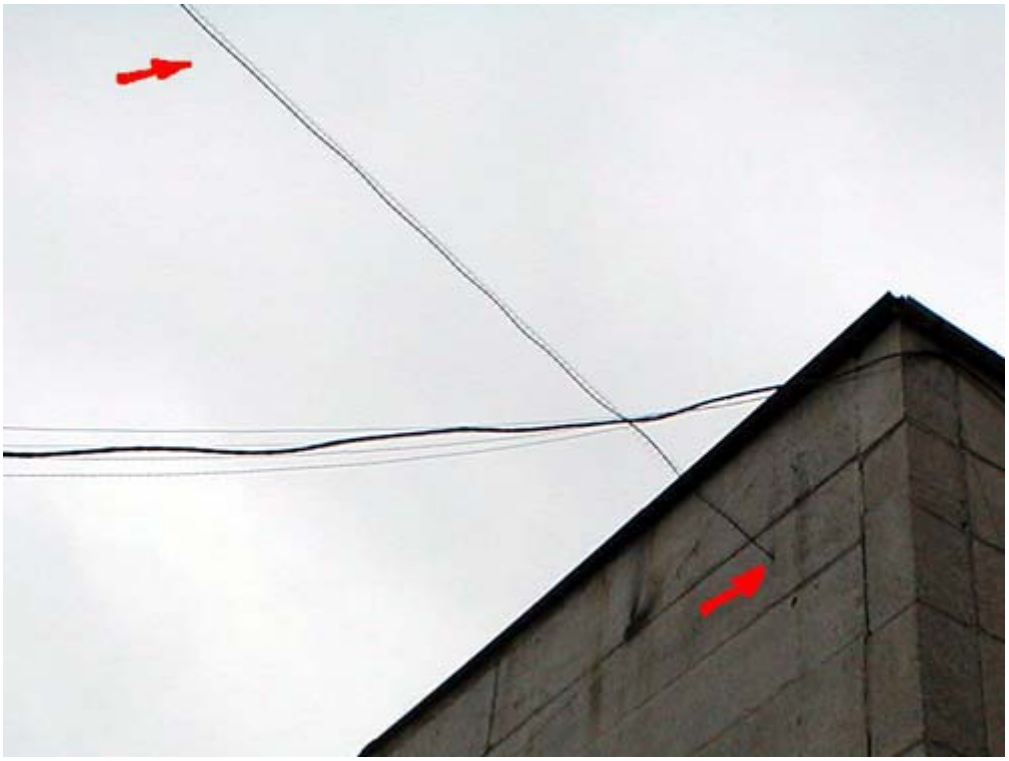

Рис. 1.50. Вид линии с крепежом "спиралью".

Если присмотреться, то видно, как извивается подвешенный кабель. Это говорит о том, что лежит он свободно, не испытывая никаких нагрузок. А что еще нужно для длительной беспроблемной работы?

Кстати, у показанной технологии есть патентованный аналог - такой способ крепежа под брендом FlexTender продвигает компания "General Corporation" (Япония).

Крепление самонесущего кабеля

Самонесущий кабель бывает двух видов - с внешним тросом (восьмерка), и с внутренними упрочняющими элементами (наиболее распространен П-296).

С креплением кабеля-восьмерки проблем не возникает. Конец несущего троса отделяется от кабеля и закрепляется наиболее удобным способом за опору. Если линия предполагается к сдаче в ГСН - желательно использовать специальный сертифицированный крепеж. В противном случае можно использовать более простой способ.

Рис. 1.51. Крепление несущего троса кабеля-восьмерки.

Красной стрелкой показан кабель, трос которого завязан на опоре. При этом узлов нет - для фиксации использована проволока.

Значительно сложнее крепить самонесущий кабель с внутренними упрочняющими элементами. Классический пример - П-296, внутренняя металлическая оплетка которого легко выдерживает нагрузку около 100 кг.

По сути единственный цивилизованный способ - спиральные зажимы. Существуют еще клиновые зажимы, но они менее удобны и заметно дороже, поэтому распространения не получили.

Рис. 1.52. Крепление при помощи спирального зажима.

Зажим представляет собой несколько сталистных проволок, соединенных вместе и скрученных в спираль. На внутреннюю поверхность нанесен абразив, препятствующий скольжению. В процессе крепежа зажим как бы наматывается на кабель, и чем больше усилие, вытягивающее его из спирали, тем плотнее сжимается зажим.

Механизм этот прост, и весьма надежен. Однако стоимость спирального зажима составляет более десяти долларов, не всегда эти средства имеются в наличии. Поэтому часто применяются решения подобные следующему:

Рис. 1.53. Крепление самонесущего кабеля подручными средствами.

В данном случае использован кусок резинового шланга для защиты изоляции, металлический пруток и сантехнические хомуты.Так же известны способы, использующие самозатягивающийся проволочный бандаж (подобно спиральному зажиму) или альпинистский инвентарь для крепления веревок.

При крайней нужде можно обернуть кабель несколько раз вокруг трубостойки, и закрепить концы проволокой. Метод не слишком красивый, но надежный и простой. Правда надо сказать, что такое обращение может выдержать только медный кабель типа П-296. С оптоволокном эксперименты проводить не рекомендуется.

Часть 3. Глава 1

Работа с П-296.

На первый взгляд, нет особого смысла отдельно описывать работу с каждым видом кабеля. Однако, для П-296 необходимо сделать исключение по причине его замечательных потребительских качеств. Что привело к его широчайшему распространению в домашних сетях России и ближнего зарубежья.

Вообще говоря, подобрать кабель для внешних прокладок было не так просто. Коаксиальный кабель подвержен большим наводкам в грозы, и уже несколько лет не используется в крупных и средних сетях. Обычная витая пара разрушается на открытом воздух под действием холода и ультрафиолета за 2-3 года. Кроме того желательно иметь кабель прочный, дальнобойный, и самонесущий (т.е. способный висеть на небольших пролетах без троса).

Таким стал военный кабель П-296.

Рис. 1.54. Вид П-296 "с торца".

Видны 4 жилы, свитые вместе, их плотная оболочка, экран, броня, и внешняя изоляция. Можно смело сказать, что этот кабель позволил так широко развиться сетям Екатеринбурга, а затем и многих других городов. И если в Москве уже с 2002 года идет активный переход магистралей на оптоволокно, то менее богатых городах П-296 будет использоваться еще очень долго.

Прочность данного кабеля позволяет (порой к сожалению) относиться небрежно к прокладкам. Линия нормально работает если кабель лежит в лужах, и по нему ходят люди, ездят машины. Или при крепеже пролетов к трубостойке обычными узлами.

Хотя П-296 достаточно тяжел (более килограмма каждые 10 метров), его можно провешивать без троса на расстояния до 100 метров. На практике даже больше - известны провесы длиной 240 метров, но это уже экстремальный и неправильный подход.

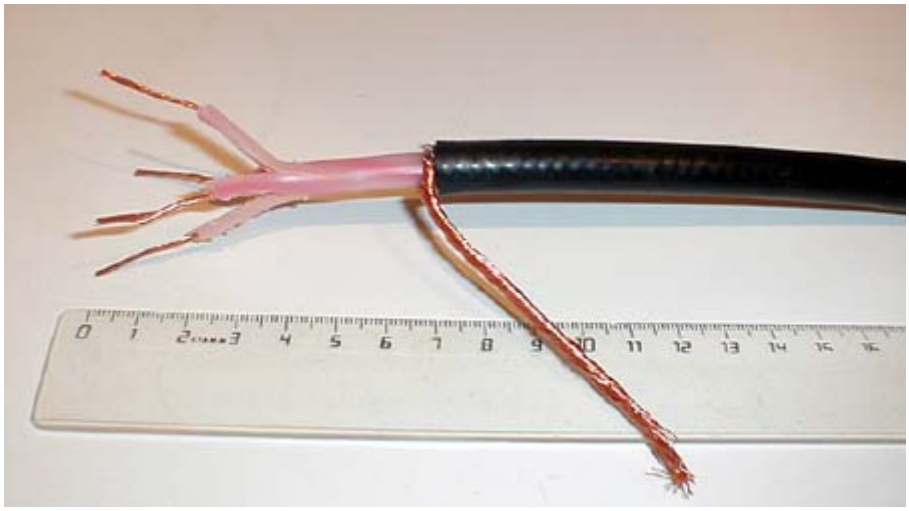

Рис. 1.55. Разделанный П-296.

Второе (порой решающее) преимущество П-296 - дальнобойность. По правилам, более 100 метров витой пары работать не должно. Понятно, что расстояние можно увеличить, снижая активное сопротивление при сохранении или незначительном ухудшении остальных параметров среды передачи. Поэтому для П-296 практическим пределом является 500 метров на 10base-T и 180-250 метров на 100base-TX на обычном недорогом активном оборудовании.

Вот краткие технические параметры:

- Кабель относится к группе "Кабели для местной и зоновой связи". Рассчитан на передачу ВЧ-сигнала для магистральных телефонных линий с использованием аппаратуры ИКМ-60 (т.е. уплотнитель на 60 каналов телефонной частоты).
- Активное сопротивление петли в 500 метров - 32 Ома.
- Диаметр жилы 0,9 - 1,2 мм.
- Волновое сопротивление нормировано и составляет 100 Ом.
- Выдерживает электрическое напряжение до 600 Вольт (удобно для фантомного питания).
- Выдерживает разрывную нагрузку до 150-180 кг.

Нужно особо отметить, что "военный" П-296 имеет несколько (или несколько десятков) разновидностей, в том числе с "гражданской" маркировкой КСПП. Особенно распространен П-270, этот кабель более толстый, имеет алюминиевый экран. По своим параметрам практически не уступает П-296, но менее удобен в работе.

Вторая известная разновидность - семейство КСПП. Такой кабель имеет однопроволочные жилы, и, как правило, лишен стальной брони. Это повышает дальнобойность, но из-за отсутствия гибкости делает неудобной работу по прокладке воздушек. Зато есть модификации с гидрофобным заполнением, что незаменимо при прокладке в подземных коммуникациях.

Еще одним большим достоинством П-296 является его устойчивость к охотникам за ломом цветного металла. Бомжи и т.п. несознательные граждане срезают кабеля не для продажи - это тяжело и рискованно, да и в хозяйстве (за его отсутствием) кабель не нужен. Зато один килограмм меди стоит примерно $1 на пункте приема цветмета. Поэтому воровской алгоритм следующий: кабель срезается, кладется в костер, оставшийся грязный кусок красноватой проволоки идет к скупщикам, легальным или не очень.

Рис. 1.56. Броня П-296.

И тут проблема - сжигаем П296 и получаем... Медную проволоку, спутанную со стальной. Такой винегрет на цветмет не примут. Охотники на кабелем иногда (увы не всегда и не сразу) думают, и возиться за бесплатно не любят.

Однако, при всех достоинствах, у П-296 имеется один большой недостаток - его невозможно обжимать в стандартных вилках RJ45 и на стандартных кроссах. А из-за толщины практически нельзя прокладывать в шахтах слаботочной проводки. Поэтому при работе с этим кабелем приходится делать переход на стандартную витую пару.

Перед началом сращивания кабелей необходимо определить, какие проводники используются для соединения:

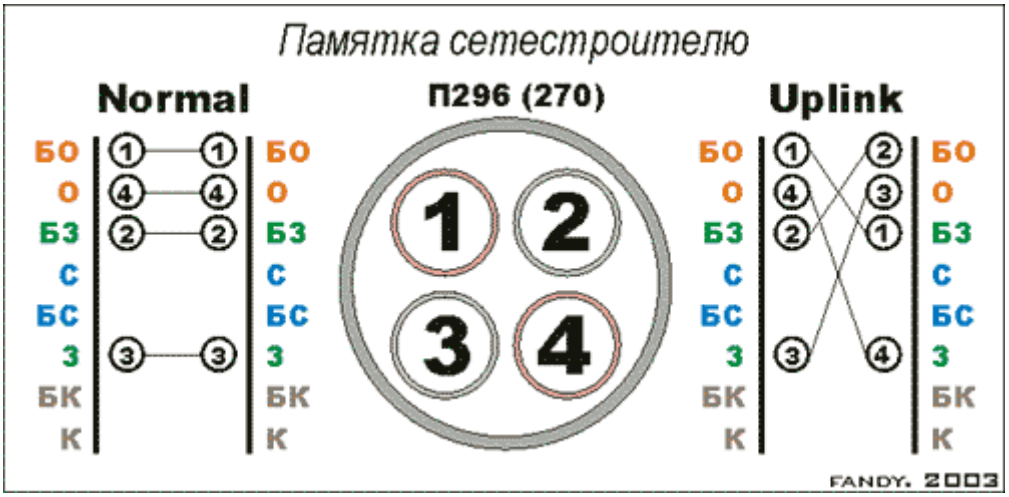

Рис. 1.57. Соединение П-296 и витой пары.

Т.е. в П-296 используются две пары, проводники которых расположены по диагонали, напротив друг-друга. В остальном все просто - пара соединяется с парой в прямом порядке, или крест-накрест, для создания UpLink.

Для применения всех типов соединений (кроме штатной муфты, которая хороша только в поле) П-296 необходимо разделать, т.е. выделить отдельные проводники.

Как говорилось выше, П-296 имеет хорошую изоляцию и прочную стальную оплетку. Более того, центральный блок представляет собой четыре многопроволочных проводника, свитых вокруг условного общего центра. Каждый провод имеет свою изоляцию, а вместе они объединены в один монолит дополнительной полиэтиленовой заливкой. Так как полиэтилен индивидуальной и общей изоляции близки по свойствам, при изготовлении и хранении происходит их прочное соединение (сплавление). Соответственно, задача разделения проводников становится достаточно не простой.

Такие эксплуатационные достоинства превращаются в большую проблему для монтажников. Освободить жилы совсем не просто. Процесс даже у специалиста может занимать до получаса на каждое соединение.

Но много говорить не надо - проще показать разделку с применением простейшего инструмента - ножа с выдвигающимся лезвием (производство Китай) и бокорезов (Россия, но желательно использовать что-то получше).

Пошаговое руководство выглядит следующим образом:

- Надрезаем (состругиваем) пластиковую оболочку до стали по окружности кабеля на длину около 15 мм. Оставшийся "хвостик" может быть любым, но обычно достаточно 100-150 мм. Действовать ножом можно смело, так как прорезать стальную оплетку невозможно (вред только один - нож быстро тупится).
- Снять оболочку с конца кабеля (как правило это не сложно), затем расплести стальную броню и аккуратно "обкусить" бокорезами мешающие проволоки.

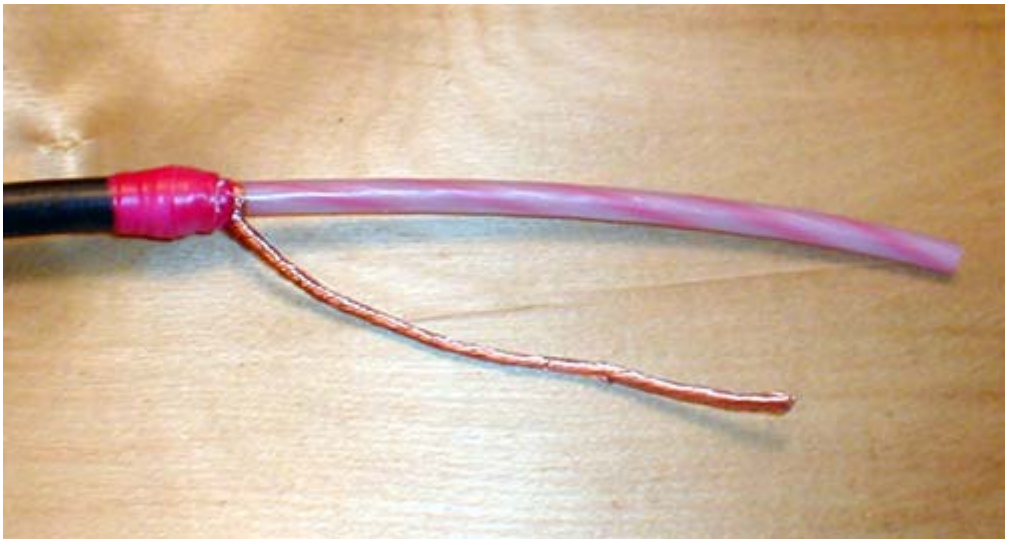

Рис. 1.58. П-296 после снятия изоляции и брони.

- Что бы не изорвать (буквально) руки остатками стальной брони, нужно обернуть место разреза оболочки несколькими слоями изоляционной ленты. Защита простая и надежная. Так же не помешает скрутить экран в плотную косичку - не будет риска запутаться в нем, и привести этим в "нетоварный" вид.
- Если присмотреться к центральному блоку, хорошо видно, как по спирали идут проводники. Поэтому можно определить место, где делать надрез - в промежутке между "красной" и "белой" жилой. Резать нужно аккуратно - соскользнувший нож может повредить окружающие предметы (в том числе руки, ноги, или другие выступающие части тела). Изолента на иллюстрации играет роль буфера.

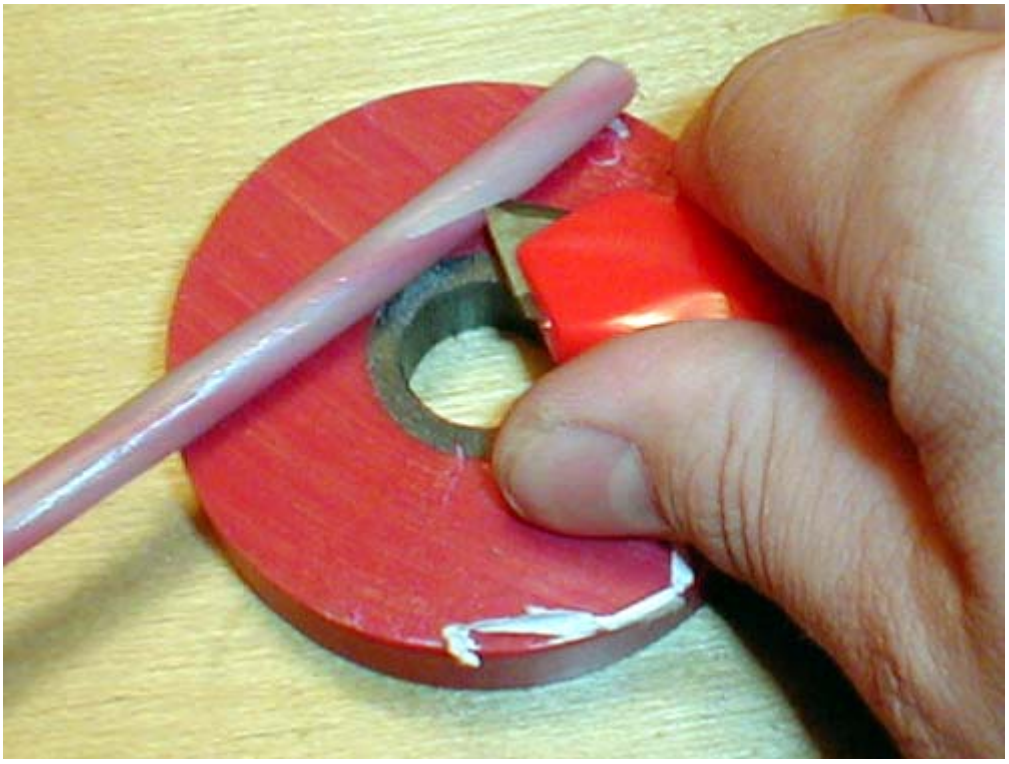

Рис. 1.59. Надрез центрального блока П-296.

Длина надреза может быть небольшой - достаточно получить "хвостики" для захвата плоскогубцами (т.е. 10-20 мм). Надрез нужно делать с двух противоположных сторон - тогда разделить центральный блок можно будет без особого труда.

- Далее остается только освободить проводники на большую длину. Проще всего это сделать "разрыванием" центрального блока вдоль сделанного надреза. Для этого используются плоскогубцы, и не помешает помощник (вместо последнего можно удерживать кабель в удобном положении ногами или дополнительным крепежом).

Рис. 1.60. "Разрывание" центрального блока вдоль сделанного надреза.

Впрочем, можно все сделать просто руками...

- Следующим этапом нужно повторить предыдущую операцию, разделяя получившиеся пары на отдельные проводники. Это сделать уже значительно проще - плоскогубцы не понадобятся
- Часто не удается сделать первоначальные разрезы идеально ровно. Надрезаются отдельные проволоки, оголяется изоляция. Да и после захвата плоскогубцами вид не красивый... Поэтому кончики настоятельно рекомендуется обрезать.
- Затем снять изоляцию с проводников - и разделка закончена.

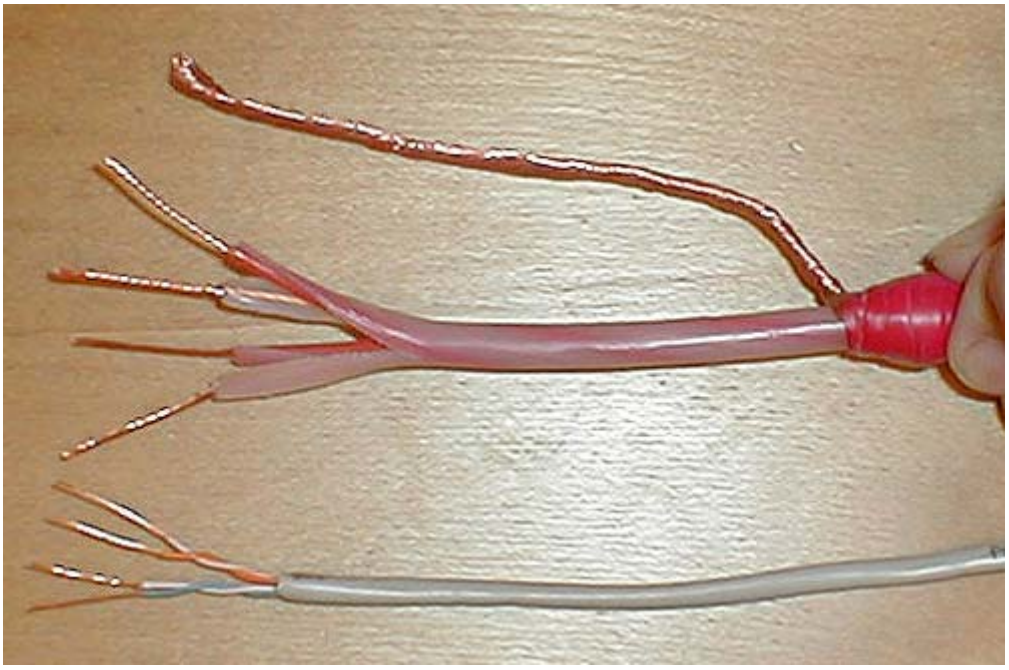

Рис. 1.61. Разделка П-296 закончена.

После разделки П-296 можно делать соединение - для которого применяют следующие способы:

- Присоединение витопарного кабеля скруткой (спайкой).
- Разделка кабеля П-296 в розетке (в кроссе).
- Соединение П-296 с витой парой при помощи Scotchlok (или подобных устройств).

Наиболее дешевым и качественным (как ни странно) является **соединение при помощи обычной скрутки**. К сожалению, оно не слишком симпатично на вид, поэтому часто его не применяют из-за имиджевых соображений. Второй минус данного способа - большая трудоемкость создания качественного контакта.

Не обходится и без небольших тонкостей. Если линия предназначена для работы с 100baseT, и на большой дистанции, рекомендуется стыковать витую пару с П-296 так, что бы направление повива обоих кабелей не менялось в месте соединения. Ну а про желательность минимального расплетения пар говорить, полагаю, излишне...

Тем не менее, способ очень распространен - его результат можно видеть на следующей иллюстрации:

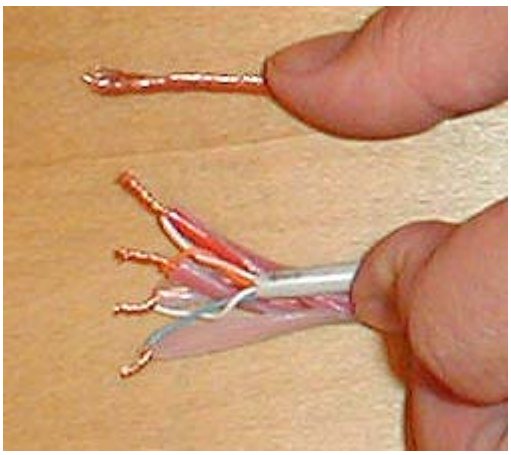

Рис. 1.62. Скрутка П-296.

Соединенные проводники желательно спаять. Хотя это не улучшит свойства соединения в части дальнобойности линии (и прочие волновые параметры), но долговечность пайки заметно увеличится, и это важнее всего остального. Для мест, удаленных от источников электричества, можно применить газовый паяльник, или просто расплавить прямо на скрутке тонкую проволоку припоя зажигалкой.

Затем остается заизолировать проводники каждый в отдельности, и потом все вместе. При необходимости провести гидроизолирующие мероприятия (наиболее часто в их качестве применяется гудрон и термоусадочный кембрик). Но на несколько лет достаточно и обычной изоленты, если ее наматывать аккуратно, плотными слоями.

Окончательный вид соединения может быть таким:

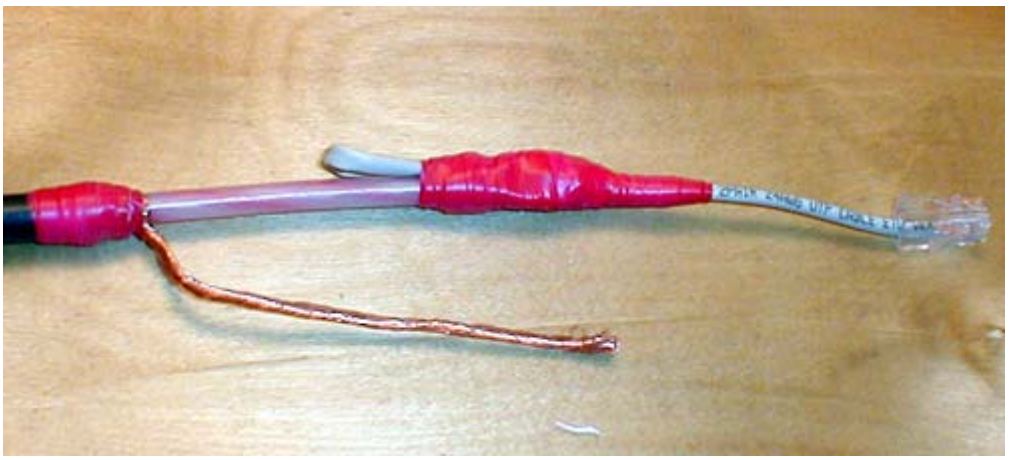

Рис. 1.63. Окончательный вид скрутки П-296.

Витая пара укладывается "петлей", и все вместе плотно заматывается изолентой. Это дает "сносный" внешний вид, защиту от кратковременного воздействия воды, пыли, и прочих агрессивных сред (включая посторонних людей).

Следующей по распространенности является **разделка кабеля П-296 в розетке**.

Похожим способом можно сделать соединение на специальном кроссе, или, например, грозозащите. Технический процесс не нуждается в пояснениях, полагаю, все понятно из фотографии.

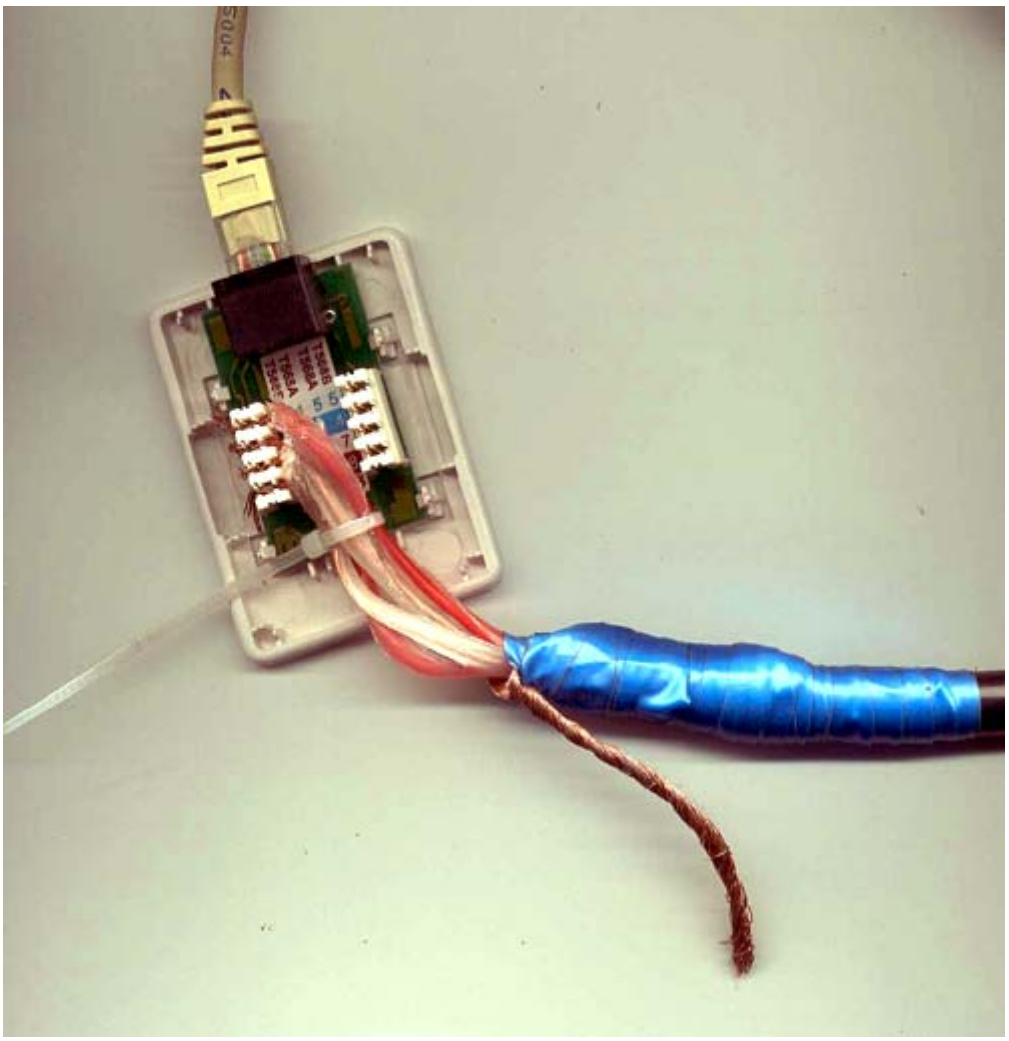

Рис. 1.64. Разделка кабеля П-296 в розетке.

Остается только добавить, что при разделке на розетке или кроссе желательно соблюдать обычные правила - минимальное расплетение пар, максимально жесткое крепление тяжелого и недостаточно гибкого П-296 (классический дефект такого соединения - механическое разрушение места крепления).

И последний способ - **соединение П-296 с витой парой при помощи Scotchlok (или подобных устройств)**.

Начать надо с того, что оперативное сращивание проводов (фактически исключенное в компьютерных СКС) широко применяется в телефонии. Для этого отрасли давно существует широкий ассортимент приспособлений. Например - "плюшки" Scotchlok от компании "3М" - которые представляют собой заполненный водоотталкивающим гелем корпус с кнопкой, при нажимании которой несколько контактов опускаются на проводники, и этим замыкают их.

Например Scotchlok типа U1R позволяют соединять жилы различного диаметра (от 0,5 до 1,2 мм), имеют двойной контактный элемент и корпус из прочного пластика. Расчетный срок службы полученного соединения - 40 лет.

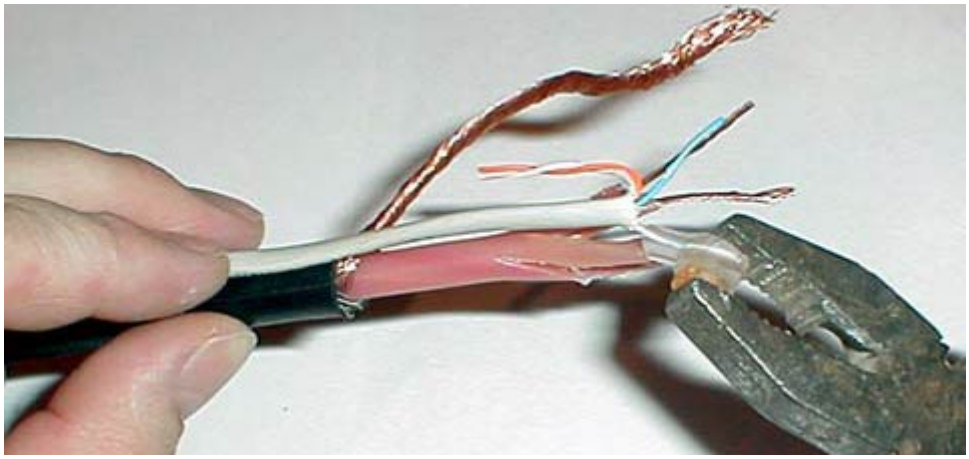

Рис. 1.65. Зажим Scotchlok.

Для соединения достаточно ввести с отверстия Scotchlok проводник витой пары (изоляцию снимать не надо), и зачищенную жилу П-296 (иначе она не проходит в отверстие). Затем просто сжать "плюшку" в плоскогубцах.

Соединение защищено от влаги (хотя струя воды все же постепенно размывает гель), механически прочно (мне не удалось выдернуть проводник из Scotchlok без его разрушения).

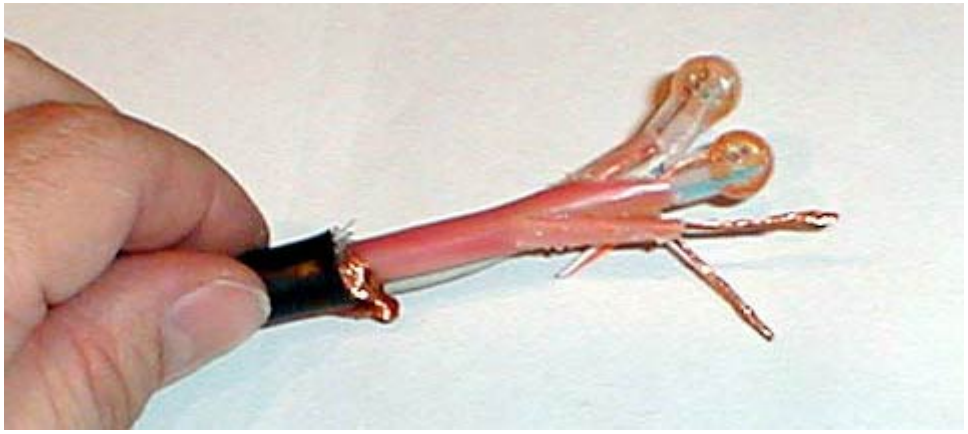

Рис. 1.66. Соединение П-296 с витой парой при помощи Scotchlok.

Полученный результат хорошо виден с обратной стороны "плюшки" через прозрачный гель. Можно уверенно рассмотреть цвета пар, и надежность их крепления в двойном зажиме.

В принципе, если подходить аккуратно и строго, можно шутя уложиться в норму расплетения для Cat 5 (1,2 см). Потери будут не намного больше, чем при скрутке или разделке в розетке. Если не слишком заботиться о эстетике, то можно закрыть место соединения изолентой.

Завершая раздел, необходимо отметить, что описанные методы применимы не только к П-296. Ведь в Ethernet-провайдинге часто используются нестандартные кабеля - КСПП, телефонные многопарники, и много другое...

Отдельные полезные советы.

Вообще говоря, существует огромное множество хитростей и приспособлений, которые сильно облегчают работу по монтажу и обслуживанию домашних сетей. Все их перечислить нереально - да и новые постоянно появляются - прогресс не стоит на месте.

Но имеет смысл показать хотя бы несколько простых приспособлений (которые вполне можно сделать своими руками и (или) с минимальными затратами. Не думаю, что приведенные примеры принесут пользу буквально, как инструкция к применению. Максимум - будут использованы в качестве прототипа. Однако надеюсь, что у монтажников возникнет желание облегчить свой труд, и... Появятся новые "полезные советы".

Начать хочется с самодельного газового паяльника:

Рис. 1.67. Газовый паяльник.

При монтаже кабельных систем очень часто бывает нужно спаивать кабеля различных типов. И подобный инструмент почти незаменим при проведении работ вдали от электрической розетки, на пересеченной местности подвалов, чердаков и крыш.

Составляющие:

- Нужно купить обычную газовую горелку (стоит она всего несколько долларов), и баллон газа для заправки зажигалок.
- Автомобильный хомут (на фото его видно, размер 16 на 23).
- 3 велосипедных спицы, диаметр 2 мм.
- Жало от 20-ти ваттного паяльника.
- Гайку с резьбой чуть меньше диаметра жала

Технология изготовления следующая:
Зажать гайку в тисках и ввернуть в нее жало. Нужно чтобы жало выступало на 5-6 мм с уже нарезанной резьбой. В гайке просверлить 2-х мм отверстия, пока не пойдет медная стружка от жала. Затем ввернуть в отверстия спицы (на спицах есть резьба), и согнуть как это можно видеть на фото. Обрезать лишнее и загнать под хомут.

Разумеется, в продаже можно найти китайские газовые паяльники. Однако у них откровенно хлипкие насадки и субтильная конструкция. А показанный вариант выдержит любого монтажника (ну или почти любого). Плюс работает надежнее, и стоит дешевле.

Но спайка не единственный способ соединения медных жил. Сварка часто бывает надежнее и дешевле. Для потребуется специальный низковольтный трансформатор.

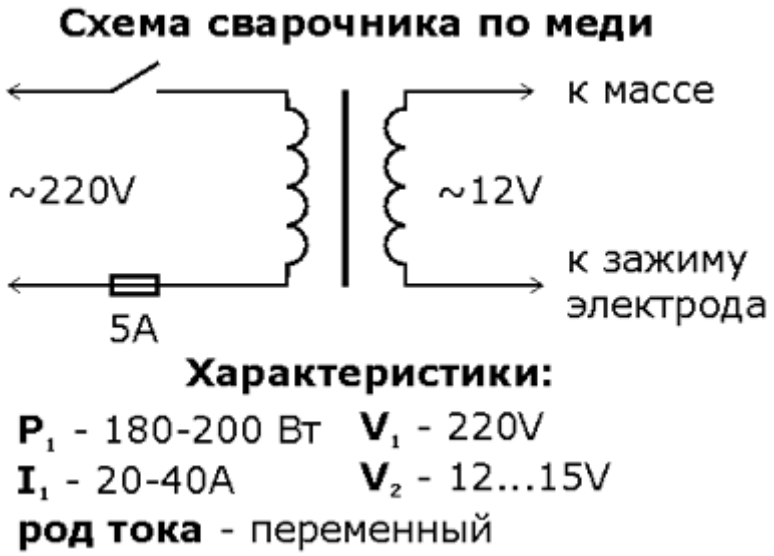

Рис. 1.68. Сварочный трансформатор.

Можно использовать силовой трансформатор от старых ламповых телевизоров типа ТС-180, ТС-160, ТС-150. Полностью удаляется вторичная обмотка, первичная обмотка на ~220V остаётся. Далее вторичная обмотка наматывается проводом марки ПЭЛ, ПЭВ, ПЭЛР, ПЭВГЛ (эмальпровод) или проводом марки ПВ-1-1х2,5; ПВ-1-1х4; ПВ-3-1х2,5; ПВ-3-1х4 (в хлорвиниловой изоляции).

В качестве электрода используется грифель от элементов питания (батареек) типа АА.

Следующее приспособление может быть использовано для натяжки проволоки или троса.

Рис. 1.69. Приспособление для натяжения проволоки или троса.

Принцип действия понятен из фотографии. Проволока зажимается между пластинами, затем посредством рычага натягивается талрепом или лебедкой. Преимущество зажима - его можно легко крепить с любом месте проволоки, легко передвигать... И все это не повреждая проволоки.

Следующая часто встречающаяся проблема в домашних сетях - подвод электропитания к активному оборудованию. Действительно, далеко не всегда можно найти рядом с узлом розетку 220V. До нее могут быть десятки и даже сотни метров.

Если проводка выполняется стандартной четырехпарной витой парой, можно использовать стандартную схему, где питание подводится по неиспользуемым в Ethernet парам (Power over Ethernet, PoE).

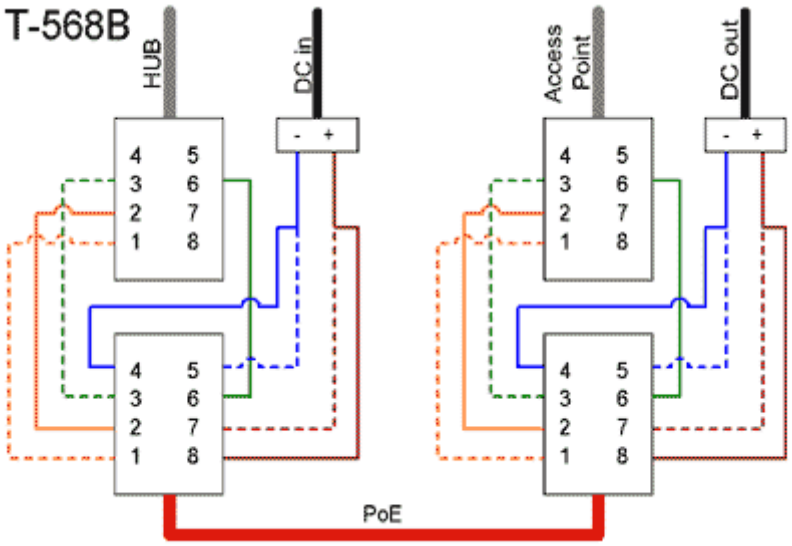

Рис. 1.70. Подвод питания по неиспользуемым в Ethernet парам.

Способ прост, недорог. Единственное, что ограничивает его применение - это дальность, вернее падение напряжения в проводниках. Предположим, что сопротивление 100-метровой линии составляет 30 Ом, а потребляемый активным оборудованием ток 1А по 12 Вольтам. Тогда падение напряжения в проводнике составит 30 Вольт, и для питания устройства придется подавать в линию 42 Вольта.

В теории, проблему можно решить подняв напряжение при передаче, и понижая его перед потребителем электричества. Но изоляция витой пары не рассчитана на высокое напряжение, и данный метод нельзя рекомендовать на практике.

Что делать, если нет свободных пар, например при использовании П-296?

Выход есть и в этом случае - фантомное питание. По тем же проводникам, которые используются для передачи полезного сигнала, можно передавать как постоянный ток, так и переменный.

Идея использования постоянного тока понятна из следующего рисунка:

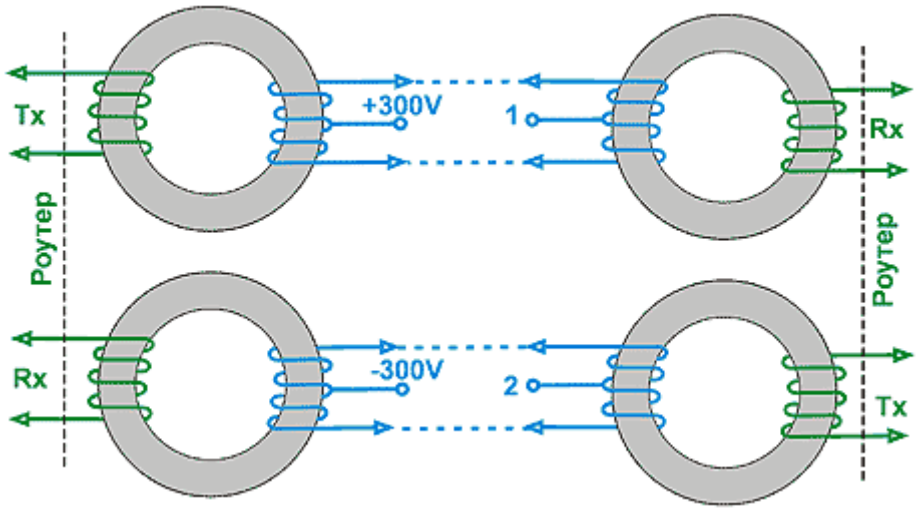

Рис. 1.71. Фантомное питание постоянным током.

В точки +300V и -300V подается выпрямленное и сглаженное конденсатором напряжение, а с точек 1, 2 его можно снять и подать в блок питания. Но и тут есть ограничения:

- Напряжение 300 Вольт можно использовать только на П296, КСПП, и аналогичных, на это рассчитанных. Для обычной витой пары использовать более 50-60 Вольт крайне опасно.
- Защита по току обязательна, хотя бы в виде плавких предохранителей.
- Первичную и вторичную обмотку надо мотать отдельно. Первичную на одной половинке кольца, а вторичную на второй, так, что бы между ними был воздушный промежуток.
- На кабелях (которые под напряжением) надо рисовать "Череп с костями" или "Не влезай, убьет".
- Обмотки с отводом от середины надо мотать двойным проводом, а потом соответственно соединять концы - так как они должны быть строго симметричны. В противном случае возможно насыщение сердечника.

Фантомное питание переменным током несколько сложнее, и его описание выходит далеко на рамки данной книги. Но такие устройства существуют:

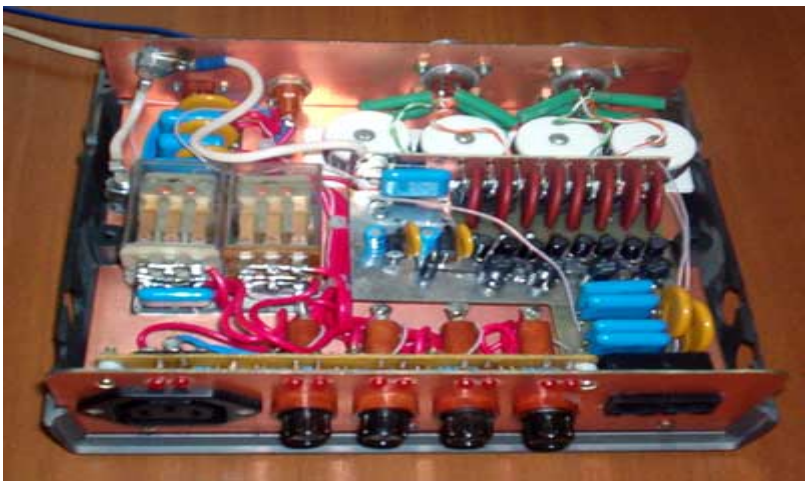

Рис. 1.72. Фантомное питание переменным током.

На фото - система фантомного питания узла (на два порта). Мощность до 3 киловатт, напряжение - 220 Вольт переменного тока. Встроена защита сигнальной линии (Ethernet) и защита силовой части. Проверенная дальность работы под нагрузкой - 200 метров на скорости 100 Мб.

В заключение несколько приспособлений для работы с П-296.

Так как катушки весьма тяжелые, для их размотки можно использовать следующую несложную конструкцию:

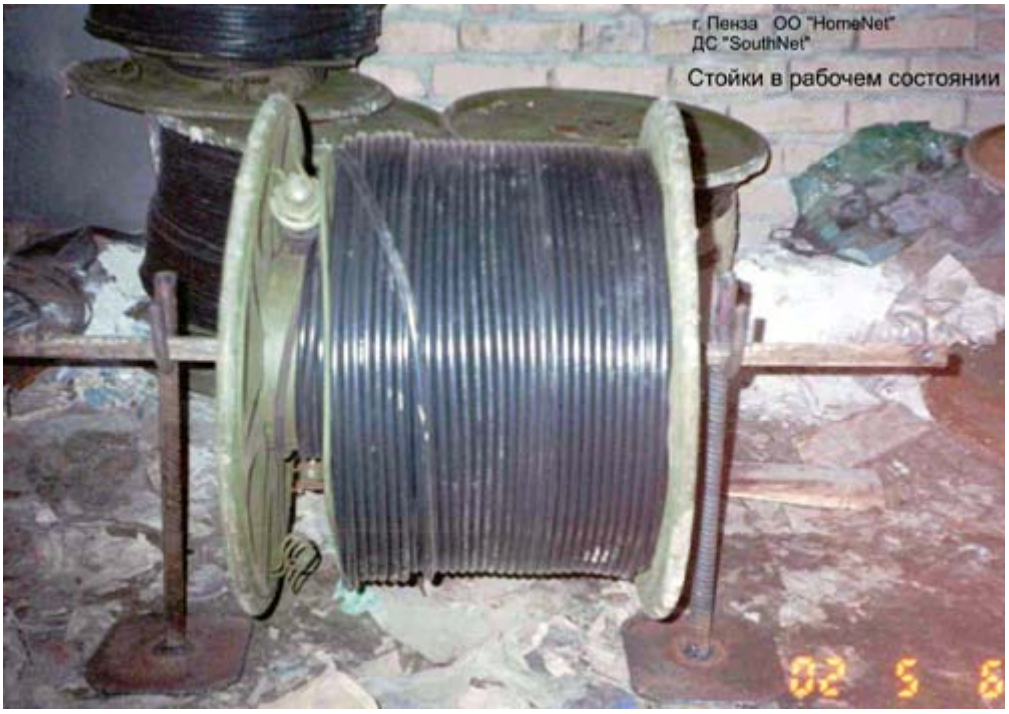

Рис. 1.73. Приспособление для размотки П-296/П-270.

Конструкция состоит из двух стоек, и перекладины-оси. Просто, удобно, и легко транспортируется. Стойки вбиваются в землю ногами или чем-то тяжелым, дальнейшее понятно из фотографии.

Кстати, если приходится разматывать П-296 на ровной поверхности, можно применить спортивный "диск здоровья". Катушка кабеля кладется боком на диск - и после этого легко вращается.

Рис. 1.74. Приспособление для перевозки и размотки П-296/П-270.

А на такой тележке кабель можно не только разматывать, но и перевозить на небольшие расстояния.

Часть 3. Глава 1

Требования муниципалитетов.

Прокладка коммуникаций Ethernet-провайдеров не осуществляется в физическом вакууме. Ее приходится проводить по жилым или административным домам, столбам освещения, подземная канализациям, и многим другим объектом, принадлежащим по большей части муниципальным предприятиям, организациям или образованиям.

Законодательство в этой сфере неполно, запутано или просто отсутствует. Поэтому и взаимоотношения провайдеров и муниципалитетов носят подчас весьма странный и экзотический характер. Однако не все так безнадежно, как кажется на первый взгляд. В данном вопросе самым интересным является то, что по "Закону о Связи" балансодержатель или собственник жилья очень сильно ограничен в своих требованиях к операторам связи.

Для примера рассмотрим ДЕЗ (дирекцию единого заказчика). Он не является собственником помещений, что следует даже из ее названия. ДЕЗ, действуя на основании лицензии Госстроя РФ на исполнение функций заказчика, принимает на себя обязательства заключения договоров с эксплуатационными предприятиями (РЭУ и т.п.).

При этом он должен (по крайней мере формально) действовать в интересах собственника жилья. Которым как правило является сам муниципалитет, либо заводы/предприятия, либо жилье находится в коллективной собственности жильцов.

Нужно понимать, что согласование строительства с собственником обязательно всегда, что по новому закону, по старому. Это, в общем, требование СНиП 11.01.95, да вполне нормальная цивилизованная практика. Но с ДЕЗом нужно это делать только в том случае, если договор собственника с ДЕЗом предусматривает передачу последнему соответствующих полномочий (а обычно это так и есть).

Важно понимать, что **для согласования строительства сети проект не требуется**. Согласование места строительства с заинтересованными организациями и выдача техусловий, как правило, проходят на этапе предпроектной подготовки (в соответствии со СНиП 11-01-95, к слову, уже не действующим, но применяющимся), и письмом Минстроя № БЕ-19-4/9 от 13.02.1996).

Т.е. необходимо отличать согласование **возможности** строительства и согласование проектов, и тем более, самих работ. После разрешения на строительство делается проект (в некоторых случаях с экспертизой), и после этого задача собственника (как правило ДЭЗа, действующего в его интересах) - отойти в сторонку, и дать возможность работать строителям.

Иначе придется признать право безвестных муниципальных чиновников вмешиваться в работу лицензированных проектных организаций и лицензированных строителей. Что, разумеется, совершенно неправильно.

Далее, только собственник (возможно ДЭЗ, если это предусмотрено) вправе требовать денег за сервитут (право ограниченного пользования чужим имуществом) для размещения оборудования связи.

Лицензия на проектирование и строительство так и называется "Государственная Лицензия на осуществление строительной деятельности>. Виды работ по ней регламентируются перечнем, являщимся неотемлимой частью лицензии. Этот перечень целиком зависит от того, что запрашивается в заявлении на лицензию. Разные пункты стоят разные деньги, и к ним для выдачи предьявляются разные требования.

Для нормальной работы по строительству объектов связи достаточно заявить:

1. Проектирование инженерных сетей для зданий и сооружений II уровня ответственности;
2. Технологическое проектирование вычислительных сетей (сети передачи данных и телематических служб)
3. Выполнение специальных разделов проектов включая сметы.

Пункты 2 и 3 состоят из большого чиста подпунктов, каждый из которых имеет свою стоимость при лицензировании.

Понятно, что такая лицензия есть у редкого провайдера. Поэтому обычной практикой является заказ проектных работ сторонним организациям. Минимальную лицензию на монтаж слаботочной проводки лучше иметь свою, стоит это не дорого и ни к чему не обязывает. А вот для прокладки "воздушек" может потребоваться что-то более сложное.

Впрочем, "строгость законов компенсируется необязательностью их исполнения", и в сложной ситуации обычно можно даже задним числом найти лицензированную организацию, которая за деньги "прикроет" уже созданные линии своей лицензией.

Далее нужно представлять, что отказать в разрешении на строительство собственнику жилья и других муниципальных объектов достаточно сложно. Разумеется, это только в том случае, если оператор связи имеет необходимые документы, лицензии и сильных юристов.

По с. 23 старого "Закона о Связи" -
...Указанные лица вправе также осуществлять строительство сооружений связи на крышах зданий, столбовых опорах, мостах, в коллекторах, туннелях метрополитена и железных дорог и на других инженерных объектах, а также устанавливать и обслуживать аппаратуру связи по согласованию с собственниками, землепользователями, в том числе арендаторами, указанных земельных участков, зданий или сооружений. Собственники, землепользователи, в том числе арендаторы, ***вправе отказать предприятиям связи в производстве указанных работ только по основаниям, предусмотренным законами и иными правовыми актами, принимаемыми в Российской Федерации***.

Нельзя сказать, что положение оператора в этом случае непробиваемо. Юристы собственника могут соглашаться со всеми требованиями, но таким образом, что выполнить соглашение будет весьма затруднительно. Либо устроить экологическую экспертизу и или общественный протест. Или просто тупо сопротивляться на уровне "что бы получить доступ в XXXX дайте за 2 недели заявление"...

Но совершенно очевидно, что большинству чиновников это все не нужно. Как только впереди начинает маячить перспектива серьезных разбирательств (тем более в суде) они быстро сдаются. Самое главное в этом случае все делать "правильно", на бумаге, и под подпись.

В моей практике РЭМП (аналог ДЭЗа) не смог в письменном виде выдать запрещение на строительство даже очевидно полулегальной сети. Т.е. разрешения они не давали то же (вполне логично требуя проект), но и официального запрещения сделать не решились (хотя в данном случае вероятно имели на это право).

Поэтому оператор может спокойно заключать договора с абонентами даже зная, что со "входом" в здание могут возникнуть проблемы. Только запрос в ДЭЗ нужно будет сразу писать письменный, и под подпись. Не ответить совсем чиновники не могут, поэтому отказ будет иметь мотивировку типа "уже заключенного договора с другим оператором", "решения собрания жильцов", и т.п. **Законное обоснование придумать трудно**.

После этого оператору нужно вчинить иск на сумму недополученной прибыли, в котором написать что-то типа "... по причине незаконного отказа, нарушающего статью 23 Закона о Связи ... понес убытки на сумму...". И письменно или лично в ДЕЗ/ЖЭК/РЕМП...

Чиновнику перспектива суда с внушительной исковой суммой и сомнительной перспективой выигрыша дела едва ли понравится. И с огромной вероятностью после этого начальник муниципального предприятия станет значительно сговорчивее. И в обмен на прекращение иска пойдет на все требуемые условия.

После этого нужно будет только постараться превратить муниципалов в друзей... На всякий случай напоминая о прекращенном иске, срок давности на который истечет только через 3 года.

Таким образом, дело Ethernet-провайдинга представляется сложным, но в общем не безнадежным.

Кстати, во многих крупных городах муниципальные организации уже формализовали требования к домашним сетям. Вот, например, перечень документов, который требуется от провайдеров в одной из префектур Москвы:

1. Свидетельство о регистрации предприятия;
2. Устав;
3. Свидетельство о постановке на учет в налоговой инспекции;
4. Свидетельство о внесении в Реестр субъектов малого предпринимательства Москвы;
5. Лицензия Минсвязи РФ на "Предоставление услуг передачи данных";
6. Свидетельство о регистрации по лицензии "Предоставление услуг передачи данных" в Управлении Госсвязьнадзора;
7. Лицензия Минсвязи РФ на "Предоставление услуг телематических служб";
8. Свидетельство о регистрации по лицензии "Предоставление услуг телематических служб" в Управлении Госсвязьнадзора;
9. Лицензия на деятельность по строительству, включая на построение внутренних и внешних инженерных коммуникаций;
10. Лицензия на проектирование, включая проектирование сетей;
11. Страховой полис на проведение работ;
12. Разрешение на эксплуатацию сооружений связи Управления государственного надзора за связью и информатизацией в Российской Федерации по г. Москве и Московской области;

В целом не простой, но "обозримый" список. Правда не знаю, можно ли заменить лицензию на проектирование и строительные работы договорами с фирмами ее имеющими. Но это было бы логично.

Только последний пункт кажется некоторым превышением полномочий - требовать разрешение на эксплуатацию сооружения связи не дело муниципалов. Это прерогатива ГСН, и более никто не должен вмешиваться в права лицензированного оператора на предоставление услуг связи.

Что же делать совсем небольшим сетям, которые не могут на законных основаниях бороться с ДЭЗами?

Вариантов не много. Главный - искать "полюбовное" соглашение, которое будет устраивать все стороны на долговременной основе. И то, никакой договор не может полностью защитить права "полузаконного" оператора... Поэтому серьезные провайдинг и нелегальная работа трудносовместимы.

И последнее. Что могут сделать муниципальные власти с оборудованием нелегальных домашних сетей? В соответствии с Кодексом об административных правонарушениях, вопросы самовольного строительства или эксплуатации сооружений связи подведомственны только Госсвязьнадзору. Поэтому любое разрушение самодельных

сетей силами милиции или ДЭЗа будет незаконным. Только по поводу излучающих ВЧ устройств милиция вправе составить протокол (с изъятием предметов правонарушения).

Однако от этого не легче. Как правило, домашние сети не могут оспорить даже незаконные изъятия оборудования или даже порчу кабелей. Потому что для этого нужно признать железо "своим", и... Получить обвинение по статье 171 УК РФ (до 7 лет с конфискацией).

Так что тут воистину - ограничивая свои обязанности - проигрываешь в правах.

Часть 3. Глава 1

Сотрудничество с коммунальными службами.

Как было показано в предыдущем параграфе, официальный оператор связи вполне может разговаривать с муниципальными властями на равных, и вполне успешно решать задачи по строительству коммуникаций в жилых зданиях.

Однако понятно, что гораздо эффективнее дружить, а не сохранять вооруженный нейтралитет (и тем более "воевать"). Ведь на самом деле коммунальным службам то же нужна сеть передачи данных масштаба района. Вполне вероятно, что они не откажутся от сбора информации с систем учета теплоносителей, лифтовой связи, сигнализации, видеонаблюдения, и т.п.

Поэтому Ethernet-провайдеры и муниципальные (коммунальные) организации скорее стратегические союзники и партнеры, чем конкурирующие фирмы. Конечно, на практике бывает и не понимание, и коррупция, и лоббирование интересов "своего" оператора... Но известны и случаи успешного сотрудничества.

Вероятно, одним из первых можно считать проект "коммунальный компьютер", запущенный в Екатеринбурге летом 2000 года. Нельзя сказать, что он был абсолютно успешным (организационная неразбериха), да и техническое решение спустя 4 года выглядит не слишком перспективным (теперь все можно сделать значительно проще и дешевле), однако тестовый участок успешно работал, и позволил накопить весьма ценный опыт.

Надо сказать, что "коммунальные сети" далеко не новая идея. Для решения муниципальных задач разработаны как отечественные решения (например "Гранч"), так и за рубежные (например Advantech). Особенностью этих систем является работа по протоколу rs-485 (большинство зарубежных систем), или по своему особому протоколу (большинство отечественных).

Эти системы достаточно надежны, продуманы, часто сертифицированы, но... Очень дороги. Непомерно дороги для отечественного хозяйства. Для них выбор зачастую стоит не в дилемме "получше-подороже или похуже-подешевле", а проще - "подешевле или ничего". Это послужило причиной описанной ниже разработки.

Опишем систему так, как она задумывалась в момент создания.

Задачи, которые нужно было решать:

1. Сбор телеметрии учета энерго и теплоносителей. Практически все современные датчики имеют возможность вывода данных на RS-232(485). Обычно сбор осуществляется или через установленный модем, или... Обходом домов с ноутбуком. Датчики используются, как правило, отечественного производства - коммунальщики в России несколько небогаты, а проще говоря бедные. Однако найти датчик с интерфейсом Ethernet совсем не проблема. Или использовать вполне серийный преобразователь RS-232(485) - Ethernet.
2. Охранная, лифтовая и пожарная сигнализация. Для этого используются датчики типа "сухой контакт". В настоящее время эти задачи решаются отдельными выделенными линиями, а где их нет - не решаются никак. Между тем, сложностей с компьютерной обработкой сигналов с подобных датчиков нет, причем на одном узле не сложно обработать даже несколько сотен устройств.
3. Лифтовая голосовая связь. Передача голосовой информации теоретически вполне решаема в ethernet сетях. Забегая немного вперед, скажу, что эта задача была успешно решена и практически.
4. Телефонная связь между ЖЭКами (ДЕЗами, прочими службами) одного микрорайона. В 2000 году это казалось сложной и дорогой задачей, но сегодня с легкостью решается VoIP, для этого даже не нужно ничего проектировать дополнительно.
5. Передача видео с веб-камер. Когда-то это было дорогим удовольствием, но с появлением широкополосных сетей решается легко и качественно - опять таки вполне серийным оборудованием.

Обратим особое внимание на ту часть, для решения которой пришлось разрабатывать дополнительное оборудование и программное обеспечение. Блок, устанавливаемый на жилом доме, должен стоить не более $100. Кто сталкивался с промышленными системами знает, насколько смехотворна для них такая сумма. Конечно, при таком подходе и речи не было о сертификации, красивом внешнем виде, и строгом соблюдении всех норм.

Нужна была работоспособность, надежность, возможность поэтапного апгрейда, т.е. использование распространенных комплектующих. Госсвязьнадзор коммунальщиков не волнует, сети строить они умеют и имеют на это право. Да и с другими контролирующими органами проблем особых нет.

Опишем устройство, которое получилось в реальности.

Основу системы составляет стандартное PC-совместимое оборудование. В каждом жилом доме участка (например, в машинном отделении одного из лифтов) размещается блок управляющего компьютера, представляющий собой PC-совместимый компьютер в промышленно-технологическом исполнении, оснащенный средствами цифрового и речевого ввода-вывода и дистанционного управления.

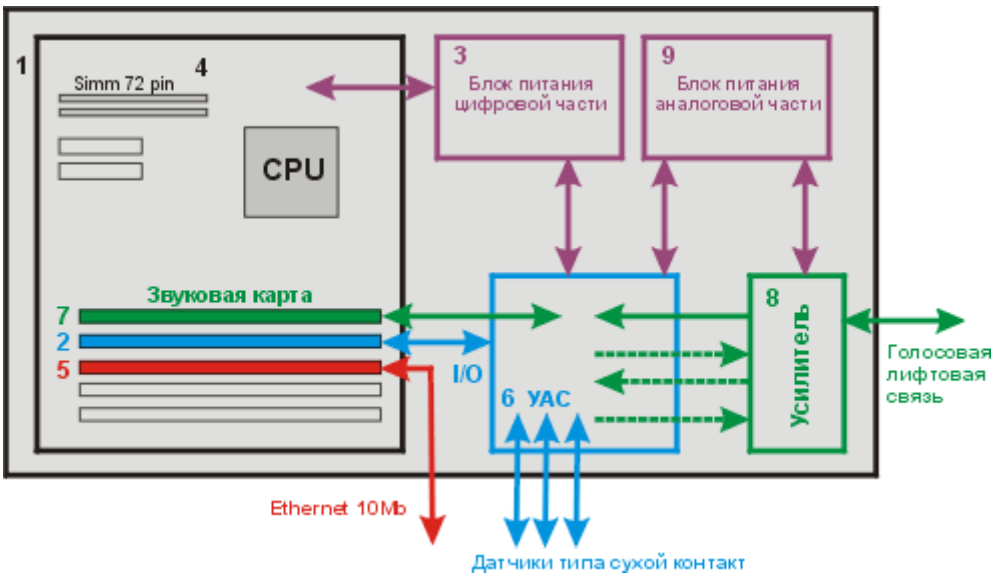

Рис. 7.1. Схема установочного блока коммунального компьютера. .

Связь с диспетчерской службой как первого уровня, так и последующих, или другими точками, осуществляется через ethernet-сеть общего назначения.

Составляющие системы:

1. Металлический ящик.

Рис. 7.2. Металлический ящик.

Стоимость изготовления с хорошим замком и окраской порошковой эмалью составила порядка $25. Толщина металла 2,5 мм. Крышка выполнена сдвижной, такую существенно

сложнее сломать. В целом конструкция весьма прочна, сломать ее без хорошей фомки/ломика затруднительно.

Дно ящика отсутствует - т.к. он все равно намертво пристреливается к стене закраинами. Вместо дна есть кронштейны для крепления монтажной панели из гетинакса (дешевле) или текстолита (дороже).

Ящик состоит из двух частей - закрытая на замок компьютерная часть, и закрытая простой крышкой "под болт" коммутационная панель. Это дает возможность разделить уровни обслуживания системы в целом.

2. Плата цифрового ввода-вывода.

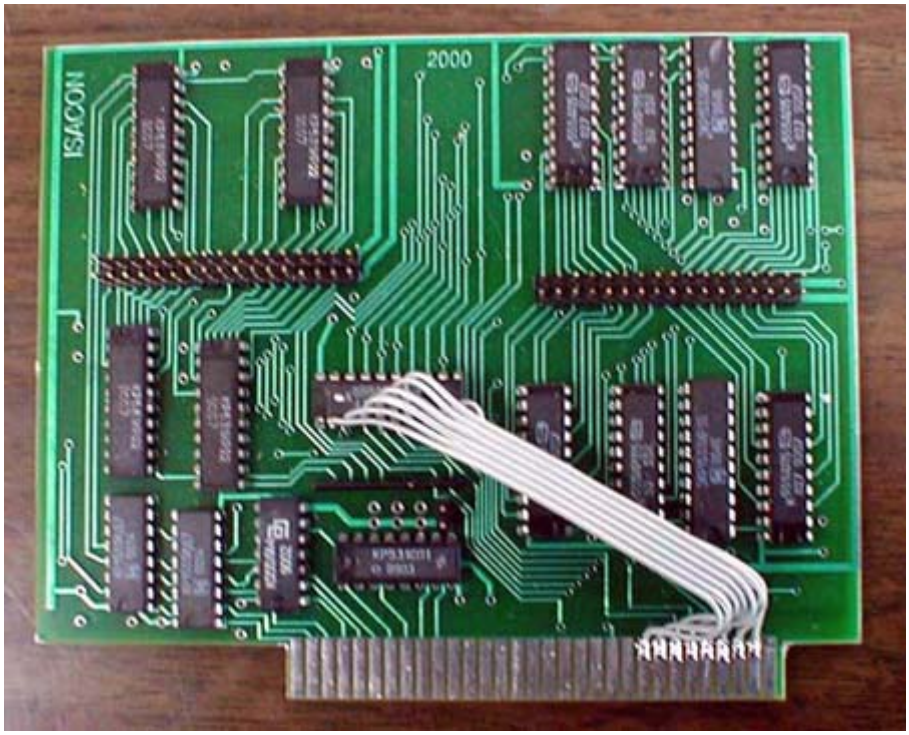

Рис. 7.3. 32/32 порта ввода-вывода.

В небольшой серии (50 шт.) ее цена составила менее $10.

В случае, если 32 порта ввода и 32 порта вывода недостаточно, можно использовать схему активной матрицы. При ее использовании возможно управлять любым разумным количеством устройств (для матрицы 32*32 - 1024 устройства). Кроме того, матрица позволяет хорошо экономить на гальванической развязке (а ее стоимость около $0,3-0,4 за линию).

При проектировании платы в спешке не были учтены кое-какие мелочи, например неудачно расположены выходные разъемы. Но в целом, изделие показало себя вполне надежным и полностью пригодным для решения поставленной задачи.

3. Блок питания.

Был использован обычный импульсный блок питания от PC-совместимого компьютера 220/12(5) В. С него сняли металлический корпус, выпаяли лишние разъемы, убрали выключатель 220 В. Вентилятор так же был снят.

Проведенный эксперимент показал, что при использовании маломощных (на 2000 год) компьютеров (486/66, P1/75) и отсутствии энергопотребляющей периферии, вполне хватает даже штатных радиаторов. Можно было заменить штатные радиаторы на самодельные большего размера, но это не потребовалось. Стоимость блоков питания при оптовой закупке менее $10.

4. Компьютер.

Макет собирался на 486-40МГц, 8 Мб ОЗУ. Стоимость его составила порядка $15 Единственный уязвимый узел - жесткий диск - в системе коммунального компьютера не использовался. Так же надо сказать, что условия в лифтовых сравнительно мало отличаются от комнатных. Температура не падает ниже нуля. Влажность невелика. Пыль не страшна системе, установленной в закрытом корпусе, без принудительного охлаждения.

При возможности, использовался процессор на минимальной частоте - для сокращения до минимума теплоотдачи. Вместо вентилятора охлаждения процессора применялся радиатор от P1 с увеличенной поверхностью.

5. Сетевая плата.

Стандартная плата ethernet под ISA слот, на 10 Мбит. Реально на блоки устанавливался один из распространенных вариантов на чипе UMC 9008, зарекомендовавший себя весьма устойчивым в работе.

Для загрузки использовался bootrom с "самодельной" прошивкой под Linux. Прошивка и серверный софт обеспечивают запуск при самых "кривых" вариантах перезагрузки. Надежность системы была в полной мере оценена при полевых испытаниях, совпавших с грозовым сезоном. Стоимость с микросхемой bootrom составила $12.

6. Устройство аппаратного согласования (УАС).

Служит для управления речевым каналом или другими специфическими устройствами, используемыми в лифтовой голосовой связи. Коммутация осуществляется при помощи портов платы цифрового ввода-вывода. Диспетчер по вызову (или без такового) может удаленно с сервера подключать к усилителю нужную линию. При этом для вызова и передачи голосовой информации используется только одна медная пара.

Так же на плате УАС размещена гальваническая развязка датчиков типа сухой контакт. С их помощью можно получать служебную лифтовую телеметрию, показания датчиков охраны, т.е. управлять или контролировать практически любую систему.

Для сохранения работоспособности в самых неблагоприятных условиях коммутация собрана на реле (дорого, но надежно). Белые корпуса - гальваническая развязка.

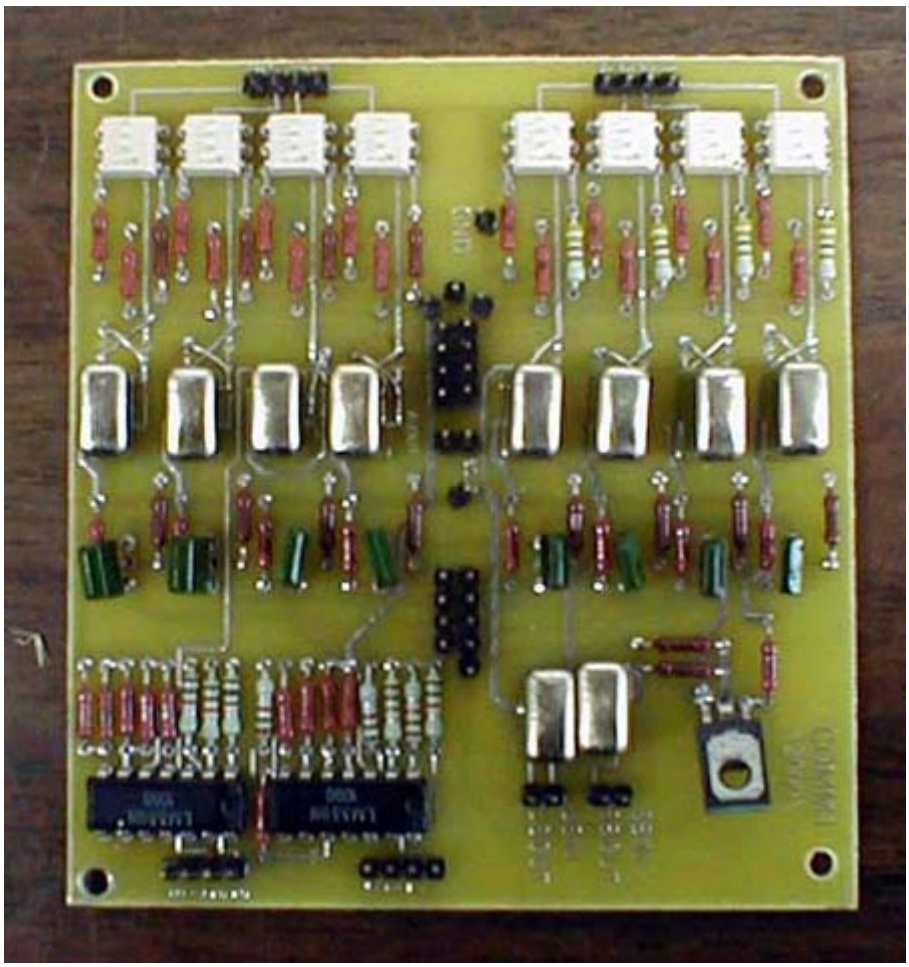

Рис. 7.4. Устройство аппаратного согласования (УАС).

Большие проблемы были при согласовании системы с существующим лифтовым оборудованием. Чего только стоил симплексный режим работы лифтовой связи... И это уже не говоря о севших динамиках времен "перестройки", странных проводах, и т.п...

В небольшой серии цена устройства составила более $20 из-за дороговизны реле и гальванической развязки.

Из недостатков надо отметить опять таки неудачно расположенные разъемы. Проблема с топологией и типами разъемов стала заметной только на этапе окончательной компоновки блока, и может быть легко решена в следующих сериях.

7. Звуковая плата.

Можно было использовать практически любую современную звуковую плату. По крайней мере на машинах пентиум. На платах 486 наблюдались некоторые проблемы, связанные с плохой реализацией технологии plug and play. Каких-либо особых требований система к звуковой плате не предъявляет.

Ориентировочная стоимость $8

8-9. Усилитель и блок питания аналоговой части был использован от недорогих компьютерных колонок. Такое решение было принято из-за недостатка времени. Нельзя сказать, что оно было удачным. Звуковой тракт дешевого усилителя в промышленных

условиях оказался подвержен наводкам, а небольшой блок питания оказался недостаточно мощным для большого количества датчиков. Тем не менее, с некоторыми оговорками, это не мешало нормальной работе системы.

Конечно, создание своего усилителя не представляет особого труда. Стоимость колонок около $15

Программная часть.

Клиентский софт загружается с bootrom, по DHCP получает IP, по TFTP вытягивает ядро (собрано из linux-2.2.12), дальше ещё один BOOTP - запрос на адрес. Потом монтирование файловой системы с NFS сервера. Из процессов остаётся только init и клиентский модуль.

Весь клиентский модуль - на C++, многопотоковый. Один поток на звук. Второй на сканирование датчиков (например раз в секунду, лишь бы не грузил процессор сильно), и входящих управляющих серверных команд. Третий на всякие потребности типа пользовательского ввода для отладки.

Звук идёт без всяких управляющих сообщений, направление определяется эвристически. Частота оцифровки - 8 кб/сек (непринципиально). Задержка определяется только временем передачи пакета.

Серверная часть: интерфейс на TCL/Tk, модуль ввода-вывода на PERL, библиотека работы со звуком - на C++. Ведение журналов. Базы статистики - MySQL (при необходимости - апплет для просмотра либо server-side с PHP). Карта и описание лифтов - в текстовых файлах.

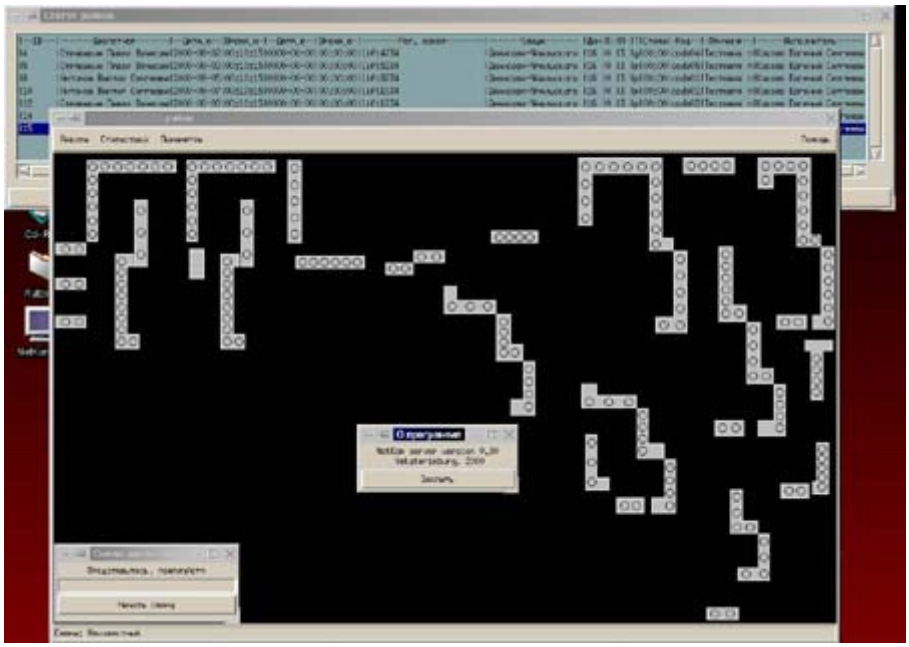

Рис. 7.5. Экран работающего сервера - еще в режиме отладки.

На карте района обозначены дома, в них кружочками отмечены лифтовые (подъезды). В зависимости от типа сработавшего датчика, кружочек окрашивается в свой цвет, одновременно подается звуковой сигнал.

Далее диспетчер может из предлагаемого меню выбрать операцию - от набора номера милиции при срабатывании сигнализации, до ответа на вызов из кабины лифта. Параллельно ведется несколько журналов учета событий (в том числе журнал выдачи тех самых желанных для сетестроителей ключей от хозпомещений). Возможен удаленный контроль системы из инстанции более высокого уровня, при условии, если сеть подключена к internet.

Данная система была успешно испытана (около 10 узлов), и должна была устанавливаться (с непринципиальными доработками) на экспериментальный участок. Однако к большому сожалению, организационные неурядицы поставили на этом проекте жирный крест...

Глава 2. Размещение активного оборудования и кабелей внутри зданий.

Конкуренция между сетями бывает
или добросовестная, или эффективная.

Следующим по важности вопросом - после построения внешних линий - является размещение активного оборудования и кабелей внутри зданий. При этом приходится одновременно решать следующие задачи:

1. Обеспечение электро- и пожаробезопасности;
2. Защита оборудования от кражи и действий вандалов;
3. Эффективное размещение с точки зрения топологии сети.

Обеспечение пожаробезопасности сетевых устройств в части Ethernet весьма условна. Сигналы с амплитудой 3 вольта угрозы не представляют. Поэтому все мероприятия сводятся по сути к соблюдению правил при прокладке электропитания и заземления (этот материал подробно изложен в четвертой Главе), и соблюдению противопожарных норм при строительстве кабельных линий.

Однако, в домашних сетях даже внешне не сложные вопросы требуют особого внимания из-за работы в неблагоприятных условиях чердаков и подвалов. В первом случае опасность представляют деревянные конструкции, во втором - сырость и возможный конденсат.

Далее, очень бы хотелось поменять местами пункты 2 и 3, но увы - российская реальность не оставляет места сомнению в именно такой очередности приоритетов. И часто приходится жертвовать качественной архитектурой, удобством монтажа, и многим другим ради элементарной сохранности инфраструктуры.

Известны примеры, когда для "спасения" кабелей их приходилось буквально замуровывать в стены. А случаи регулярных краж коммутаторов порой перерастают в систему, сломать которую возможно только плотным взаимодействием с органами МВД или охранными структурами.

Перед переходом к рассмотрению практических ситуаций нужно особо отметить, что на сегодня качество строительства домашних сетей далеко от идеала. Поэтому в примерах

размещения оборудования и подвода электропитания будет показан хоть и совершенно реальный, но скорее негативный (с формальной точки зрения) опыт.

С удовольствием бы привел примеры "совершенных" сетей. Если бы только они встречались на практике... Полагаю, что в сложившейся ситуации необходимо лишь корректировать недопустимые случаи до терпимых, не более того. Это обязательно нужно учитывать при проектировании и построении домашних сетей - и возможно эту главу придется вскоре переписать к более жестким требованиям.

Часть 3. Глава 2

Пожаробезопасность внутридомовых узлов.

Первый принцип, которого нужно придерживаться при строительстве внутридомовой разводки - не в коем случае не навредить существующей инфраструктуре, и тем более не создать опасности для имущества или, того хуже, жизни людей.

Сразу договоримся не брать в расчет санитарно-гигиенические требования (до них в ближайшем будущем дело все равно не дойдет), да и ничего слишком вредного в сетях не применяется. По крайней мере химическое или радиоактивное загрязнение исключено. Но вот с правилами пожарной безопасности считаться необходимо. Тут ответственность высока (вплоть до уголовной), а суммы ущерба могут достигать астрономических размеров.

Но не смотря на это, трудно найти в России нормы, которые бы так часто нарушались, как противопожарные. Например, шахты слаботочной проводки должны быть закрыты между этажами несгораемыми пробками. Однако, за несколько лет работ ни разу не удалось найти такую перемычку не только в жилых, но и офисных зданиях. В общем, массовое, повальное несоблюдение этих требований является системой у подавляющего большинства строительных и обслуживающих организаций, включая ЖЭКи, связистов, лифтеров, и т.п.

Разумеется, хорошего в этом ничего нет, но и представлять на этом фоне сети чем-то недопустимо опасным не стоит. Активное оборудование надежно, сертифицировано (если не унас, так в других странах), не имеет большого потребления электроэнергии. Поэтому целесообразно руководствоваться если не духом законов, то хотя бы здравым смыслом.

Впрочем, если все же нужны нормативные акты, то можно в рабочем проекте и при строительстве руководствоваться требования СНиП 2.09.02-85* п. 1.1; СНиП 21-01-97* (п. 5.17, п. 6.25); СНиП 2.07.01-89, прил. 7; ТСН 21-302-2000 МО (ТСН ПТ-99 МО).

Электропроводка.

Самая опасная с точки зрения любого пожарного инспектора часть - силовая электропроводка. Да и ГСН на это сильно обращает внимание. Хотя часто расстояние от узла до электрощитка ограничивается несколькими метрами, все же бывают случаи, когда нужно делать удаленные выносы.

Сечение проводников в этом случае можно рассчитать исходя из требуемой нагрузки, но на практике редкий узел потребляет более, чем бытовые электроприборы. Соответственно

и кабель подойдет самый обычный, например с медными многопроволочными проводниками в двойной изоляции.

Проводка может быть как открытая (проложенная по поверхности стен, потолков и другим строительным элементам), так и закрытая (в трубах, гибких металлических рукавах, коробах, каналах и пустотах строительных конструкций, и т.п.).

В принципе, кабель в двойной изоляции можно использовать для открытой проводки в любых условиях, в том числе подвалах и чердаках (чердаки, имеющие несущие конструкции из сгораемых материалов вообще вынесены в отдельную пожароопасную категорию). Но если линии идут в зоне досягаемости людей, крыс, домашних животных, их настоятельно рекомендуется закладывать их в трубы или металлорукав.

По стенам сухих помещениях жилых и офисных зданий, коробах, шахтах силовой проводки можно прокладывать плоские провода в однослойной изоляции. Однако, при малейших подозрениях на неблагополучность, имеет смысл использовать гофрошланг (металлорукав, трубы).

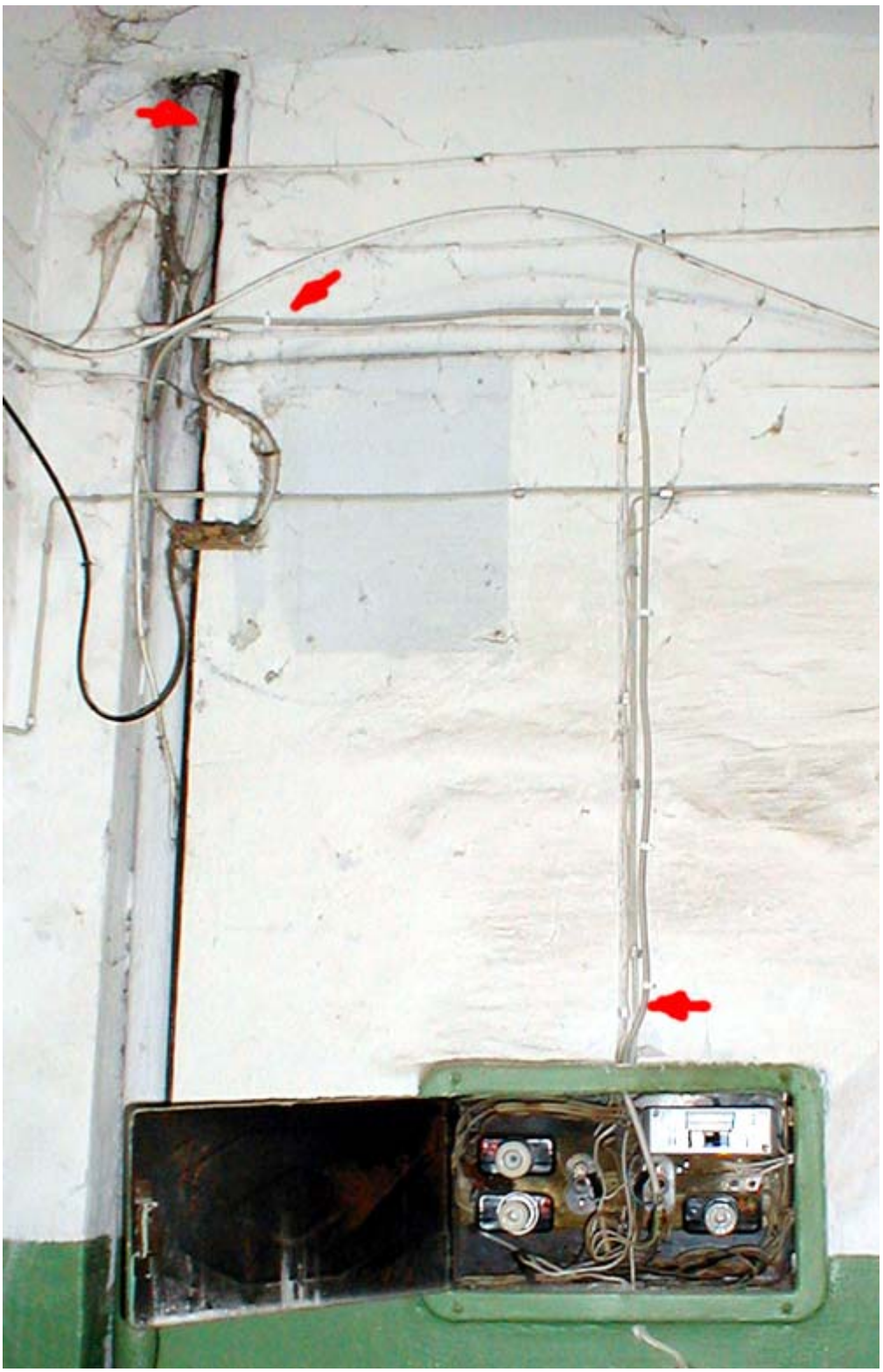

Рис. 2.1. Прокладка кабеля по стене.

Как видно на фотографии, силовой кабель достаточно естественно смотрится даже в условиях весьма "устаревшего" окружения. Да и работать он будет явно дольше электрощитка.

Соединения кабелей можно выполнять спайкой, в муфтах под болт, в крайнем случае скруткой. Но наиболее правильным будет следующий способ:

Рис. 2.2. Соединение силового кабеля.

Данное соединение выполнено зажимами в специальной коробке.

Главное, из-за электрокоррозии нельзя скручивать между собой медные и алюминиевые проводники. Это можно сделать только через переходные муфты.

Если нужно сделать разъемное соединение (штекер, вилка), желательно использовать качественные комплектующие с надежными контактами. Ухудшение соединения и, как следствие, нагревание, может вызвать цепную реакцию - разрушение конструкции, обгорание изоляции, затем короткое замыкание. Обычно при этом все кончается сгоревшими предохранителями, но до беды совсем не далеко...

Кабельные линии.

Понятно, что кабельные линии Ethernet сами по себе возгорания вызвать не могут. Единственная их пожароопасность заключается в возможности горения, выделения дыма и вредных химических веществ. Существует множество отечественных и зарубежных стандартов, которые нормируют эти свойства.

Можно перечислить IEC 1034 (эмиссия дыма), IEC 754 (коррозийная газовая эмиссия), IEC 332-3C - испытание распространения огня в пучке кабеля. Либо "наши" ГОСТ Р МЭК 332-1-96, УДК 621.315.2.001.4:006.354 Группа Е46, ОКС 29.060.20, ОКСТУ 3509.

Впрочем, все эти испытания существенны для толстых пучков кабелей, которыми отличаются современные СКС. Отдельно взятая витая пара поддерживать горение не будет, и химических веществ много не выделит. Так что проблема для домашних сетей не слишком актуальна.

Хотя в особо ответственных случаях можно использовать специальные кабеля, у которых в качестве внешней оболочки используется материал LSHF-FR (малодымящий при возгорании, не содержит галогенов) или его аналог. Такая витая пара обычно имеет оранжевый цвет.

Несколько хуже обстоят дела с толстыми кабелями внешней проводки. В них есть чему гореть, поэтому существует ограничение на их размещение внутри здания. По стандартами допустимая длина составляет около 15-ти метров (этого обычно достаточно для установки переходной муфты). Впрочем, в некоторых случаях ограничение можно обойти путем обмотки кабеля негорючим материалом или прокладкой в металлической трубе (рукаве).

Следующий момент, на которой стоит обратить внимание - шахты слаботочной проводки в высотных зданиях. В них могут накопиться пучки существенного объема, а противопожарные межэтажные обычно "пробки" отсутствуют. При такой "архитектуре" горение может по кабелю быстро распространяться между этажами. Но... Едва ли это проблема Ethernet-сетей. Обычный телевизионный или силовой кабель содержит горючего материала больше, чем целый пучок витой пары.

И последнее. Часто в домашних сетях упрощают монтаж и используют для прокладки кабелей неподходящие места - короба вентиляции, квартирные вытяжки, и т.п. Излишне говорить, что с точки зрения стандартов это грубое нарушение. Но если не уходить далеко от здравого смысла, неправильно проложенные один-два кабеля обычно не способны причинить какой либо "пожарный" ущерб.

Часть 3. Глава 2

Место размещения узлов.

Строители (и особенно проектировщики) отечественного жилья мало думали о будущей информационной инфраструктуре. Часто в шахтах слаботочной проводки нет места для кабелей, и еще чаще - отсутствует место для размещения оборудования. Поэтому построение абонентской системы здания превращается в очень сложную задачу.

Из этой главы исключены теоретические вопросы по сетевой топологии - они уже были подробно рассмотрены в 6 Главе первой части. Но в контексте данного материала будет удобно привести еще раз следующие основные тезисы по абонентской системе здания:

- Хаотичное расположение оборудования (узлы размещены по дому беспорядочно);
- Структурирование по подъездам (один подъезд - один узел, плюс один общий на дом);
- Один дом - один узел.

Разумеется, в реальности идеальные схемы встречаются редко, но все же на уровне идеологии почти всегда можно определить к какому типу тяготеет любая сеть.

Перейдем от общего к частному. Выбор мест размещения не велик, и можно довольно легко перечислить все доступные места. Но их достоинства и недостатки придется приводить с учетом подвода кабелей, так что задача поиска удачного места может по праву считаться одним из самых сложных вопросов сетестроения.

Начнем сверху.

- **Лифтовая**. Есть хорошее электропитание, ввод в шахту слаботочной проводки, заземление, выдержан температурный режим, ограничен доступ (часто даже установлена сигнализация). Если удастся договориться с лифтовой службой и (или) технадзором - это безусловно одно из лучших мест для размещения.

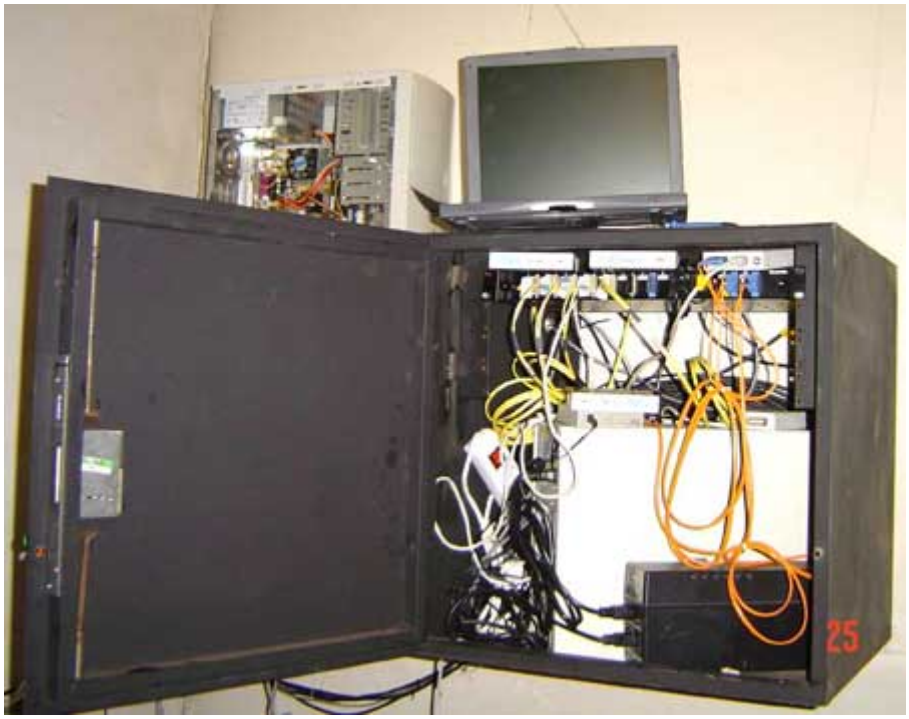

Рис. 2.3. Установка в лифтовой.

Но договориться очень не просто. Подобное размещение прямо запрещено службой, следящей за безопасностью лифтов.
Бывает, что коммунальные лифтеры в общем не возражают против установки, но им это в директивном порядке запрещают наблюдающие инстанции. Тем не менее, это часто не мешает существованию "в запретной зоне" даже крупных узлов.

- **Техэтаж**. Сносные температурные условия, нет особых проблем с электропитанием и заземлением. Удобно делать межподъездную разводку по варианту "один дом - один узел". Так что это неплохой вариант.

Рис. 2.4. Установка на техэтаже.

Главный минус - место легкодоступно для воров и вандалов. Против этого можно защититься, например, прочным ящиком.

- **Чердак** 3-5 этажек. Нет питания, заземления, высокая пожароопасность. Часто недоступны шахты слаботочной проводки (если они вообще есть). Проблемы с температурой и влажностью. Очень легкий доступ для воров и вандалов. В общем, это один из самых неприятных вариантов.

Рис. 2.5. Установка на чердаке.

Выглядят обычно такие узлы ужасно (фотографию ни в коем случае нельзя принимать в качестве образца для подражания, тем не менее, это реальность). Видимо, обстановка способствует соответствующему отношению.

- **Стена подъезда**. Все, кроме беспроблемного питания и комнатной температуры, идет в минус. Заметность, опасность воровства, сложности с подводом коммуникаций по варианту "один дом - один узел".

Рис. 2.6. Установка в подъезде.

Вместе с тем подъезд часто единственное место для размещения оборудования, особенно по варианту "Структурирование по подъездам".

- **Подъездный электрощиток** (часть слаботочной проводки). Почти то же самое, что и размещение на стене подъезда, но прибавляется необходимость уложиться в крайне небольшие габариты. Защиту от воров можно делать только путем маскировки - другие методы фактически неприменимы.


Рис. 2.7. Установка в электрощитке.

Данный способ используют почти все начинающие сети - размещение дешево и в общем удобно. А потеря 30-ти долларовых хабов не слишком большая потеря. Впрочем, надо заметить, что в некоторых проектах домов электрощитки отгораживают железными дверями жильцы, что резко повышает привлекательность этого метода установки.

- **Электрощитовая** (отдельное помещение на первом этаже). Очень неплохой вариант - питание, температура, заземление, защита от злоумышленников - на уровне. Минус - если ввод в здание производится с крыши, и, хуже того, подвал недоступен для разводки, возникают существенные сложности с прокладкой кабелей по узкой шахте слаботочной проводки.
В случае доступности подвала для прокладки линий данный вариант почти идеален, даже значительно лучше, чем лифтовая из-за хорошей грозозащищенности. Увы - нормальные электрощитовые и подвалы попадаются в российских домах не слишком часто.
- **Подвал**. По своим ТТХ сильно напоминает техэтаж. Недостаток - возможна высокая влажность и повреждение кабелей крысами. Преимущество - хорошая грозозащищенность (что очень важно).
- **Квартира жильца**. Все условия близки к идеальным, кроме одного - что делать если жильца нет дома (он в долгосрочном отпуске, командировке)? Сбой работы оборудования - и хоть прокладывай кабель в обход...

Рис. 2.8. Установка в квартире или офисе.

Тем не менее, этот способ часто практикуют начинающие сети. Удобно и дешево - конечно, до определенной степени.
Надо сказать, что и более серьезные фирмы используют такую технологию. Только размещают оборудование не в частных квартирах, а арендуют "угол" в офисах юридических лиц.

- **Установка на улице**. Конечно, для России это экзотика, но помнить у существовании такой возможности не помешает.

Рис. 2.9. Установка на улице.

Какому варианту отдать предпочтение? Это нужно решать каждому оператору применительно к своим условиям. Из общих рекомендации можно сказать лишь очевидное - при "верхней" разводке желательно размещать оборудование ближе к крыше, при "нижней" (подвальной) - соответственно наоборот. Остальное будет зависеть прежде всего от вида домов, затем от способа их соединения в сеть, и далее - от целого комплекса труднопредсказуемых технических и (или) юридических моментов.

Так, важнейший фактор при выборе места узла - условие его долгосрочного существования. Ведь к активному оборудования сводятся кабеля, и переносить их через год-два будет очень дорого. Поэтому административный пресс довлеет над техническими предпочтениями. Приходится ставить оборудование в те места, на которые есть разрешения (договора) с владельцами или балансодержателями.

В этом процессе нужно учитывать извечную российскую проблему - легче получить разрешение на уже установленное, чем договориться заранее. Особенно при фактическом отсутствии нормативной базы. Почти все небольшие любительские сети начинали с размещения оборудования в удобных местах без всяких согласований. И, надо сказать, что подавляющее большинство провайдеров по мере роста спокойно легализовало свою инфраструктуру - разумеется при условии, что она была изначально сделана грамотно и никому не мешала.

Но хорошие ли отношения сложились с коммунальщиками, или не очень - все равно удобные места для размещения - редкость. То нет доступа к чердаку, то к подвалу (или они отсутствуют), и т.п. Соответственно, приходится выбирать менее худшую из зол, ставить там, где имеется хоть малейшая возможность. А для защиты оборудования использовать дорогие вандалоустойчивые ящики, пробивать перекрытия для прокладки своих коммуникаций.

В завершение нужно заметить, что установка оборудования в сложных условиях неизбежно ведет к использованию самых дешевых сетевых устройств. Дорогие устанавливать жалко из-за их больших габаритов или слабой защиты от злоумышленников. А недорогое оборудование, в свою очередь, вовсе не способствует повышению качества услуг.

Поэтому при выборе базовой топологии абонентской разводки здания необходимо задумываться о будущем - когда вместо дешевых и компактных хабов придется использовать многопортовые, большие по габаритам и цене управляемые коммутаторы. Которые просто не поместятся, например, в электрощитки.

А значит удобное на первом этапе развития хаотичное расположение оборудования в дальнейшем может легко привести к необходимости полной перекладки кабелей (или невозможности выгодной продажи сети). Из-за большой цены ошибки выбор топологии (и соответственно мест расположения узлов) лучше сделать заранее, и подойти к этому вопросу со всей серьезностью, которая возможна **перед** прокладкой кабелей.

Часть 3. Глава 2

Способы защиты оборудования.

Российская реальность сурова. Где бы ни было размещено оборудование, нельзя пренебрегать угрозой его воровства или порчи. Разумеется, где-то такая опасность меньше (например за железными дверями лифтовой), где-то больше (на стене подъезда). Но защита все равно нужна в большинстве случаев.

К сожалению, удобного и универсального метода нет. Как обычно, хорошая защита дорога, а дешевая неэффективна. Поэтому рассмотрим достоинства и недостатки основных способов сохранения имущества.

Пассивные средства зашиты.

- Сохранения мест установки оборудования в тайне, маскировка.
- Приведение оборудование в состояние непригодности для продажи.
- Использование прочных металлических коробок.
- Ограничение доступа в помещения с установленным оборудованием.

Еще несколько лет назад достаточно было не афишировать места установки оборудования, и даже дорогие разветвители могли находится на чердаках и в подвалах без всякой защиты, в простейших электротехнических коробках "под болт".

Но эффективность таких мер последнее время сильно снизилась. Сети бурно растут. Тайну местоположения сохранить при нескольких десятках кабелей уже нереально. Стоимость оборудования то же в среднем повысилась - многопортовый (и тем более управляемый) коммутатор за $100-200 привлекает злоумышленников больше, чем 5-8 портовый за $25.

Однако начинающая сеть может вполне успешно некоторое время использовать маскировку и в настоящее время.

Рис. 2.10. Замаскированный хаб.

Можно ли предположить, что в этом месте находится узел небольшой сети? Особенно если участь, что освещение на фото от вспышки, и в обычно тусклом свете фонарика рассмотреть что-то вообще невозможно.

Но вот несколько кирпичей убрано:

Рис. 2.11. Замаскированный хаб.

Надо отметить, что в данном примере хорошо скрыто не только само устройство, но и все кабеля (по которым хаб можно легко найти). Злоумышленники обычно не любят сложные поиски на темном и пыльном чердаке, да и в сетях разбираются слабо (а профессионалы за "таким" не пойдут). Поэтому шансы на выживание узла весьма велики.

Необходимо только отметить, что данное решение ни в коем случае не должно быть образцом для подражания из-за неудачного подвода питания. Напряжению в 220 Вольт не место в такой близости от деревянных перекрытий. А в остальном - этот узел существует уже три года, и за это время при полностью открытом чердаке ни один хаб не был украден.

Следующий недорогой способ - приведение оборудования в непродажное состояние. Основные минусы - потеря гарантии и неприменимость метода для сложного и дорого оборудования (например маршрутизаторов, радиобриджей, xDSL модемов).

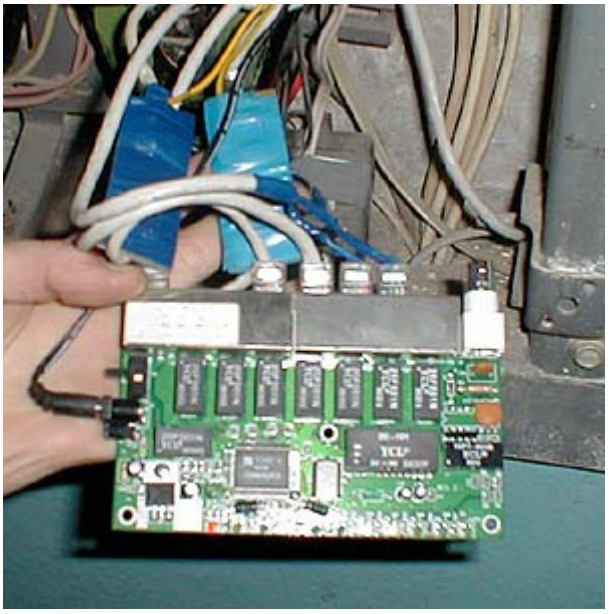

Рис. 2.12. Хаб без корпуса.

Самый простой способ лишения товарного вида - снять корпус. Так можно даже не потерять гарантию. Но для более надежной зашиты от воров придется покрасить хаб, нанести на чипы неудаляемую маркировку (гравировку). Или вообще присоединить к несущей стене так, что для кражи придется неизбежно сломать устройство.

В принципе, для небольшой любительской сети данный способ можно считать приемлемым. Но для оказания серьезных услуг (и дорого оборудования) придется использовать что-то другое.

А именно металлические ящики и (или) усиленные люки и двери в тех-помещения. Так как вопрос ящиков достаточно серьезен, его рассмотрение вынесено в отдельный (следующий) параграф настоящей книги.

Защита оборудования при помощи установки в помещения, снабженные своими прочными дверями едва ли не самый лучший способ из всех. Если есть такая возможность - то можно эффективно использовать электрощитки в коридорах "за железными дверями", лифтовые, даже чердаки или подвалы, если выходы на них "под замком".

Однако надо помнить, что доступ к техническим помещениям имеют многочисленные технические службы, электрики, лифтеры, телевизионщики, сантехники... А значит и ключи от соответствующих дверей могут легко попасть в чужие руки. Конечно, из-за недорогого хаба никто специально не будет заниматься, скажем, подкупом сантехника. Но в случае серьезного узла эту возможность исключать нельзя.

Надежную защиту дает только сигнализация.

Вариантов ее использования достаточно много. Но если их классифицировать, то принципиально отличаются три организационных направления. А конкретно:

- Привлечение специальных охранных служб.
- Использование своих сил.
- Средства взятия "на испуг".

Понятно, что первый путь дороже, но значительно спокойнее и надежнее. Технология простая - шлейф сигнализации подключается на специальное недорогое радиопередающее устройство (разумеется совершенно легально). При сработке в срок не позднее 5 минут должны приехать несколько бойцов с автоматами, и (вполне легально, подчеркну) "принять" нарушителей периметра.

Стоит такое удовольствие (в одной из Екатеринбургской служб) 600 рублей в месяц. Это для квартиры, в розницу. Думаю, что для защиты сети могут быть и другие, более выгодные, условия.

Понятно, что не надо защищать таким образом всю сеть до последнего хаба. Хватит центральных узлов и нескольких (случайно выбранных) периферийных. Есть надежда, что при таких мерах нехорошие люди долго на свободе не проходят. Попадутся если не на первый раз, так на третий-пятый-десятый.

Есть только несколько ограничений. Во-первых, не везде есть охранные службы. Во-вторых, защита в виде дверей или металлического ящика все же необходима. Ведь от сработки сигнализации до доступа к оборудованию должно пройти не менее 5-10 минут - охранной службе надо успеть добраться до нужного места.

Зато уже после первого же ареста можно спать спокойно. Слухи в криминальной среде разносятся быстро, и в дальнейшем охраняемые (или "подозрительные" в этом смысле) узлы будут обходить стороной.

Защита своими средствами не сложна технически. При использовании "пинговалки" или управляемого коммутатора определить факт наличия устройства в сети проще простого. Но в случае пропадания связи, спасать оборудование скорее всего будет, увы, поздно.

Потребуется отдельная система (радио, телефонная, или другого типа). Немного менее правильно, но все же можно в качестве средства раннего предупреждения использовать любые устройства, способные преобразовать факт срабатывания в сигналы Ethernet, которые можно контролировать штатными средствами. Тут могут подойти от управляемых коммутаторов до установленых в потайных местах веб-камер.

Но зафиксировать кражу - еще половина дела. Что делать дальше? Давать отпор похитителям самостоятельно небезопасно как в физическом плане, так и законодательном. Случаи, к сожалению, бывают разные. Поэтому защита своими средствами не слишком эффективна - с ней может быть больше проблем, чем пользы.

И о "пугательных" методах. Использовать датчик присутствия с речевым генератором не слишком сложно, и относительно не дорого. Но... Это явно одноразовое средство, и не поможет против квалифицированных воров. Так же не совсем понятно, что делать при отключении электропитания (хотя UPS спасет положение).

Не лучше и опасные средства типа подвода к корпусу высокого напряжения или капканов. Как правило от этого страдают сами владельцы. Да и запрещены такие действия законодательством РФ...

Значение легального размещения оборудования.

Рассмотрим гипотетическую ситуацию.

Злоумышленник спокойно снимает оборудование. На этом его буквально за руку хватают сотрудники милиции. В ответ вор спокойно заявляет - это мое железо, что хочу, то с ним и делаю. Да и документ есть - вот, неделю назад я этот свитч покупал, там-то и там-то. А ключ от коробки, увы, потерял...

Как определить в такой ситуации истинного хозяина? По серийному номеру? По спиленному особым образом уголку чипа? Свидетелей собирать? Все методы сложны, неоднозначны, и в общем заведомо известно что "дело" дальше заявления не пойдет.

Таким образом, очевидно, что если сеть не имеет официальных разрешений на работу, проекта, документации - совершенно невозможно защитить устройства организационно. Подготовленный злоумышленник (например конкурент или бывший партнер) при определенных условиях вполне сможет безнаказанно причинить коммуникациям серьезнейший ущерб.

Заключение.

Можно сказать известную фразу - "Спасание утопающих - дело рук самих утопающих". Никто, кроме самих провайдеров, проблему сохранности оборудования не решит. На МВД надежда слабая - факт кражи очень сложно доказать (только ловить за руку, или брать "на испуг" при продаже). Поэтому и приходится сетям обзаводиться прочными металлическими ящиками - которые и играют на практике роль основного защитного механизма.

И мечтать (увы, пока только мечтать) о следующей компоновке узлов:

Рис. 2.13. Узел домашнего провайдера в Канаде.

УПС, мощный коммутатор, и небольшой медный и оптический кросс - что еще нужно для надежной, качественной работы? Все это в симпатичном (но не слишком прочном) ящике. Надеюсь, когда-нибудь и в России узлы Ethernet-провайдеров будут выглядеть похожим образом...

Часть 3. Глава 2

Конструкции ящиков.

В обычных локальных сетях вопрос выбора места размещения оборудования как правило не стоит. В особо малобюджетных вариантах коммутаторы и маршрутизаторы ставится на пол, столы, или, реже, подвешиваются на стены.

На более серьезных узлах используются 19-ти (реже 10-ти) дюймовые ящики или стойки на 5 юнитов и более (1U - "один юнит" - единица, применяемая для обозначения высоты оборудования, устанавливаемого в стойку. 1U равен 1,75 дюйма или 44 мм).

В таких конструкциях удобно компактно размещать много устройств, декорировать нагромождение кабелей. Кроме этого, они защищают от неосторожного обращения малоквалифицированного персонала (классический пример - уборщица помещения).

Однако стандартные ящики СКС хоть и присутствуют на рынке в широком ассортименте, но совершенно непригодны для решения главной задачи домашних сетей - защите оборудования от злоумышленников всех видов.

Конечно, за рубежом используются и вандалоустойчивые конструкции. Но в Россия их даже не завозят - стоимость высока, а защита явно недостаточна против отечественных воров и вандалов.

Попробуем сформулировать требования к идеальному ящику для Ethernet-провайдера или серьезной домашней сети.

- Коробка должна быть рассчитана на установку оборудования 19-ти дюймового стандарта. Так или иначе, но все серьезное телекоммуникационное оборудование выпускается под этот размер. Сети растут, в одну точку сводятся все больше кабелей, и менять через несколько лет небольшие ящики под новый размер будет не слишком приятной перспективой.
- Коробка должна иметь удобный кросс для разводки как П-296, так и витой пары.
- Должно быть предусмотрено место для установки не только компактного источника бесперебойного питания, но и более громоздких аккумуляторов и инвертора.
- Предусмотрены удобные вводы кабеля и его организация внутри коробки (известно, что в стойках классических СКС находятся в основном кабеля, в домашних сетях ситуация вполне похожая).
- Сравнительно надежная защита от воров и вандалов, которая должна обеспечивать стойкость хотя бы в 10 минут. Этого достаточно, что бы успели приехать работники охранной фирмы при сработке сигнализации (если такая будет когда-либо установлена).
- Сносный внешний вид (легализация неизбежна, да и просто так приятнее работать), и хотя бы потенциальная возможность получения сертификатов.

Приблизительный эскиз:

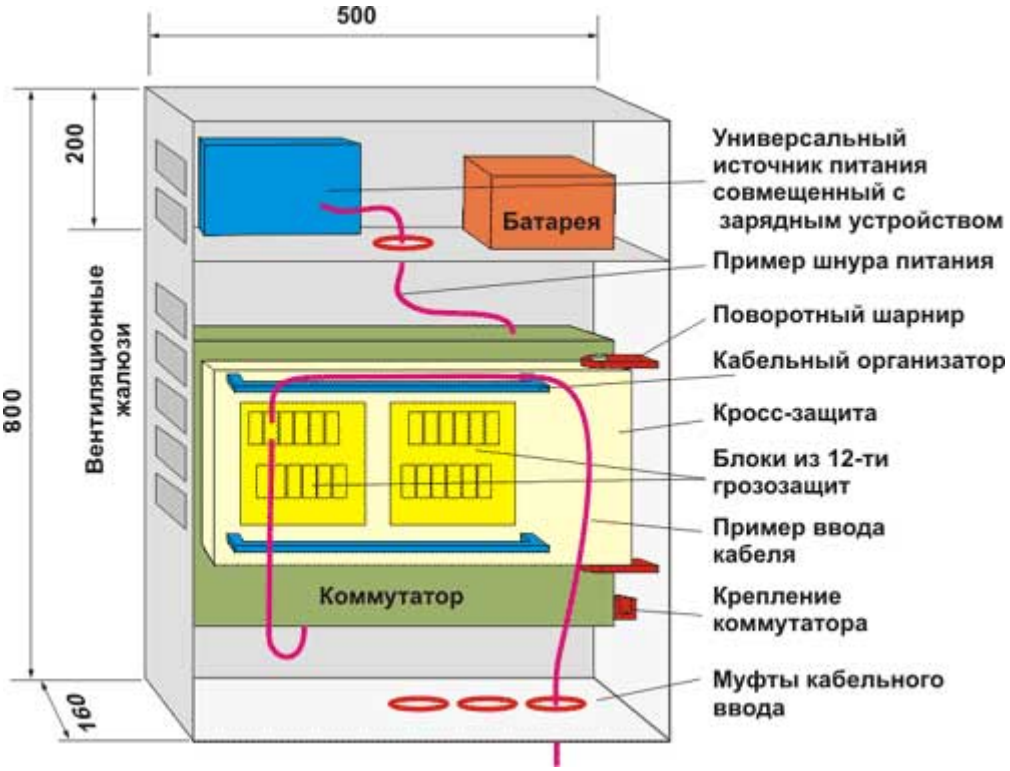

Рис. 2.14. Ящик для домашней сети (теория).

- Металл - 3 мм внешняя крышка, 2 мм каркас, желательно прочная порошковая окраска.
- Дверь съемная (без шарниров), замок сейфового типа (на 3-4 стороны).
- Активные устройства располагаются вертикально, разъемами RJ45 вбок или вниз (что бы не в них не попадала пыль).
- Так как кроссовая панель и кабельные организаторы занимают много места, они должны быть расположены над активным оборудованием. При этом кроссовая пластина может быть "открыта" на шарнирах, предоставляя возможность снять устройство (коммутатор, маршрутизатор) или переключить порты. Естественно, делать это нужно не разбирая "приходящие" линии.
- Кросс должен быть совмещен с грозозащитой. Вводной зажим проводников RJ45 или болтовой (для П-296), выходной - RJ45 (есть возможность коммутации шнурами).
- Опционально устанавливается универсальный источник питания с выходными напряжениями 5, 7, 9, 12, 15, 220 Вольт. Он же обеспечивает при необходимости подзаряд аккумуляторов.
- Могут быть установлены средства сигнализации, контроля температуры, и т.п. мониторинга/управления.

Главный недостаток показанной конструкции - высокая стоимость. Отечественным домашним сетям еще только предстоит привыкнуть к мысли, что оборудование узла может стоить значительно дороже, чем установленное в нем активное оборудование.

Стихийное развитие сетей начиналось с установки хабов в картонные коробки (или совсем без них), металлические ящики появлялись только через некоторое время, после участившихся случаев воровства. Затем оборудование усложнялось, увеличивались его количество и размеры... Можно сказать, что "ящикостроение" то же проходит эти стадии.

Для начала, андеграундный этап. Корпус сварной из кусков швеллеров, гаражный шарнир, внутренний крепкий замок. Не всякий лом поможет против такой конструкции. Серьезно выглядит.

Рис. 2.15. Андеграундный ящик.

Особая красота не нужна. Чем страшнее, тем надежнее. А чтоб не утащили все вместе - приварить к металлоконструкциям техэтажа наглухо. Или забетонировать. Или пристрелять дюбелями. Ну в крайнем случае - на болты, и резьбу заклепать.

Следующая конструкция уже вполне серийная, и предназначена для размещения небольших устройств настольного форм-фактора. Предусмотрено улучшенное питание, место для установки грозозащиты, подсветка, крепеж, и прочие приспособления.

Рис. 2.16. Малобюджетный ящик-"пенал".

Хотя ящик выполнен не из 1-2 мм листового металла. В нем нет шарниров, которые легко разбить или спилить. Крышка задвигается в пазы и крепится винтовым замком, который изготовлен из толстостенной трубы (пилить долго). Пазы расположены с трех сторон, что не позволяет ломиком поддеть крышку с боков.

Такое решение в общем вполне удобно для сетей низкой плотностью портов (например 2-3 этажные дома), или недорогих выносов. Основной минус - недостаточная прочность против серьезно настроенных злоумышленников и малый объем.

Развитием этой системы можно считать ящик следующей конструкции (размер - 800*600*230):

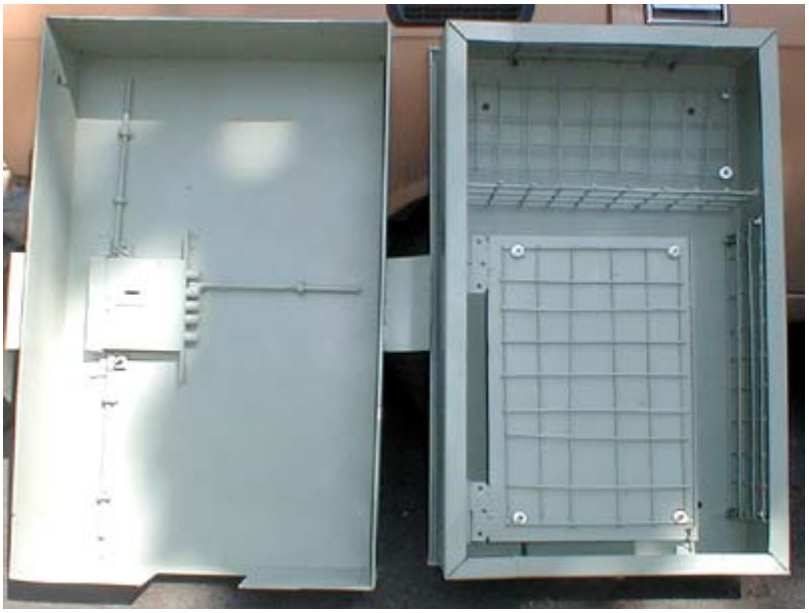

Рис. 2.17. Ящик типа "обувная коробка".

Крышка из 3-х мм железа одевается сверху так, как это делается в обувной коробке. Только ее края доходят до "дна", и утоплены в паз окантовки, выполненной из уголка. "Сломать" такой ящик можно только "болгаркой".

Основные параметры:

- Крышка имеет сплошные сварные швы только на ребрах, длинные боковые поверхности цельногнутые. Т.е. сломать по шву невозможно.
- Замок внутренний и обеспечивает закрывание в три стороны.
- Снизу крышка закрыта прочной окантовкой из уголка. Поддеть ломом не представляется возможным.
- Есть поворотная пластина, которая обеспечивает доступ к коммутатору, позволяя устанавливать активное оборудование в несколько "этажей". Параллельно, передняя поверхность пластины предназначена для установки грозозащит, кроссов, и кабельных организаторов.
- Боковые стенки ящика покрыты съемными решетчатыми панелями, что позволяет легко крепить как кабеля, так и активное оборудование
- Большой вес (около 40-50 кг) препятствует краже оборудования вместе с ящиком. В полном снаряжении и стесненных условиях чердака он просто неподъемный даже для 2-х человек.

Основным недостатком подобной конструкции является сложность обслуживания. Тяжелую крышку не просто снять, и физически тяжело одеть (особенно на весу).

Поэтому большое распространение получил промежуточный вариант:

Рис. 2.18. Ящик с дверцей.

Внутреннее оборудование в общих чертах похоже на предыдущую конструкцию. Но вместо крыши "обувного" типа используется обычная дверь, усиленная прямоугольным профилем. Рама ящика то же усиленная. В закрытом состоянии дверь со стороны шарниров дополнительно фиксируется специальными шпонками.

К сожалению, надежность ящика с дверью (особенно таких больших размеров) не слишком высока даже несмотря на все меры усиления. Достаточно поддеть угол хорошим ломиком (а его в свою очередь можно забить кувалдой), и коробка будет вскрыта.

С другой стороны понятно, что идеальной защиты вообще нет. А такой вариант выглядит достаточно удачным компромиссом простоты использования и прочности.

Кроме самодельных конструкций антивандальных ящиков можно применять и стандартные сейфы. Новые модели конечно слишком дороги для сетей, но вот старый засыпной сейф порой можно приобрести за $100-200.

Защита при этом будет лучшая из возможных. Но вес конструкции и трудоемкость установки то же "на высоте". Поэтому данный метод стараются применять в том случае,

когда другие уже не помогают. Или оборудование слишком ценное, что бы экономить на защите.

И в завершение. Если узел находится в относительно защищенном помещении, достаточно будет следующего варианта:

Рис. 2.19. Простой ящик.

Прочность не высока - для взлома достаточно монтировки. Но, тем не менее, это вполне достаточна защита от излишне любопытного электрика или сантехника, которые могут оказаться в закрытой электрощитовой, подвале или техэтаже.

Часть 3. Глава 2

Разводка кабелей по дому.

Вопрос внутридомовой проводки внешне выглядит весьма простым. Действительно, нет проблем с выбором кабеля - стандартная витая пара годится практически на все случаи жизни.

Работа в тепле, можно сказать уюте (по сетевым понятиям), даже организационный риск минимален - из лицензий нужен только "монтаж слаботочной проводки".

В принципе, спорить с этим нет смысла. Сложность строительства внутридомовой разводки действительно сильно уступает не только прокладке внешних линий, но и установке активного оборудования. Но и на этом этапе работ есть свои тонкости.

Для начала, кабельные линии можно разделить на вертикальные и горизонтальные. К терминологии СКС это не имеет особого отношения, так как плотность портов в жилом доме явно недостаточно для такого переноса понятий.

Горизонтальные линии связывают между собой пользователей или узлы в разных подъездах, и могут быть проложены:

- По крыше снаружи. Этот способ обычно не слишком удобен, и очень уязвим от неблагоприятных погодных условий, разрядов молний, вандалов. Использовать его имеет смысл только в самой неблагоприятной ситуации, когда другие возможности отсутствуют.

Рис. 2.20. Прокладка по крыше.

- По чердаку или техэтажу. Наиболее простой и безопасный способ - хотя иногда придется подумать о хорошем и труднодоступном способе крепления кабелей.

Рис. 2.21. Прокладка по чердаку.

- По подвалу. Технология достаточно несложная, и идеальная в плане грозозащищенности. Из минусов - возможное повреждение линий крысами и (или) влагой.
- По наружной стене дома. Этот метод Ethernet-провайдеры обычно недооценивают, и используют исключительно редко. Хотя для телефонистов в старой малоэтажной застройке это почти стандарт - и не зря. Делается такая прокладка просто, согласований требуется минимум.

Разумеется, прокладка кабельных линий должна быть хорошо увязана с местами размещения активного оборудования. Тянуть толстый пучок проводов через весь дом снизу вверх (или сверху вниз) дело конечно реальное, но все же лучше избегать подобных конфигураций.

Вертикальные линии для подключения конечных пользователей (реже узлов) можно прокладывать следующими способами:

- По шахтам слаботочной проводки. Способ можно безусловно считать основным. Это законно и удобно. К сожалению, иногда доступ к шахтам затруднен технически или организационно (например блокирован жильцами нескольких квартир). Или стояки просто отсутствуют - что типично для домов старой постройки.
  Бывает и такое:

Рис. 2.22. Состояние шахты слаботочной проводки.

Через такое нагромождение проводов проложить новую линию не так-то просто. Впрочем, подобная картина не типична для жилых домов, хотя в офисных зданиях встречается очень часто.

- Прокладка собственных стояков слаботочной проводки. Способ очень дорогостоящий, но при реализации долгосрочных проектов возможны и такие жертвы. Особенно в старых домах, где шахты слаботочной проводки полностью отсутствуют. Самый распространенный материал для подобных работ - металлические трубы различного сечения или прямоугольные профиля.
- По вентиляционным коробам, вытяжкам, и прочим неприспособленным для прокладки кабелей местам. Иногда этот способ удобен и недорог, но его главный недостаток - незаконность. Если владельцы (или ответственные организации) обнаружат такую линию, она в лучшем случае будет удалена. В худшем возможны штрафные санкции. Правда справедливости ради нужно сказать, что даже вероятность обнаружения очень мала, а уж санкции и вовсе редкость.
- Прокладка по внешней стене дома. Такой метод часто практикуется начинающими сетями, но стандартная витая пара служит в таких условиях недолго (обычно от полугода до 2-3 лет). Да и вид фасада портится. Но в сложной ситуации прокладка по внешней стене вполне применима - особенно при использовании витой пары для наружных работ.

- Так могут применяться разнообразные экзотические способы - прокладка в недействующем мусоропроводе, водосточной трубе, по архитектурным элементам... Но разумеется, к массовым технологиям это отнести нельзя.

Следующий момент, на который необходимо обратить внимание - соединение кабелей. В обычных СКС кабель прокладывается строго одним куском от кросса до розетки (соединение допускается только в одной "консолидационной" точке). Однако в трудных условиях внутридомовой разводки так действовать очень сложно.

Ведь прокладка делается не один раз на все случаи жизни, а последовательно, по одному кабелю. Да и конфигурация сети может меняться с течением времени в достаточно широких пределах. Поэтому кабеля часто соединяют между собой. Иногда это делают следующим образом:

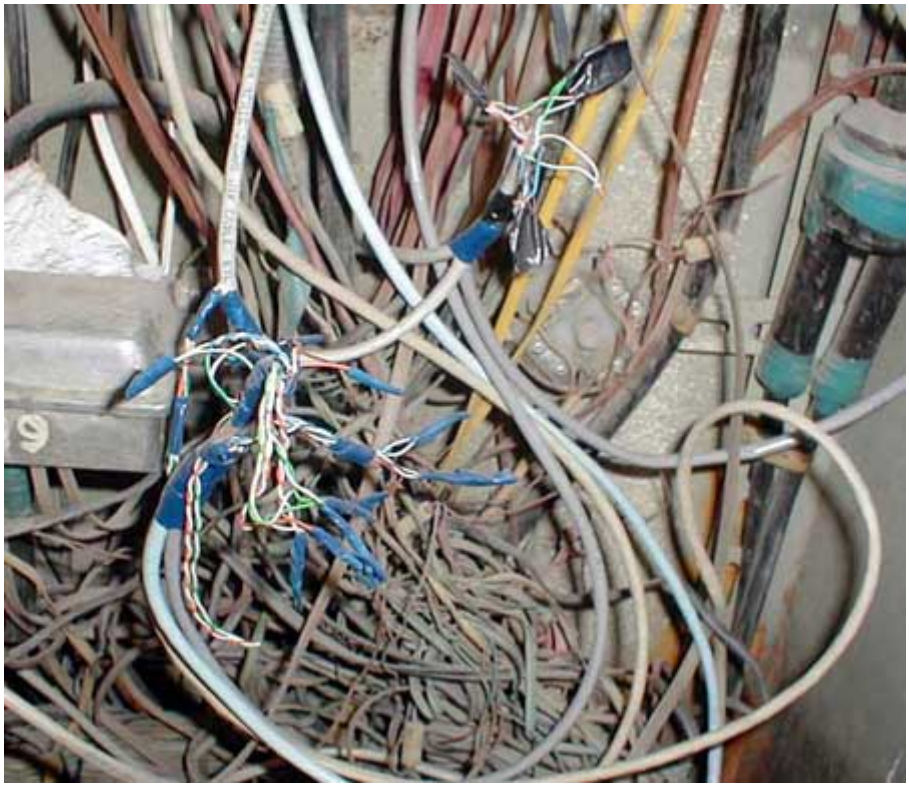

Рис. 2.23. Соединение кабелей.

Несмотря на "страшноватый" вид, эта 10-ти мегабитная линия работает совершенно нормально уже несколько лет. Скорее всего, не возникнет проблем и при переходе на 100 мегабит, но тут уже ничего нельзя сказать наверняка.

Вообще, стандарт 10baseT может выдерживать очень серьезные отклонения от правил СКС. Хотя пренебрегать последними и не стоит, но помнить о большом технологическом запасе можно - это может позволить экономить заметные суммы.

Впрочем, в любом случае более правильным будет использование простого кросса:

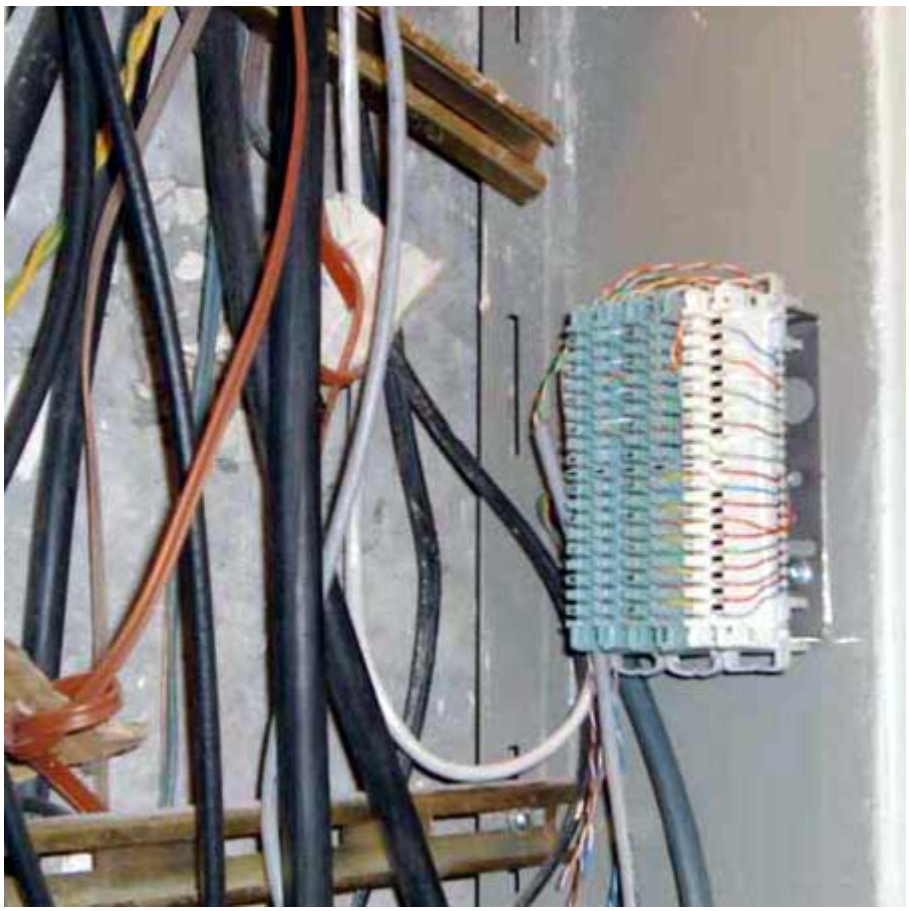

Рис. 2.24. Кросс с жилом доме.

Симпатичная, компактная конструкция - и никаких проблем с надежностью и удобством обслуживания.

Кроме специальных кроссов можно использовать розетки, грозозащиты, клеммные коробки, соединители типа скотчлок, и тому подобные приспособления. Важно только помнить, что для 10 мегабит достаточно соблюдения требований Категории 3 (по сути, требуется "телефонное" качество). Но если предполагается использовать 100 мегабит - придется обеспечивать Категорию 5, и соответственно стоимость соединения сильно возрастет (или заметно упадет качество линии).

В заключение, два небольших организационных вопроса, которые часто выпадают из поля зрения начинающих провайдеров.

Во-первых, при строительстве внутридомовой разводки очень важно разделить зону ответственности за проложенный кабель. Как правило, провайдер обслуживает за свой счет только линию только до квартиры пользователя. Прочие работы ведутся за счет абонента. В некоторых кооперативах весь кабель обслуживается пользователем, но большого распространения такой подход по понятным причинам это не получил.

Хотя известен по крайней мере один экзотический случай, когда для приема в сетевое сообщество требуется сдать небольшой техминимум. И это в сети на несколько сотен абонентов.

Во-вторых, кабелям нужна хорошая (и главное подробная) маркировка, причем желательно не только около портов активных устройств, но и в некоторых местах по ходу

следования линий. Опыт СКС малоприменим не только из-за больших длин линий, но и разных идеологических подходов к сети. "Домашняя сеть" (в отличии от СКС) не статичная инфраструктура, она непрерывно развивается.

Способов маркировки достаточно. Но большинство стандартных малоудобны из-за низкой информативности. При работе монтажнику желательно знать как можно больше о линии - по крайней мере код (идентификационный номер), имя пользователя, адрес, IP. Постоянно носить с собой шпаргалку-расшифровку конечно можно, но не сложно предположить что из этой затеи выйдет в реальности.

Хорошо себя показали следующие варианты:

- Самый недорогой и надежный - нарезаный линолеум. Кусочек, сантиметра полтора шириной, 3-4 длиной. Два отверстия, в которые пропускается кабель. Надписи делаются шариковой ручкой.
- Внешне красивый способ - специальные бирки для ключей. Цветная пластмасса с бумажной вставкой, закрытой целлулоидом. При замене IP бумажка легко вытаскивается и заменяется на новую. И по цветам бирки могут отличаться как входящие, исходящие и пользовательские.
- Бумажная бирка (часто закрытая скотчем). Способ не очень удобный, однако широко применяющийся на практике. Может быть выполнена как "флажком" (что иногда мешает при большом количестве портов), так и плотно примотанной к кабелю (маркировка трудноразличима).
- Надпись по кабелю шариковой кучкой или специальным маркером. Это еще более неудобно, чем бумажная бирка, но то же широко используется...

Разбираться в кабельных линиях без маркировки удовольствие, мягко говоря, ниже среднего. Особенно если они проложены кем-то другим. Поэтому требовать от монтажников маркировку совершенно необходимое условие благополучного действия сети в течении длительного времени.

Глава 3. Работа с оптоволокном.

Для быстрой езды нужна не только
широкая полоса, но и ровный асфальт.

У традиционных "медных" коммуникаций есть масса достоинств - дешевизна, простота монтажа, устойчивость к внешним условиям... Но есть два недостатка, которые не позволяют говорить о таких кабелях как о будущем Ethernet-провайдинга.

Это подверженность электрическим наводкам (от грозовых разрядов или других факторов) и недостаточная дальность передачи на высокоскоростных протоколах. И то, и другое существенно тормозит развитие сетей в техническом плане и заметно снижает надежность даже простых (и недорогих) решений.

Действительно, несмотря на все грозозащитные мероприятия, воздушные линии очень уязвимы. И можно считать хорошим результатом, если за год от наводок выйдет из строя не более 3-5% портов. Для дорогого высокоскоростного оборудования это непозволительные потери.

С другой стороны, расстояния между стандартными активными устройствами для передачи со скоростью 2Мб могут достигать трех километров, при 10Мб - 500 метров (при использовании П-296), для 100Мб - не более 200-300 метров. Это не только ограничивает дальность передачи, но вдобавок не позволяет использовать эффективные топологические решения (звезда, кольцо).

Оптоволокно не имеет указанных недостатков, но имеет свои минусы. Прежде всего это высокая стоимость и сложность работы как с самим кабелем, так и отдельными волокнами. Тем не менее, очевидно что рано или поздно подавляющее большинство междомовые линий домашних сетей будет прокладываться при помощи оптоволокна.

И готовится к этому нужно уже сейчас - закладывая оптоволоконные решения если не по всей сети, то по крайней мере на важнейших ее участках.

Пожалуй, главная сложность работы с оптоволокном - психологическая. Но нужно пониимать, что пока волокно покрыто оболочками, оно не сломается при соблюдении максимальных радиусов изгиба - около 20 наружных диаметров. Для волокна в полиакрилате (в самой тонкой оболочке - 0.25 мм) он составляет около 5 мм.

Работать с хрупким кварцевым стеклом после "меди" просто страшно. Поэтому перед началом работы рекомендуется отрезать от кабеля кусок длинной в пару метров, и поэкспериментировать. Разделать, вытащить волокна. Попробовать их сломать. Потом попробовать сломать их в буфере, а потом - в буфере и модуле (если он есть).

Убедиться, что это не просто, что волокно достаточно прочно, и может выдержать самые тяжелые испытания. Например, модуль с ним можно завязать узлом, и даже затянуть узел - все равно не сломается. Конечно, могут возникнуть микротрещины, но надо ведь как-то преодолеть страх перед "стеклом".

После этого можно сделать вывод - так ли страшно оптоволокно, как кажется. И разумеется, начать его применять в повседневной работе.

Часть 3. Глава 3

Три дилеммы.

Прежде чем приступить к работе по протяжке кабеля нужно твердо определиться со всеми техническими нюансами последующей работы линии. С оптоволокном нельзя поступать как с "медью" - сначала проложить кабель, а потом решать, какое оборудование использовать.

Главные критерии выбора можно свести к трем пунктам:

- Одномодовое или многомодовое волокно;
- Плотный или свободный буфер;
- Склеивать, сваривать, или использовать другие технологии.

Самое простое в данном случае - определиться с типом волокна. Технические особенности как "одномода" так и "многомода" подробно изложены в восьмой главе настоящей книги, и останавливаться еще раз на них не имеет смысла.

Однако необходимо определиться в каких условиях выгодно использовать тот или иной тип волокна.

Экономические предпосылки на лето 2003 года следующие: одномодовый кабель на 20-30% дешевле чем многомодовый, но конвертеры для него примерно втрое дороже. Однако, стоимость конвертеров постоянно снижается, и можно предполагать что разница в цене со временем будет уменьшаться.

Объяснение такой ситуации следующее. Традиционно для многомодового волокна в качестве излучающего элемента использовались светодиоды, а для одномодового - более дорогие лазеры. Но в настоящее время появились недорогие светодиоды и для одномода. Поэтому единственной причиной увеличения стоимости являются ужесточённые допуски как на сами источники, так и на фурнитуру в целом. Тем более, приёмники на одномод и многомод одинаковые.

В результате, прокладка многомодового кабеля на расстояния более 300-400 метров стала просто не выгодной. В то же время, нет предпосылок что одномодовый кабель вытеснит все другие виды - слишком велика уже инсталлированная база.

Поэтому представляется целесообразным использовать мультимод для оконечной междомовой разводки на длины 50-200 метров в качестве грозоустойчивой замены витой пары. Удобно использовать тонкий претерминированный (т.е. оконцованный коннекторами) кабель с волокнами в плотном буфере. В остальных случаях выгоднее использовать одномод.

Отличие между плотным и свободным буфером требует более обстоятельного разъяснения.

Какова самая главная задача конструкции оптического кабеля? Ответ тривиальный - защита волокна от повреждения. На память приходит многослойная громоздкая конструкция с множеством элементов не совсем понятного назначения. В недрах которой совсем теряется несколько тонких и хрупких волокон.

Но прогресс не стоит на месте. Уже давно в офисах прокладываются оптоволоконные системы с кабелями, которые мало отличаются по виду от обычной витой пары. Где грань между такими непохожими конструкциями?

Можно сказать, что первое и основополагающее различие - применение волокон в свободном или плотном буфере.

В конструкции со свободным буфером волокно защищено только базовым покрытием (обычно 250 μм) из полиакрилата (оргстекла). И расположено в пластиковой трубке (модуле) с внутренним диаметром, который намного больше, чем само волокно (около 5 мм).

Возможно наличие только одного волокна в модуле (так называемый неуплотнённый кабель), или нескольких - уплотнённый. Модули обычно изготавливают из полимера, сокращённо называемого ПБА. Он более твёрдый, чем полиэтилен, и не изменяет так сильно своих размеров от температуры.

Внутреннее пространство модуля обычно заполняется водоотталкивающим гелем, иногда капроновыми волокнами. Такая конструкция прекрасно изолирует волокно от

температурных колебаний, влаги и внешних механических сил, воздействующих на кабель.

Если составить несколько модулей, добавить трос, жесткий каркас, загнать под единую оболочку, или броню - получится как раз то, что массово применялось и применяется для прокладок под землей и по воздуху.

Рис. 3.1. Кабель в свободном буфере.

Один наполненный гелем модуль, диэлектрический, армированный, годится к применению при внешних работах.

К недостаткам можно отнести как высокую стоимость самого кабеля, так и сложность разделки (совершенно необходимы специальные кроссовые коробки, сплайсы, сварка, пигтейлы).

Другая техника защиты волокна - **плотный буфер** - использует непосредственную экструзию (выдавливание) пластика вокруг базового покрытия волокна. Такие конструкции способны выдерживать сильные ударные и давящие нагрузки без повреждения волокна. Плюс легкость и удобство работы, что, безусловно, дорогого стоит.

Минусы волокна с плотным буфером - низкая защита от влаги, напряжений и изменений температуры.

На первый взгляд все вышеизложенное позволяет рекомендовать однозначный выбор - свободный буфер для улицы,
плотный буфер для помещения.

Однако времена меняются. И все больше продавцов кабеля настойчиво предлагают плотный буфер для наружных прокладок. Это дешевле в прокладке, и намного удобнее в

оконцовке. При помощи несложных и относительно недорогих инструментов можно наклеить разъемы прямо на кабель, и обойтись без коммутационных коробок и сложных операций разделки и сварки.

И вообще - с такой оптикой можно работать почти как с обычной витой парой.

Рис. 3.1. Кабель в плотном буфере.

На рисунке влагоустойчивый кабель с плотным буфером 900μм, пригодный для внутренних и внешних работ. Температура использования от -40 до +80.

Без всяких сомнений, у оптического кабеля с волокнами в плотном буфере масса достоинств и большое будущее. Остается только недоверие к его сегодняшним эксплуатационным характеристикам. Уж больно хрупок и незащищен на первый взгляд. И не известно, как отреагирует на российский холод...

Что выбрать для строительства сети с массовыми прокладками "по открытому воздуху" между домами?

Если это многомодовый кабель для коротких линий междомовой разводки - скорее всего имеет смысл применить кабель с плотным буфером. Он удобнее в работе, легко проводится по стоякам слаботочной проводкии, занимает мало места в ящиках (и тем более не требует специальных кроссовых колодок).

Если нужно проложить многоволоконную магистраль на большое расстояние, выбор, вероятно, следует сделать в пользу модульной конструкции со свободным буфером. Это более долговечное и надежное решение в российских климатических условиях.

Хотя скорее всего, в будущем следует ожидать появления кабелей с волокнами в плотном буфере, которые будут более устойчивы к внешней среде, и их можно будет использовать для внешних работ без опасений.

Третья дилемма заключается в способе терминирования кабеля. Разъемы можно приклеивать, сваривать волокно кабеля с готовым пигтейлом, или использовать другие технологии типа сплайсов или обжима.

Споры по выбору технологии подчас не уступают религиозным войнам "Windows против Linux". поэтому и ответ будет похожий - лучший способ тот, которым хорошо владеют ваши монтажники.

Обоснованно считается, что сварка самый надежный и самый качественный способ. И не обязательно самый дорогой. Себестоимость сварного соединения очень низка. Требуется только термоусадочная гильза и... Дорогостоящий сварочный агрегат (от 3 до 30 тысяч долларов). Можно сказать, что оборудование окупится через несколько тысяч соединений.

Если такого объема работ нет, то можно пригласить специалиста (фирму) уже имеющую такой агрегат. Такая услуга обойдется от 10 до 30 долларов за волокно.

Однако, часто качество и надежность сварки избыточна для большинства линий домашних сетей. В этом случае можно использовать приклейку коннекторов или сплайсы. В принципе, данные способы пригодня для всех типов кабеля. Однако особенно выгодны, когда волокна в плотном буфере - в этом случае можно обойтись вообще без специальных ящиков, защищающих волокна и место соединения от повреждения.

При соблюдении технологии надежность и качество клеевого соединения мало уступает сварке, а стоимость заметно меньше. Плюс к этому, работу можно выполнять недорогим инструментом и своими силами. Часто это намного удобнее.

Соединение с использованием сплайсов дороже предыдущих способов (сплайс стоит около $10). Однако оно очень быстро и может выполняться монтажниками с самой невысокой квалификацией. Хотя сплайсы первоначально предназначались для быстрого (и временного) ремонта кабелей, сейчас производители соединений дают длительную гарантию на свои изделия (до 10 лет). Поэтому немагистральные линии вполне можно терминировать таким способом.

Кроме этого, существует несколько фирменных технологий обжимного присоединения разъемов. Эти способы быстры, эффективны, но дорогостоящи. Поэтому на российском рынке применяются редко.

На этом можно закончить краткое перечисление способов терминации кабеля и перейти к подробному рассмотрению каждой технологии в отдельности.

Часть 3. Глава 3

Клеевое соединение. Подготовка.

Для небольших, но постоянных объемов работ (например 20-30 волокон в месяц) приклейка коннекторов скорее всего будет наиболее удобным способом. Свой сварочный аппарат в этом случае покупать не рентабельно, а заказывать 1-2 раза в неделю работы на стороне - дорого и (или) хлопотно.

Вопреки распространенному мнению, качественно выполненная склейка практически не уступает по своим потребительским свойствам сварному соединению. Точнее сказать, в последнем случае к волокну кабеля присоединяется пигтейл - отрезок волокна с разъемом, который был наклеен в заводских условиях. Конечно, промышленная полировка лучше "наколенной" (если она на самом деле сделана на хорошем оборудовании). Но разница может быть совершенно несущественной для линий "междомовой" или "межрайонной" длинны.

Так что основными недостатками клеевой технологии нужно признать большое время работ (в несколько раз дольше сварки), и необходимость высокой квалификации монтажников. А основным достоинством - возможность выполнения работ своими силами, в удобное время. И именно этому посвящен следующий материал.

Предположим, конец оптоволоконного кабеля уже заведен в помещение, где он должен быть разделан.

Первое, что нужно сделать - подготовить цивилизованную рабочую площадку (насколько это реально). Желательна положительная температура (но промышленный тепловой пистолет позволит обойтись и без этого), хорошее освещение, и хоть что-то, напоминающее стол. Теоретически реальны варианты, предусматривающие установку палатки прямо на крыше здания, но желательно обойтись без такой экзотики.

Внешняя оболочка

Кабели бывают разные по конструкции. Простейший принцип снятия внешней оболочки - сделать кольцевой надрез на всю глубину изоляции, включая бронепокровы, затем "сломать" оболочку и стянуть её через свободный конец. Надрез удобнее всего делать с помошью кабельного ножа с регулируемой высотой выступания лезвия, но вполне можно обойтись и обычным. Так как оголить нужно не менее метра волокон, операцию придется повторить несколько раз (по 20-30 см).

Если бронепокров представляет собой стальную ленту или стальные проволоки, сделать кольцевой разрез будет невозможно. В этом случае снятие внешней оболочки можно делать в следующем порядке. Ножом срезать полиэтиленовую наружную оболочку вдоль кабеля на необходимую длину. Затем снять ее, расплести проволоки, и хорошими кусачками перекусить их у основания (осторожно! Как правило используется проволока, прошедшая термообработку, иначе говоря "калёная").

В случае возникновения трудностей при снятии кусков внешней оболочки на уже зачищенном участке можно удалить ненужные внутренности кабеля (силовой элемент, пустые оптические элементы, замотанные ленты и нити). Силовой элемент отрезать "под корень" нельзя, его очень желательно в недалёком будущем надёжно закрепить.

Если кабель имеет плотный буфер, то после снятия оболочки можно сразу приступать к наклейке разъемов, как это будет описано в следующем параграфе.

Но для кабеля с гидрофобным заполнением все только начинается. Так как гидофоб является немного загущенным маслом, самый первый шаг - герметично изолировать остаток кабеля от места разделки. Это можно сделать изолентой. Затем можно протереть несколько раз модули газетой или подобной мягкой бумагой. Далее нужна ветошь и жидкость для растворения гидрофоба.

Рис. 3.3. Кабель со снятой внешней оболочкой.

На фотографии хорошо видны модули. Это пластиковые трубки, обычно заполненные гидрофобным (отталкивающим влагу) гелем, в которых находится оптическое волокно (или несколько волокон).

Для очистки модулей снаружи как правило используется уайт-спирит, реже бензин, ацетон или подобные растворители для ЛКМ (они слишком сильно пахнут). Хорошо подходит фреон (хладон) - запаха нет, а чистит за один проход.

Но внимание! Всё вышеописанное не относиться к гидрофобу внутри оптического модуля. Его сильными растворителями чистить нельзя, только спиртом (изопропиловым или этиловым). Спирт рекомендуется применять с минимальным содержанием воды. Хорошо подходит этиловый из аптечных бутылочек с надписью "Раствор медицинский антисептический".

После снятия грязной внешней оболочки с кабеля и очистки модулей необходимо тщательно вымыть руки. Волокно грязи не любит.

Модули

Модуль можно зачистить скальпелем (лезвием, острым ножом), если аккуратно надрезать с открытого конца вдоль модуля. При кольцевых нардрезах есть очень большой шанс перерезать волокно, хотя при помощи стриппера это можно сделать без риска.

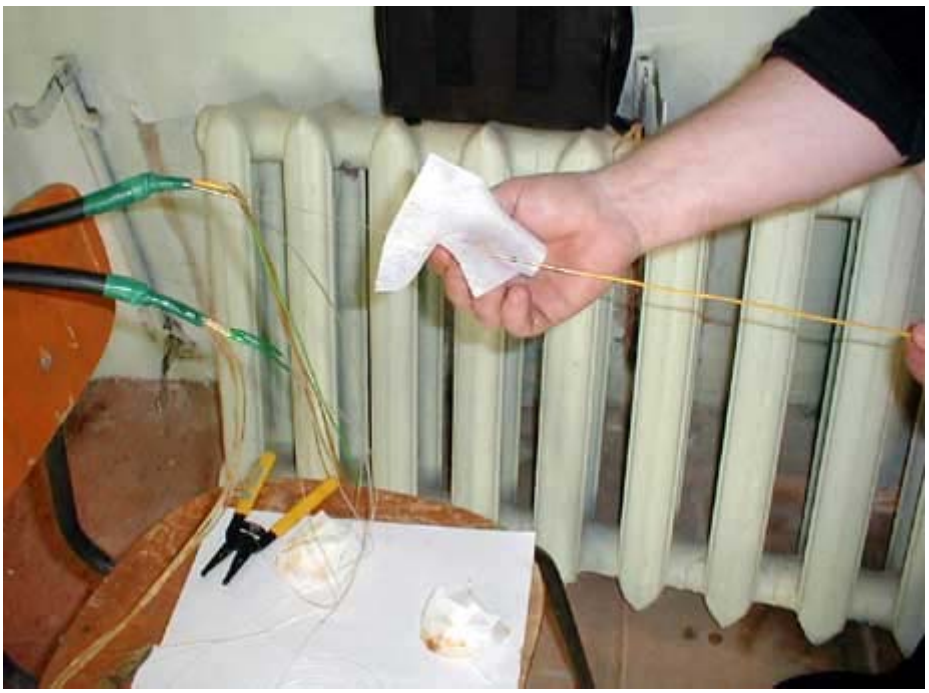

Рис. 3.4. Снятие модуля.

Оголять нужно столько, сколько нужно для удобной работы. Если конец кабеля лежит на столике (пусть и импровизированном), то может хватить и 30 см. Хотя не помешает запас на случай неудачной приклейки, под укладку в коробку, и т.п. Хоть по нормам и положено оголять не менее 2 метров, но, на мой взгляд, это совершенно излишне.

Если конец кабеля закреплён под 4-х метровым потолком, то лучше зачистить его весь, чтобы не делать полировку на весу.

Волокно необходимо протереть от остатков геля. Это можно сделать любой ветошью или обычной салфеткой. Специальные безворсовые салфетки имеет смысл использовать только для протирки торцов разъёмов.

Рис. 3.5. Разделанное волокно.

Оголенным волокно оставлять, конечно, нельзя. Как уже говорилось выше, его может разрушить влага даже несмотря на защитное покрытие (буфер). Да и механической прочности перед укладкой в коробку прибавить не помешает.

Для этого используется тонкая пластиковая трубочка - кембрик. На фотографии ее можно видеть на стуле, свернутой в кольцо (почти не видно, тонкая и прозрачная). Для более легкого проталкивания волокна в кембрик в последний набирают спирт, по инструкции даже существуют специальные приспособления. Видеть их в работе не удалось. Реальность проще. Наверно, несложно догадаться, чем засасывается спирт в кембрик на практике.

Стык кембрика и модуля уплотняется термоусадочной трубкой (на фото зеленая трубочка, лежащая на стуле). При ее отсутствии подойдет и изолента - при наличии навыка работы с ней.

В качестве кембрика так же можно использовать снятую оболочку модуля, желательно, отмытую спиртом от гидрофоба. Но как правило, она слишком жесткая, и неудобная в работе. Еще один вариант - китайская термоусадка, но она стоит дороже обычного кембрика.

Рис. 3.6. Волокна с надетым кембриком.

Шприцы, лежащие на стуле, содержат в себе клей. Прозрачный однокомпонентный набран из АМПовского тюбика (лежит на стуле). Два других с двухкомпонентным клеем от Lucent. Он не портится длительное время, и его так и носят от объекта к объекту - в шприцах.

Снятие буфера

Голубое пластиковое устройство сложной формы - стриппер - служит для снятия буфера, и его работу можно видеть на рисунке ниже.

Рис. 3.7. Снятие буфера с волокна.

Несмотря на игрушечный вид, стоимость устройства около $100. При малом опыте использования, возможны царапины на волокне, но для этого надо специально стараться.

Вообще, инструмент для снятия полиакрилатного буфера бывает нескольких видов. На мой взгляд, самый удобный инструмент типа "Miller" - похож на обычный стриппер для зачистки изоляции медных кабелей, но содержит калиброванную под оптоволокно дырку. После некоторой тренировки им возможно снимать все типы полиакрилата и буферных покрытий 0.9 мм, включая отечественные, самые жесткие.

Стрипперы типа "No-Nik" и разнообразных прищепок (подобно показанной на рисунке) удобны для мягких покрытий, но не так универсальны. Так же существует термомеханический стриппер "УСП", производимый Владимирским заводом "Элетех", стоимостью $100.

Есть и кустарная технология снятия буфера. Для этого надо волокно опустить на некоторое время в ацетон (желательно нагретый, это ускоряет дело). После такой процедуры буфер снимается просто ногтем.

Ну, а если руки очень опытные, можно снять буфер и с помощью бритвочки. Особенно хорошо для этого подходит старая добрая "Нева" ("Жиллет" не годится).

Проверка волокна.

Последнее, что стоит сделать на стадии подготовки - проверить как волокно входит в разъем. Конечно, если используется качественный импортный кабель, и разъемы известной фирмы - это скорее всего лишняя операция. Но на практике, домашние сети предпочитают дешевизну качеству.

Поэтому желательно **перед** манипуляциями с клеем сначала попробовать засунуть волокно в чистый капилляр разъёма. Были случаи, когда это сделать не удавалось

(эллипсоидное, неравномерное по сечению волокно - пожалуй самый страшный брак отечественных кабелей).

Многомод должен входить в капилляр без усилий. Одномод может и с усилием, но разумным. Если вталкивать слишком сильно, волокно может обломиться. Осколки удаляются специальной калиброванной проволокой (125 мкм).

В совсем тяжелых случаях (некачественных коннекторах) рекомендуется проверять капилляр разъёма сначала проволокой, еще до волокна.

Часть 3. Глава 3

Клеевое соединение. Приклейка и полировка.

После разделки кабеля и проверки коннекторов можно приступить к наклейке коннекторов.

Самое главное в этом процессе - сам клей. Поэтому нужно для начала сказать о нем несколько слов.

В общем случае клей для оптоволокна должен быть:

1. Прочным;
2. Водостойким;
3. Не давать усадки;
4. Не давать пузырей;
5. Медленно схватываться в обычных условиях и быстро – в специальных.

Кроме обязательных физических условий, на сегодняшний день правила выбора клея можно расширить следующими пунктами:

1. Клей должен быть эпоксидный двухкомпонентный;
2. Клей должен смешиваться из компонентов 1:1;
3. Клей должен быть высокотемпературной сушки;
4. Желательно изменение цвета клея после застывания.

На практике, мне пришлось столкнуться с двумя типами - Lucent'овским двухкомпонентным, и AMPовским однокомпонентным. Так же известны двухкомпанентные TRA-BOND F123, H05-100-R2 производства FIS, эпоксидная смола EpoTek 353ND...

Первый показался намного более практичным, особенно для неопытного склейщика. Не портится, можно пользоваться шприцами (в которых его удобно хранить) хоть полгода. Так же он медленнее высыхает при обычной температуре, а значит больше шансов исправить ошибку.

Однокомпонентный AMP по удобству работы не далеко ушел от "супер-клея". Похож и по запаху, и по скорости высыхания. Набирать его в шприц можно только непосредственно

перед работой. Тюбик с ним показан на одной из фотографий предыдущего обзора. После работы неиспользованные остатки можно смело выкинуть. Хотя, при массовой склейке в удобных условиях (например, кросс линий на 100 в офисном помещении), AMP может оказаться удобнее и быстрее в работе.

Вообще, фирменных видов клея существует не один десяток. Поэтому не имеет смысла пытаться их все описать - все равно придется использовать то, что есть у ближайшего продавца. Да и работа от типа клея зависит не слишком сильно.

Стоит специально отметить, что на крайний случай можно обойтись вообще без специального клея. В опытных руках сгодится "Супер-клей" китайского или отечественного производства. Хотя он не водостойкий, и схватывается при любой температуре (надо все делать быстро и с первой попытки).

Второй вариант - эпоксидная смола. Особенно, если ее развести ацетоном и добавить пластификатора (касторки). Но это процесс тонкий, непредсказуемый, и использовать его стоит только в совсем безвыходной ситуации.

Склейка

Предположим, что двухкомпонентный клей выбран, коннектор проверен, и нужно приступать к работе.

Рис. 3.8. Нанесение клея на коннектор.

В калиброванное отверстие коннектора клей продавливается шприцом так, что бы с наружной стороны выступила небольшая капелька (это доказывает, что весь канал заполнен).

Рис. 3.9. Нанесение клея на волокно.

Затем наносят клей на зачищенное волокно. В случае, если используется двухкомпонентный состав, на коннектор наносят клей, а на волокно - отвердитель. Или наоборот - разницы нет никакой.

Главное не забыть надеть заранее на волокно пластиковый хвостовик-чехольчик. А после него - обжимную втулку. После приклейки коннектора это будет уже невозможно.

Далее приходит черед первой, но не последней операции, которая требует твердой руки и отсутствия похмельного синдрома. Можно заранее потренироваться на вдевании нитки в иголку.

Рис. 3.10. Ввод волокна в коннектор.

Волокно медленно и аккуратно вводится в коннектор. Зазоры "нулевые" (а на одномоде и того меньше), вылезают все огрехи. Начиная от плохо снятого буфера, и кончая "эллипсным" волокном.

Именно на этой стадии удобны двухкомпонентные клеи. Всегда можно остановиться, прочистить канал, и начать заново. Если при ошибке клей успеет "схватиться", то коннектор (2-3 доллара) можно выкинуть.

Вводить волокно нужно до тех пор, пока буфер не упрется в край. Это сразу чувствуется. Больше чем нужно протолкнуть все равно не удастся.

Дальше нужно дождаться полимеризации клея. Можно оставить работу до следующего дня, можно нагреть разъемы в специальной муфельной печке (ее роль с успехом заменяет тепловой пистолет). Кстати, в этом процессе более удобны металлические разъемы ST. Пластиковые SC при неравномерном или слишком сильном нагреве могут покоробиться.

После высыхания клея можно приступить к следующей операции.

Скалывание

Пожалуй, самая ответственная часть всего процесса. Ошибка приводит к порче коннектора и возвращению к началу всего процесса.

Рис. 3.11. Скалывание.

Суть процесса проста - отрезать (сколоть) хвостик волокна, торчащий из коннектора для последующей шлифовки. Сколоть больше - будет каверна, которую не исправить. Оставить много - волокно может неровно отколоться при начале шлифовки.

Главный инструмент так и называется - "скалыватель". О них написаны целые трактаты в прайсах. На фото, например, стеклянный с алмазным напылением. Стоит что-то в районе

400 долларов. Приходилось использовать и другой - с твердосплавным наконечником (около 200 долларов). Особого отличия не увидел - но профессионалы на стеклянный не нахвалятся.

Впрочем, в скалывателе нет ничего хитрого. Если все сделано правильно, и на конце разъема есть микрокапля (выдавленная из канала), то скалывать можно почти любым предметом, способным нанести дефект на стекло. Подойдет хорошо заточенная керамическая пластинка, заготовка для токарного резца из твёрдого сплава, даже острый нож или бритва.

В этом случае более чем вероятно, что при шлифовке кривизна скола "уйдет" в каплю клея, и не дойдет до торца коннектора. Но надо отметить, что при большой капле шлифовать торец придется заметно дольше.

После нанесения дефекта на волокно, движением перпендикулярным оси волокна, пальцами движением вдоль волокна аккуратно снимаем обломок. Его нужно аккуратно убрать в заранее приготовленную коробочку, так как из обломков получаются отличные занозы. Их не видно даже под лупой и избавление от них происходит только естественным путём.

Полировка

Если после скалывания кончик волокна остался заметно длинный - попробуйте для начала "снять" лишнее об шлифовальную бумагу "на весу", легкими (но не резкими) касаниями.

Из инструментов понадобятся:

- Оправка, причем крайне желательна именно металлическая. Пластиковую часто "наволакивает"". Хотя, при цене 5 баксов против 50 стоит и подумать о выборе.
- Стекло-столик. Стекло должно быть, разумеется, полированным. Что бы не мучаться с поиском (не думаю, что его легко купить отдельно), можно использовать качественное зеркало (но ни в коем случае не использовать оконно-тепличный вариант). Размер стекла по вкусу.
- Полировочная пленка, она же шкурка. Продается по цене около 1-2 долларов за большой лист (хватает на 4-8 коннекторов). Бывает нескольких типов. Мне пришлось работать с "рыжей" и "зеленой" от Lucent. Первая "крупная", 10 микрон. Вторая для окончательной доводки, с зерном в 1 микрон.

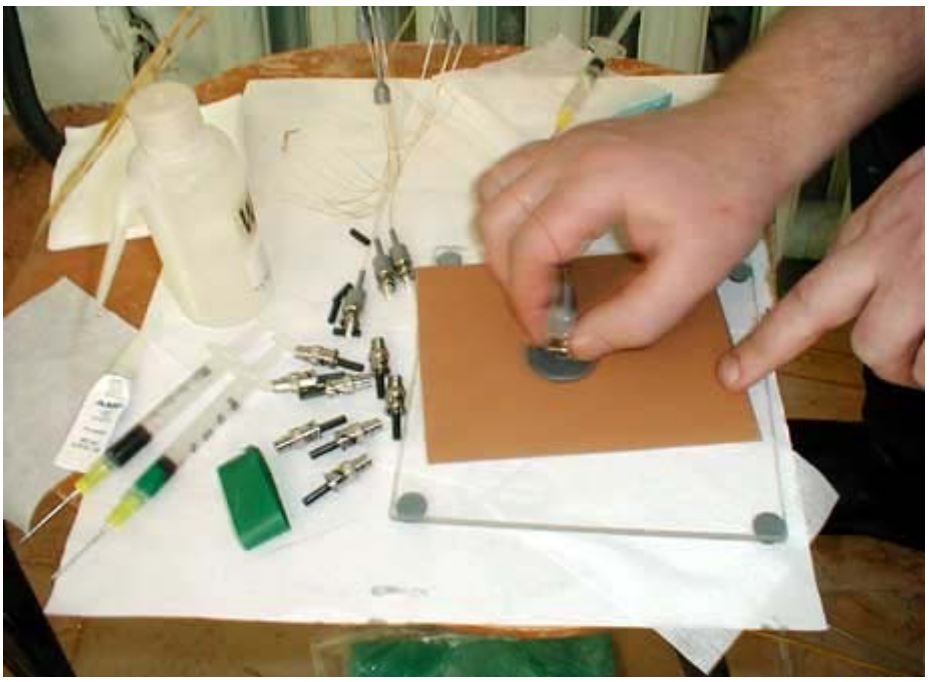

Рис. 3.12. Первичная полировка.

Перед вставлением коннектора в оправку, ее надо хорошо протереть, особенно отверстие. Допуски настолько малы, что коннектор в грязное отверстие оправки просто не войдет, или хуже того, застрянет на половине.

Работа ведется движениями, похожими на "восьмерку" или "бесконечность". Кому что ближе. Кругами или "туда-сюда" полировать нельзя.

Экономить на бумаге можно - внешне ее износ не виден. Но работа при этом резко замедляется. Снять с торца коннектора слой больше нормы невозможно - керамику (ферул) "рыжая" и "зеленая" шкурка не берет. Остается вероятность сделать каверну на торце волокна, но для этого нужно очень сильно постараться.

Рис. 3.13. Окончательная полировка.

После грубой "рыжей" коннекторы обрабатываются на тонкой "зеленой" пленке. Если все сделано хорошо, то процесс быстрый и не рискованный.

Момент перехода операций, и окончательной готовности, определяется при помощи микроскопа. Можно, конечно, обойтись методом "тыка". Но на мой взгляд именно микроскоп совершенно необходим в сумке инструментов. Это последнее устройство, без которого можно обойтись, несмотря даже на его относительно не маленькую (около 150 долларов) цену.

Рис. 3.14. Виды дефектов. Слева направо: перекос, глубокий скол, недостаточно обработанный торец.

Картинка, которую можно видеть в микроскоп, не слишком разнообразна. Идеальной будет равномерно темная (или светлая) внутренняя окружность. Если проверять работу по ходу полировки почаще, то все становится понятным и очевидным.

Если небольшая каверна не выводится полировкой, применяют специальную алмазную шкурку, которая может снимать слой с керамического торца разъема. Причем, работа ведется с водой (в отличии от полировки, которая делается только "всухую").

Рис. 3.15. Шлифовка ферула.

Теоретически, можно вывести даже миллиметровый скол. Но работа долгая и утомительная. И если "не получилось" проще приклеить другой коннектор. Хорошо, что применять такой способ приходится не часто.

Укладка в коробку

После приклейки можно, наконец, уложить все в коробку. Подсоединить коннекторы к оптическим соединителям. Разложить волокна. Крепко закрепить оболочку кабеля на коробке (делали мощными капроновыми стяжками).

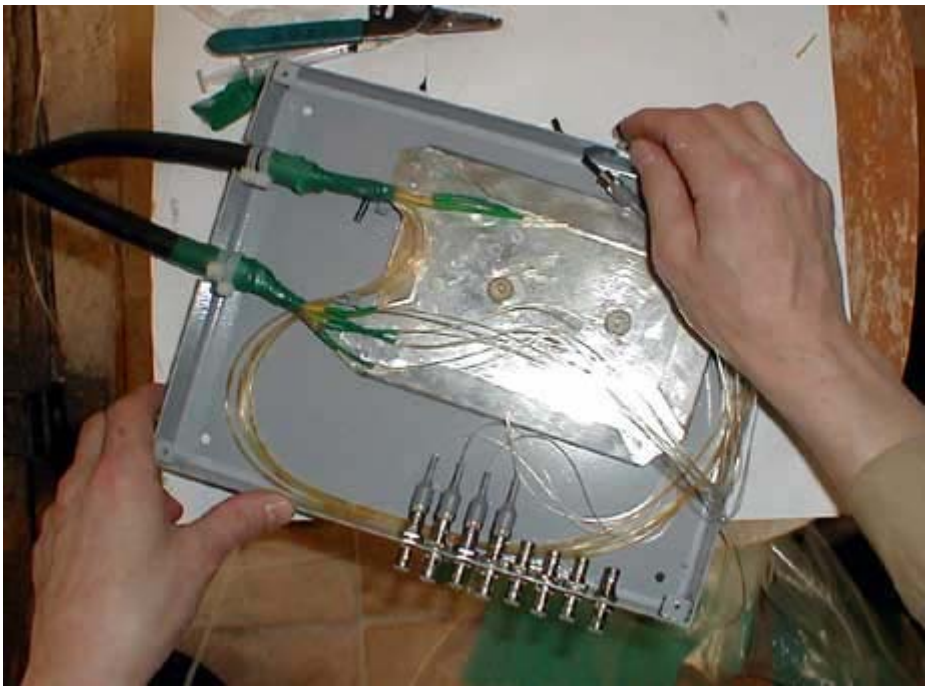

Рис. 3.16. Укладка в коробку.

На фотографии показана недорогая полусамодельная коробка. Но внешнему виду и удобству она конечно уступает фирменным аналогам, но зато стоит менее $20.

Вообще, подойдет практически любая коробка (вообще можно смонтировать кабель на стене и залить монтажной пеной). Но нужно соблюдать следующие условия:

1. Кабель должен быть надёжно закреплён как оболочкой, так и силовым элементом;
2. В разделанное место не должна попадать вода и пыль;
3. В коробке должно быть места столько, чтобы выдержать все нормы на максимальный радиус изгиба кабелей и зачищенного волокна.

Кстати, неплохие коробки получаются из электрошкафчиков. Места много, есть кабельный крепёж. И сертификаты то же в наличии.

Определить, какое волокно откуда, по цвету оплетки обычно невозможно. Вот так Российские производители экономят на красителе. Страшного в этом ничего нет. Волокна надо "просветить" и отмаркировать.

Сделать это можно при помощи обычного фонарика, а в его отсутствие хватит и светодиода ближайшего хаба. Свет, направленный с противоположного конца кабеля, отчетливо виден невооруженным глазом как яркая точка на торце коннектора. Еще удобнее смотреть на это в микроскоп - в этом случае можно просветить волокно даже спичкой.

Заодно будет понятно, не было ли сломано волокно где-то в процессе приклейки коннекторов.

Если остались лишние разъемы, или большие петли волокна - их обязательно нужно закрепить. На крайний случай - даже скотчем.

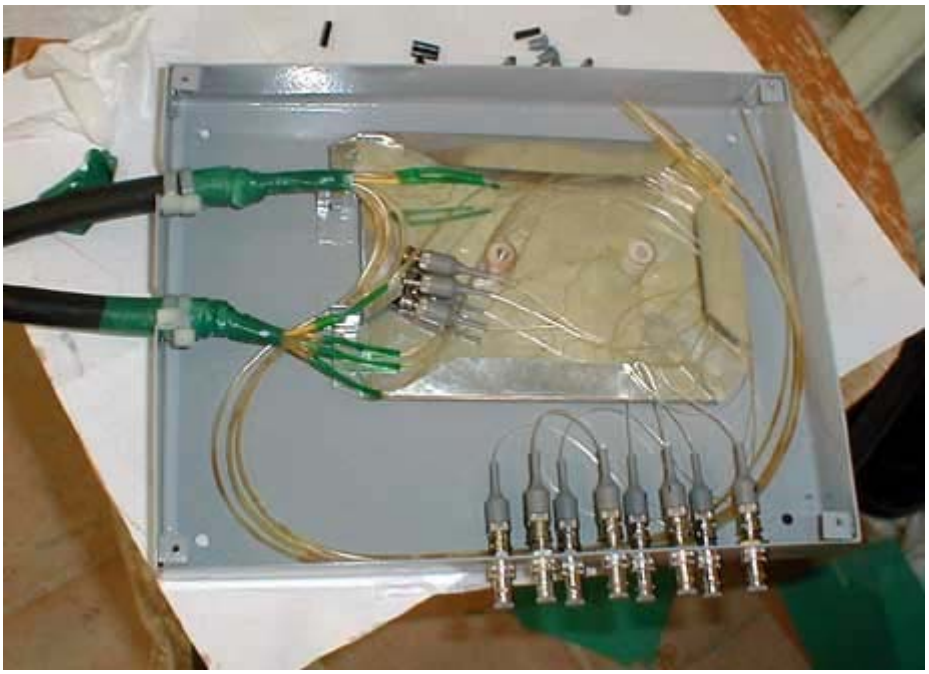

Рис. 3.17. Приклейка коннекторов закончена.

Далее остается закрыть коробку крышкой, и повесить на стену в заранее выбранном месте.

Список необходимого инструмента

Вот примерный набор инструмента, который нужен для клеевого монтажа разъемов на оптоволокно.

1. Кабельный нож для поперечной и продольной надрезки оболочки кабеля. Заменяется обычным.
2. Тросокусы для борьбы с силовыми элементами. Заменяется хорошими кусачками и пассатижами
3. Стриппер оптического модуля 3 мм. Ищется у электромонтажников, они им провода зачищают. Заменяется скальпелем.
4. Стриппер оболочек волокна (рекомендуется CFS-2). Заменяется бритвой.
5. Ножницы для резки упрочняющих нитей. Заменяются бытовыми с плотно прилегающими и достаточно острыми лезвиями.
6. Муфельная печь. Заменяется тепловым пистолетом.
7. Скалыватель. Заменяется твердосплавным или керамическим резцом.
8. Оправка и шкурки для полировки. Заменять не целесообразно, так как стоимость все равно небольшая.
9. Микроскоп. Желательно не заменять.
10. Универсальный кримп для обжатия коннекторов (нужен не для всех видов кабелей).

Часть 3. Глава 3

Сварка оптоволокна.

Нет сомнения, технологии соединения оптических волокон непрерывно совершенствуются. Повышается надежность, снижается стоимость, упрощается инструмент... Но не смотря ни на все инновации сварное соединение по прежнему остается самым качественным и самым недорогим способом.

Но есть одна оговорка - высокая стоимость оборудования для сварки волокон. На этом факте придется остановиться подробнее.

Физический принцип сварки прост. Нужно очистить волокно от буфера, обеспечить его ровный скол (с точностью до 1 градуса). Зафиксировать в сварочном аппарате. Затем сблизить торцы волокон, оплавить их, после чего расплавить с одновременным сведением. Но когда дело доходит до мелочей, становятся видны сложности.

Во-первых, нужен очень ровный скол волокна. Если для клеевого соединения в качестве скалывателя можно использовать даже бритвочку (а приличный инструмент стоит от $50-100), то для сварки этого совершенно не достаточно. Скалыватели напоминают маленькие станки, и стоят от нескольких сотен до 2-3 тысяч долларов.

Во-вторых, торцы волокон перед сваркой нужно очень точно совместить. В принципе, это можно сделать и механически, при помощи микроскопа и микровинтов. Но юстировка в двух плоскостях дело не простое, трудоемкое, и не слишком точное. Поэтому механические аппараты уже давно не применяются, они вытеснены дорогими автоматическими или полуавтоматическими устройствами.

Большинство из современных моделей использует систему выравнивания волокон по изображению в параллельном пучке света (PAS-система). При таком методе юстировки волокна освещаются сбоку параллельным пучком света так, что оболочка и сердцевина фокусируют свет, действуя как цилиндрические линзы. Таким образом формируется изображение, на котором видны границы сердечника (это особенно важно) и оболочки волокна, что позволяет определить эксцентриситет в каждом из волокон.

Такая система особенно распространена в аппаратах японских производителей. Она используется и для грубой юстировки, и для тонкой подстройки волокон.

У европейских производителей PAS-система используется для грубой настройки. Тонкая юстировка у аппаратов фирмы Siemens осуществляется по максимуму мощности излучения, передаваемого через сварное соединение (LID-система). У аппаратов фирмы Ericsson тонкая настройка осуществляется по тепловому изображению сердцевины и оболочки в дуге электрического разряда.

И в-третьих, кроме проблемы выравнивания есть сложности при сварке разных типов волокон. Это в общем менее важно, чем юстировка, но длительность и интенсивность электрической дуги то же имеет значение.

Более того, на самых современных моделях применяются сложные алгоритмы повышения качества соединения. Например, оси волокон предварительно разводятся на такое

расстояние, на которое (согласно компьютерному расчету) надо развести оси сердцевины волокон для совмещения их силами поверхностного натяжения при сварке.

Такие меры позволяют достигать минимальных потерь на соединение на сварном стыке (порядка 0,02 дБ), что в десятки раз меньше, чем при использовании других технологий.

Как ни странно на первый взгляд, сварка более качественна, чем наклейка разъемов, при которой само промежуточное соединение отсутствует. Проблема тут в сложности ручной полировки торцов разъемов. Для обеспечения точности работ нужен мощный 400-кратный микроскоп, измеритель обратных потерь, специальные пасты, и желательна химическая полировка на последней стадии. Кроме этого, при "полевой" работе затруднительно соблюдение геометрии керамического наконечника.

Однако, все вышесказанное имеет большое значение только для серьезных магистральных каналов. Но в случае небольшой разводки масштаба микрорайона преимуществом "в потерях" сварка не обладает.

Поэтому основными достоинствами сварки будет долговечность, надежность, и невысокая стоимость соединения (если не учитывать стоимость оборудования). Учитывая появление на рынке б/у сварочных аппаратов стоимостью менее пяти тысяч долларов, сварка становится вполне привлекательным способом при активном использовании оптоволокна.

Особенно удобна сварка при соединении кабелей в муфтах (т.е. там где стандартные разъемы просто не нужны). Именно такой случай рассмотрен в следующем примере.

Следующий чердак можно назвать кошмаром сетестроителя, но именно на нем нужно установить муфту на оптоволоконный кабель.

Рис. 3.18. Кошмар сетестроителя.

Разделка кабеля делается вполне традиционным способом. Снятие буфера то же. Но вот для скалывания применялся следующий аппарат (стоимость около $1500):

Рис. 3.19. Прецезионный скалыватель.

Работа с таким инструментом проста и по сути не требует навыков. Скалывать "взводится", в него вкладывается конец волокна. Затем пружина освобождается, нож падает, и... Скол готов.

Рабочее место в данном (экстремальном) варианте было сделано из подручного материала.

Рис. 3.20. Рабочее место сварщика.

Вместо стула - ведро. Стол - кусок ДСП, установленный на 4 стопках кирпичей. Смотреть страшно. Кругом голубиный помет. И на всем этом стоит аппарат за 18 тысяч долларов.

Все кабеля перед сваркой заведены в муфту-треххвостку, их оболочки намертво закреплены на специальной площадке. Модули сняты. После этого работа идет только с волокнами.

Сварка на автомате Fujikura выглядит не романтично. Волокно вкладывается в аппарат, фиксируется простыми зажимами, и... все. Совмещение, сварка, проверка - все на автомате, да еще с показом процесса на жидкокристаллическом мониторе. Главное, не забыть вовремя надеть трубочку защитной гильзы.

После сварки автомат проверит прочность соединения на разрыв и приблизительно измерит качество шва.

Конечно, перед работой есть этап настройки на волокно, но он не занимает много времени.

После сварки место стыка волокон герметизируют гильзой (термоусадочной трубочкой, с вставленным внутрь для жесткости металлическим штырьком). Для нагрева гильз на сварочном аппарате предусмотрено специальное приспособление-печка.

Рис. 3.21. Муфта изнутри.

Затем получившуюся гильзу аккуратно укладывают в гнездо муфты, если такое есть в наличии. Самодельщики - просто приклеивают на скотч. Результат не так красив, но муфту можно сделать из первой попавшейся герметичной коробки. Но вообще говоря, серийные муфты стоят не дорого (от $30), и заменить их чем-то сторонним без катастрофической потери качества сложно.

Желательно только промаркировать волокна (даже если муфта неразборная, она служит десятки лет, за это время может случиться всякое). Не помешает положить внутрь мешочек с силикогелем для поглощения влаги.

Герметизируется вся конструкция при помощи толстой пластиковой трубы, и термоусадочных чехлов с отводами под кабеля, закрывающих края. Изнутри чехлы покрыты специальным клеем. При нагревании тепловым пистолетом все схватывается намертво. Главное не перегреть, не расплавить сам кабель.

Рис. 3.22. Готовая муфта.

Так выглядит готовая конструкция. При достаточно неприглядном внешнем виде у соединения меньше шансов пострадать от рук вандалов, поэтому крепеж выполнен нарочито небрежно и неаккуратно.

Часть 3. Глава 3

Прочие технологии монтажа оптических разъемов.

Кроме традиционной сварки и приклейки разъемов существует более полудюжины "фирменных" технологий монтажа оптических разъемов и (или) соединения волокон. Следующий материал представляет собой краткий обзор некоторых из них.

Hot Melt (размягчение при нагревании) от фирмы 3M

Данная технология наиболее (из всех остальных) близка к "классической" приклейке разъемов. Отличие заключается в использовании специальных разъемов, предварительно заполненных специальным компаундом еще на стадии производства.

При нагревании до 80C компаунд размягчается, и в него можно ввести очищенное заранее волокно. После остывания оно прочно фиксируется в канале разъеме, и может быть отполировано обычным (вернее упрощенным из-за отсутствия остатков клея) способом.

Для удобства работ 3M предлагает даже специальную печку на батарейках, но скорее всего можно обойтись и обычным тепловым пистолетом.

Однако, достоинства - многоразовое использование разъема, отсутствие операции склейки и ускорение полировки - направлены в основном на экономию времени, при заметном росте себестоимости соединения. Плюс к этому появляются недостатки (продолжения достоинств) - нестойкость разъема при повышенной температуре (80С в общем не слишком много для узла на жаркой крыше) и сложность скалывания волокна (спасительной капельки клея в этом случае нет).

Случаев использования данной технологии в домашних сетях неизвестны, хотя, в принципе, Hot Melt должен быть достаточно удобен для этой области применения. Возможно, останавливает стоимость разъемов, но скорее, дело в малой известности метода.

Cold Cure (холодная полимеризация), Easy Fit (легкая вставка), Fast Epoxy (быстрая эпоксидная смола)

Фирменные способы наклейки разъемов от BICC Brand Rex, Huber&Sunnor, AT&T и AMP практически идентичны с обычной технологией. Главное отличие - использование специальной эпоксидной смолы с холодной полимеризацией.

Исключение из работы нагревания и охлаждения конечно ведет к ускорению работы, но не на столько, что бы вытеснить остальные способы приклейки. К минусам можно отнести быструю фиксацию волокна. Малейшая ошибка ведет к непоправимой порче разъема.

Fiber Grip (зажим волокна, Amphenol), Crimplock (фиксация обжимом, 3M), Light Crimp (легкий обжим, AMP)

Данные технологии существенным образом отличаются от представленных выше. При монтаже разъемов не используется никаких клеящих или связывающих составов. Фиксация волокна в сердцевине разъема осуществляется при помощи специальных механических элементов.

Технология Fiber Grip в качестве механического фиксирующего элемента использует цанговый зажим, который в процессе монтажа запрессовывается в тело разъема вместе с волокном и прочно его фиксирует. Недостаток метода также заключается в использовании металлического фиксирующего элемента (цанги), которая имеет отличный от волокна коэффициент теплового расширения. Кроме этого металлический элемент при монтаже может повредить волокно, особенно если оно имеет нестандартные размеры (что часто бывает с отечественными волокнами).

При использовании Crimplock оптическое волокно вставляется в тело разъема, внутри которого расположен металлический фиксирующий элемент. Специальное приспособление, называемое активатором, закрывает этот элемент и прочно фиксирует волокно внутри разъема. Эта технология имеет самый узкий рабочий температурный диапазон (от -10С до +60С) из перечисленных. Дополнительное ограничение на использование накладывает сложная и дорогая оснастка.

В отличии от Fiber Grip и Crimplock в технологии Light Crimp основным фиксирующим элементом являются три шарика из пластифицирующего материала, расположенные в

основании сердечника разъема в виде устойчивой тройки. В момент запрессовки в разъем специального плунжера (который также выполняет вспомогательную фиксирующую функцию), он своим торцом раздавливает эти шарики и запрессовывает их в специальное коническое углубление.

Коэффициент теплового расширения полимера, из которого изготовлены шарики, близок к волокну, в результате условия эксплуатации разъемов составляют диапазон от -40С до +85С. Кроме того, эти разъемы можно устанавливать как на "голое" волокно, так и волокно в буфере 250 мкр, 900 мкр, и даже 2,5 или 3 мм.

Можно сказать, что обжимные технологии серьезно упрощают монтаж оптических кабелей. Но они не устраняют самый медленный и сложный этап - скол волокон и полировку разъемов. Поэтому, на мой взгляд, для домашних сетей с их небольшими объемами работ (нет требований к скорости), и небольшими финансами данные технологии не слишком удобны. Если к этому добавить частое использование низкокачественных отечественных волокон, то можно сказать, что недостатки технологий при данном применении превалируют над достоинствами.

Light Crimp Plus

Технология Light Crimp Plus разработана фирмой AMP, и является дальнейшим развитием технологии Light Crimp. Главное отличие заключается в том, что внутри сердечника разъема в заводских условиях установлен кусочек уже отполированного волокна и залит специальный гель. В результате из процесса монтажа исключается весь цикл скола и полировки волокна, со всеми вытекающими экономическими последствиями.

К недостаткам этого типа разъемов можно отнести наличие в теле разъема дополнительной неоднородности в виде соединения двух волокон, но на самом деле общий коэффициент затухания на разъеме не превышает 0,2 дБ, что характерно и для обычных клеевых соединений.

Так как эта технология является наиболее отличной от клеевых методов, остановимся на ней немного подробнее.

Можно смело сказать, что основное для Light Crimp Plus - это набор инструментов (ну и конечно специальные разъемы).

Рис. 3.23. Комплект инструментов.

К специфическим устройствам можно отнести обжимные многофункциональные клещи, и держатели для разъемов (без него сложно вводить разъем со вставленным волокном в клещи). Скалыватель типа прищепки то же оригинален (имеет разметку), но такая же конструкция используется для сплайсовых и (реже) сварных соединений.

Ниже представлен один из моментов обжима Light Crimp Plus.

Рис. 3.24. Обжим Light Crimp Plus.

Нельзя сказать, что работа с Light Crimp Plus проста, но после 2-3 дневного обучения особых проблем у монтажников обычно не возникает.

Гораздо хуже, что стоимость комплекта инструментов высока (более $500), да и сами разъемы не дешевые. Поэтому обоснованным такой выбор для домашней сети назвать сложно. Но если инструменты попали в руки "по случаю" - почему бы их и не использовать "по полной программе"...

Механические сплайсы.

К данному типу можно отнести CoreLink (соединение световодных каналов, АМП), Fibrlok (фиксация волокон, 3М), а так же несколько отечественных разработок. Они позволяют осуществлять соединения волокон между собой. Т.е. присоединять к кабелю пигтейлы (отрезки волокна с разъемом, установленным фабричным способом), либо соединять кабеля между собой в муфте или коммутационной коробке.

Первоначально данный тип соединения предназначался для быстрого но краткосрочного ремонта кабельных линий, как замена сварке. Однако получилось удачная конструкция, которая допускает многократное использование (!) и способна работать годами и даже десятилетиями.

Принцип действия заключается в том, что волокна при помощи специального механического приспособления центрируются и затем фиксируются. Так в отечественной разработке фиксирующим элементом служат три кварцевых стержня, между которыми и зажимается волокно. В разработках фирм AMP и 3M волокно зажимается между двух пластинок, в теле которых выполнены прецизионные центрирующие канавки. Пластины поддерживаются в закрытом состоянии пружинными элементами.

Выглядит CoreLink следующим образом:

Рис. 3.25. CoreLink.

Понятно, что перед фиксацией волокна необходимо зачистить от защитных оболочек и сколоть специальным прецизионным инструментом таким образом, чтобы не параллельность торцов составляла не более 1-2 градусов (требования почти как при сварке, но все же гораздо менее жесткие).

Оставшийся воздушный зазор между торцами волокон заполняется иммерсионной жидкостью (коэффициент преломления равен коэффициенту преломления световодного канала волокна). В случае технологии фирмы AMP иммерсионная жидкость уже находится между пластинами. Изделия серии CoreLink (AMP) отличает также то, что для монтажа и демонтажа разъемов необходим только маленький ключик и фактически монтаж может быть осуществлен на весу в очень ограниченном пространстве.

Не удивительно, что именно эта технология приобретает последнее время все большую популярность. Возможно, что она уже более распространена, чем наклейка разъемов. Стоимость сплайса порядка $10 - что вполне сравнимо с работой монтажника или сварщика. Инструменты нужны минимальные, квалификация высокая не требуется.

Более того, с каким бы прицелом "на будущее" не прокладывали линии, на практике приходится большую часть из них перекладывать в течении 3-5 лет. То проблемы с собственником здания, то пожар, то ремонт, то дом на трассе строят... Причин, увы, хватет. Поэтому стремиться к сварке с расчетом "простоит 30 лет" не имеет смысла.

А по экономическим показаниям CoreLink уступает сварке только при существенных объемах работ.

MT-RJ

Вообще говоря, MT-RJ это не технология, а новый тип разъема, разработанный фирмой AMP. Он имеет такие же габариты и фиксацию как RJ45, и из-за этого хорошо подходит к СКС с высокой плотностью портов. Он активно применяется в оборудовании Cisco Systems, 3Com, Cabletron, и др.

Суть технологии присоединения к волокну заключается в том, что внутри разъема помещено некоторое подобие соединителя CoreLink. С одной стороны в него в заводских условиях уже установлен и отполирован отрезок волокна. С другой стороны, волокно вставляется во время монтажа и фиксируется в разъеме простым поворотом ключа.

Главный минус - существенное, до 0,5 Дб затухание (что совсем не страшно в традиционных СКС и домашних сетях).

На сегодня это дорогой, и все же экзотический тип. Но в будущем вполне возможно, что он станет так же привычен, как ST-SC.

Глава 4. Электропитание и заземление.

Делай как должно и пусть будет что будет...

В любой серьезной ЛВС кроме "слаботочной" части, есть силовая проводка питания активного оборудования. Для ее правильного построения и эксплуатации желательно знать терминологию и понимать основные принципы работы сети 220/380 Вольт. Хотя нужно учитывать, что строго говоря, это прерогатива людей, имеющих специальные знания и разрешения. А любые самостоятельные действия могут быть связаны с реальным риском для жизни.

Поэтому не помешает повторить еще раз: **Все работы, связанные с прокладкой и обслуживанием электрических сетей, должны выполняться только квалифицированным электротехническим персоналом с соответствующей группой допуска электробезопасности!**

Вторая часть данной главы связана с защитой сетей от различных электрических явлений - начиная с выходом из строя электросети, и закачивая грозами (атмосферными наводками). Хоть эти вопросы прямо не связаны с силовой проводкой, но их рассмотрение, так или иначе, приводит к общей (и ключевой) теме заземления.

Следующая особенность нижележащего материала - обширное цитирование ПУЭ (правила устройства электроустановок), которые безусловно являются главным документом, регламентирующим вопросы электрических сетей. Можно без преувеличения назвать их библией электрика. Разумеется, путаницы в ПУЭ заметно меньше, чем в 2-х тысячелетнем прототипе. И материи рассматриваются более земные. Тем не менее, вопросы электропитания достаточно сложны, и их лишнее толкование как минимум не помешает.

Дополнительная сложность заключается в том, что на часть ПУЭ есть новая, 7 редакция. И ее отличия от предыдущего варианта достаточно принципиальны (что случается в Российском законотворчестве не часто). Поэтому нужно ориентироваться на новую редакцию, и использовать ее как основу. Но при этом иметь в виду, что подавляющее большинство электросетей построено по старой (или очень старой) версии этого документа.

Краткие рекомендации:

При работе с электропроводкой желательно выполнять следующие рекомендации:

1. Работу с электричеством проводить в твердом уме, трезвом виде, и только вдвоем. Своевременная помощь друга может спасти жизнь.
2. Всегда проверять отсутствие напряжения даже в "отключенной" сети. Отверткой, тестером - сделать несложно, а риск снижается заметно. Кроме этого, стоит

позаботиться о себе на случай непредвиденного включения (практика показывает, что табличка "не включать, работают люди" действует не на всех адекватно). Самый простой способ защиты - занулить подводящие проводники чем-то надежным, и приличного сечения (мягкая медная проволока должна быть обязательным атрибутом комплекта инструментов монтажника). Тогда в случае случайного включения пострадают только предохранители.

3. Оборотная сторона п. 2. Не включать автомат (рубильник, УЗО, пакетный выключатель), кем-то отключенный, при малейшем подозрении на проведение монтажных работ.
4. Если возникла настоятельная необходимость (в нарушение всех норм) работать "под напряжением", это нужно делать только одной рукой, и стоя на хорошей "изолирующей" поверхности. Вторую руку лучше от греха подальше спрятать в карман.
5. До самого недавнего времени сеть в квартирах выполнялась алюминиевым проводом. При необходимости присоединения другого провода (например для переноса розетки), никогда не скручивайте медь с алюминием - возникает гальваническая пара, металл в месте контакта активно разрушается, переходное сопротивление растет, возникает подгорание, что, в конце концов, может привести к пожару. Медный и алюминиевый проводники соединяются между собой через переходную колодку.
6. При проводке питания для активного оборудования в сложных условиях чердаков и подвалов думайте о электробезопасности и пожаробезопасности. Например, Боже упаси на деревянную крышу вывести 220 В, да еще не в трубах или металлорукаве, а прямо витой парой на скобках. Пожарники могут пришибить на месте - и будут совершенно правы. Только 9-12 вольт, и с оглядкой.
7. И последнее. Нужно заботиться о надежности источника питания. Тут не помешает грамотный проект, но - будем реалистами, делается он на практике очень редко. Очевидно и то, что качественный монтаж обязателен. Но кроме этого, будет неприятно, если питание коммутатора случайно попадет на неудачный, перегруженный автомат, или, например, сторож неожиданно начнет отключать именно этот этаж (дом, квартал на ночь или на день). Еще хуже, если линия помешает электрикам, хуже пожарникам - и нет питания, да еще и скандал, если слишком много норм нарушено. Такие "случайные проблемы" то же приходится учитывать…

Часть 3. Глава 4

Термины по "ПУЭ".

Как обычно, в начале главы - унылые термины. Однако без них в дальнейшем изложении (и тем более в ПУЭ) просто невозможно будет что-то понять.

7.1.3. Вводное устройство (ВУ) - совокупность конструкций, аппаратов и приборов, устанавливаемых на вводе питающей линии в здание или в его обособленную часть. Вводное устройство, включающее в себя также аппараты и приборы отходящих линий, называется вводно-распределительным (ВРУ).

7.1.4. Главный распределительный щит (ГРЩ) - распределительный щит, через который снабжается электроэнергией все здание или его обособленная часть. Роль ГРЩ может выполнять ВРУ или щит низкого напряжения подстанции.

7.1.5. Распределительный пункт (РП) - устройство, в котором установлены аппараты защиты и коммутационные аппараты (или только аппараты защиты) для отдельных электроприемников или их групп (электродвигателей, групповых щитков).

7.1.6. Групповой щиток - устройство, в котором установлены аппараты защиты и коммутационные аппараты (или только аппараты защиты) для отдельных групп светильников, штепсельных розеток и стационарных электроприемников.

7.1.7. Квартирный щиток - групповой щиток, установленный в квартире и предназначенный для присоединения сети, питающей светильники, штепсельные розетки и стационарные электроприемники квартиры.

7.1.8. Этажный распределительный щиток - щиток, установленный на этажах жилых домов и предназначенный для питания квартир или квартирных щитков.

7.1.9. Электрощитовое помещение - помещение, доступное только для обслуживающего квалифицированного персонала, в котором устанавливаются ВУ, ВРУ, ГРЩ и другие распределительные устройства.

7.1.10. Питающая сеть - сеть от распределительного устройства подстанции или ответвления от воздушных линий электропередачи до ВУ, ВРУ, ГРЩ. 7.1.11. Распределительная сеть - сеть от ВУ, ВРУ, ГРЩ до распределительных пунктов и щитков.

7.1.12. Групповая сеть - сеть от щитков и распределительных пунктов до светильников, штепсельных розеток и других электроприемников.

Устройство сети 220/380 Вольт

Надежное питание для сети передачи данных - важнейшее составляющее долгой и успешной работы. Наиболее распространенной в России является трехфазная сеть с напряжением 380 Вольт, и получаемая из нее однофазная с напряжением 220 Вольт. Классическую схему можно видеть на следующем рисунке:

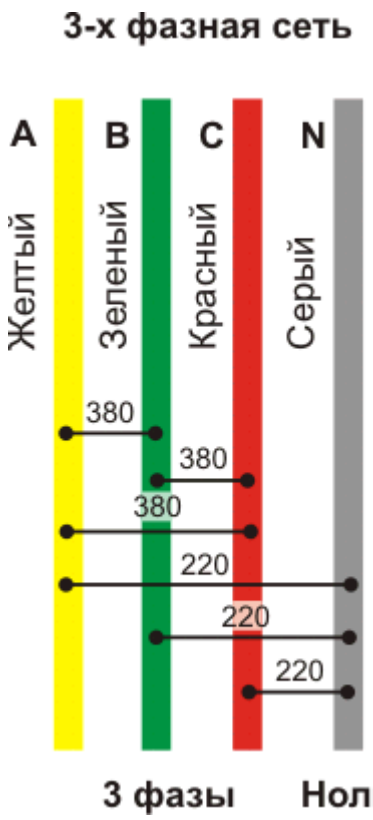

Рис. 4.1. Сеть 220/380 Вольт.

Три фазы (A, B, C) имеют между собой разницу в напряжении 380 вольт (если брать мгновенное значение), и каждая из фаз имеет потенциал 220 вольт относительно нуля (N). Соответственно, если необходимо получить однофазное питание, следует подключить один из проводов к фазе, а другой к нулю (обычно корпусу электрощитка).

И наоборот, питание от двух фаз практически никогда не используется. Более того, подключение устройства 220В к двум фазам скорее всего надолго выведет его из строя.

Если воспользоваться сетевым жаргоном, то можно сказать, что трехфазные линии - бэкбон силовой сети. Все магистральные каналы, вплоть до вводов в здания (этажи, отсеки, цеха) выполнены по трехфазной схеме. Так же запитаны и некоторые мощные потребители - асинхронные электродвигатели, крупные нагреватели, и т.п. Но для питания активного сетевого оборудования такой способ подключения фактически никогда не используется.

Однако на этом внешняя простота построения силовой сети заканчивается. Если фазные провода всегда одинаковые, то по типам заземления удобно различать следующие схемы: TN-C, TN-S, TN-C-S, TT, IT. Такая запись практически не применяется в "ПУЭ", да и редка в отечественной литературе. Однако, в связи с активной экспансией европейских норм, применяется на практике все чаще.

В этом типе записи первая буква определяет тип заземления источника питания. "T" - означает прямое соединение нейтрали источника питания с землей, а в варианте "I" все токоведущие части изолированы от земли (последний вариант для России экзотичен).

Вторая буква показывает тип заземления открытых проводящих частей (например корпуса электрощитка): "T" - непосредственная связь с землей, независимо от способа заземления

источника питания; "N" - связь открытых проводящих частей с точкой заземления источника питания.

В последнем случае различают характер этой связи, точнее говоря, устройство нулевого защитного и нулевого рабочего проводников. В варианте "S" функции и нулевого рабочего (N) и нулевого защитного (PE) проводников обеспечиваются раздельными проводниками, "C" - используется один общий проводник (PEN).

Кроме этого, схемы могут быть комбинированными, например при TN-C-S, когда внутреннее оборудование выполняется по схеме TN-S, а наружное остается в варианте TN-C.

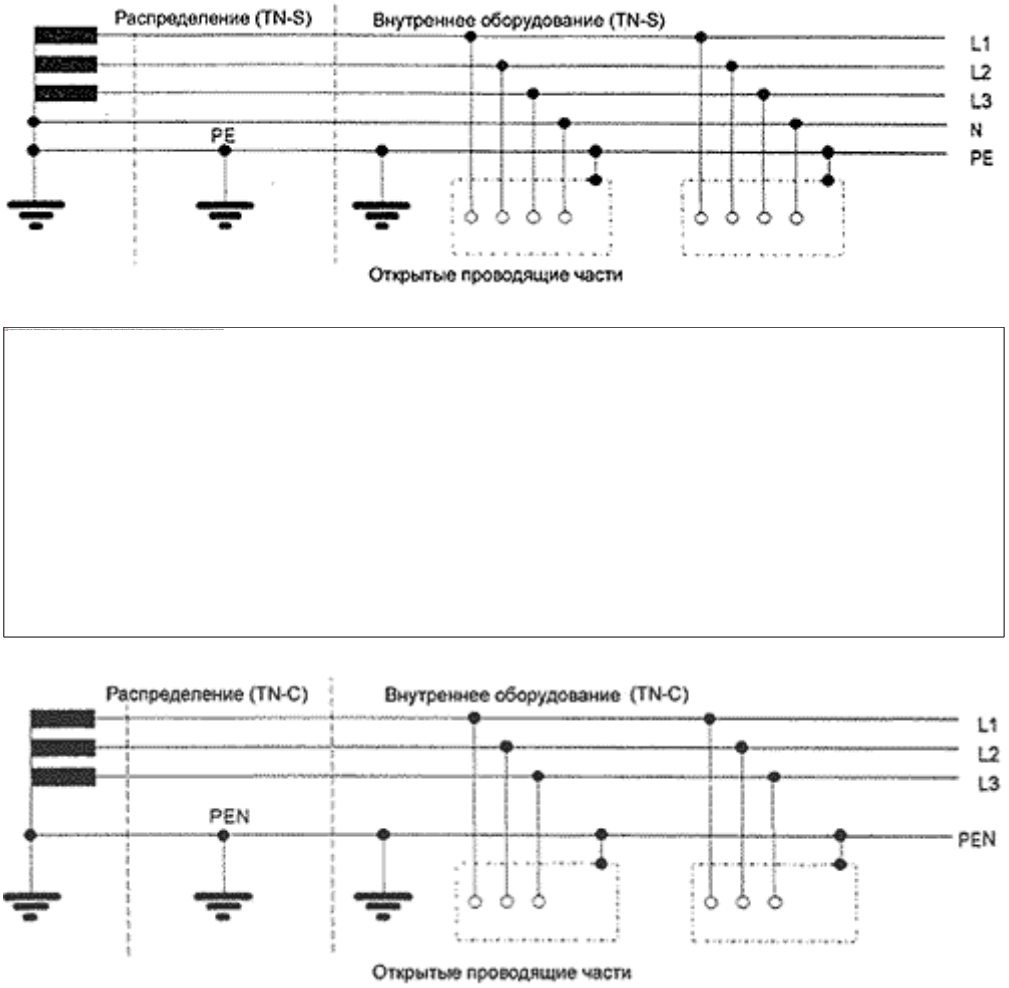

Рис. 4.2. Варианты TN-C, TN-S, TN-C-S.

Сложно сейчас сказать наверняка, почему в России нашла свое применение схема TN-C. Возможно, сыграла свою роль низкая стоимость, а электробезопасность во времена СССР стояла далеко не на первом месте. Но на сегодня более 90% силовых сетей выполнены именно по этой схеме.

Повсеместное использование общего проводника (PEN) даже повлекло распространение термина "зануление" - именно так "приходится именовать" заземление в схеме TN-C.

Но к этому вопросу мы вернемся ниже, уже на базе рекомендаций отечественного ПУЭ.

Элементная база силовой сети.

В общем случае реальная сеть может иметь весьма сложную и запутанную конфигурацию. Но классическая "упрощенная" схема выглядит таким образом:

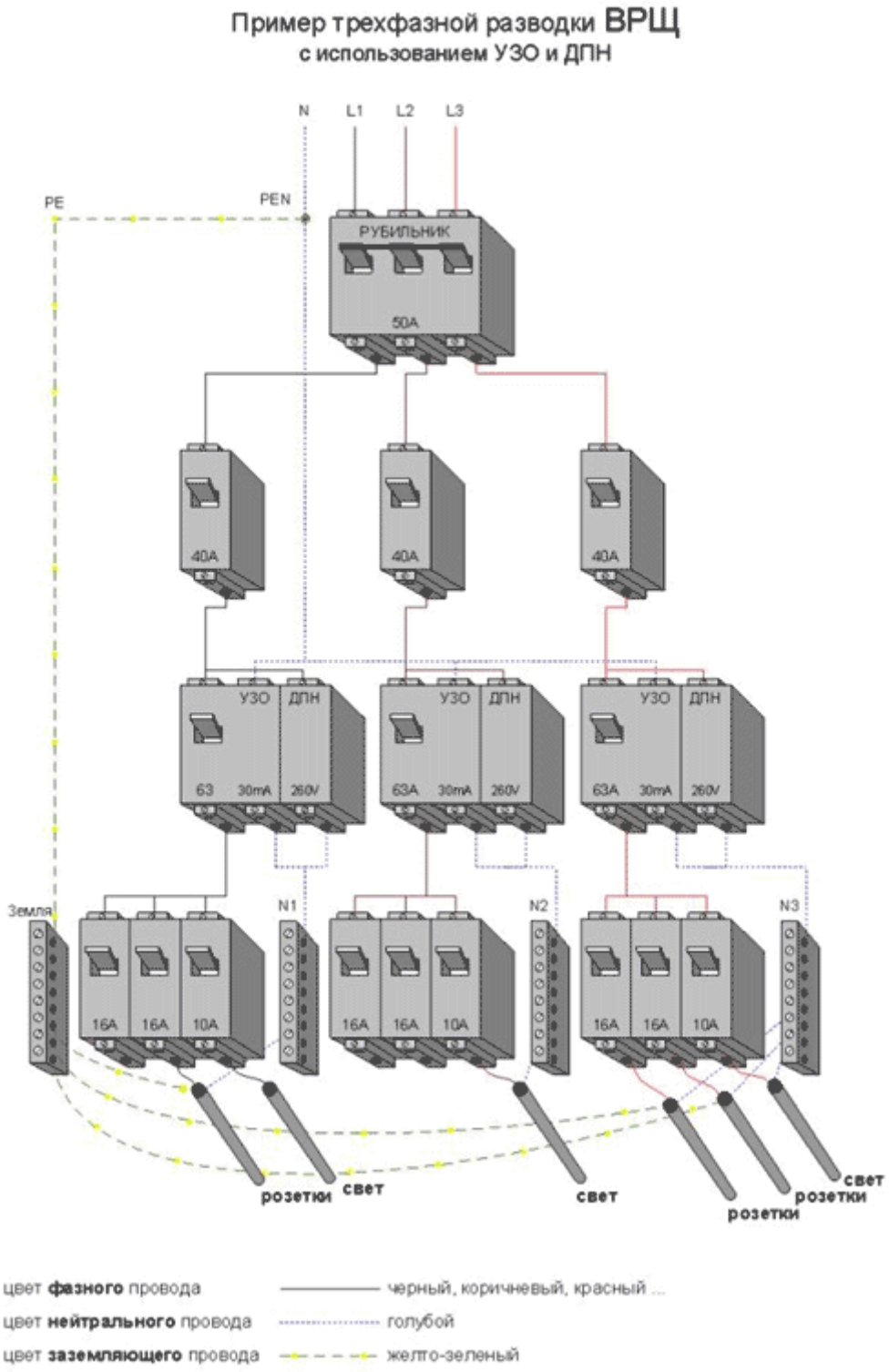

Рис. 4.3. Типовая схема сети электропитания.

На рисунке наиболее распространенный на сегодня вариант TN-C-S, позволяющая обеспечить достаточный уровень электробезопасности в сети без коренной реконструкции последней.

С внешнего ввода кабель заводится на главный рубильник (3 фазы), далее разводится по группам потребителей, каждая из которых имеет свой автомат выключения, и защиту в виде УЗО и ДПН.

Можно выделить следующие элементы силовой сети:

1. Автоматические выключатели. Устройства простые, и совмещают в себе выключатель и предохранитель. Бывают с электромагнитным, тепловым и комбинированным расцепителем.

В случае использования Электромагнитного расцепителя срабатывание происходит при прохождении через обмотку тока выше определенного значения. Такие автоматы защищают сеть от короткого замыкания. Тепловой расцепитель устроен проще - цепь разрывает биметаллическая пластина, изменяющая свою форму при нагревании, и служат для защиты от длительной перегрузки.

Надо заметить, что деление во многом условно, тем более сейчас распространены комбинированые типы устройств.

2. УЗО - устройство защитного отключения, принцип работы которого основан на втором законе Кирхгофа (алгебраическая сумма токов в каждом узле равна нулю). Так как при повреждении изоляции, прикосновении человека к токоведущему проводу и прочих угрожающих безопасности явлениях неизбежно появляются токи утечки, их можно отследить и отключить линию.

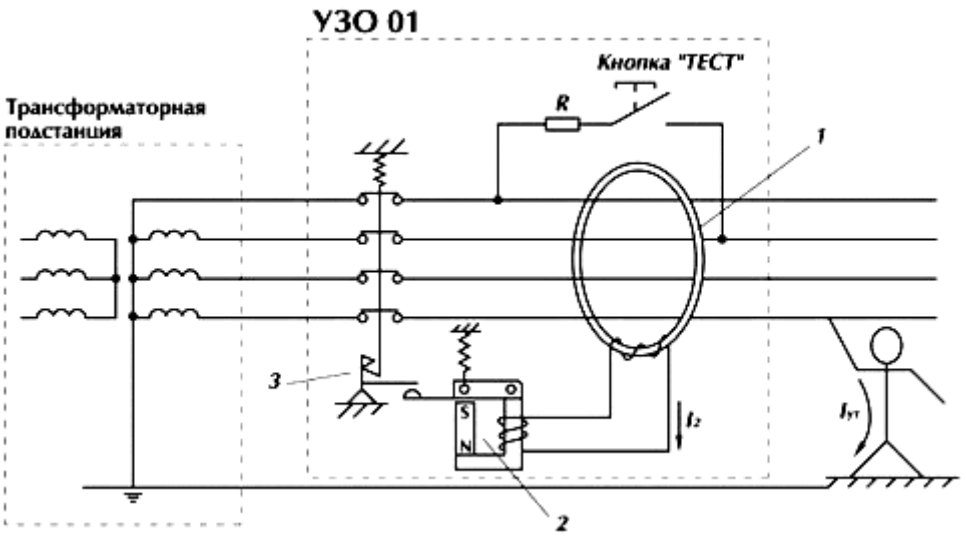

Рис. 4.4. Устройство защитного отключения.

Таким образом, УЗО можно и нужно рассматривать как простой и надежный способ защиты от поражения электрическим током. Но есть и отрицательные моменты в применении таких устройств.

Установка УЗО на линиях, питающих телекоммуникационное оборудование и вычислительную технику, может привести к перерыву связи, потере данных, и даже порче оборудования. Поэтому, пункт 7.1.81 ПУЭ прямо запрещает применение УЗО для электроприемников, отключение которых может привести к ситуациям, опасным для потребителей (классический пример - пожарная сигнализация).

Понятно, что нарушение связи можно так же рассматривать как чрезвычайную и недопустимую ситуацию. И стараться защищать питание узлов связи другими способами (хотя бывают случаи, в которых спорить с энергонадзором сложно).

3. Автомат защиты от перенапряжения (ДПН). Принцип работы прост - при превышении напряжения питающей сети выше порога (обычно 260 В), ДПН отключает потребителя от повышенного напряжения (или дает команду на отключение УЗО).

4. Кабеля, как без них. Для начала, сечение проводника можно определить исходя из тока - не более 10 Ампер на 1 кв. мм (точнее нужно смотреть в специальных таблицах). Ток можно рассчитать как I=P/220 для однофазной сети, где P - совокупная мощность потребителей.

Проводники могут быть однопроволочные и многопроволочные. Многопроволочные используются обычно в тех случаях, когда от требуется гибкость или мобильность (времянки, переноски, удлинители). Однопроволочные служат для неподвижных соединений, стационарной проводки. Многопроволочные дороже, имеют несколько больший диаметр, сложно крепятся в болтовых соединениях.

В качестве следующего важнейшего параметра можно назвать материал проводов. В любой ситуации рекомендуется медный кабель, алюминиевый использовать нежелательно. В отрасли компьютерных сетей и провайдинга просто нет задач, на которых сказывается дешевизна алюминиевых проводов.

Часть 3. Глава 4

Заземление (зануление).

Говоря в общем, можно заметить, что великая и ужасная сила электричества давно описана, подсчитана, занесена в толстые таблицы. Нормативная база, определяющая пути синусоидальных электрических сигналах частоты 50 Гц способна ввергнуть любого неофита в ужас своим объемом. И, несмотря на это, любому завсегдатаю технических форумов давно известно - нет более скандального вопроса, чем заземление.

Масса противоречивых мнений на деле мало способствует установлению истины. Тем более, вопрос этот на самом деле серьезный, и требует более пристального рассмотрения.

Основные понятия

Если опустить вступление "библии электрика" (ПУЭ), то для понимания технологии заземления нужно обратиться (для начала) к Главе 1.7, которая так и называется "Заземление и защитные меры электробезопастности".

В п. 1.7.2. сказано:

Электроустановки в отношении мер электробезопасности разделяются на:

- *электроустановки выше 1 кВ в сетях с эффективно заземленной нейтралью (с большими токами замыкания на землю), ;*

- *электроустановки выше 1 кВ в сетях с изолированной нейтралью (с малыми токами замыкания на землю);*
- *электроустановки до 1 кВ с глухозаземленной нейтралью;*
- *электроустановки до 1 кВ с изолированной нейтралью.*

В подавляющем большинстве жилых и офисных домов России используется глухозаземленная нейтраль. Пункт 1.7.4. гласит:

Глухозаземленной нейтралью называется нейтраль трансформатора или генератора, присоединенная к заземляющему устройству непосредственно или через малое сопротивление (например, через трансформаторы тока).

Термин не совсем понятный на первый взгляд - нейтраль и заземляющее устройство на каждом шагу в научно-популярной прессе не встречаются. Поэтому, ниже все непонятные места будут постепенно объяснены.

При описании остальных вариантов устройств электроустановок проще всего поступить как в одном из вариантов инструкции на Роллс-Ройс - "если автомобиль сломался, Ваш водитель наверняка знает, что нужно делать". По крайней мере схемы, отличные от глухозаземленной нейтрали, встречаются при строительстве домашних сетей немногим чаще, чем Роллс-Ройсы на улицах.

Введем немного терминов - так можно будет по крайней мере говорить на одном языке. Возможно, пункты будут казаться "вытащенными из контекста". Но ПУЭ не художественная литература, и такое раздельное использование должно быть вполне обоснованно - как применение отдельных статей УК. Впрочем, оригинал ПУЭ вполне доступен как в книжных магазинах, так и в сети - всегда можно обратиться к первоисточнику.

- *1.7.6. Заземлением какой-либо части электроустановки или другой установки называется преднамеренное электрическое соединение этой части с заземляющим устройством.*
- *1.7.7. Защитным заземлением называется заземление частей электроустановки с целью обеспечения электробезопасности.*
- *1.7.8. Рабочим заземлением называется заземление какой-либо точки токоведущих частей электроустановки, необходимое для обеспечения работы электроустановки.*
- *1.7.9. Занулением в электроустановках напряжением до 1 кВ называется преднамеренное соединение частей электроустановки, нормально не находящихся под напряжением, с глухозаземленной нейтралью генератора или трансформатора в сетях трехфазного тока, с глухозаземленным выводом источника однофазного тока, с глухозаземленной средней точкой источника в сетях постоянного тока.*
- *1.7.12. Заземлителем называется проводник (электрод) или совокупность металлически соединенных между собой проводников (электродов), находящихся в соприкосновении с землей.*
- *1.7.16. Заземляющим проводником называется проводник, соединяющий заземляемые части с заземлителем.*
- *1.7.17. Защитным проводником (PE) в электроустановках называется проводник, применяемый для защиты от поражения людей и животных электрическим током. В электроустановках до 1 кВ защитный проводник, соединенный с*

глухозаземленной нейтралью генератора или трансформатора, называется нулевым защитным проводником.

- *1.7.18. Нулевым рабочим проводником (N) в электроустановках до 1 кВ называется проводник, используемый для питания электроприемников, соединенный с глухозаземленной нейтралью генератора или трансформатора в сетях трехфазного тока, с глухозаземленным выводом источника однофазного тока, с глухозаземленной точкой источника в трехпроводных сетях постоянного тока. Совмещенным нулевым защитным и нулевым рабочим проводником (PEN) в электроустановках до 1 кВ называется проводник, сочетающий функции нулевого защитного и нулевого рабочего проводников. В электроустановках до 1 кВ с глухозаземленной нейтралью нулевой рабочий проводник может выполнять функции нулевого защитного проводника.*

Рис. 4.5. Отличие защитного заземления и защитного "нуля"

Итак, прямо из терминов ПУЭ следует простой вывод. Различия между "землей" и "нулем" очень небольшие... На первый взгляд (сколько копий сломано на этом месте). По крайней мере, они обязательно должны быть соединены (или даже могут быть выполнены "в одном флаконе"). Вопрос только, где и как это сделано.

Попутно отметим п. 1.7.33.

Заземление или зануление электроустановок следует выполнять:

- *при напряжении 380 В и выше переменного тока и 440 В и выше постоянного тока - во всех электроустановках (см. также 1.7.44 и 1.7.48);*
- *при номинальных напряжениях выше 42 В, но ниже 380 В переменного тока и выше 110 В, но ниже 440 В постоянного тока - только в помещениях с повышенной опасностью, особо опасных и в наружных установках.*

Иначе говоря, заземлять или занулять устройство, подключенное к напряжению 220 вольт переменного тока совсем не обязательно. И в этом нет ничего особо удивительного - третьего провода в обычных советских розетках реально не наблюдается. Можно сказать, что вступающий на практике в свои права Евростандарт (или близкая к нему новая редакция ПУЭ) лучше, надежнее, и безопаснее. Но по старому ПУЭ у нас в стране жили десятки лет... И что особенно важно, дома строили целыми городами.

Однако, когда речь идет о заземлении, дело не только в напряжении питания. Хорошая иллюстрация этого - ВСН 59-88 (Госкомархитектуры) "Электрооборудование жилых и

общественных зданий. Нормы проектирования" Выдержка из главы 15. Заземление (зануление) и защитные меры безопасности:

15.4. Для заземления (зануления) металлических корпусов бытовых кондиционеров воздуха, стационарных и переносных бытовых приборов класса I (не имеющих двойной или усиленной изоляции), бытовых электроприборов мощностью св. 1,3 кВт, корпусов трехфазных и однофазных электроплит, варочных котлов и другого теплового оборудования, а также металлических нетоковедущих частей технологического оборудования помещений с мокрыми процессами следует применять отдельный проводник сечением, равным фазному, прокладываемый от щита или щитка, к которому подключен данный электроприемник, а в линиях питающих медицинскую аппаратуру, - от ВРУ или ГРЩ здания. Этот проводник присоединяется к нулевому проводнику питающей сети. Использование для этой цели рабочего нулевого проводника запрещается.

Получается нормативный парадокс. Одним из видимых на бытовом уровне результатов стало комплектование стиральных машин "Вятка-автомат" моточком одножильного алюминиевого провода с требованием выполнить заземление (руками сертифицированного специалиста).

И еще один интересный момент:. *1.7.39. В электроустановках до 1 кВ с глухозаземленной нейтралью или глухозаземленным выводом источника однофазного тока, а также с глухозаземленной средней точкой в трехпроводных сетях постоянного тока должно быть выполнено зануление. Применение в таких электроустановках заземления корпусов электроприемников без их зануления не допускается.*

Практически это означает - хочешь "заземлить" - сначала "занули". Кстати, это имеет прямое отношение к знаменитому вопросу "забатареивания" - которое по совершенно непонятной причине ошибочно считается лучше зануления (заземления).

Параметры заземления

Следующий аспект, которые необходимо рассмотреть - числовые параметры заземления. Так как физически это не более чем проводник (или множество проводников), то главной его характеристикой будет сопротивление.

1.7.62. Сопротивление заземляющего устройства, к которому присоединены нейтрали генераторов или трансформаторов или выводы источника однофазного тока, в любое время года должно быть не более 2, 4 и 8 Ом соответственно при линейных напряжениях 660, 380 и 220 В источника трехфазного тока или 380, 220 и 127 В источника однофазного тока. Это сопротивление должно быть обеспечено с учетом использования естественных заземлителей, а также заземлителей повторных заземлений нулевого провода ВЛ до 1 кВ при количестве отходящих линий не менее двух. При этом сопротивление заземлителя, расположенного в непосредственной близости от нейтрали генератора или трансформатора или вывода источника однофазного тока, должно быть не более: 15, 30 и 60 Ом соответственно при линейных напряжениях 660, 380 и 220 В источника трехфазного тока или 380, 220 и 127 В источника однофазного тока.

Для меньшего напряжения допустимо большее сопротивление. Это вполне понятно - первая цель заземления - обеспечить безопасность человека в классическом случае попадания "фазы" на корпус электроустановки. Чем меньше сопротивление, тем меньшая

часть потенциала может оказаться "на корпусе" в случае аварии. Следовательно, в первую очередь нужно снижать опасность для более высокого напряжения.

Дополнительно нужно учитывать, что заземление служит и для нормальной работы предохранителей. Для этого необходимо, что бы линия при пробое "на корпус" существенно изменяла свойства (прежде всего сопротивление), иначе срабатывания не произойдет. Чем больше мощность электроустановки (и потребляемое напряжение), тем ниже ее рабочее сопротивление, и соответственно должно быть ниже сопротивление заземления (иначе при аварии предохранители не сработают от незначительного изменения суммарного сопротивления цепи).

Следующий нормируемый параметр - сечение проводников.

1.7.76. Заземляющие и нулевые защитные проводники в электроустановках до 1 кВ должны иметь размеры не менее приведенных в табл. 1.7.1 (см. также 1.7.96 и 1.7.104) .

Приводить всю таблицу не целесообразно, достаточно выдержки:

Для неизолированных медных минимальное сечение составляет 4 кв. мм, для алюминиевых - 6 кв. мм. Для изолированных, соответственно, 1,5 кв. мм и 2,5 кв. мм. Если заземляющие проводники идут в одном кабеле с силовой проводкой, их сечение может составлять 1 кв. мм для меди, и 2,5 кв. мм для алюминия.

Заземление в жилом доме

В обычной "бытовой" ситуации пользователи электросети (т.е. жильцы) имеют дело только с Групповой сетью (*7.1.12 ПУЭ. Групповая сеть - сеть от щитков и распределительных пунктов до светильников, штепсельных розеток и других электроприемников*). Хотя в старых домах, где щитки установлены прямо в квартирах, им приходится сталкиваться с частью Распределительной сети (*7.1.11 ПУЭ. Распределительная сеть - сеть от ВУ, ВРУ, ГРЩ до распределительных пунктов и щитков*). Это желательно хорошо понимать, ведь часто "ноль" и "земля" отличаются только местом соединения с основными коммуникациями.

Из этого в ПУЭ сформулировано первое правило заземления:

7.1.36. Во всех зданиях линии групповой сети, прокладываемые от групповых, этажных и квартирных щитков до светильников общего освещения, штепсельных розеток и стационарных электроприемников, должны выполняться трехпроводными (фазный - L, нулевой рабочий - N и нулевой защитный - PE проводники). Не допускается объединение нулевых рабочих и нулевых защитных проводников различных групповых линий. Нулевой рабочий и нулевой защитный проводники не допускается подключать на щитках под общий контактный зажим.

Т.е. от этажного, квартирного или группового щитка нужно прокладывать 3 (три) провода, один из которых защитный нуль (совсем не земля). Что, впрочем, вовсе не мешает использовать ее для заземления компьютера, экрана кабеля, или "хвостика" грозозащиты. Вроде бы все просто, и не совсем понятно, зачем углубляться в такие сложности.

Можно посмотреть на свою домашнюю розетку... И с вероятностью около 80% не увидеть там третьего контакта. Чем отличается нулевой рабочий и нулевой защитный

проводники? В щитке они соединяются на одной шине (пусть не в одной точке). Что будет, если использовать в данной ситуации рабочий ноль в качестве защитного?

Предполагать, что нерадивый электрик перепутает в щитке фазу и ноль, сложно. Хоть этим постоянно пугают пользователей, но ошибиться невозможно в любом состоянии (хотя бывают уникальные случаи). Однако "рабочий ноль" идет по многочисленным штробам, вероятно проходит через несколько распределительных коробочек (обычно небольшие, круглые, смонтированы в стене недалеко от потолка).

Перепутать фазу с нулем там уже намного проще (сам это делал не раз). А в результате на корпусе неправильно "заземленого" устройства окажется 220 вольт. Или еще проще - отгорит где-то в цепи контакт - и почти те же 220 пройдут на корпус через нагрузку электропотребителя (если это электроплита на 2-3 кВт, то мало не покажется).

Для функции защиты человека - прямо скажем, никуда не годная ситуация. Но для подключения заземления грозозащиты типа APC не фатальная, так как там установлена высоковольтная развязка. Впрочем, рекомендовать такой способ было бы однозначно неправильно с точки зрения безопасности. Хотя надо признать, что нарушается эта норма очень часто (и как правило без каких-либо неблагоприятных последствий).

Надо отметить, что грозозащитные возможности рабочего и защитного нуля примерно равны. Сопротивление (до соединительной шины) отличается незначительно, а это, пожалуй, главный фактор, влияющий на стекание атмосферных наводок.

Из дальнейшего текста ПУЭ можно заметить, что к нулевому защитному проводнику нужно присоединять буквально все, что есть в доме:

7.1.68. Во всех помещениях необходимо присоединять открытые проводящие части светильников общего освещения и стационарных электроприемников (электрических плит, кипятильников, бытовых кондиционеров, электрополотенец и т.п.) к нулевому защитному проводнику.

Вообще, это проще представить следующей иллюстрацией:

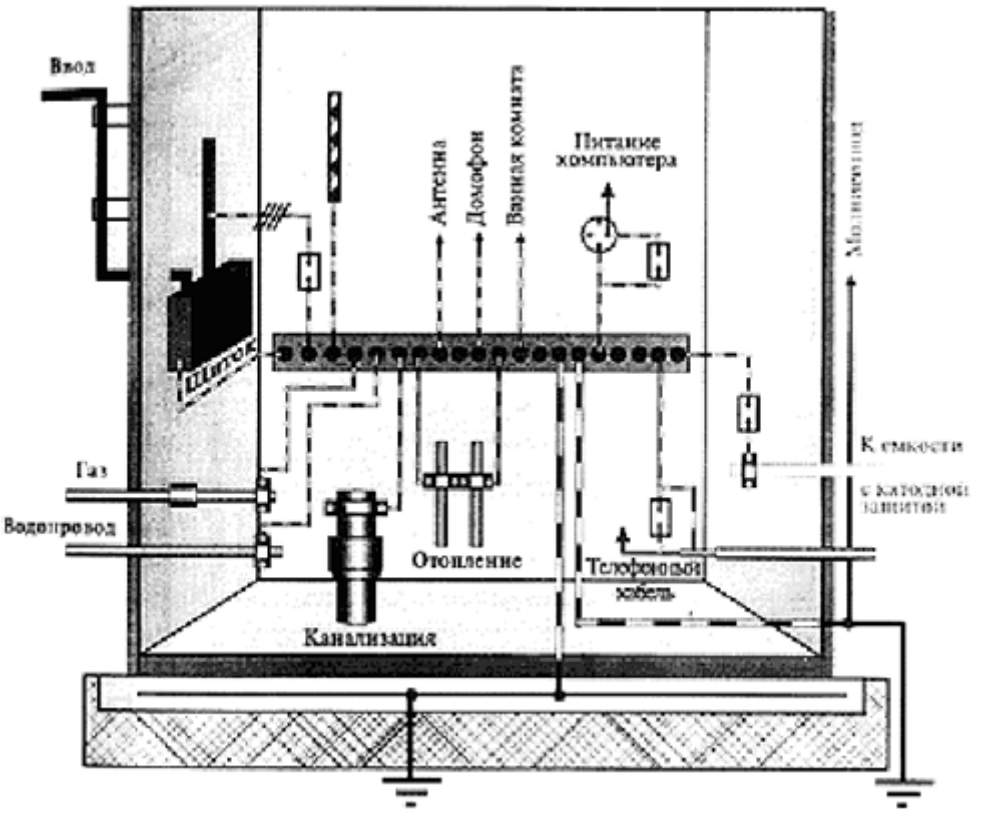

Рис. 4.6. Схема заземления.

Картина довольна необычная (для бытового восприятия). Буквально все, что есть в доме, должно быть заземлено на специальную шину. Поэтому может возникнуть вопрос - ведь жили без этого десятки лет, и все живы-здоровы (и слава Богу)? Зачем все так серьезно менять? Ответ простой - потребителей электричества становится больше, и они все мощнее. Соответственно, риски поражения вырастают.

Но зависимость безопасности и стоимости величина статистическая, и экономию никто не отменял. Поэтому слепо класть по периметру квартиры медную полосу приличного сечения (вместо плинтуса), заводя на нее все, вплоть до металлических ножек стула, не стоит. Как не стоит ходить в шубе летом, и постоянно носить мотоциклетный шлем. Это уже вопрос адекватности.

Так же в область ненаучного подхода стоит отнести самостоятельное рытье траншей под защитный контур (в городском доме кроме проблем это заведомо ничего не принесет). А для желающих все же испытать все прелести жизни - в первой главе ПУЭ есть нормативы на изготовление этого фундаментального сооружения (в совершено прямом смысле этого слова).

Подводя итоги вышесказанному, можно сделать следующие практические выводы:

- Если Групповая сеть выполнена тремя проводами, для заземления/зануления можно использовать защитный ноль. Он, собственно, для того и придуман.
- Если Групповая сеть выполнена двумя проводами, желательно завести защитный нулевой провод от ближайшего щитка. Сечение провода должно быть более, чем фазного (точнее можно справиться в ПУЭ).

При двухпроводной сети нельзя заземлять корпус устройства на рабочий ноль. В крайнем случае, и соблюдая осторожность, можно так заземлить выводы грозозащиты с высоковольтной развязкой.

На этом можно было бы закончить изложение, если бы сеть располагалась в пределах одного здания (вернее, одной комнаты с единой шиной). Реально домашние сети имеют большие воздушные пролеты (и что самое неприятное, выполнены на приличной высоте). Поэтому нужно отдельно и подробно рассмотреть вопрос молниезащиты.

Часть 3. Глава 4

Молниезащита кабелей.

Можно сформулировать основную задачу. Это, во-первых, защитить сеть от грозы (в основном атмосферных электрических разрядов), во-вторых, сделать это, не принеся вреда существующей электрической разводке (и подключенным к ней потребителям). При этом часто приходится решать "сопутствующую" задачу приведения в нормальное состояние заземления и устройства выравнивания потенциалов в реальной распределительной сети.

Основные понятия.

Если говорить о документах, то молниезащита должна соответствовать РД 34.21.122-87 "Инструкция по устройству молниезащиты зданий и сооружений" и ГОСТ Р 50571.18-2000, ГОСТ Р 50571.19-2000, ГОСТ Р 50571.20-2000.

Вот термины:

1. Прямой удар молнии - непосредственный контакт канала молнии с зданием или сооружением, сопровождающийся протеканием через него тока молнии.
2. Вторичное проявление молнии - наведение потенциалов на металлических элементах конструкции, оборудования, в незамкнутых металлических контурах, вызванное близкими разрядами молнии и создающее опасность искрения внутри защищаемого объекта.
3. Занос высокого потенциала - перенесение в защищаемое здание или сооружение по протяженным металлическим коммуникациям (подземным и наземным трубопроводам, кабелям и т.п.) электрических потенциалов, возникающих при прямых и близких ударах молнии и создающих опасность искрения внутри защищаемого объекта.

От прямого удара молнии защититься сложно и дорого. Над каждым кабелем громоотвод не поставить (хотя можно полностью перейти на оптоволокно с неметаллическим несущим тросом). Остается надеяться на ничтожную вероятность такого неприятного события. И мириться с шансом испарения кабеля и полного выгорания оконечного оборудования (вместе с защитами).

С другой стороны, занос высокого потенциала не слишком опасен, конечно, для жилого дома, а не порохового склада. Действительно, длительность наведенного молнией импульса - много менее секунды (в качестве тестового обычно принимают 60 миллисекунд, или 0,06 секунды). Сечение проводников витой пары - 0,4 мм.

соответственно, для заноса большой энергий потребуется напряжение очень большой величины. Такое, к сожалению, бывает - так же как вполне реально прямое попадание молнии в крышу дома.

Повредить типичный силовой источник питания коротким высоковольтным всплеском малореально. Трансформатор его просто не пропустит дальше первичной обмотки. Да и у импульсного преобразователя есть достаточная защита.

В качестве примера можно привести силовую проводку в сельской местности - где кабеля подходят к зданию по воздуху, и конечно, подвергаются значительным наводкам во время гроз. Никакой особой защиты при этом обычно не предусматривается (кроме плавких предохранителей или искровых промежутков). Но случаи выхода из строя электроприборов не слишком распространены (хотя бывают чаще, чем в городе).

Система выравнивания потенциалов.

Таким образом наибольшую практическую опасность представляет вторичные проявления молнии (иначе говоря наводки). При этом поражающими факторами будут:

- возникновение высокой разности потенциалов между токопроводящими частями сети;
- наведение высоких напряжений в длинных проводниках (кабелях)

Защитой от этих факторов служат, соответственно:

- выравнивание потенциалов всех токопроводящих частей (в простейшем случае - соединение в одной точке), и малое сопротивление заземляющего контура;
- экранирование защищаемых кабелей.

Начнем с описания системы уравнивания потенциалов - как с того фундамента, без которого применение любых защитных устройств не даст положительного результата.

7.1.87. На вводе в здание должна быть выполнена система уравнивания потенциалов путем объединения следующих проводящих частей:

- *основной (магистральный) защитный проводник;*
- *основной (магистральный) заземляющий проводник или основной заземляющий зажим;*
- *стальные трубы коммуникаций зданий и между зданиями;*
- *металлические части строительных конструкций, молниезащиты, системы центрального отопления, вентиляции и кондиционирования. Такие проводящие части должны быть соединены между собой на вводе в здание.*
- *Рекомендуется по ходу передачи электроэнергии повторно выполнять дополнительные системы уравнивания потенциалов.*

7.1.88. К дополнительной системе уравнивания потенциалов должны быть подключены все доступные прикосновению открытые проводящие части стационарных электроустановок, сторонние проводящие части и нулевые защитные проводники всего электрооборудования (в том числе штепсельных розеток)...

Схематически заземление экрана кабеля, грозозащит и активного оборудования по новой редакции ПУЭ должно производиться следующим образом:

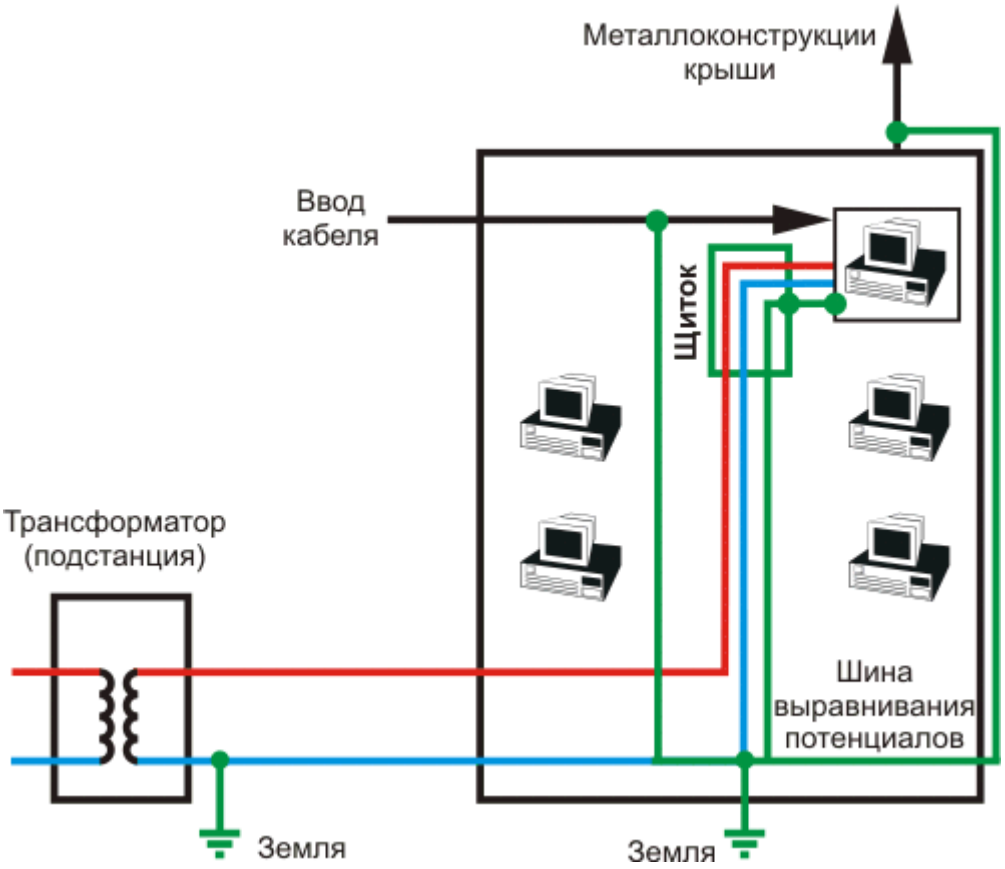

Рис. 4.7. Заземление экранов кабелей, грозозащит и активного оборудования по новой редакции ПУЭ.

В то время как старая редакция предусматривала такую схему:

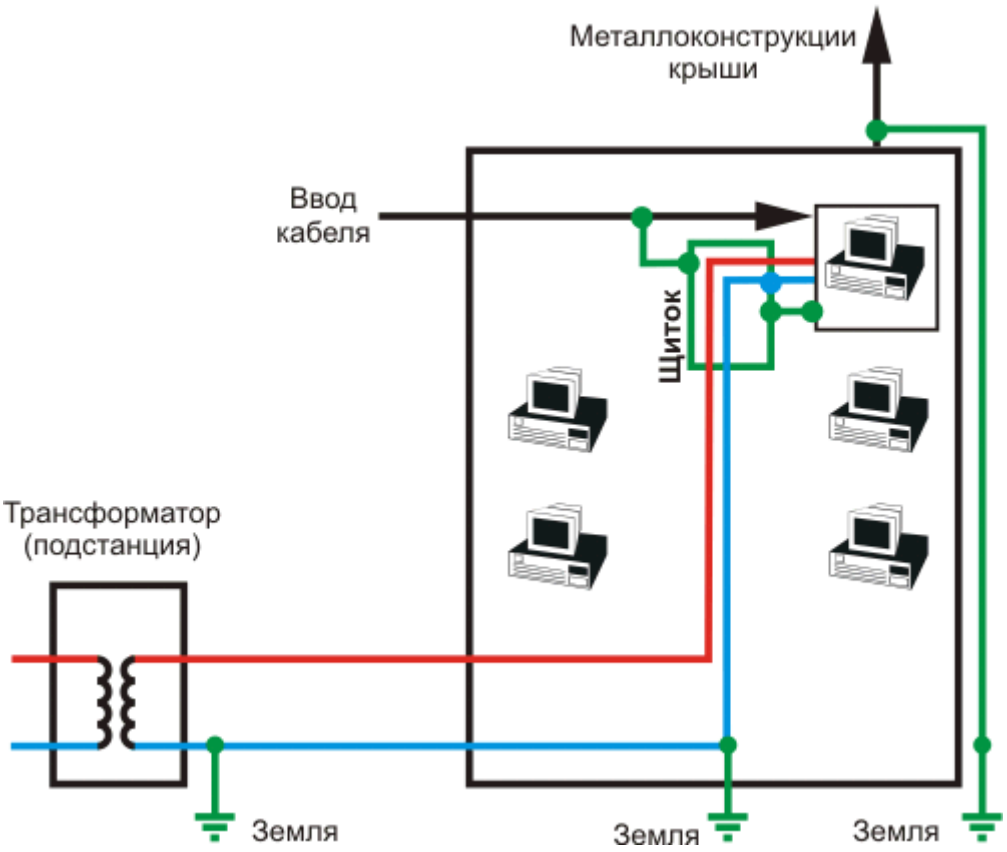

Рис. 4.8. Заземление экранов кабелей, грозозащит и активного оборудования в старой редакции ПУЭ.

Отличия, при всей внешней незначительности, достаточно принципиальны. Например, для эффективной грозозащиты активного оборудования желательно, что бы все потенциалы колебались вокруг единой "земли" (причем имеющей низкое сопротивление заземлителя).

Увы, слишком мало пока в России построено зданий по новому, более эффективному ПУЭ. И можно твердо сказать - "земли" в наших домах нет.

Что делать в этом случае? Вариантов два - переделывать всю сеть электроснабжения дома (нереальный вариант), либо грамотно использовать то, что есть в наличии (но при этом помнить, к чему надо стремиться).

Заземление кабелей и оборудования.

С заземлением активного оборудования сложностей обычно не бывает. Если оно промышленной серии, то наверняка имеет для этого специальную клемму. Хуже с недорогими настольными моделями - в них понятия "земли" просто нет (и заземлять, соответственно, нечего). И больший риск повреждения сполна компенсируется низкой стоимостью.

Вопрос кабельной инфраструктуры значительно сложнее. Единственный элемент кабеля, который можно заземлить без потерь полезного сигнала - это экран. Целесообразно ли использовать такие кабеля для прокладок "воздушек"? Для ответа мне бы хотелось просто привести длинную цитату:

В 1995 году независимой лабораторией была проведена серия сравнительных испытаний экранированной и неэкранированной кабельных систем. Аналогичные тесты проводились также осенью 1997 года. Контролируемый отрезок кабеля длиной 10 метров прокладывался в защищенной от внешних помех эхопоглощающей камере. Одно окончание линии подключалось к сетевому концентратору 100Base-T, а второе - к сетевому адаптеру персонального компьютера. Контрольная часть кабеля подвергалась воздействию наводок напряженностью поля 3 В/м и 10 В/м в диапазоне частот от 30 МГц до 200 МГц. Были получены два существенных результата.

Во-первых, уровень наводок в неэкранированном кабеле категории 5 оказался большим в 5-10 раз, чем в экранированном при напряженности радиочастотного поля 3 В/м. Во-вторых, при отсутствии сетевого трафика, концентратор сети, выполненной на неэкранированном кабеле, показал на некоторых частотах загрузку сети более 80%. Уровень сигналов протокола 100Base-T на частотах свыше 60 МГц очень мал, но очень важен для восстановления формы сигнала. Однако, даже при наличии помех на частоте свыше 100 МГц неэкранированная система не выдержала испытаний. При этом отмечалось снижение скорости передачи данных на два порядка.

Экранированные кабельные системы выдержали все испытания, однако для их успешного функционирования чрезвычайно важно наличие эффективного заземления.

Тут нужно сделать важное замечание. В традиционных СКС заземление выполняется по всей длине линии - непрерывно от одного порта активного оборудования до другого (хотя по идее, должно быть предусмотрено заземление в одной точке). Нормально заземлить

большую распределенную сеть чрезвычайно сложно, и большинство инсталляторов не использует экранированные кабеля принципиально.

В "домашних" сетях нужно говорить не о заземлении сети, а о заземлении отдельных линий. Т.е. можно представить каждую отдельную линию как неэкранированную витую пару, проложенную в металлической трубе (ведь цель экрана защита "воздушной" части линии).

Это сильно упрощает дело. Как следствие, использование экранированного кабеля более чем целесообразно. Но только при хорошем заземлении при вводе в здание. Желательно сделать это с двух сторон по следующему правилу:

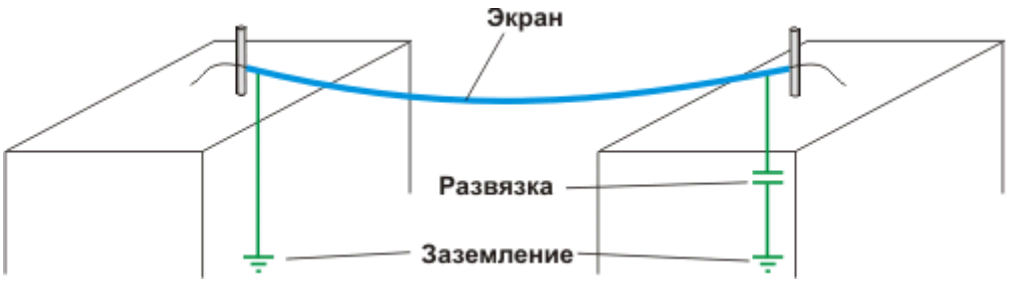

Рис. 4.9. Заземление экрана кабеля.

С одной стороны выполняется "глухое" заземление. С другой - через гальваническую развязку (разрядник, кондернсатор, искровой промежуток). В случае простого заземления с обеих сторон в замкнутой электрической цепи между зданиями могут возникнуть нежелательные уравнивающие токи и/или паразитные наводки.

В идеале желательно провести заземление отдельным проводом приличного сечения до подвала дома и присоединить его там прямо к шине выравнивателя потенциалов. Однако практически достаточно использовать ближайший защитный ноль. При этом эффективность грозозащиты сети снижается, но не слишком значительно, только незначительно (скорее в теории, чем на практике) увеличивается вероятность повреждения электропотребителей в доме занесенным потенциалом.

Часть 3. Глава 4

Грозозащита оборудования.

Можно сказать, что три предыдущих параграфа были большим и важным вступлением к главному - защите магистрального и конечного оборудования от поражения атмосферными электрическими разрядами.

Ведь надежное заземление - не самоцель. Это главное и совершенно необходимое условие для сохранения оборудования и коммуникаций. Без заземления нет смысла разговаривать о грозозащите вообще - это просто не имеет смысла.

Активное оборудование Ethernet

Подойдем к проблеме "с обратной стороны". А точнее - рассмотрим классическую сетевую карту (схему можно взять тут).

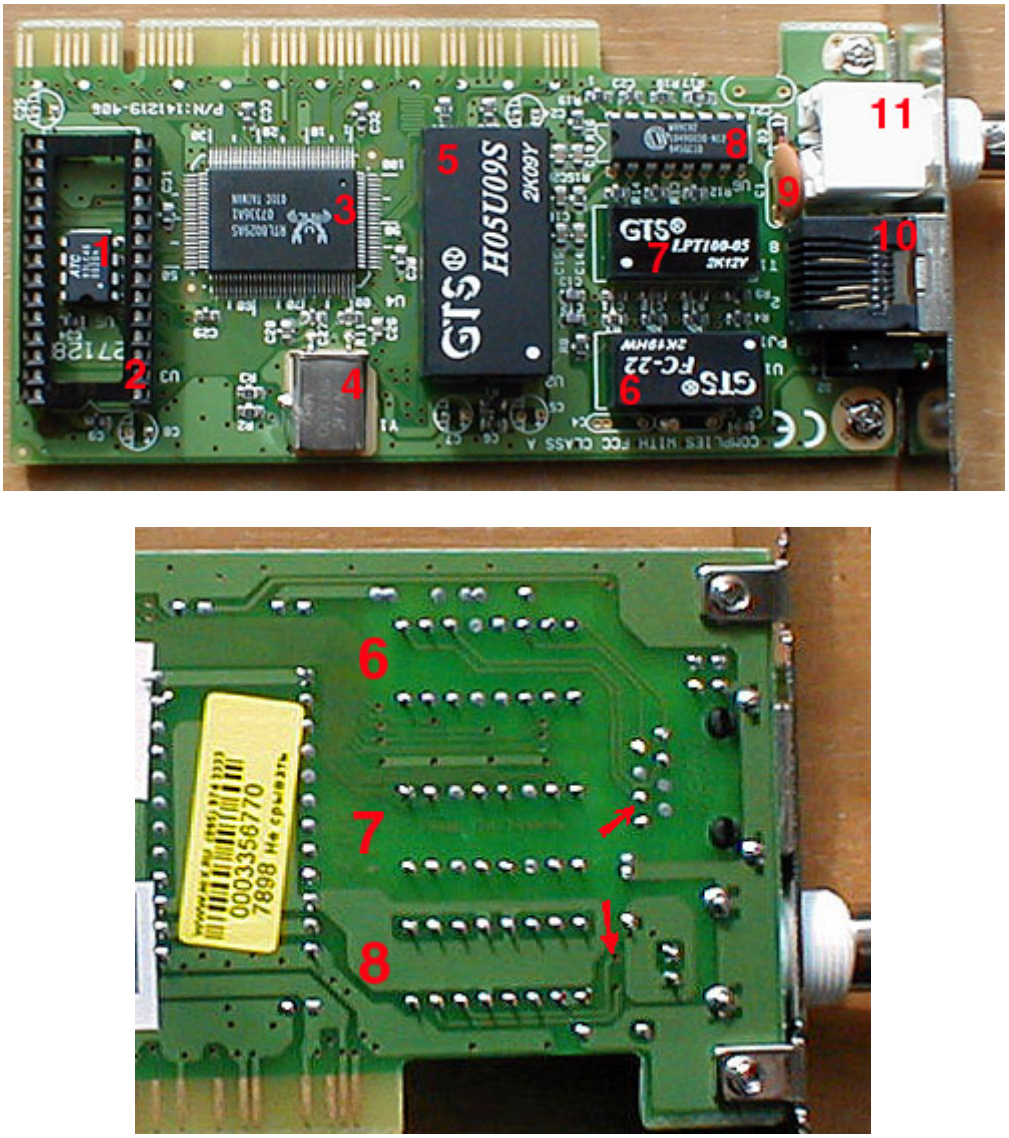

Рис. 4.10. Сетевая карта.

Один из самых распространенная вариантов, Realtek 8029, $5-7 в любом компьютерном магазине. Устройство хабов и свитчей в смысле грозозащиты похоже на сетевую карту, поэтому рассматривать их отдельно не имеет особого смысла.

Рассмотрим (в свете грозоустойчивости) части этого адаптера.

1. Память ЕЕПРОМ. Выходит из строя очень редко, для ремонта можно перепаять из ненужной аналогичной карточки (если таковая имеется).
2. Кроватка под boot-rom. Не ломается.
3. Центральный чип. Если проблема в нем - карточку (как и любой современный коммутатор) можно сразу списать в утиль. Чинить в принципе можно, но экономически не выгодно.
4. Кварцевый генератор. Иногда "стрясается", это можно определить по звуку, если потрясти карточку (не сильно!).
5. Преобразователь напряжения из 5 в 9 Вольт. Нужен для питания трансивера 8. В карточки "только TP" не ставится.

6 и 7. Трансформаторная сборка для витой пары и коаксиала соответственно. При желании, схему можно взять тут. Служит для согласования, и гальванической развязки. Вывести из строя можно только очень сильной наводкой или прямым попаданием молнии. Однако, этот элемент очень важный - в любом случае именно через него поражающий разряд проникает внутрь устройства.
8. Трансивер. Работает на коаксиальный кабель. Самый уязвимый элемент сетевой карты, известны случаи выхода его из строя при наводке без подключенного кабеля (т.е. на голый разъем). Схема тут. Если вы делаете сеть на коаксиале, сразу ставьте кроватки для его быстрой замены. И запасайтесь этими микросхемами.
9. Разрядник. Развязывает экран коаксиала и "землю" шины компьютера. Никакой грозозащиты, вопреки расхожему мнению, из себя не представляет.
10 и 11. Разъемы витой пары и коаксиального кабеля. Выходят из строя очень редко.

При рассмотрении разводки платы отчетливо видно, что проводники от коаксиального разъема идут прямо на микросхему трансивера (8). И центральная жила, и оплетка. А ведь это даже не симметричная линия. Наводка в экране намного больше, чем в жиле. Понятно, что может случиться, если несколько сотен (или несколько тысяч) Вольт попадут на микросхему. В этом случае не спасет даже самое хорошее заземление, ведь рассчитан трансивер на амплитуду сигнала в 3 (ТРИ) Вольта.

Защита, конечно, помогает и в этом случае. Но уж слишком колоссальна сила наводки. Мне встречались APC ProtectNet с практически выгоревшей печатной платой. Элементы - в уголь. Защищаемое устройство - со сгоревшими дорожками. Терминаторы, **приварившиеся** к Т-коннектору...

Значительно лучше обстоят дела с витой парой.
Во-первых, это симметричная линия. Как было показано в предыдущих главах, в идеальном случае между проводниками витой пары наводка должна полностью отсутствовать. Увы, в реальности это не совсем так (повив неидеален).
Во-вторых, на рисунке легко заметить, что дорожки от разъема идут напрямик к трансформатору (6). Сам по себе трансформатор вывести из строя намного сложнее, чем трансивер.

Статистика защиты

Но в любом случае, есть обидная истина - 100% защиты от гроз не дает даже оптоволокно. Имеет смысл только статистический подход к проблемам защиты оборудования. В большой сети что-то все равно сгорит. Задача - минимизация потерь.

Мне пришлось "пережить" 3 грозовых лета с более-менее большими сетями (и еще несколько лет наблюдать ситуацию в чужих сетях). Вот краткие эмпирические выводы из этого:

Используемая технология	Вероятность выживания в течении сезона
"Тонкий коаксиал", RG-58	5%
"Тонкий коаксиал", RG-58, с грамотным заземлением	20%
"Тонкий коаксиал", RG-58, с заземлением и защитой типа ProtectNet от APC	40%

Витая пара, 10baseT	50%
Экранированная витая пара, 10baseT, с заземлением экрана	70%
Экранированная витая пара, 10baseT, с защитой типа ProtectNet от APC	80%
Экранированная витая пара, 10baseT, с заземлением экрана и защитой типа ProtectNet от APC	90-95%

Думаю, никто не удивится, что первая большая сеть Екатеринбурга, построенная на коаксиале, оказалась последней. Сгоревшие за несколько минут 11 репитеров "закрыли" этот путь надолго. Это при всех удобствах RG-58 (дальнобойность, стойкость у погодным условиям, шинная топология, дешевизна).

Репитеры, конечно, тогда починили (но не все). И сеть еще поработала. Но таких новых линий уже никто не делал.
И через 2 года лето унесло жизнь 6 хабам из 120 установленных. Еще около 20 частично "подгорели". И это при том условии, что "весна, как обычно, наступила неожиданно".

В связи с бесперспективностью защиты коаксиальных линий передачи данных (по крайней мере в рамках серийного оборудования Ethernet), дальнейшее изложение будет посвящено защите оборудования, использующего симметричные линии (витую пару).

На сегодня в применении грозозащит превалирует два подхода:

- Ставим на жилу витой пары неонку или разрядник из прибора с работы (свалки), авось пронесет.
- Используем схему APC (только упрощенную), потому что буржуи давно так делают. Полученное устройство неплохо защищает, а лучше сделать будет слишком дорого.

Вообще, оба подхода имеют право на существования, и себя оправдывают. Но в условиях массового промышленного применения "защита на 95%" явное слабое звено.

Процессы, происходящие при наводке

Попробуем понять, что происходит в грозу. При этом нет смысла рисовать сложные схемы растекания наводки, и понимать механизмы распространения электромагнитных волн во влажном городском воздухе.

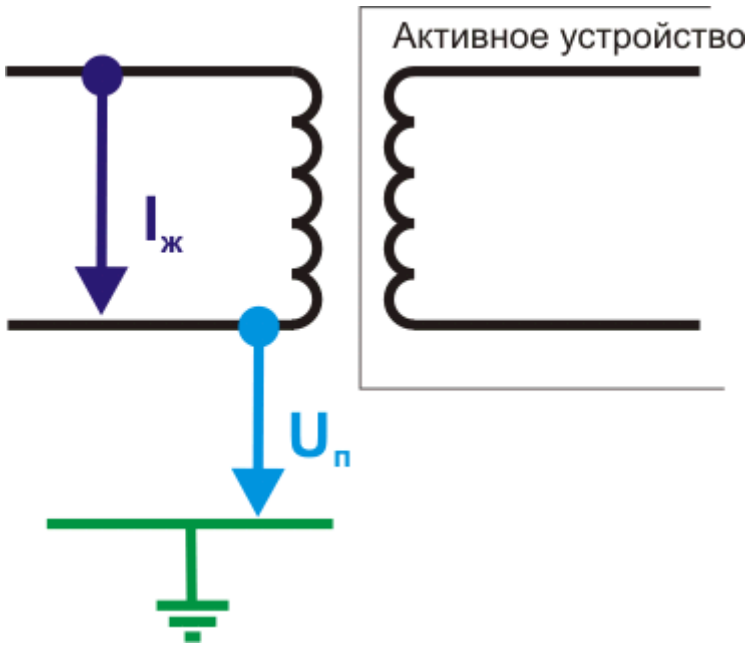

Рис. 4.11. Явления при наводке на витую пару.

Результат будет все равно один. Через первичную обмотку трансформатора активного устройства будет течь ток (Iж), и вместе с тем эта же обмотка получит напряжение (Uп). Других заметных физических результатов не сможет добиться ни одна наводка.

Поражение активного устройство может пройти следующими способами:

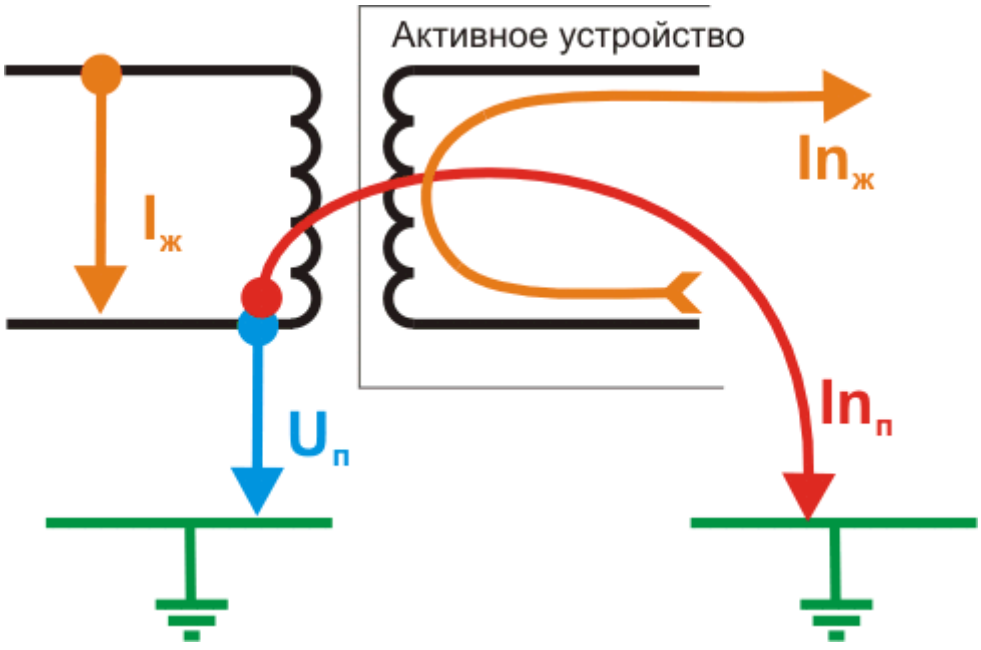

Рис. 4.12. Поражение устройства наводкой на витую пару.

Во-первых, это пробой на землю сетевой карты или коммутатора (Inп).
В этом случае напряжение Uп должно "пробить" трансформаторную сборку (которая выдерживает порядка 1,5 кВ), затем "вскрыть" несколько конденсаторов на плате, центральный чип устройства или (и) оставить следы разряда на печатной плате.

Встречаются ли такие повреждения на практике? Безусловно - около 3-5% случаев с использованием простых мер грозозащиты имеют именно такую клиническую картину. А без использования защитных средств - до трети устройств выходят из строя подобным образом.

Во-вторых, "просачивание" высокочастотной составляющей наводки через емкость трансформаторной сборки.

Скорее всего, это главный поражающий фактор. При этом трансформаторная сборка вполне может оставаться целой, невредимой, как и все элементы обвязки. Устройство будет выглядеть "совсем" как живое. Только не работать. Совсем как в анекдоте про автомобили и ремни безопасности.

Проверка простая - на выгоревший таким образом хаб перепаивается центральный чип - и он начинает нормально работать (многократно проверено).

В-третьих, наводка на вторичную обмотку трансформаторной сборки.
Никакой защиты от этого в диапазоне частот Ethernet нет. Т.е. если на вход придет 20-30 Вольт с частотой 10 МГц, то наведенный ток вызовет напряжение 20-30 Вольт на вторичной обмотке, и далее в чипе активного устройства. Для последнего это верная смерть.

Вывод. Простые схемы (обычно клоны APC) достаточно надежно спасают от пробоя на землю, но почти не помогают от индуктивной или емкостной наводки на вторичную обмотку трансформаторной сборки.

Вернемся к классической схеме грозозащиты, снятой с APC:

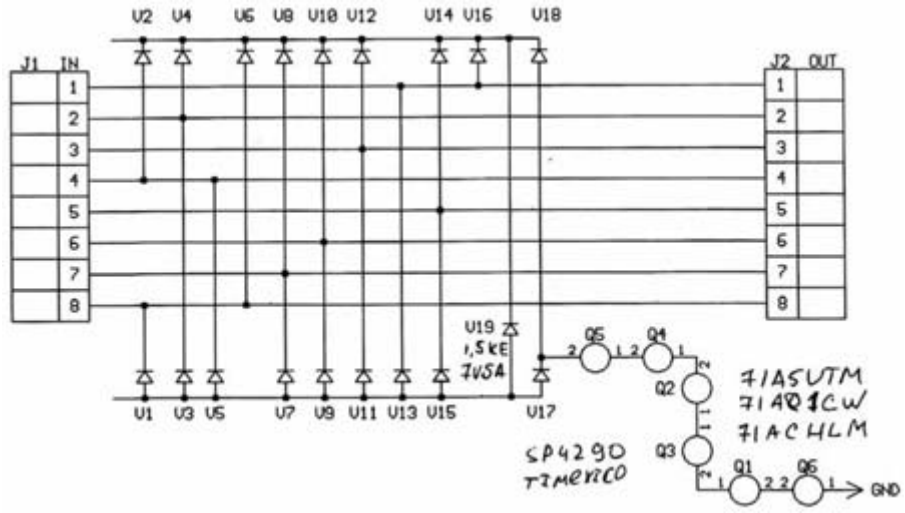

Рис. 4.13. Схема грозозащиты APC. Описание диода 1n4006, ограничителя напряжения 1.5ke7M5A. Описание последних элементов (Q1-Q5) так и не удалось найти, но по смыслу они прекрасно заменяются разрядником или даже искровым промежутком.

Принцип действия: При нормальной работе диоды запираются за счет встречно включенного ограничителя напряжения (и энергии полезного сигнала). При превышении порога срабатывания ограничителя на нем превращается в тепло выпрямленный на диодах сигнал. При повышении напряжения относительно земли более 500 В (в самодельных версиях от 70 Вольт), срабатывает разрядник, или что его заменяет.

В принципе, все просто и надежно. Но, как было показано выше, есть и минусы.

1. Несмотря на все меры, устройства продолжают выгорать от наведенного на вторичную обмотку высокочастотного сигнала;
2. Несмотря на то, что в самодельных защитах используются разрядники, защита не спасает от мощных импульсов после разрушения части диодов, так как не имеет предохранителей;
3. Современные сети так или иначе переходят на 100 Мб магистрали. При этом расходование энергии сигнала на запирание диодов становится непозволительной (в техническом плане) роскошью.

Как можно бороться наводкой на вторичную обмотку?

Представим, что на вход подан сигнал с амплитудой 5000 Вольт. Как поведет себя ограничитель напряжения? Время его реакции около 200 нс (5 МГц). Реально он, конечно, сработает - но пропустив заметную энергию высокочастотного импульса.

Газовый разрядник еще хуже. Его время срабатывания 1-5 мкс... Лучшие образцы - до 200-500 нс. Поэтому целесообразно применять его в качестве первичной защиты для "сброса" наводок большой мощности, либо для создания потенциальной "развязки" от "земли" (для исключения влияния последней на работу защиты).

Какие есть методы борьбы с явлением? Только резко уменьшить время срабатывания защитных элементов. Например, использованием быстродействующего варистора фирмы EPCOS. Время срабатывания - менее 0,5 нс. Блестящий результат, обеспечивающий применение в грозозащитах по типовой схеме:

Рис. 4.14. Схема грозозащиты с варистором. Минусы - стоимость (10 рублей варистор, а их нужно 4), и сравнительно низкая мощность (могут сгореть даже с дополнительным ограничителем напряжения или разрядником). Как не мала на первый взгляд стоимость в 40 рублей - реально это заметно удорожит итоговую стоимость изделия.

Следующий вариант несколько нетривиален. Диоды стандартной схемы АРС можно запереть дополнительным напряжением, и им же держать открытым ограничитель напряжения (на микротоке). В результате, имеем низкую емкость (диоды заперты), и малое время срабатывания при грозовой наводке, так как ограничитель напряжения **уже открыт**.

Остается застраховаться от разрушения диодов (или варисторов) при сверхмощных наводках плавкими предохранителями. Логика тут простая. Диоды должны сначала сгореть "в гайку", а уже потом рассыпаться. Пока они не рассыпались - линия в общем защищена. И до этого момента должны успеть сработать плавкие предохранители.

Конечно, простые плавкие предохранители имеют недостаток - перегорают безвозвратно. Самовосстанавливающиеся элементы дороги (около 10 рублей) и сильно гасят полезный сигнал. Поэтому нельзя выбрать слишком маломощные вставки. Но известно, что на практике диоды горят редко - поэтому с данным недостатком проще мириться.

Последний вариант грозозащиты - конструкция, содержащая приемо-передатчик (по сути, упрощенный 2-х портовый хаб, возможно не содержащий цифровой части). Такая защита способна спасать оборудование в самых тяжелых ситуациях, однако - ценой сравнительно высокой стоимости.

При современных ценах на коммутаторы и оптику ее масштабное использование едва ли целесообразно.

Еще одну особенность необходимо отметить отдельно. Широко распространен метод защиты конечного клиента методом "отключения". Т.е. в грозу абонент должен сам позаботиться о себе, и вытащить разъем из сетевой карты. Метод вполне надежный и логичный, но...

Что происходит при этом с проводом? Один из его концов становится разомкнутым. Т.е. исчезает то спасительное самовыравнивание потенциалов проводников витой пары. Сетевая карта, конечно, остается целой. А вот порт на хабе выгорает с большей вероятностью. Экономически представляется вполне целесообразным установить у всех клиентов грозозащиты. И клиенту проще, и порты целее.

Вариант с простыми "закоротками" (вынул кабель из карточки - закоротил специальным разъемом) годится только для небольших и дисциплинированных сетей. Коммерческим клиентам всего и не объяснишь...

Итоги

Вот основные моменты, повышающие шансы выживания сети. Если, конечно, у вас не оптика. :-)

- Использование экранированной витой пары.
- Заземление (зануление) экрана.
- Установка грозозащит как со стороны оборудования провайдера, так и со стороны абонента.
- Использовать решения, наименее зависящие от пограничных свойств элементов.
- Желательно хотя бы раз в несколько лет обновлять грозозащиты...
- Использование кольцевых топологий для минимизации времени простоя.

Немного про экономику. Казалось бы, при современных ценах на хабы (от $25), вполне достаточно просто статистически вывести потери на приемлемый уровень. Даже если сгорит 20% - это не так страшно. Для большой сети в 100 хабов (это 300-500 человек) потеря за сезон 500 баксов несущественна. Что там, 1-2 бакса на человека.

Но реально, не так существенны потери от сгоревшего оборудования. Велики потери от простоя абонентов. И именно из-за них приходится выводить статистику на качественно другой уровень. Применять защиты, оптоволокно. Постоянный ремонт, плюс недовольство "почему так долго" обходится в такие деньги, что потери на сгоревших хабах становятся просто малозначимыми.

Поэтому, все же, будущее за оптоволокном, по крайней мере на магистралях. Но и про "медь" еще долго не забыть. Ведь подвержены наводкам и линии внутри домов, особенно если они идут по чердаку. Даже оптоволоконно-витопарный конвертер (FO-TP) нуждается в этом случае в защите. :-)

Глава 5. Смежные технологии передачи данных. Обзор.

Не хлебом единым...

Как бы ни был хорош Ethernet как среда передачи данных, все необходимые для работы провайдера функции он может выполнять только при небольшом масштабе работ. При массовом оказании услуг находится масса мест, где удобнее применять иные технологии.

Это могут быть арендованные кабеля, отдаленные точки, непроходимые для самостоятельных прокладок расстояния между домами, и многое другое. Поэтому нужен хотя бы минимальный обзор технологий, с помощью которых можно эффективно связывать отдельные сегменты сетей.

Краткое описание технологий:

- xDSL. Сокращение DSL расшифровывается как Digital Subscriber Line (цифровая абонентская линия). Технология позволяет значительно расширить полосу пропускания "классических" медных пар (телефонных линий). При этом возможны скорости от 32 Кбит/с до более чем 50 Мбит/с. Обычное расстояние, на котором возможна высокоскоростная связь, составляет 5-6 км.
- HomePNA. Предназначена для недорого соединения в сеть "поверх телефонной проводки" пользователей внутри одной квартиры или коттеджа. При этом обеспечиваются произвольная топология соединения кабелей и скорости от 1 Мбит/с (HomePNA 1.0 и 1.1) до 10 Мб (HomePNA 2.0) на расстояния порядка 300-500 метров. Для передачи данных используется диапазон частот 5,5 — 9,5 МГц.
- Радио-Ethernet. Название говорит само за себя - это передача данных через эфир на частотах гигагерцового диапазона (обычно для недорогих решений используется 2,4 ГГц). Скорости - от 1 Мб до 50 Мб (и возможно выше), расстояния до нескольких десятков километров.
- Линии кабельного телевидения (гибридные сети). Технология предназначена для передачи данных через коаксиальные сети КТВ, и использует отличные от ТВ-сигнала диапазоны. Решения данного типа могут быть весьма сложными, но проработанными до мелочей из-за широкого распространения в некоторых странах (например США).
- Связь по силовой проводке. Пожалуй, это самая новая из технологий, представленных в данном списке. Она позволяет (по крайней мере в теории) передавать данные по стандартной электрической проводке 220 Вольт на скорости до 11 Мб и на расстояния в сотни метров.

- Использование атмосферных лазеров. Передача сигналов в оптическом (как правило инфракрасном) диапазоне. Как правило решение позиционируется в России как не требующая лицензирования замена Радио-Ethernet. Однако у лазерной технологии есть и другие достоинства - высокая скорость (до гигабита), сложность перехвата данных, возможность организации сложных по топологии сетей. К сожалению, недостатков то же достаточно.
- Экзотические способы (различные модификации Ethernet, связь через com-порты, частные технологии, однопроводная связь, и т.п.). Тут комментарии излишни.

Таким образом видно, что у Ethernet масса конкурентов, заметно превосходящих его в частности. И эти достоинства надо использовать в полной мере. Подробный разбор технологий выходит далеко за рамки данной книги, однако обзорное описание просто необходимо, и оно приведено с следующих параграфах.

Часть 3. Глава 5

xDSL.

Исторически самым узким местом последней мили считалась абонентская телефонная линия (медная пара). Проблема увеличения скорости передачи данных на этой дистанции решалась разными способами, но в рамках одной общей концепции.

Рассмотрим теорию.

Традиционные модемы передают аналоговые сигналы в диапазоне частот, предназначенных для обычной телефонной связи (300 Гц - 3400 Гц). Практически все возможности увеличения скорости в этой полосе уже исчерпаны, можно сказать, что на стандарте V.90 достигнут теоретический предел (56к).

Дальнейшее развитие возможно только при использовании более высоких частот и цифровых сигналов. При этом данные не смогут пройти через аппаратуру телефонных станций, и линия может быть использован только на участке абонент - АТС (или на обычной выделенной медной паре). Это заметно снижает возможности применения DSL, но преимущества в скорости оказались слишком велики, и технология начала бурно развиваться.

Буквально за несколько было разработано несколько десятков видов DSL, отличающихся методами модуляции, используемых для кодирования данных. На сегодня можно выделить следующие основные стандарты:

- ADSL - Asymmetric Digital Subscriber Line. Асимметричная цифровая абонентская линия.
- SDSL - Simple Digital Subscriber Line. Симметричная высокоскоростная цифровая абонентская линия, работающая по одной паре.
- VDSL - Very High Speed Digital Subscriber Line. Сверхвысокоскоростная цифровая абонентская линия.

Рассмотрим подробнее каждую из технологий.

ADSL.
Система была разработана в Северной Америке в середине 90-х годов. В то время считалось, что будет широко востребована услуга видео по запросу (причем в кодировке MPEG) для которой, собственно, ADSL и создавалась. Кроме несимметричной скорости под нужды потокового видео использовалась высоконадежная упреждающая коррекция ошибок. Из-за этого системы ADSL (особенно ранние) при передаче данных имеют большую задержку (до 20 мсек, что почти в 10 раз больше чем у систем SDSL или HDSL).

Но все же главным практическим признаком ADSL является асимметричность передачи данных. От сети к пользователю скорость значительно выше ("нисходящий" поток от 1,5 Мбит/с до 8 Мбит/с), чем в противоположном направлении ("восходящий" поток данных от 640 Кбит/с до 1,5 Мбит/с). Наибольшая скорость достигается на расстоянии до 3 км, а максимальное расстояние для устойчивой связи на минимальной скорости около 5-6 км.

Так же можно выделить разновидность G.Lite ADSL, которая представляет собой более дешёвый и простой в установке вариант технологии ADSL, обеспечивающий скорость "нисходящего" потока данных до 1,5 Мбит/с и "восходящего" до 512 Кбит/с (или по 256 Кбит/с в обоих направлениях).

Конечный пользователь обычно потребляет значительно больший трафик, чем отдает, поэтому данная технология весьма удобна для организации доступа в сеть Интернет. Так как это считается массовой услугой, устройства организации канала для оператора и абонента резко отличаются. На стороне провайдера устанавливается сложный многопортовый (сотни портов) мультиплексор-маршрутизатор (DSLAM), а на стороне пользователя - простейший модем.

В России широко используются DSLAM Cisco 6200 и Lucent Stinger. Стоят такие устройства несколько тысяч долларов, и практически неприменимы для нужд "домашних" сетей. Известны и примеры оборудования для организации каналов ADSL точка-точка (Pairgain MegabiModem 320/310), но особого распространения они не получили.

Нужно отметить, что большим достоинством ADSL является возможность работы по одной линии параллельно с телефоном (и не мешая друг другу). Принцип хорошо демонстрирует следующая диаграмма:

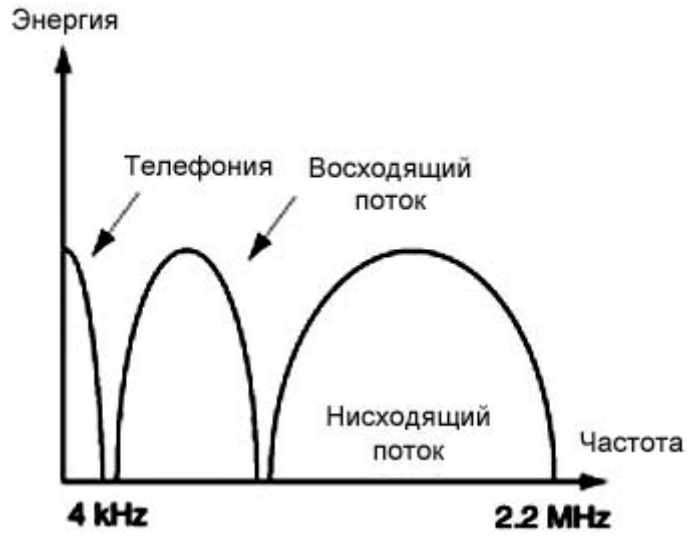

Рис. 5.1. Частоты ADSL.

Для того, что бы телефон и ADSL не мешали друг другу на одной линии используют сплиттер (POTS Splitter) - пассивное устройство которое разделяет частоты (либо ограничивает "верхний диапазон" перед телефонным аппаратом). Спектр частот ADSL обычно начинается с 25 кГц, поэтому полоса от 4 кГц до 25 кГц используется сплиттером в качестве переходной полосы.

В общем можно сказать, что ADSL не слишком удобна для организации связи между удаленными сегментами сетей Ethernet по следующим причинам:

- По сути отсутствует подходящее оборудование (точка-точка или малопортовые DSLAM);
- Асимметричность передачи данных неудобна для равномерного межсегментного трафика;
- Относительно большие задержки заметны во многих широкополосных приложениях (например в играх).

Тем не менее, ADSL широко используется телефонными монополистами в качестве недорогой услуги подключения к сети Интернет, поэтому часто у "домашних сетей" просто нет выхода. Приходится использовать то, что доступно, а не то, что удобно.

SDSL.
Эта технология фактически явилась развитием HDSL (High Speed Digital Subscriber Line, высокоскоростная цифровая абонентская линия), который в свою очередь берет свое начало от стандарта ISDN-BA. Когда разработчики DSL пытались повысить тактовую частоту ISDN, оказалось, что даже простая 4-уровневая модуляция PAM позволяет работать на скоростях до 800 Кбит/с практически во всей зоне обслуживания телефонного оператора (3-5 км).

Были разработаны устройства, работающие по одной паре на скорости 784 Кбит/с, и 1,544 Мб/с по двум парам (скорость 1,5Мб важна для передачи распространенных с США потоков T1). Дальнейшее развитие привело к появлению SDSL (симметричная скорость 2,3 Мб/с), для которой рекомендованы амплитудно-импульсная модуляция 2B1Q и более "дальнобойная" амплитудно-фазовая модуляция без несущей (CAP).

Технологий SDSL применяется в основном для связи точка-точка, используемое оборудование обычно одинаково для обоих сторон канала. Реже встречаются малопортовые DSLAM (например Lucent DSLMAX20 на 8-32 линии). Стоимость устройств SDSL несколько больше, чем ASDL.

Очевидно, что симметричные линии предназначены для связи удаленных сегментов корпоративных или "домашних" сетей, но не слишком удобны для конечного пользователя.

Часто считается, что SDSL не может функционировать на одной линии параллельно с телефоном. Но это не совсем верно. При скоростях более 700 Кб/с частоты SDSL и обычной телефонии разделены вполне достаточно для использования сплитеров (например Aviv16-SS) для нормальной совместной работы. Это заметно расширяет возможности применения данной технологии.

Последнее время SDSL все чаще заменяется ShDSL (Symmetric High bit-rate DSL), который отличается только типом кодировки (TC-PAM в отличии от 2B1Q или CAP). Этот стандарт на 10-15% более "дальнобойный", чем SDSL, но имеет и свой недостаток.

Частотное уплотнение на ShDSL не работает, поэтому не редко модемы выпускаются со встроенными портами IP-телефонии.

К сожалению, из-за более высокой стоимости SDSL (ShDSL) "телефонные" операторы редко предлагают такую услугу даже в том случае, если место конечного пользователя занимают несколько небольших "домашних" сетей.

VDSL.
Технология VDSL является наиболее современной и "быстрой" технологией xDSL. Скорость передачи данных "нисходящего" потока составляет от 11 до 52 Мбит/с, "восходящего" - в пределах от 1,5 до 2,3 Мбит/с. На некоторых моделях оборудования доступен синхронный режим со скоростями до 26 Мб/с.

VDSL можно рассматривать как высокоскоростной ADSL, рассчитанный на небольшие расстояния (до 1 км.). Устройства просты, весьма недороги, и получают последнее время все большее распространение. на небольших кампусных сетях.

Использование VDSL по обычным телефонным кабелям возможно, но с серьезными ограничениями. Для этой технологии используются частоты мегагерцового диапазона, на который ТПП не рассчитан (у SDSL предел в сотни кГц). Поэтому две VDSL линии в одном кабеле вполне могут не работать из-за взаимных наводок.

И если в случае использования 2-3 линий может помочь перебор пар, то при более плотном заполнении вероятно полное или частичное прекращение работы любых DSL технологий.

С другой стороны как пользователи, так и производители оборудования перестали рассматривать VDSL как дорогую WAN-технологию. Он позиционируется скорее как удлинитель Ethernet, со всеми вытекающими ценообразовательными последствиями. Появляются комбинированные коммутаторы Ethenret - VDSL, в которых последний играет ту же роль, которую обычно предназначали оптоволокну.

Поэтому представляется, что VDSL имеет очень большие перспективы в сетях Ethernet-провайдеров. Однако их, все же, не нужно переоценивать. Дальность (и сама возможность) работы VDSL явно недостаточна для вытеснения как ADSL так и SDSL, и им предстоит достаточно мирное сосуществование в разных технических нишах.

В перспективе можно ожидать появление единого стандарта, сочетающего достоинства всех рассмотренных технологий. Предпосылки к этому уже есть сейчас, но все же практическое внедрение - дело не слишком близкого будущего.

Часть 3 Глава 5

HomePNA и Cisco RLE.

Если технология xDSL пришла в домашние сети со стороны "традиционных" операторов связи, то HomePNA, наоборот, первоначально была разработана даже не для офисного, а исключительно для домашнего, бытового применения.

История технологии в общем достаточно проста. В больших, двух-трех этажных американских коттеджах начало появляться по несколько компьютеров, которые хотелось с минимальными затратами связать в одну сеть. Из имеющейся инфраструктуры - силовая и телефонная проводка. Последнюю, как наиболее удобную, и решили использовать для создания ЛВС.

Отвечая на потребность рынка, в 1996 году несколько производителей телекоммуникационного оборудования создали альянс, получивший название Home Phoneline Networking Alliance. В 1998 году появился стандарт передачи данных по телефонным линиям, названный HomePNA.

Решение в теоретическом плане было выбрано достаточно очевидное.

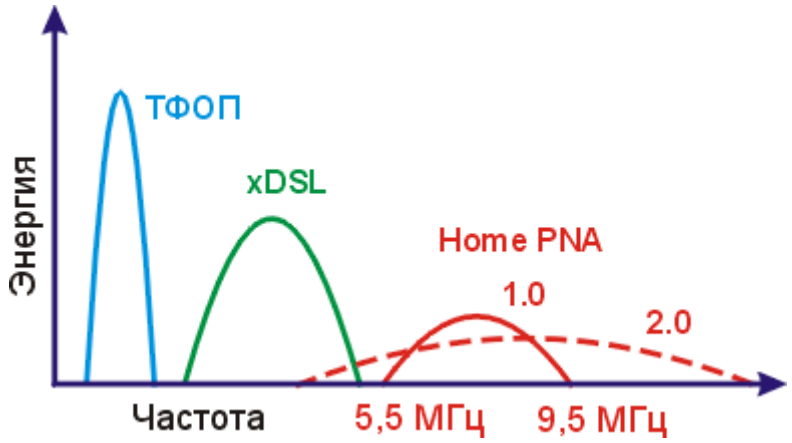

Рис. 5.2. Частоты HomePNA.

Частоты HomePNA вынесены выше не только телефонии, но и xDSL, поэтому они все вместе могут использоваться в одной и той же медной паре (со сплитером). Скорость HomePNA стандарта 1.0 и 1.1 составляет 1 Мбит/с на полосе от 5,5MHz до 9.5MHz, и методе доступа к физической среде 802.3 CSMA/CD. Дальность работы - от 300 метров до 1 километра в зависимости от линии и оборудования.

Т.е. фактически это то же Ethernet, только более "дальнобойный" и помехоустойчивый. Для этого применяется многократная кодировка одиночного битового импульса, плюс запатентованный метод модуляции MLCM включает в себя цепь, способную адаптироваться к различным уровням помех, которые могут возникнуть в линии. В дополнение к этому, передающая цепь может изменять уровень сигнала в зависимости от условий работы.

Кстати, подобный механизм очень удобен для массовых инсталляций, например ADSL G.Lite поддерживает аналогичные функции.

Высокая помехоустойчивость позволяет HomePNA работать практически на любом типе абонентских линий, и главное, на любой их топологии (как это обычно и получается в домашней телефонной разводке). А ориентация на домашний сегмент рынка делал сетевые адаптеры и бриджи доступными по цене (от $20 сетевая карта и $80-100 бридж).

Развитием технологии HomePNA является версия 2.0, позволяющая осуществлять передачу данных со скоростью 10Мбит/с, и совместимая на уровне активного оборудования с предыдущей версией 1.0. При этом был использован частотный диапазон от 2 до 30 МГц и более эффективный 8-ми битный метод кодирования одного символа.

Дальнейшее развитие было вполне предсказуемым. Квартирное (по сути) решение попытались использовать операторы "последней мили". Появились многопортовые устройства HomePNA (например 12 портовый City Netek 1412M), предназначенные для оказания услуг передачи данных в многоквартирном доме или кампусе, а так же дальнобойные системы (до 1-1,5 км).

Но это было возможно только для стандарта 1.x. Более скоростной 2.0 давал слишком сильную помеху на соседние порты, и не было технической возможности объединить их в один конструктив. Таким образом технология разделилась на два параллельных направления.

Стандарт HomePNA 1.x получил развитие в топологии "звезда", где каждый пользователь подключается к отдельному порту коммутатора, и работает на скорости 1 Мбит/сек. Возможность подключения нескольких пользователей к одному порту по линии произвольной топологии обычно сохраняется, но как правило не используется из-за нестабильной работы подобной конфигурации.

Стандарт HomePNA 2.0 предназначен для топологии "шина", в которой полоса пропускания делиться между всеми пользователями. Их количество в теории может достигать 32, но на практике даже 3-4 абонента встречаются редко. Значительно чаще HomePNA 2.0 используется для соединения "точка-точка", как недорогая замена xDSL.

Можно сказать, что небольшую нишу в провайдинге HomePNA в России получил. Известны громкие (и не очень) проекты интернетизации жилых домов и офисных зданий с использованием телефонной проводки. Несколько менее были распространены попытки использовать "под Интернет" сети радиофикации. Однако заметных успехов на данном поприще замечено не было.

Рожденная для среднего американского коттеджа, технология так и не смогла закрепиться в провайдинге.

Главной причиной можно назвать нестабильную работу и отсутствие методов и способов контроля. Непредсказуемость в коммерческой передаче данных совершенно неприемлема, а с HomePNA была масса примеров необъяснимой работы на сверхдальние дистанции, и отказов на "идеальных" линиях.

Да и экономика внесла свою лепту. Проложить заново что одну пару, что две - разница в цене совсем небольшая. Использовать же для передачи данных "чужую" сеть в России организационно сложно, дорого, да и перспектива совместной работы через несколько лет представляется туманной (договора мало что значат, и велик риск вообще остаться без сети, у "разбитого корыта").

Но еще хуже оказалось то, что HomePNA плохо работает (или даже совсем не работает) в многопарных кабелях. Одно это могло сразу вычеркнуть HomePNA из списка операторской техники, да сыграла свою роль привлекательность дешевизны.

Но окончательно "звезда" HomePNA закатилась с распространением VDSL, который примерно в той же нище обеспечивает стабильное, предсказуемое качество - и с большей скоростью. Правда HomePNA продолжает выигрывать в цене благодаря наличию в линейке оборудования сетевых карт (чего нет в VDSL), но эта разница не велика в абсолютных цифрах ($30 за NIC HomePNA и $100 за бридж VDSL), и особого влияния на ситуацию не оказывает.

Более того, попытки ассоциации HomePNA выйти из кризиса с 100-мегабитной версией 3.0 судя по всему обречены на провал. Стандарт фактически никто не поддержал.

Таким образом рекомендовать HomePNA к активному применению нельзя, хотя в некоторых случаях вполне можно использовать для решения локальных вопросов.

Cisco LRE

Примерно во время появления HomePNA в недрах Cisco был разработан свой вариант удлинения Ethernet. Так как Cisco LRE (Long-Reach Ethernet) сразу позиционировался для сетей кампусов и офисных зданий, его параметры значительно превосходят HomePNA:

- 5 Мбит/с симметричный трафик, дальность до 1524 метров;
- 10 Мбит/с симметричный трафик, дальность до 1220 метров;
- 15 Мбит/с симметричный трафик, дальность до 1050 метров

Многопортовые устройства были выпущены на основе Catalyst 2900XL, что позволяет использовать всю мощь стандартных функции серии (QoS, VLAN) на LRE портах (а это само по себе не мало). Абонентские Cisco 575 LRE то же имели свой ADSL-прототип.

Техническое решение получилось красивым и мощным (во многом морально устаревший LRE превосходит современные системы VDSL, и тем более, HomePNA). В кампусах или офисных зданиях система нашла свое применение, и вполне успешно работает.

К сожалению, были и недостатки, которые помешали широкому распространению LRE:

- Прежде всего высокая стоимость. Несколько сотен долларов за порт оказались слишком большой величиной для рынка.
- Отсутствие решения точка-точка (только коммутатор-точка). Это удобно для развернутой сети, но в то же время сильно поднимает стоимость начальной инсталляции.
- Полная неработоспособность в многопарных телефонных кабелях.

Все вышеперечисленное привело к фактической стагнации LRE-проека, а распространение недорогого VDSL вообще сводит на нет шансы возрождения данной технологии в руках операторов Ethernet-сетей. Тем не менее, если случайно (или недорого) удалось получить Catalyst 2900XL LRE - его не стоит выкидывать, применение этой мощной системе найдется.

Часть 3. Глава 5

Беспроводные сети.

Если вспомнить историю, то Ethernet идеологически начинался именно как "эфирная" радиосеть. Поэтому возвращение к истокам (хоть и в совершенно новом качестве) должно было когда-нибудь произойти. И показательно, что сегодня радиомодуль беспроводной связи становится такой же обычной принадлежностью компьютеров как, например, встроенный модем или сетевая карта.

Но если по логике работы беспроводные сети весьма похожи на Ethernet (по крайней мере в наиболее распространенных стандартах), то на физическом уровне отличия более чем

заметны. Да это и понятно - свойства "воздушной" среды очень далеки от "медного" кабеля. Настолько, что успешное использование беспроводной широкополосной связи немыслимо без нескольких технологических инноваций, с изложения которых и нужно начать эту тему.

Шумоподобные сигналы

Основная идея передачи и приема шумоподобных сигналов весьма проста - это принудительное расширение спектра (Spread Spectrum, SS).

Любой (в том числе прямоугольный) сигнал можно представить как набор синусоидальных гармоник с разной амплитудой и частотой. Но при этом основная энергия импульса будет сосредоточена в спектральной полосе, соответствующей длительности передаваемого сигнала.

Ширина спектра = 1/ти, где ти - длительность импульса. Отсюда следует, что чем меньше длительность импульса, тем большую полосу займет сигнал. Но так сложно передать сигналы небольшой мощности.

Повысить надежность приема оказалось несложно. Достаточно внести в него избыточность, например числовую последовательность (часто называемую шумоподобным кодом или чипом). в этом случае энергия сигнала "размазывается" по всему спектру.

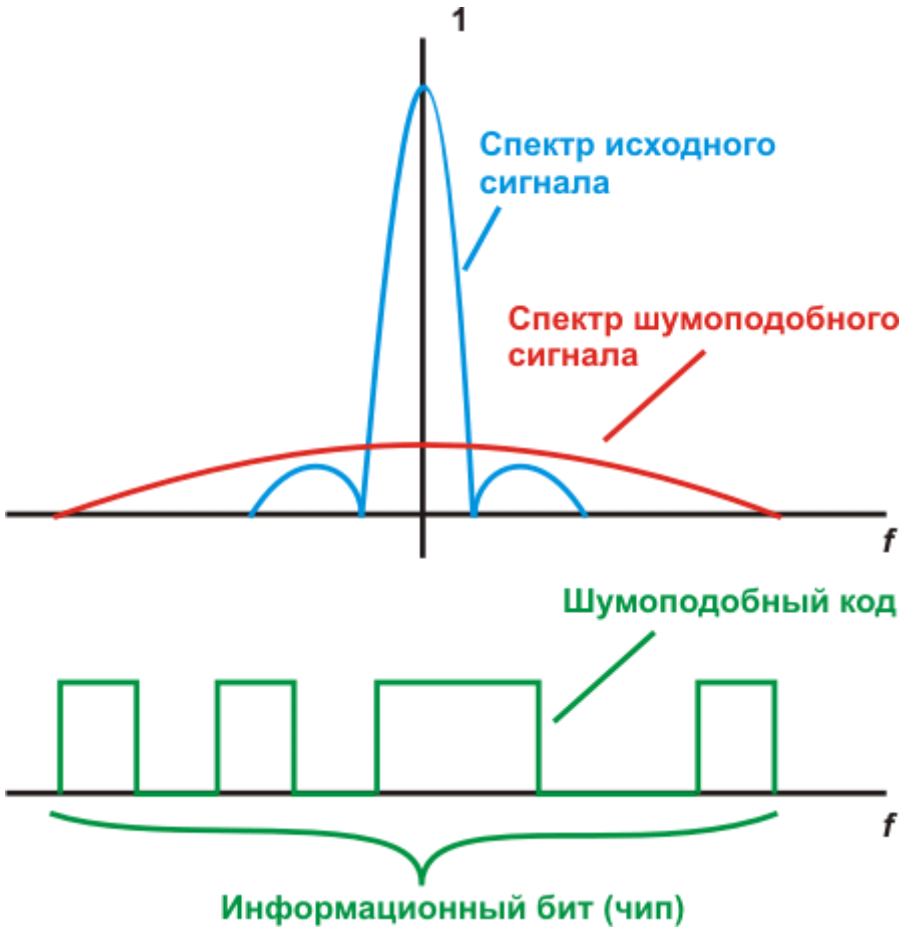

Рис. 5.3. Шумоподобный сигнал.

Для того, что бы можно было выделить чип из шума (который в эфире обязательно присутствует), используются специальные последовательности, обладающие свойствами автокорреляции. Т.е. при наложении на саму себя с некоторым сдвигом совпадение кода будет только в случае нулевого смещения. Наиболее известен в этом качестве 11-ти разрядный код Баркера (11100010010), прямой и инверсный вариант которого часто используется для передачи 1 и 0. Таким образом, передавая сигнал на уровне шума можно надежно его выделить и преобразовать в обычный узкополосный.

Нетрудно посчитать, что при информационной скорости в 1 Мб/с, чипы длительностью 1/11 мкс будут следовать на 11 Мчип/с, и ширина спектра составит 22 Мгц (частота соответствует 2/T, где T - длительность импульса). При этом надо помнить, что при помощи более сложных механизмов представления данных (например комплиментарных кодов) можно поднять сигнальную скорость в 2 и более раза.

Можно добавить, что при передаче сигналов в большинстве систем RadioEthernet используется обычная фазовая модуляция сигналов, не слишком отличающаяся по своей физической сути от методов, используемых в многих других системах, например xDSL.

Диапазон частот

В большинстве стран распределение частот осуществляется по разрешению национальных телекоммуникационных служб. Причем по ныне действующему распределению радиочастот, зафиксированному Всемирной Административной Радио Конференцией (ВАРК), диапазоны частот 2400-2483,5 МГц и 5725-5875 МГц отведены для использования "высокочастотными установками, предназначенными для промышленных, научных и медицинских целей" (так называемые ISM-диапазоны - Industrial, Scientific, Medical).

В США постановлением FCC (Федеральной Комиссии по Коммуникациям) в 1986 году, и спустя несколько лет в Западной Европе, было официально разрешено безлицензионное использование ISM-диапазонов широкополосными средствами связи, и в частности устройствами Radio-Ethernet, при условии ограничения мощности передатчика предельной величиной в 100 мВт.

Это вызвало бурный рост беспроводных технологии (Wireless LAN). Создавались они по большей части для решения обеспечение мобильности пользователей на территории одного дома, или их группы (кампуса). Естественно, за использование частоты не взималась плата. Надо отметить, что в России Wireless LAN никогда не были популярны, а оборудование использовалось в основном для связи нескольких сетей между собой на территории района, города или даже области.

Но, к сожалению, совсем не так обстоит дело в России. Мало того, что тут требуется немалая плата за использование частоты, так и процедура регистрации чудовищно сложна и запутана. Масштаб данного изложения не позволяет привести процедуру целиком, но за сложность говорит стоимость работ, которая составляет тысячи (или даже десятки тысяч) долларов США. И пока нет особой надежды на изменение ситуации - если только в 2003 году был упрощен порядок регистрации для сетей, расположенных внутри дома. Продолжения ждать придется долго.

Однако при всем этом эффективные средства борьбы с пиратскими линиями связи просто отсутствуют. В результате в большинстве крупных городов диапазон 2,4 ГГц стал свободным "явочным порядком". Количество пиратских линий выросло на столько, что

вынудило легальных операторов искать другие, свободные диапазоны (при этом деньги, потраченные на легализацию частот были, по сути, потеряны).

Да и как можно эффективно бороться с радиопиратами, когда стоимости активного оборудования опустилась ниже $100 (реквизиция никого не пугает), да еще чуть не каждый второй новый ноутбук имеет встроенный радиомодуль, а значит потенциальный "пират"?

Причем можно предположить, что "следующие" диапазоны постигнет та же участь. По мере снижения цен на оборудование диапазонов 3,4 и 5,2 ГГц количество пиратов будет быстро расти.Окончательный же результат предсказать пока сложно. Однако очевидно, что политика жесткого государственного регулирования провалилась, и не может эффективно защищать права "официальных" операторов.

Методы передачи

Для использования широкой полосы частот было разработано две принципиально различающихся между собой технологии. Это метод прямой последовательности (Direct Sequence Spread Spectrum - DSSS) и метод частотных скачков (Frequency Hopping Spread Spectrum - FHSS).

В режиме FHSS весь диапазон 2,4 ГГц используется как одна широкая полоса (с 79 подканалами). В режиме DSSS этот же диапазон разбит на несколько широких DSSS-каналов, так что до трех таких каналов может использоваться независимо и одновременно на одной территории. Номинальная скорость каждого канала 2 Мбит/с.

Метод DSSS позволяет достигать значительно большей производительности (2 Мбит/с на один канал, 6 Мбит/с на весь диапазон 2,4 ГГц), а кроме того, обеспечивают большую устойчивость к узкополосным помехам (выбором поддиапазона для передачи можно отстроиться от помех), и большую дальность связи.

FHSS выпускается значительно большим количеством компаний, она проще и дешевле, однако и пропускная способность ее ниже. Однако, достоинство FHSS-устройств состоит в том, что они, в отличие от DSSS, могут сохранять работоспособность в условиях широкополосных помех - например, создаваемых DSSS-передатчиками. Недостаток - сами они при этом мешают обычным узкополосным устройствам.

Взаимодействие устройств

Теоретические вопросы работы **локальных** сетей Radio Ethernet регламентированы стандартами семейстава IEEE 802.11. В нем определяется порядок организации беспроводных сетей на уровне доступа к среде передачи данных (MAC-уровень) и на физическом уровне (PHY-уровень).

Изначально стандарт IEEE 802.11 предполагал возможность передачи данных по радиоканалу на скорости 1 Мбит/с и опционально на скорости 2 Мбит/с. В более поздней версии - IEEE 802.11b, фактически являющейся дополнением к основному стандарту, определяется скорость передачи 1, 2, 5.5 и 11 Мбит/с. Следующие версии (a, g) еще более "подняли" скорость.

При взаимодействии устройств на MAC-уровне определяется два основных типа инфраструктуры сетей - Ad Hock и Infrastructure Mode. В первом случае возможен режим

точка-точка (узлы непосредственно взаимодействуют друг с другом), во втором - взаимодействие идет через точку доступа (Access Point), который играет роль концентратора. При этом возможны два режима взаимодействия - BSS (Basic Service Set), все станции связываются только через точку доступа, и ESS (Extended Service Set), при которой узлы могут взаимодействовать друг с другом.

Для доступа к среде передачи (PHY-уровень) применяется знакомая по Ethenret система доступа с обнаружением несущей (CSMA/CA, Carrier Sense Multiple Access/Collision Avoidance), только вместо обнаружения коллизий используется технология их избегания. Перед отправкой кадра в эфир станция посылает специальное сообщение (RTS, Ready To Send), которое говорит о готовности начать передачу, а так же ее продолжительности и адресате.

Соответственно, другие узлы могут задержать передачу, кроме принимающего, который передает сигнал готовности (CTS, Clear to send). Успешная передача подтверждается кадром ACK, после чего все возобновляется снова и снова. Упрощенно говоря, коллизии между абонентами допускаются только при резервировании (в процессе "соревнования" за занятие канала), а передача данных начинается уже без возможности коллизий.

С другой стороны, активно развивается рынок беспроводного оборудования операторского класса. Это достаточно большой круг систем, включающих в себя MMDS, LMDS, OFDM (будущий 802.16a), а так же ряд фирменных технологий. Среди этого разнообразия оборудования, технологий, цен и возможностей разобраться бывает нелегко даже специалисту, не говоря уже о начинающих.

Попробуем прояснить ситуацию, которая сложилась на практике.

Группа IEEE 802.11.

В настоящий момент эта группа, безусловно, доминирует на рынке. Однако, сразу необходимо отметить, что данные стандарты изначально разрабатывалась (и продолжают разрабатываться) как технология **локальных сетей** внутри помещений.

Грубо говоря, устанавливая точку доступа 802.11, получаем концентратор (хаб) с характеристиками, несколько ухудшенными относительно его "проводных" аналогов. Таким образом, на одну точку пропускной способностью 11Mb/s (802.11b) для большинства приложений возможно подключить до 10-15 клиентов.

Это обстоятельство делает фактически невозможным применение подобного оборудования в сетях доступа масштаба города или хотя бы района. Несмотря на то, что подобные сети были построены во многих городах, услугу нельзя назвать массовой (или качественной).

Достойным "outdoor" применением оборудования 802.11b являются соединения точка-точка или разнос на 2-3 точки на расстояниях до 7-8 километров.

Приведем краткую таблицу характеристик для группы 802.11

Стандарт	802.11	802.11b	802.11a	802.11g
Частоты	2,4-2,483 ГГц	2,4-2,483 ГГц	5,15-5,25 ГГц 5,25-5,35 ГГц	2,4-2,483 ГГц

			5,725-5,850 ГГц	
Метод передачи	DSSS,FHSS	DSSS	DSSS	DSSS
Скорость	1,2Мб/с	1,2,5.5, 11Мб/с	6,9,12,18, 24,36,48,54Мб/с	6,9,12,18, 24,36,48,54Мб/с
Метод модуляции	BPSK, QPSK	BPSK, QPSK, CCK	BPSK, QPSK	BPSK, QPSK
Дальность связи	До 50 км	До 50 км	До 40 км	До 40 км

Необходимо отметить, что в описаниях любого оборудования максимальная дальность связи указывается для условий, близких к идеальным. Да еще, как правило, с использованием весьма дорогостоящего антенно-фидерного оборудования.

Крупные зарубежные операторы связи очень редко применяют данное оборудование в своих сетях в основном из-за отсутствия каких либо гарантированных характеристик канала, которые собственно и являются продаваемым товаром.

Наиболее распространенными реализациями данных стандартов является оборудование таких компаний как Cisco (aironet), Proxim (ORiNOCO), Micronet (SP), D-Link, Linksys и т.п.

MMDS и LMDS подобное оборудование

Исторически эта группа оборудования разрабатывалась как система беспроводного многоканального телевидения с переносом в высокочастотные спектры. Позже появились реализации, позволяющие наложить сеть стандарта DOCSIS v1.0 на существующую радиосеть (DOCSIS - стандарт цифровой передачи в кабельных сетях). Таким образом, все характеристики цифрового тракта соответствуют данному стандарту (Downstream до 38 Mbps, разделяемый, Upstream от 0,3 до 9Mbps, на каждого пользователя).

Наложение цифровой сети оставляет возможность транслировать определенное количество телевизионных каналов (в зависимости от общего спектра системы). Высокая мощность передатчика обеспечивает значительную зону покрытия (до 40км).

Основной недостаток подобного рода систем - чрезвычайно высокая стоимость. Инсталляция одной базовой станции потребует от $150000, не считая затрат на получение частотного разрешения.

С частотами так же существуют определенные проблемы, обусловленные шириной спектра, требуемого системой. Общая стоимость развертывания сети на средний город оценивается в $700000-1000000. Таких средств у отечественных операторов как правило нет.

Фирменные технологии

Отсутствие стандарта на беспроводные сети с гарантированными характеристиками канала привело к появлению большого числа фирменных разработок. Наиболее

известными на текущий момент являются Tsunami (Proxim), Ultima3 (Wi-Lan), PacketWave(Aperto Networks) и Revolution (CompTek).

Рис. 5.4. Пример небольшой операторской базовой станции.

Относительно невысокая стоимость, $800-1600 за клиентское устройство (CPE) и $7000-30000 за базовую станцию, высокая надежность и возможность предоставлять лини с гарантированными характеристиками, делают подобное оборудование привлекательным для построения городских сетей доступа, или в качестве дешевой альтернативы ЦРРЛ.

Остается добавить, что уже идет работа по принятию стандарта IEEE 802.16a, в основу которого и ляжет OFDM. Поэтому велика вероятность, что в недалеком будущем недорогое оборудование LAN-уровня получит большую часть достоинств сегодняшних "фирменных" технологий.

Что, в свою очередь, позволит строить надежные радиосети большего размера, и с большей скоростью обмена данными.

Беспроводные сети. Антенны, кабеля и разъемы.

Для работы радиоканала кроме качественного активного устройства потребуется пассивная часть - антенна и подводящий кабель (антенно-фидерный тракт). Причем часто их стоимость существенно превышает цену простого радиобриджа.

С кабелем все в общем понятно - чем меньше затухание (dB Loss), тем он лучше. Причем надо помнить, что затухание нужно смотреть именно на той частоте, на которой будет работать канал. В качестве демонстрации можно привести паспортные данные на следующие кабеля:

RG-8x doublescreen

Параметр	Значение			
Частота (мгц)	300	900	1800	2400
Затухание (дб/м)	0,24	0,42	0,64	0,76
Внешний диаметр (мм)	7,5			
Диаметр центрального проводника (мм)	1,65			

Belden H-1000

Параметр	Значение			
Частота (мгц)	300	900	1800	2400
Затухание (дб/м)	0,07	0,12	0,18	0,24
Внешний диаметр (мм)	10,3			
Диаметр центрального проводника (мм)	2,5			

Параметры привычного для локальных сетей RG58 приводить не имеет смысла - потери на нем превысят всякие допустимые пределы (вплоть до 5-8 Дб/метр). Поэтому при любом расстоянии до антенны имеет смысл использовать специальный высокочастотный кабель, тем более сейчас он не слишком дорог - от 0,5 до 2,5 долларов за метр.

Понятно, что чем длиннее кабель, тем больше в нем потери. Так, 20 метров RG-8x внесут затухание порядка 20 * 0,76 = 15,2 Дб. Что сравнимо с усилением очень приличной антенны. Кроме больших потерь на затухание, длинный кабель является хорошей антенной, которая собирает все помехи из эфира. Конечно, на входе в активное устройство стоит узкополосный фильтр, но и он может не справляться с мощной помехой. А установка дополнительного - минимум минус 3 Дб.

Таким образом вынос активного устройства как можно ближе к крыше можно рассматривать как насущную необходимость, при длине фидера более 30-40 метров связь скорее всего будет невозможна без усилителей и мощных антенн.

Разъемы

Следующий по значению элемент высокочастотного тракта - разъемы. В радиоезернет широко применяются N-type, SMA, TNC и отечественный РК-50. Несколько менее распространены BNC, UHF, F-type, и другие "фирменные" стандарты. Практически все типы имеют конструктивы под обжим, пайку, а так же разнообразные переходники и разветвители.

Затухание в правильно смонтированных разъемах невелико, и эквивалентно 1-2 метрам кабеля. Но даже небольшая грязь или влага способны его резко увеличить - до нескольких Децибел, и невозможности связи. Поэтому работа с разъемами не слишком сложна, но требует большой аккуратности.

Основная причина неисправности в условиях крыш и чердаков - попадание воды в разъем или даже кабель (если в нем в качестве диэлектрика использован воздушный зазор). Поэтому герметизация соединений является одним из самых важных этапов монтажа.

Антенны

Антенны - в отличии от кабелей и разъемов - существенно более тонкая материя. Каких только типов не придумали специалисты на "эфирное" столетие. Панельные, коллинеарные (всенаправленные), волновой канал, логопериодические, спиральные, параболические, вибраторные... Но подробное рассмотрение технических характеристик перечисленных устройств выходит далеко за рамки данного материала. Поэтому придется ограничиться только кратким обзором.

Если не учитывать конструктивные отличия, все антенны можно разделить на всенаправленные (Co-Linear), секторные, и узконаправленные. Их различия понятны из названия. На практике всенаправленные антенны используются для небольших базовых станций, рассчитанных на работу с несколькими (максимум несколькими десятками) точек. У них мал коэффициент усиления, недостаточная помехозащищенность... В общем, при сложной эфирной обстановке всенаправленные антенны фактически неработоспособны, и тем более, не годятся для связи между сегментами Ethernet-сетей.

Более мощные базовые станции строят из нескольких секторов (антенн, имеющих диаграмму направленности в 60-180 градусов. При этом соседние сектора устанавливаются на разные частотные диапазоны, и не мешают друг - другу. С той же целью часто практикуется совместная установка двух антенн в разной поляризации (вертикальной и горизонтальной).

Но понятно, что при строительстве домашних сетей наиболее удобны узконаправленные антенны. Причем чем уже диаграмма направленности, тем лучше (к сожалению, антенну на 2,4ГГц с диаграммой меньше 30 градусов сложно изготовить). Меньше помех принимается, и меньше излучается, что то же немаловажно - особенно при безлицензионном использовании.

Наибольшее распространение получили панельные антенны и "волновой канал". Они просты в изготовлении, недороги, и обладают неплохими характеристиками. Вот пример панельной антенны FA-20 (усиление 20 Дб).

Рис. 5.5. Антенна FA-20 (модификация FA-16).

Стоимость такого решения порядка $50-70. Основной недостаток - высокая стоимость (при среднем усилении) и хорошая "заметность" антенны на крыше. Достоинство - узкая диаграмма направленности (порядка 20 градусов)

Следующая антенна относится к типу "волновой канал", марка POLARIS-2450 (усиление 17 Дб).

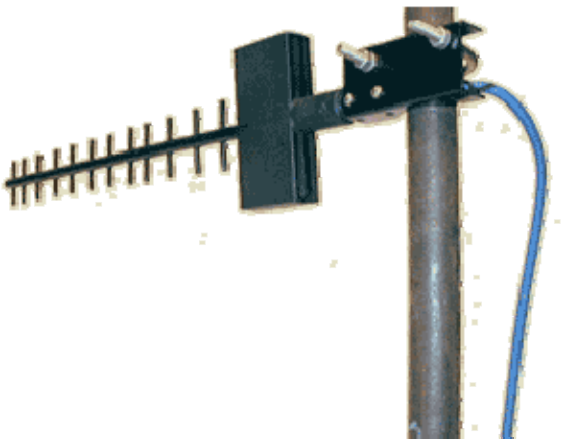

Рис. 5.6. POLARIS-2450-17. Это наиболее дешевый ($20-40), и в общем, наименее качественный вариант. Но недорог, и дает вполне сносные результаты. Главное достоинство - такие антенны легко маскируются на крыше под телевизионные.

В заключение можно упомянуть еще один экзотический тип антенн, которые часто используются в кустарных сетях. Это "баночная" антенна.

Рис. 5.7. Баночная антенна.

В качестве серьезного средства связи данное устройства рассматривать сложно. Тем не менее, технические параметры "банки" вполне на уровне - 7-8 Дб усиления можно получить даже без особых расчетов конструкции.

Грозозащита.

Так как антенна обычно ставится на крыше, нужно особо выделить такое ее свойство, как грозозащитные свойства. Почти все современные типы антенн являются короткозамкнутыми по постоянному току. Это само по себе весьма надежное средство против атмосферного электричества, только нужно заботиться что бы крепеж антенны (или трубостойка) были надежно заземлены.

В случае использования антенн экзотического типа, самодельных, и т.п. не короткозамкнутых, нужно либо устанавливать их в негрозоопасных местах, либо применять отдельную газовую или четвертьволновую грозозащиту (последнее, по сути, замыкает фидер по постоянному току на землю).

Непрямая видимость.

При использовании беспроводной связи в локальных сетях (и для связи локальных сетей) обычно никто не утруждает себя расчетом возможности связи. Есть прямая видимость - все нормально. Нет - работать не будет (разве что в пределах нескольких комнат).

В принципе, это верно. Но из повседневной практики известно и другое - уверенный прием телевизионного сигнала часто возможен и без прямой видимости. Радиоволны отражаются от стен домов и других поверхностей, и этого может быть вполне достаточно для работы радио-Ethernet.

В наиболее новых устройствах беспроводной связи возможность работы "на отражениях" поддержана на уровне методов кодирования, поэтому работает вполне эффективно. Настолько, что продавцы оборудования говорят о возможности связи "в отсутствии

прямой видимости". Отчасти это правда - но далеко не всегда. Причем достоверно предсказать результат без проведения испытаний невозможно.

Часть 3. Глава 5

Связь по силовой проводке.

Телефонная и силовая проводка - вот пожалуй все коммуникации, которые прокладывались в жилых домах еще несколько лет назад. Не удивительно, что к сетям 110/220 Вольт разработчики новых технологий уже давно присматривались на предмет передачи данных.

И в принципе, нельзя сказать, что безуспешно. Телеметрия, передача служебной информации - это все давно и успешно работает в электрическом хозяйстве. Вот только скорости при этом используются смешные по современным меркам - не более 9600 бит/с.

Для широкополосного доступа этого заведомо недостаточно. Большую скорость достичь очень сложно - все же силовой провод не коаксиал, и не витая пара - для высокочастотных сигналов он совершенно неприспособлен.

Однако, прогресс возможен и на таких сложных объектах. И уже несколько лет рекламные буклеты от производителей оборудования PowerNet не дают спокойно спать провайдерам домашних сетей. Поэтому рассмотрим технологию на следующем примере.

Примерно таким образом выглядит обычный сетевой адаптер для связи через силовую сеть:

Рис. 5.8. Сетевая карта для силовой сети.

Отличие, пожалуй, только в разъеме. Он имеет надежный, солидный габарит и снабжен дополнительной винтовой фиксацией заменителя RJ-45.

Но не стоит торопиться и просто соединять компьютеры через розетки в соседних комнатах. С вероятностью 66% связи не будет, потому что для работы объединяемые в сеть устройства должны быть подключены на одну фазу.

Это сразу и серьезно ограничивает возможности технологии - попробуй разберись кто и как проводил проводку в доме лет эдак 20 назад. А схема разводки для России вещь хоть и положенная к существованию всеми должностными инструкциями, но обычно не имеющаяся в наличии.

Так что для создания сети придется потратить изрядное время на согласование с электриками и владельцами (балансодержателями) здания для нахождения места включения по следующей схеме:

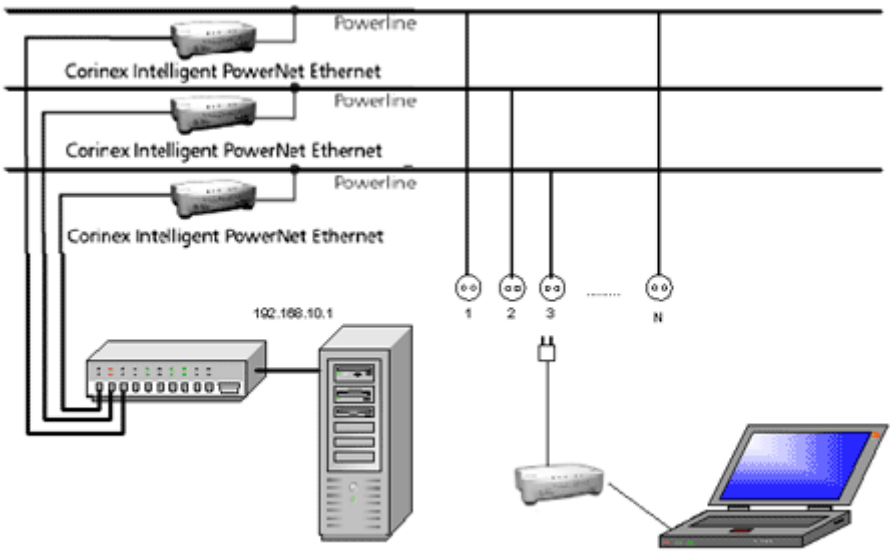

Рис. 5.9. Схема разводки сети по силовой проводке.

По такой схеме с активным оборудованием Corinex PowerNet были проведены натурные испытания в офисном здании постройки 80-х годов прошлого века, 7 этажей, 18 х 42 м. Точка подключения находилась приблизительно в геометрическом центре здания.

Наихудший линк выдал скорость 1,7 Мбит до подвала и некоторых комнат на 7 этаже, наилучший - по соседним комнатам 4 этажа - 7,2 Мбит. За суточный прогон трех точек падений линков не наблюдалось. От указанного в ТТХ (11 Мегабит на 300 метров) далековато, но для подачи Интернета по зданию более чем достаточно.

Однако сеть работала только в одном подъезде (т.е. на одном стояке силовой проводки). При переносе узла в подвал (в точку соединения нескольких силовых стояков) даже до 4-го этажа линия работала с трудом, а выше - связь отсутствовала в принципе.

На основе эксперимента можно сделать следующие выводы.

- Вполне вероятно, что для подключения трех абонентов (если они попадут на разные фазы) понадобится шесть устройств PowerNet. Это сильно увеличивает стартовые расходы.
- Нужно ставить "узел" на каждый силовой стояк. Так как "через подвал" работать не будет. Причина скорее всего в том, что именно там находится основное разветвление проводки, и мощность сигнала серьезно ослабляется. Серьезный минус.
- Одного узла на 12-16 этажей скорее всего будет недостаточно. Запаса по скорости нет уже через 3-4 этажа, через 6-8 может и не подняться вообще.
- В эксперименте не проверена работа с существенной нагрузкой. Например, на какой скорости будут связываться узлы, если из будет 20-30 в одной сети.

Выходит, говорить о использовании PowerNet в "домашних сетях" пока рано. Дорого, непредсказуем результат. Сейчас работает, завтра сосед подключил стиральную машину 20-ти метровым удлинителем и...

Таким образом, на первый взгляд это очередное решение "масштаба коттеджа". Но есть некоторые факты, говорящие о высоком потенциале технологии в сфере предоставления провайдерских услуг.

Все рассмотренные устройства Corinex PowerNet достаточно умные. Управляются по SMNP весьма сложной и многофункциональной программой. Основное - автоматическое распознавание топологии сети, тестирование сети, мониторинг (с графиками и статистикой).

Присутствует защита. Невозможно прослушивать, и подключаться к сети без знание правильного пароля. Скорее всего, этот механизм похож на используемый в радио-ethernet. С другой стороны, администратор сети удаленно может изменять настройки безопасности (пароль) каждого клиента удаленно, а также создавать пользовательские сети со своими настройками безопасности.

Оператор может управлять подключением/отключением пользователя. Установка любого дополнительного Powerline устройства требует взаимодействия с оператором.

Так что вопрос по использованию PowerNet в "домашних сетях" пока нельзя считать окончательно закрытым. Технология в будущем может быть усовершенствована.

А пока - есть еще один вариант решения нестандартных ситуаций. К сожалению, на практике более чем достаточно случаев, когда нельзя проложить кабель ни за какие деньги, а связь нужна почти "любой ценой".

Часть 3. Глава 5

Подключение через сети КТВ.

Сети кабельного телевидения можно назвать широкополосным "пережитком" аналоговой эры. Полосе передачи TV-сигнала позавидует большинство СПД, да и физическая основа - коаксиальный кабель - едва ли не лучшая среда для высокоскоростной связи.

Но для КТВ достаточно односторонней передачи от головной станции к телевизору пользователя, и это существенно ограничивает возможности кабельных сетей для подключения пользователей к Интернет. Впрочем, еще 5-6 лет назад были попытки использовать кабельные сети для односторонней передачи данных, а обратный канал делать с помощью коммутируемого доступа (подобно подключению через спутниковый канал). Но сейчас эта технология устарела и невостребована.

Выход из положения был легко найден. По мере роста телевизионных сетей им самим понадобились средстава управления линейными устройствами. И обратный канал был заложен в нормы и активное оборудование. Российским ГОСТом для обратного канала отведена достаточно узкая полоса частот (5-30 МГц). Этого на сегодня вполне достаточно для нужд провайдеров, но расширение в рамках существующих систем невозможно, а их масштабная замена стоит недешево.

Типичная схема двухсторонней передачи данных через сети КТВ выглядит следующим образом:

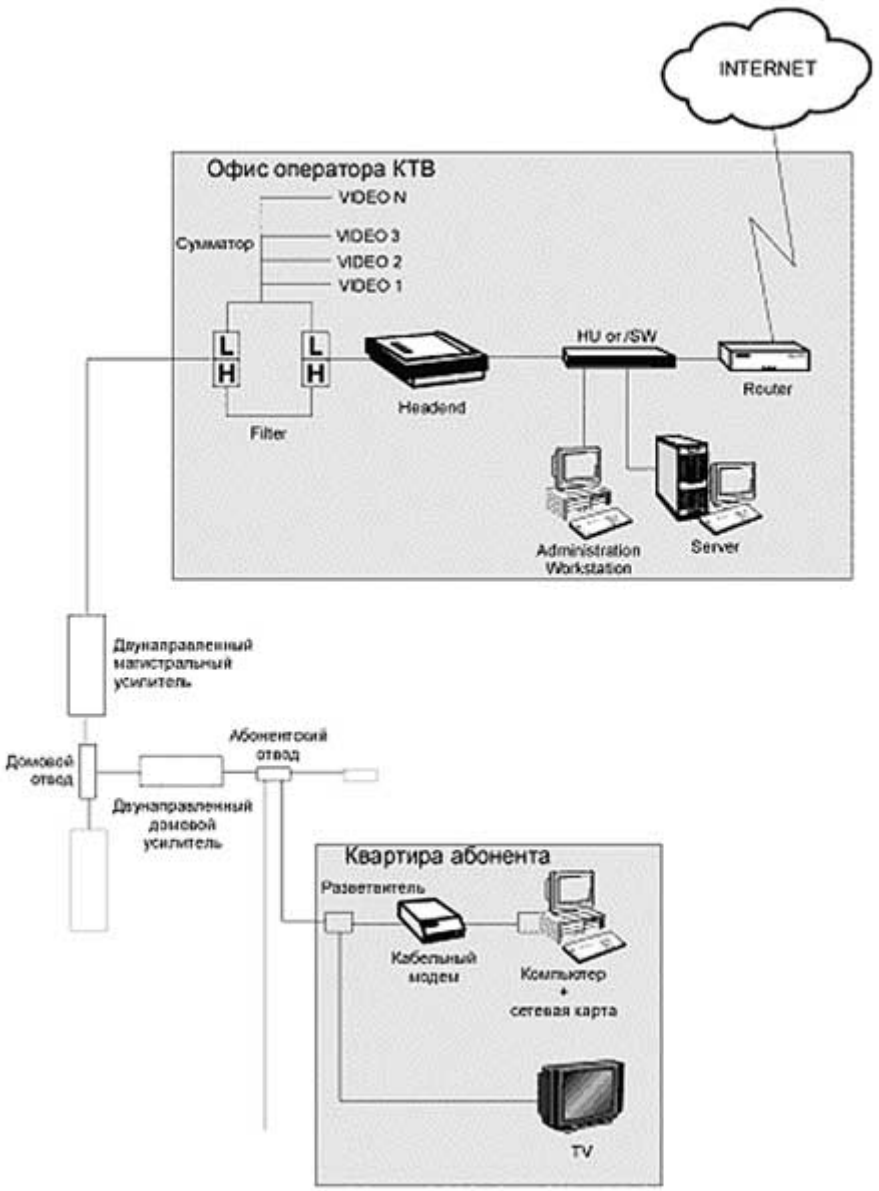

Рис. 5.10. Схема подключения абонента через сеть КТВ.

Вполне работоспособная схема, только головная станция для передачи данных не дешевая ($5000-$20000), и скорость ограничена несколькими десятками мегабит "на всех".

Однако, на эту внешне безоблачную картину наложилась Российская реальность.

Сети КТВ появились и выросли очень похоже на современные "домашние" Ethernet-сети. Только примерно на 10 лет раньше.

Все начиналось переделки привычной "антенны на подъезд" (по сути пассивной сети с направленными частотно-зависимыми ответвителями) в инфраструктуру масштаба нескольких домов, или даже квартала. Технически это задача не слишком сложная, и сети росли как грибы.

Дальше шел обычный процесс укрупнения, повышения качества услуг, и т.п. Но важно отметить, что сети строились как правило без серьезного финансирования и единого проекта. Понятно, что о будущем никто не задумывался, оборудование и кабели использовались наиболее дешевые.

В результате на сегодня средняя сеть представляет собой головную станцию с поканальной обработкой сигналов и конвертированием каналов по частоте, которая выдает сигнал на широкополосные магистральные и домовые усилители с полосой пропускания 40-240 МГц без обратного канала. Далее на линиях установлены частотно-независимые магистральные ответвители и абонентские разветвители. Плюс ко всему менее чем среднее качество монтажа и материалов.

Очевидно, что использовать такую сеть для высокоскоростной передачи данных невозможно без коренной реконструкции, которая может вылиться в полную замену всей головной и магистральной части.

Не случайно из многочисленных попыток Ethernet-провайдеров использовать сети КТВ относительным успехом закончились только единичные проекты. Обычным итогом было разочарование в технологии и (или) убытки.

Но история на этом, понятное дело, не остановилась.

Началось внедрение широкополосных КТВ с обратным каналом 40-862 МГц в прямом направлении и 5-30 МГц - в обратном. Топология и архитектура этих сетей уже изначально проектировалась с учетом возможности передачи данных.

Параллельно с этим КТВ переходит на оптоволокно. Процесс этот весьма мучительный для бюджета, так как задача передачи широкополосного аналогового сигнала в "стекле" решается недешево. Но и оцифровывать видеосигнал то же не просто и стоит немалых денег. В общем, цены для привыкших к Ethernet операторов покажутся сногсшибательными.

Однако выхода нет, оптоволокно удобно применять и при росте сетей, и при объединении коаксиальных сегментов, и при развитии дополнительных сервисов. Так появилась концепция гибридной сети, в которой магистральная часть строится на оптоволокне, а абонентская (на один дом или группу домов) - по прежним коаксиальным кабелям.

По сути, это позволяет с одной головной станции раздать сигнал без потерь по множеству точек, в которых ранее нужны были свои головные станции. Экономия выходит заметная, и технология медленно (из-за очень существенных начальных затрат), но верно (пока особых конкурентов таким сетям нет) пробивается в реальную жизнь.

И уже есть разделение на несколько направлений. Первое - передавать в одном канале все виды услуг (видео, речи и данных), и при переходе с оптики на коаксиал переносить каждую в отведённый диапазон частот. Понятно, что коаксиальный сегмент сети требует применения дуплексных усилителей, обеспечивающих двухстороннюю передачу сигналов. Такой вариант получил название HFC (Hybrid Fiber Coax).

Существует и развитие этой технологии - HFPC (Hybrid Fiber Passive Coax). В нем коаксиальные сегменты меньше по размеру (близко к одному большому дому, или 2-3 средним), из-за чего в этой части можно обойтись без активного оборудования. Качество передачи сигналов (особенно в обратном канале) такой сети значительно выше, эксплуатационные расходы ниже. Мешает широкому распространению данного типа сетей только высокая стоимость оборудования для оптико-коаксиального преобразования.

Следующий вариант - транспортировать по оптоволокну только видео, а данные и голос передавать отдельно (или в том же оптическом кабеле, но в другом канале). Все сигналы объединять только на входе в коаксиальный сегмент.

Однако в сетях HFPC (Hybrid Fiber Passive Coax) по сути нет места классическим (работающим по коаксиальному кабелю) кабельным модемам. Если волокно уже приходит в дом или небольшую группу домов, дешевле его раздать отдельным кабелем по Ethernet, чем ставить дорогостоящую головную станцию и кабельные модемы.

Таким образом, более перспективная технология HFPC может легко выродиться в отдельные сети Ethernet, и отдельные - видео, объединенные только общей оболочкой оптического кабеля. Это, конечно, может дать некоторую экономию при строительстве сети, но оценить ее более чем в 20-30% нельзя. Тем более организационные сложности дальнейшей эксплуатации могут легко перекрыть полученный экономический эффект.

Подводя итог, можно сказать, что будущее гибридных сетей КТВ в передаче данных далеко не безоблачно. Относительно успешными получаются только реализации проектов в небольших городах (и Москве), где TV-сеть строится по "социальному заказу" (и с политическим финансированием), а возможности подключения к Интернет достаются по сути "в нагрузку".

Разумеется есть некоторое число сетей, в которых оператор КТВ сам начал заниматься провайдингом, и смог неторопясь "подогнать" свои сети под нужны передачи данных. Однако, это скорее исключения, чем правило - примеров "заброшенных" проектов гораздо больше. Например в Екатеринбурге из 3 проектов подключения к Интернет через КТВ все 3 оказались убыточными и были заброшены.

В завершение, остается сказать несколько слов о некоторых удачных решениях. Тем более, их не так и много.

Наиболее распространенным на сегодня операторским оборудованием является Cisco uBR7200 (Universal Broadband Router). Это универсальный маршрутизатор с поддержкой передачи широкополосного сигнала. Маршрутизатор uBR7200 имеет, разумеется, много общего с "классическими" маршрутизаторами Cisco, в частности он поддерживает самые разнообразные интерфейсы для подключения устройства к локальным или глобальным сетям.

Главным отличием uBR7200 является поддержка кабельных модемов, т. е. наличие соответствующих плат расширения и совместимость с оконечными устройствами, поддерживающими стандарт DOCSIS. При этом "окно", необходимое для передачи данных, составляет 6 МГц (стандартная ширина полосы для одного телевизионного канала в Северной Америке). Или, согласно модификации стандарта Euro DOCSIS, 8 МГц — стандартная ширина полосы телеканала в Европе.

В этом окне данные могут передаваться со скоростью 30–42 Мбит/с в зависимости от типа модуляции. Доступная пропускная способность используется совместно всеми абонентами сети, пользующимися услугой. На практике каждый абонент может без особых проблем получить канал на 0,5-1,5 Мбит/с.

Передача обратного (upstream) трафика осуществляется в диапазоне 5–42 МГц, поддерживаемая скорость передачи в зависимости от метода модуляции сигнала достигает 0,5-10 Мбит/с (совокупно для всех абонентов).

Кабельные модемы устанавливаются как правило не у каждого пользователя (это для России слишком дорого), а "один на дом" или "один на подъезд", и сразу на магистраль. Далее разводка по дому делается Ethernet. Это позволяет решить сразу несколько проблем.

Во-первых, данный способ дешевле. Во-вторых, позволяет отложить на время дорогостоящую реконструкцию внутридомовых сетей, и в-третьих, обойти проблему ингресс-шума в обратном канале (так как самая "шумная" часть сети оказывается изолированной от обратного канала).

Часть 3. Глава 5

Экзотические способы передачи данных.

Говоря в общем, в перечислении экзотических способов передачи данных можно легко дойти до азбуки Морзе или даже до сигнальных костров древних индейцев. Поэтому в данном параграфе будет описана лишь небольшая часть методов, которые в принципе (хоть и с некоторой натяжкой) можно применять в Ethenret-провайдинге.

Пожалуй, из нерассмотренного в предыдущих параграфах, наиболее близка к реальному провайдингу технология, использующая атмосферные лазеры.

Самое интересное, что в этой нише до сих пор соседствуют любительские решения и промышленные. Верный признак того, что технология еще не "устоялась", не все понятно как с производством, так и применением. Хотя последние варианты промышленных лазерных установок (судя по всему) могут решить большинство вопросов. Но обо всем по порядку.

Эксперименты с передачей данных при помощи лазерного луча начались еще в 60-х годах (причем в России), но прошли без успеха, и направление было надолго, и в общем обоснованно заброшено. С появлением новых технологий (и как следствие снижения цен на комплектующие) интерес к атмосферным лазерам появился вновь.

Как в России, так и зарубежом появились монстрообразные установки, предназначенные для работы на расстояние до нескольких километров с приемлемым уровнем надежности. Как классический пример можно привести серию "МОСТ" государственного Рязанского Приборостроительного Завода.

Рис. 5.11. "МОСТ" 100/500.

Скорость передачи данных - 4xE1 G.703, в более поздних вариантах появились модели под Fast Ethernet. Тип излучающего элемента - лазер, приемного элемента - pin фотодиод, излучаемая оптическая мощность - 500мВт. Плюс к этому дорогая и сложная многолинейная оптическая система.

Зарубежные производители выпускали целый рад в чем-то похожих моделей, применяя автонастройку лазера, точную оптику, и т.п. меры. Это позволило "вытянуть" линии до 5 км, но стоимость систем оказалась, мягко говоря, заоблачной. И это при весьма средней надежности, более годной для резервного, а не основного канала. Кстати, как ни странно, именно в резервировании по принципиально нетрадиционной технологии особо критичных проектов лазеры в основном и применялись.

В общем, подобные мощные и совершенные системы делаются и сейчас - но в очень ограниченном количестве, и интереса для Ethernet-провайдеров явно не представляют.

Второй волной были любительские системы. В России бум совпал с появлением "лазерных" указок, использовавших недорогие полупроводниковые излучатели (лазерами их назвать сложно). Известно даже несколько работающих на этом принципе любительских конструкций (так называемый удлинитель com-порта на лазере).

Кое-где даже дошло дело до создания любительских сетей, узлы которых были связаны атмосферными лазерами. Наиболее известен проект **Ronja**, который разработал Karel 'Clock' Kulhavy из Чехии.

Устройства имели простую компоновку (отдельные приемник и передатчик), сравнительно небольшую дальность работы... Но они стоили дешево и оказались вполне рабочим решением.

Фактически по той же схеме были налажены несколько небольших, но все же промышленных конструкций атмосферных лазеров. Как пример можно привести "БОКС" от НПК "Катарсис".

Рис. 5.12. "БОКС".

При разумной (менее $1000 за комплект) стоимости они пользуются небольшим спросом там, где нужен полностью "легальный" канал, но нельзя проложить провод. Решения на

основе радио в России слишком сложно узаконить. По крайней мере для единичной линии лазерная связь обходится дешевле.

Однако там, где есть возможность обойтись без полной легальности, radio-ethernet безусловно и полностью выигрывает, так как стоит примерно в 10 раз дешевле.

В конце концов до "лазерной" технологии добрались китайские производители. Они убрали из лазерной "головки" практически всю электронику, оставив там только линзы и... Световод из удаленного блока. По сути, они сделали атмосферный преобразователь на обычный оптоволоконные медиаконвертер.

Это позволило резко снизить стоимость, поднять надежность и вандалоустойчивость конструкции. И наконец сделать атмосферные лазеры рентабельными для передачи данных на маленькие расстояния. Впрочем, пока это скорее теория из рекламных проспектов.

Реального оборудования подобного класса на рынке нет. Но есть шансы, что скоро появится.

Следующие устройства передачи данных по сути являются модификацией обычного Ethernet, и предназначены для решения каких-либо узких задач (как правило увеличения дальности работы).

100C5

Может быть это покажется несколько неожиданным, но самый простой способ увеличить дальность работы Fast Ethernet - сделать downgrade оборудованию типа 1000base-T (на деле немного сложнее, но суть именно такая).

Опустить скорость в 10 раз при сохранении способа кодировки PAM-5 (пять уровней напряжения в сигнале). И - победа математики - частота передачи по каждой паре составит не более 6,25 МГц. Что почти вдвое ниже, чем на привычном 10base-T.

Немного похоже на вымерший протокол 100VG, только наоборот. Вместо использования кабеля более низкой категории (CAT-3) на стандартное расстояние, современный кабель (CAT-5) применяется на большей длиннее (до 1 км.)

Были даже попытки одного из производителей (Marvel) выпустить на этой основе стандартный чип, но идея как-то постепенно заглохла...

10base-T4

Еще одна похожая идея - 10base-T4. Этот протокол даже претендовал на ieee 802.3ah. В него явно заложена техническая ассоциация с давно забытым стандартом 100base-T4, но выполнено все на существенно более высоком техническом уровне.

Передача ведется сразу по 4-м парам, причем независимо, по 2,5 мегабита по каждой паре. Дальность работы - до 4-х километров. Причем скорость может автоматически повышаться или понижаться.

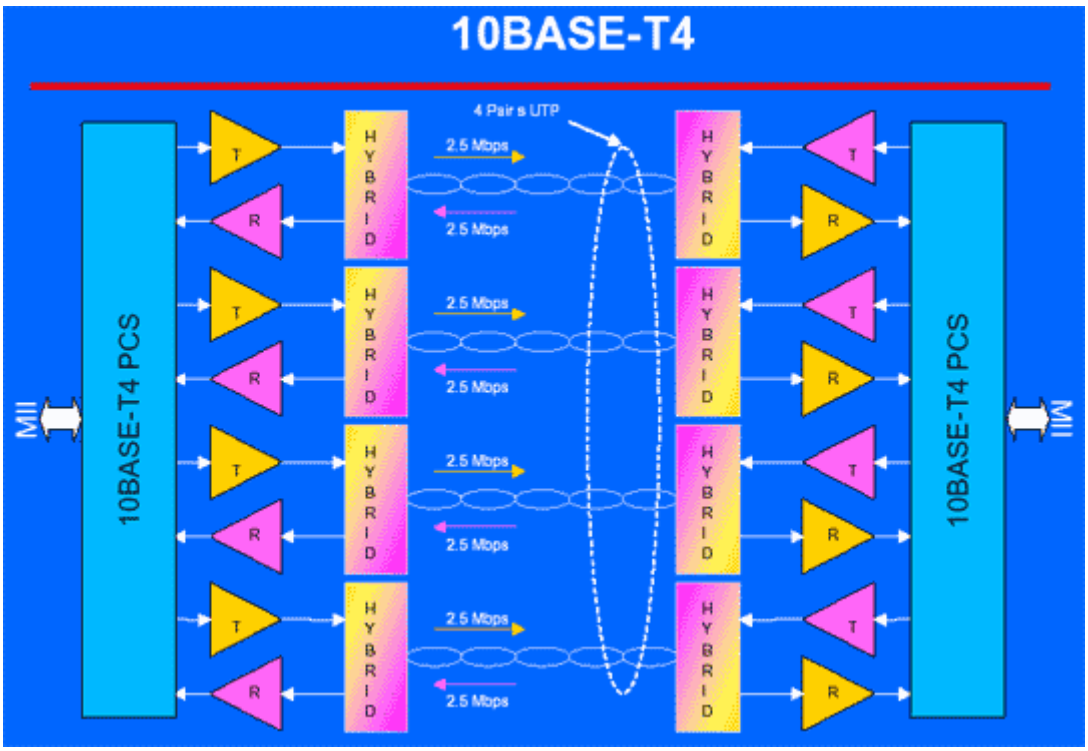

Рис. 5.13. 10base-T4

Технически нет никаких сложностей - если xDSL может легко передавать по одной паре 2,5 мегабита, то кто мешает 10base-T4 это делать сразу по 4 парам? Частота и кодирование похожи (или просто одинаковы). И расстояние для диапазона 600 кГц получается вплне обычным.

Тут уж впору задать вопрос - как создателям нашумевшего HomePNA удалось получить такие посредственные показатели для своего детища. Не иначе, оставляли нишу для своей же линейки xDSL. Ее то же надо продавать. Или как обычно - сделали что "попроще, и ценою подешевле"...

Российский производитель не остался в стороне. Правда способностей хватило только на простые кустарные переделки сетевых адаптеров на меньшую скорость и большую дальность.

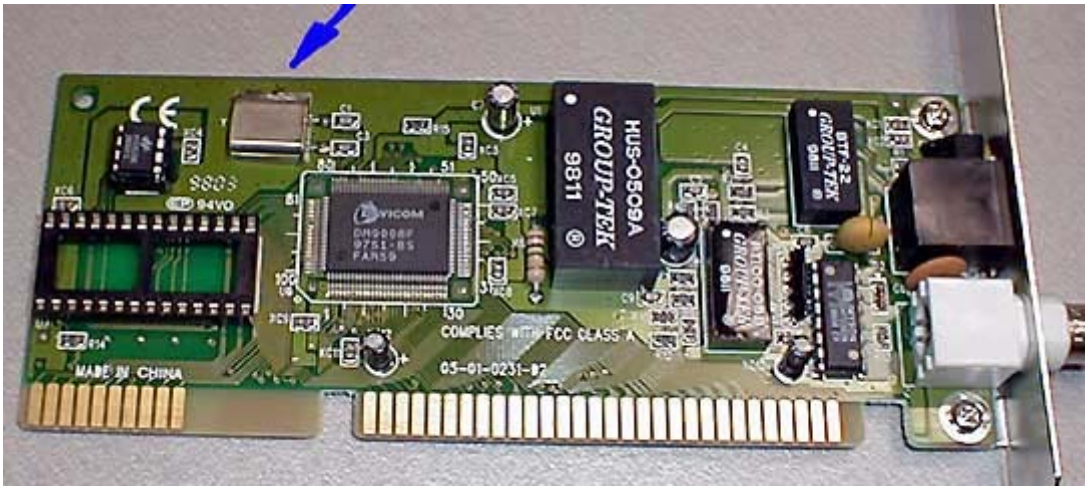

Рис. 5.14. Downgrade 10base-TX

На карточке просто перепаевается кварц (на в 2 раза более медленный), и... все. Скорость 5 мегабит, дальность работы 300 метров.

К сожалению, подходят не все типы карт (только ISA от некоторых производителей), да и для преобразования скорости не обойтись без маршрутизатора с ISA-слотами.

Кроме показанных способов известные еще многие (или даже многие десятки) попыток улучшить Ethernet, однако с резким удешевлением xDSL, появлением HomePNA, VDSL, это движение практически затихло...

Коммерческой ценности, понятное дело, эти технологии на сегодня не представляют.

Кстати сказать, попытки "улучшения" или "упрощения" коснулись не только Ethernet. Затронуло это и xDSL. Как пример можно привести технологию **AuDSL**, которая хоть и представляет собой техническую шутку, но может навести на интересные мысли.

AuDSL (Audio Digital Subscriber Line) позволяет использовать старую звуковую карту для организации выделенной линии. Идея простая - вместо дорогого и специализированного DSP процессора - софт компьютера. Немного похоже на Win-модем.

Конечно, объем вычислительных операций пропорционален скорости. И на 2 мегабитах нужно очень быстро считать. Но ведь и винмодем еще 5 лет назад казался невозможным. А сейчас ставится в каждый третий-четвертый новый компьютер...

Прототипы AuDSL успешно соединяются на скорости 96 кбит/с на расстояние в несколько километров по обычной медной паре. В качестве компьютера используется PC с AMD K6-2-333 и звуковыми картами Ensoniq AudioPCI. Программный модем поглощает около 38% ресурсов центрального процессора.

Для реального использования, конечно, загрузка слишком велика. Да и xDSL стоит уже не так много. Но что-то мне подсказывает, что времена Win-DSL не за горами. ;-)

Однопроводные линии.

Волноводы однопроводных линий представляют собой металлический проводник, покрытый слоем диэлектрика. Конструкция показана на рисунке. Чтобы волновод линии с поверхностной волной имел низкие потери, он должен быть медный или биметаллическим (сталь с покрытием медью). Диэлектрический слой должен быть изготовлен из изоляционного материала с низкими потерями.

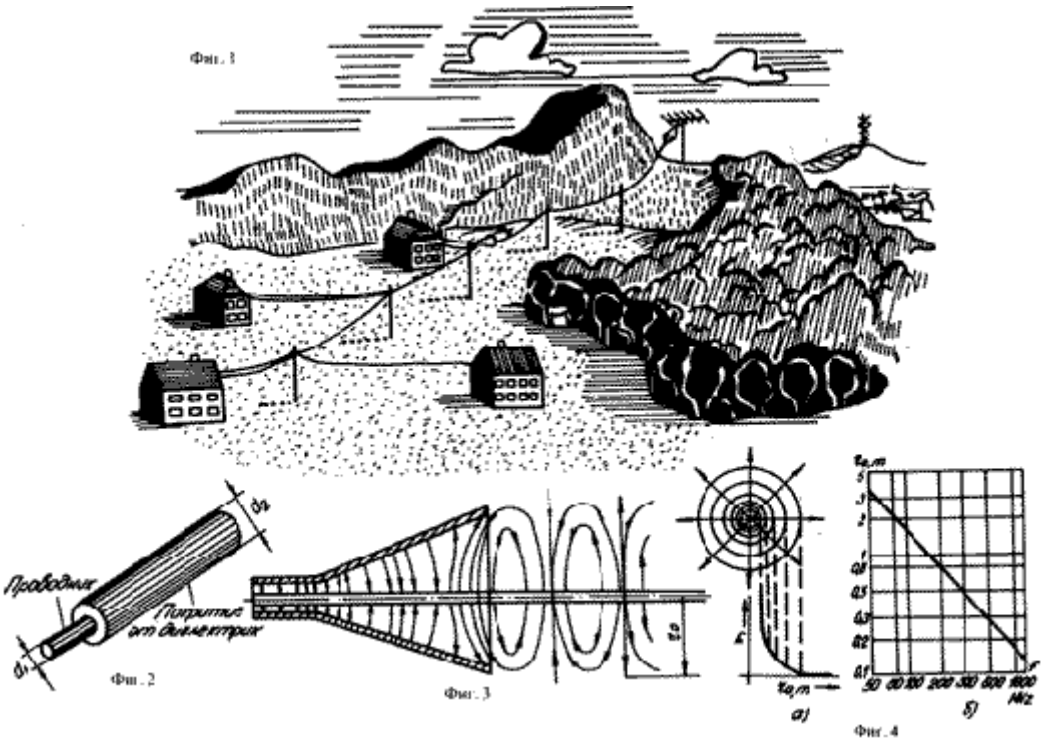

Рис. 5.15. Однопроводные линии.

В электропроводящей линии с поверхностной волной электромагнитная энергия распространяется около волновода на всем его протяжении. В начале и на конце линии смонтированы устройства, называемые рупорами. Они исполняют две основные задачи - возбуждают электромагнитную энергию (волну) в линии и согласуют подходящий коаксиальный кабель с однопроводной линией.

Технические детали работы такой линии слишком сложны для данного изложения. Однако общий принцип понятен, а практическое использование в городских условиях все равно совершенно невозможно...

В заключение этого небольшого обзора остается добавить, что новые технологии передачи данных постоянно появляются и, наоборот, исчезают. Что-то становится популярным и часто используемым. Что-то проходит незамеченным. Такова судьба провайдинга - одной из самых быстроразвивающихся отраслей рынка.

Глава 6. Безопасность в локальных сетях.

Тсс… Враг подслушивает.

Большинство людей, использующих какую-либо систему передачи данных, хотят изолировать информацию от окружающих.

Этот вопрос важен даже при использовании локальной корпоративной сети, не говоря уже об Интернет. Проблема далеко не новая, и сейчас администратор ЛВС имеет в своем арсенале достаточно возможностей обеспечения приватности как данных компьютера пользователя, так и сетевого трафика. Для этого он может управлять рабочими станциями

и другими активными устройствами, контролировать физическую топологию сети, в крайнем случае, применять различные административные меры.

Доступ в публичный Интернет так же может быть ограничен узкими рамками. Для этого применяют специальные брандмауэры, сетевые экраны и другие средства ограничения доступа и обнаружения сетевых атак. В крайнем случае, шлюз (firewall) может быть настроен пропускать только один протокол (и только по одному порту), оставляя все прочие сервисы за пределами защищенной сети (демилитаризованной зоны).

Часть 3. Глава 6

Уязвимые точки сетей Ethernet.

Перед коммерческой сетью передачи данных задача обеспечения безопасности стоит намного более остро, чем в корпоративной сети. Как правило, нет никакой возможности контролировать узлы конечных абонентов, и необходимо пропускать все возможные типы протоколов передачи данных без ограничений.

Можно выделить несколько моментов, представляющих потенциальную опасность клиенту или оператору услуг.

- Проникновение в сеть снаружи, из публичной сети Интернет.
- Получение доступа к узлу внутри сети, угроза "от соседа".
- Подделка учетных данных пользователем для получения несанкционированного доступа к ресурсам оператора;

Проникновение в сеть снаружи далеко не новая проблема. Надежной защиты от этого на сегодня нет вообще, и пользователей спасает низкая цена вопроса - едва ли кого-то могут заинтересовать частные пользователи. То есть, от непрофессионального взлома достаточно средств операционной системы и простейших персональных фаерволов, а серьезная атака слишком маловероятна.

В конце концов, пользователь сам должен заботиться о сохранении своих конфиденциальных данных, так как это не относится к сфере обязанностей оператора связи. Существуют предприятия, специально занимающиеся вопросами безопасности и защиты данных, но это отдельные (и весьма не дешевые) услуги.

Гораздо более опасна "внутренняя" угроза. Защита тут значительно слабее, и вдобавок для известного пользователя ("да это соседний магазин!") возможна ясная мотивировка "взлома" или "вредительства".

При этом надо сказать, что протокол Ethernet в своей основе не имеет механизмов защиты абонентов друг от друга. Он изначально создавался для связи пользователей внутри сети, а не предоставления закрытых каналов передачи данных. Соответственно задачи обеспечения даже самой минимальной безопасности фактически не ставились. Поэтому, в "классическом" Ethernet единственным способом отделения узлов друг от друга была установка сетевых экранов (брандмауэров), и разделение проходило на 3 (сетевом) уровне модели OSI.

В то же время, внутри ЛВС все устройства работают в единой среде на 2 (канальном) уровне, соответственно соседние узлы могут получить физический доступ к "чужим" кадрам, со всеми вытекающими из этого последствиями. Так, возможно устанавливать прямые соединения, "прослушивать", получать, и даже пропускать через свой фильтр "чужой" трафик.

Можно без преувеличения сказать, что некоммутируемый Ethernet вообще беззащитен. Все узлы физически получают все проходящие по сети кадры, и для этого не нужны специальные средства - достаточно простейшей программы "сниффера" (например, на Win-платформе широко известна программа NetXray, под юникс - tcpdump). При этом нешифрованные пакеты (в том числе ICQ, почта, IRC) могут совершенно свободно читаться соседом по сети.

В коммутируемой сети (построенной на неуправляемых коммутаторах) прямое прослушивание несколько затруднено, но защита все же недостаточна. Известно по крайней мере два простых способа перехвата кадров в такой ситуации. Это переполнение CAM-таблицы соответствие коммутатора (при этом он начинает работать подобно обычному хабу), и использование ложного ARP-сервера (в этом случае MAC-адрес атакующего узла замещает в CAM-таблице место граничного маршрутизатора).

Строго говоря, все эти проблемы присущи и передаче информации через Интернет. Операторы связи безусловно имеют доступ к нешифрованным сообщениям. Однако у них (кроме оговоренных законодательством обязанностей) значительно меньше мотивировка к "прослушиванию" сети.

С другой стороны, для провайдера ситуация то же не слишком удобна. Невозможность контролировать каждого пользователя в сети "по отдельности" означает, что сеть Ethernet фактически закрыта для надежного администрирования и управления. Оператор не может проконтролировать наверняка соответствие учетных данных и реального пользователя.

В простейшем случае, достаточно узлу сменить свой IP адрес на "соседский", и система учета трафика будет считать, что соединением пользуется "сосед", со всеми вытекающими из этого финансовыми последствиями для последнего. Контроль на уровне MAC-адреса то же не решает проблему - сменить его не многим сложнее, чем IP. А ведь только эти два адреса полностью характеризуют узел в обычной Ethernet-сети.

Хуже всего то, что при использовании большинства типов неуправляемых коммутаторов вполне возможна одновременная работа в сети двух узлов с одинаковыми IP и MAC адресам. Очевидно, что при этом большинство централизованных (установленных на маршрутизаторе) систем ограничения доступа не способно различить узлы, что открывает самые широкие возможности воровства трафика.

Не хотелось бы лишний раз описывать возможности такого рода (и особенно технические нюансы реализации), однако при желании всю необходимую информацию можно найти в Интернет, да и полигон для испытаний собрать по силам любому.

Можно применять различные методы контроля - от административной работы до профилактической проверки физического соответствия порта пользователю. Разумеется, это полумеры. Решить описанные выше задачи можно при помощи создания виртуального соединения (канала передачи данных, так или иначе "наложенного" на сеть), в котором можно задавать особые правила доступа к информации.

Остается добавить, что на сегодня существует много способов для достижения поставленной цели, что позволяет превратить Ethernet в мощный и недорогой транспортный инструмент. Однако их использование не слишком значительно, но неизбежно поднимает стоимость инфраструктуры передачи данных.

Часть 3. Глава 6

Способы создания виртуальных соединений.

Исторически телекоммуникационные технологии, и локальные сети развивались своими независимыми путями. Поэтому одна и та же проблема создания виртуальных соединений (виртуальных сетей) была фактически решена принципиально разными способами.

Поэтому (с некоторой долей условности), можно выделить два пути:

Телекоммуникационный. Предполагает создание виртуальных каналов (туннелей) "поверх" транспортного протокола (обычно IP или Ethernet). Узел-клиент, используя свои учетные данные, устанавливает соединение "точка-точка" с сервером доступа, и уже через этот вновь образованный канал осуществляет передачу/прием данных.

При этом как процедура авторизации, так и информационный обмен может быть зашифрован вся, либо частично (только заголовка и пароля авторизации).

Локальный. Строится на базе коммутируемого Ethernet с использованием виртуальных сетей (VLAN). Разделение происходит на уровне коммутатора, который имеет возможность выделять на канальном уровне одного или нескольких пользователей в группу по некоторым признакам (порту или MAC-адресу).

Твердой границы между способами нет (да и названия очень условны), так же возможно параллельное использование обеих технологий в одной сети передачи данных. Так же в настоящее время весьма спорным является вопрос наиболее удобной технологии.

С одной стороны, для домашних сетей "телекоммуникационный" вариант кажется проще, дешевле и даже привычнее (особенно провайдерам, знакомым с dial-up). С другой - корпоративный рынок ЛВС практически однозначно сориентирован на "локальное" регулирование отношений между пользователями. Поэтому окончательную точку в борьбе ставить рано.

На стороне VPN быстрорастущая производительность серверов и клиентских компьютеров, которые способны проводить шифрование трафика в реальном времени. Плюс легко доступные мощнейшие криптографические алгоритмы, взломать которые не по силам даже государственным службам безопасности.

В пользу VLAN говорит стремительно уменьшающаяся стоимость управляемых коммутаторов. Легко предположить, что через 1-2 года такие устройства полностью вытеснят неуправляемые модели, и позволят гибко и надежно управлять подключением абонента на самом удобном уровне - входном порту.

Часть 3. Глава 6

"Локальные" виртуальные соединения.

Рассмотрим подробнее "локальный" метод. По сути, он сводится к организации виртуальных сетей (иначе говоря, Virtual LAN, VLAN) "поверх" общего Ethernet'а при помощи специального активного оборудования ЛВС (коммутаторов).

Существует несколько способов построения виртуальных сетей. Ниже приведены три наиболее распространенных:

- Группировка портов. Трафик каждого порта можно отнести к той, или иной виртуальной сети. Так же можно назначить на один порт несколько виртуальных сетей. При этом информация о таком VLAN содержится только непосредственно на коммутаторе, и по сети не передается.
- Группировка MAC-адресов. В этом случае кадр относится к какой-либо Vlan на основании MAC-адреса (по специальной таблице, заполняемой администратором сети). Этот подход считается излишне трудоемким, устаревшим, и рассматривать его подробно не имеет особого смысла.
- Использование дополнительных меток (тегов) в поле данных кадра Ethernet. Способ принят в качестве стандарта ieee 802.1q. При этом к кадру Ethernet добавляются два байта, которые содержат информацию по его принадлежности к Vlan, и о его приоритете (тремя битами кодируется до восьми уровней приоритета, 12 бит позволяют различать до 4096 Vlan, а один бит зарезервирован для обозначения кадров сетей других типов).

При одинаковом названии и области применения способы создания виртуальных сетей отличаются друг от друга кардинально, и требует рассмотрения в отдельных параграфах.

Организация VLAN с помощью тэгов.

Наиболее очевидным (но далеко не самым простым технически) способом разделения сетей будет присваивать каждому кадру Ethernet специальной метки (тэги), в соответствии с которым свитчи будут коммутировать их путь по сети. Для этого было придумано не мало корпоративных решений (ISL Cisco, VLT 3com), но в конце концов появился единый стандарт IEEE 802.1q, который в настоящее время можно считать общепринятым.

Тегированные кадры позволяют построить виртуальную сеть для каждого пользователя (или их группы). Связь между различными виртуальными сетями должна осуществляться на сервере (или коммутаторе 3-го уровня) посредством IP маршрутизации на 3-ем (сетевом) уровне модели OSI,

При этом создается полное ощущение, что каждый пользователь имеет свой свою выделенную линию (с негарантированной скоростью) до центрального узла, и подключен к отдельному сетевому адаптеру маршрутизатора.

Технически подобная схема выглядит следующим образом:

Каждый пользователь находится в своей, виртуальной сети (VLAN). Кадр, попадая от него в коммутатор, получает 2-х байтовую метку (тэг), которая назначена на данный порт. Он

размещается в поле данных кадра Ethernet, из-за чего его длина увеличивается (и может быть неправильно обработана какими-либо устройствами). Далее кадр может пройти несколько свитчей, которые будут направлять его в соответствии с установленными правилами. В случае, если коммутатор не имеет функции распознавания тэгов, кадр будет обработан в соответствии с общими правилами коммутируемого Ethernet.

Можно выделить три типа порта. Входной, на котором тэги устанавливаются, выходной, на котором они убираются, и транковый, через который они передаются между активными устройствами (в одном физическом канале несколько виртуальных сетей). Таким образом может быть построена защищенная сеть очень больших размеров.

Нужно специально отметить, что имеется в виду именно транк (объединение) на уровне протокола. Дело в том, что такой термин может означать нечто совсем иное - а именно объединение портов в группу, для увеличения скорости передачи данных между двумя коммутаторами (или коммутатором и многопортовой сетевой картой). Такая линия с точки зрения пользователя выглядит как один более скоростной порт. Получается передача со скоростью 200, 300, 400... до 800 Мбит, соответственно, при объединении 2,3,4...8 портов.

Самое неудобное, что оба термина могут присутствовать одновременно не только в технической документации. На сгруппированных в транк портах может быть сконфигурирован транк нескольких VLAN. Поэтому нужно очень аккуратно использовать этот термин.

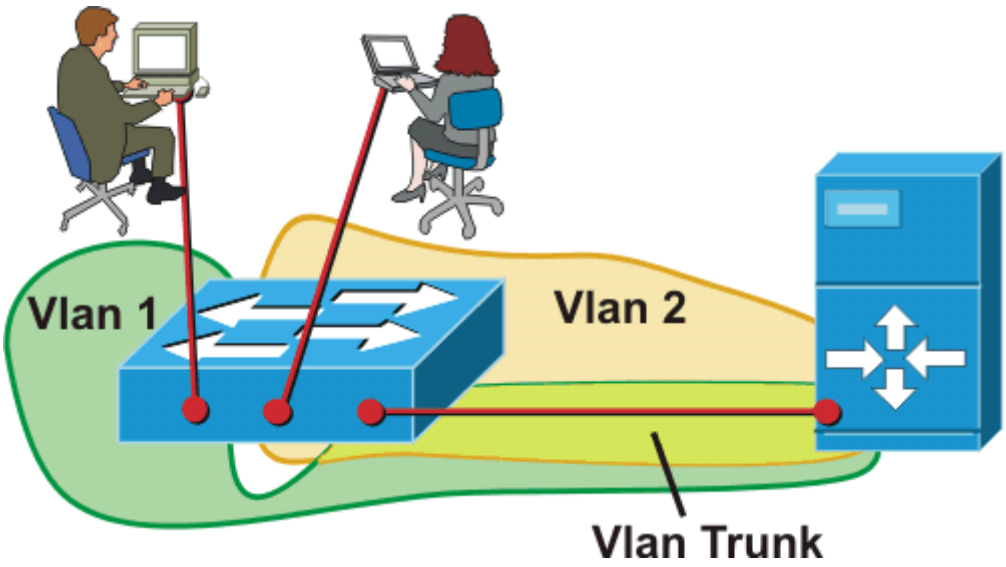

Рис. 6.1. Виртуальные сети на основе тэгов

Что нужно для работы по такой привлекательной схеме? Всего-то поддержку устройствами стандарта IEEE 802.1q, или собственного корпоративного аналога. При этом двух байт, добавленных в кадр Ethernet, вполне хватает для распознавания "своих" данных (и не только для этого).

Следует отметить, что VLAN может быть настроен как вручную, так и фирменными средствами производителя оборудования. Например, Cisco использует протокол VTP, который служит для распространения информацией о виртуальных сетях. Он позволяет вести их базу централизовано, и распространять ее по технологии клиент-сервер (несколько похоже на механизм DHCP).

Подобная система образования виртуальных сетей достаточно удобна. Но ее широкому распространению в области недорогих сетей мешает не только достаточно высокая стоимость подобного оборудования (на сегодня не менее $600 за устройство). Построение (и эксплуатация) подобных сетей требует высокой квалификации как инсталляторов решения, так и обслуживающего персонала.

Системному администратору необходимо хорошо понимать не только работу программного обеспечения, но логику использования Vlan. Наиболее простой пример - входной порт не может принадлежать сразу нескольким виртуальным сетям, так как коммутатор не в состоянии определить, какой тег присвоить пришедшему кадру (однако, это может быть реализовано на устройствах высшего уровня).

С другой стороны, цены на подобные модели быстро падают, веб-интерфейс становится проще, нагляднее, и можно предполагать, что в недалеком будущем использование возможностей VLAN будет обычным делом даже в самой небольшой сети.

VLAN'ы, использующие группировку портов.

Очевидно, что стоимость коммутатора в немалой части состоит из цены использованного программного обеспечения. При разработке устройства VLAN (как многие сложные протоколы работы) требуют высоких затрат. Можно на них идти (что неизбежно скажется на итоговой цене конечного продукта), можно обойтись меньшим, выпустив на рынок промежуточный вариант.

Таким компромиссом (вполне удачным для офисного применения) стали свитчи, которые позволяют манипулировать с виртуальными сетями на уровне портов. Соответственно, технологию 802.1q они не поддерживают, и работать по описанной выше "идеальной" схеме не могут. Соседние устройства о создании подобных vlan информации не имеют.

Пока вся сеть состоит только из одного такого устройства, механизм прекрасно работает. Имеет смысл даже представить большой коммутатор в виде нескольких более маленьких. А если нужно маршрутизировать разные сети через сервер - в него можно установить несколько реальных (физических) сетевых карт, соединить их реальными кабелями с реальными портами, прописать нужные Vlan. Только таким способом можно получить полностью изолированные "виртуальные" сети.

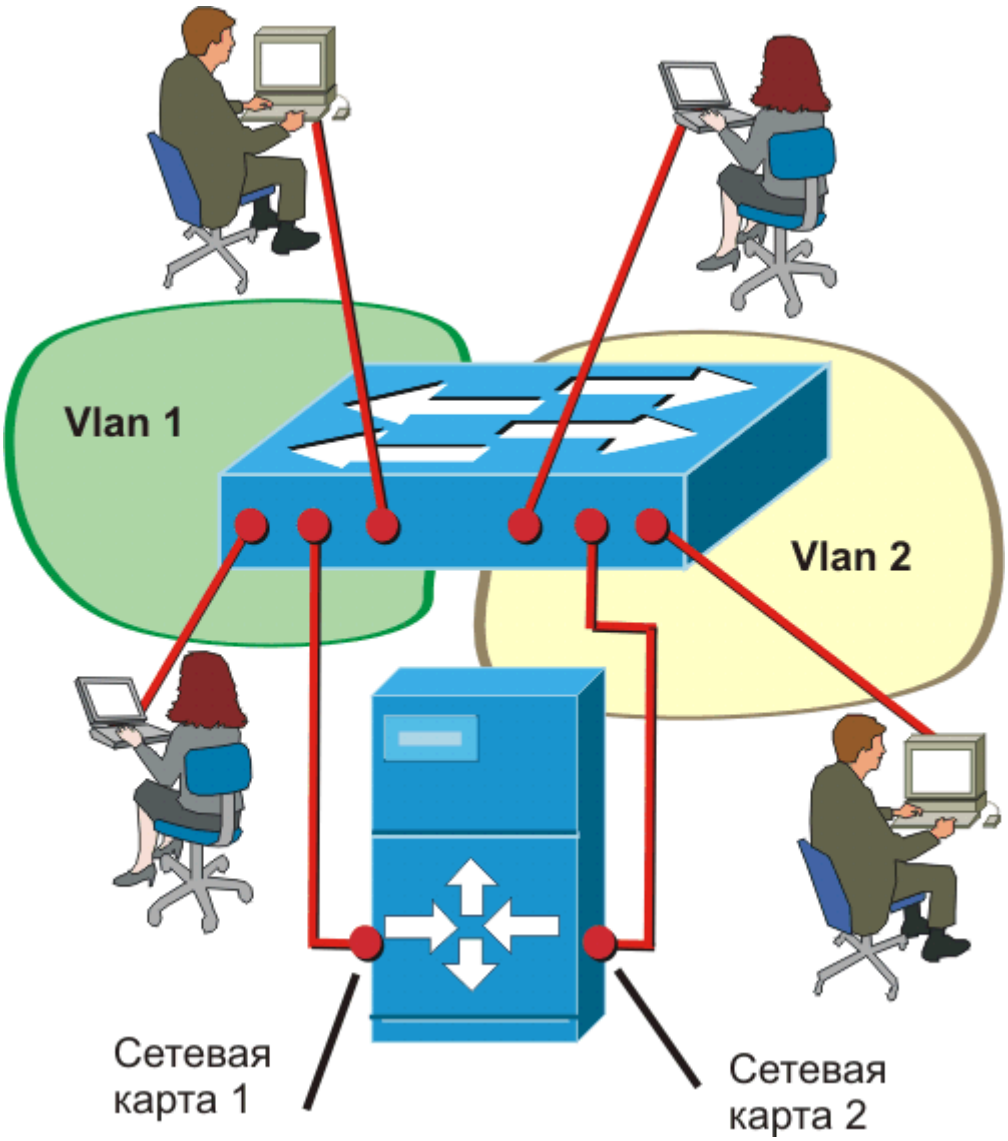

Рис. 6.2. Vlan, использующий группировку портов устройства.

Такое "экстравагантное" решение имеет вполне осмысленное экономическое обоснование - мощное управляемое устройство намного удобнее, и обычно дешевле, чем несколько более слабых. Да и пользователей в группы можно помещать удаленно, не производя физических переключений. Так что для небольшой офисной ЛВС такой инструмент может оказаться даже более удобным, чем Vlan на основе протоколов (типа 802.1q). Просто, надежно, достаточно безопасно и не дорого.

Однако для сети передачи данных (или даже крупной ЛВС), обеспечить работу пользователей в отдельных виртуальных сетях не удастся полностью. Но разумный компромисс возможен, особенно для сетей, имеющих явно выраженную "древовидную" структуру доступа к данным.

Реальное применение - сплошь и рядом. Представим, что к единственному коммутатору подключен шлюз в интернет. АДСЛ, оптоволоконный конвертер, просто магистральный маршрутизатор сети провайдера. Или, нескольким рабочим группам нужно работать с базой данных, расположенной на центральном сервере.

В этом случае можно поступиться защитой, надежностью, и сделать один порт общим для всех vlan. Для него даже придумано специальное название - серверный.

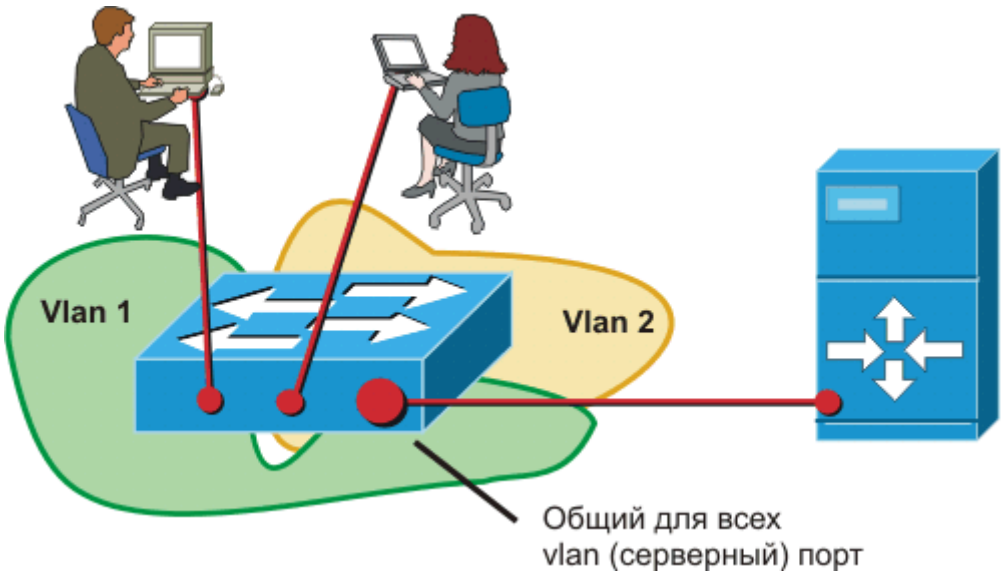

Рис. 6.3. Подключение пользователей через серверный порт.

Логика работы (но не алгоритм) при этом относительно запутанная, и часто зависит от производителя. В большинстве случаев все исходящие кадры (2-го сетевого уровня по модели OSI) пересылаются на единственный серверный порт, и оттуда уходят в сеть передачи данных.

Но надо заметить, что есть варианты устройств, которые пересылают кадры с неизвестным адресом назначения (destination address, DA) на все порты. В случае, если устройство с таким адресом подключено к одному из портов, оно ответит на кадр. Но ответ в этом случае не будет передан "напрямую" через коммутатор, так как он пойдет с адресом назначения, уже известном таблице соответствия коммутатора.

В обратном направлении кадры от пограничного маршрутизатора (или сервера) поступают на серверный порт, который распоряжается ими как обычный неуправляемый коммутатор. Широковещательные отправляет на все порты, кадры с известным адресом назначения (DA) - только адресату.

Очевидно, что полной защиты пользователей друг от друга такая сеть не имеет. Тем не менее, с некоторыми допущениями можно сказать, что с помощью VLAN на основе группировки портов можно построить сеть, в которой абоненты не смогут обмениваться трафиком иначе, чем через сервер (шлюз).

При этом важным становится правильный дизайн сети. Если она сделана как "дерево" из коммутаторов, поддерживающих VLAN на основе группировки портов, то разделение на виртуальные сети хоть и с оговорками, но будет работать. Но если "серверные" порты коммутаторов будут связаны через обычный неуправляемый коммутатор, или хаб - система рушится. То же самое произойдет при неправильной настройке сервера (шлюза).

Пользователи начинают работать друг с другом напрямую, как это бывает, если они находятся в одной сети Ethernet, и о виртуальных сетях не может быть и речи.

К сожалению, у рассмотренного способа образования VLAN есть и еще одно уязвимое место. Недорогие устройства далеко не идеальны, и часто работают по алгоритму, ведомому только производителю.

Часто простота идет в ущерб надежности - как классический пример можно привести образование VLAN с помощью ограничения ARP-запросов (некоторые модели Surecom, Compex). Понятно, что в этом случае пользователь может "прописать" ARP-таблицу вручную, и работать не обращая внимания на VLAN.

Часть 3. Глава 6

"Телекоммуникационные" способы создания виртуальных соединений.

При создания соединений через виртуальную частную сеть (ВЧС, VPN, Virtual Private Network), основной протокол работы сети передачи данных используется лишь как транспортная основа, поверх которой создаются соединения "точка-точка". Иначе говоря, создаются туннели, которые представляет собой логические сетевые соединения, установленные между двумя оконечными устройствами, и позволяющее включать данные одного протокола в пакеты другого.

В качестве транспортного может быть использован либо сетевой уровень (например IP, по модели OSI, для протокола L2TP), либо канальный (Ethernet для протокола PPPoE). В обоих случаях, связь между узлами устанавливается через поле данных кадра (дейтаграммы) транспортного протокола.

Как кадры достигают места назначения в этом случае не важно - в сети могут использоваться как простейшие концентраторы, так и дорогие коммутаторы. Более того, абонент может быть включен в сеть (получить доступ к внешним ресурсам) из любой точки сети по своим учетным данным - имени и паролю. В общем случае даже скорость не является принципиальным фактором.

Не удивительно, что такие способы создания виртуальных соединений (несмотря на относительно недавнее появление) уже широко используется в крупных офисах, и у Ethernet-провадеров.

Виды виртуальных частных сетей

Прежде всего, не следует понимать термин ВЧС как что-то однотипное. По назначению можно выделить следующие типы систем:

- Клиентские (Intranet VPN). Используются для подключения отдельных узлов (рабочих станций) к центральному серверу посредством туннелированного протокола (как правило PPP). Изначально эта схема предназначалась для доступа сотрудников внутри корпорации, но быстро получила признание провайдеров и в настоящее время широко используется в домашних (территориальных, кампусных) сетях;
- Корпоративные (Extranet VPN). Служат для соединения удаленных офисов (с большим количеством пользователей) через частные туннели (PPP) поверх публичной сети Интернет, или путем шифрования пакетных данных с помощью IPSec. Таким образом могут быть построены сети очень значительно (мирового) масштаба;

- Маркетинговые схемы. В этом случае термин ВЧС может означать любую удобную оператору общность узлов в СПД, если существуют правила, позволяющие разграничить доступ между различными сетями по какому-либо признаку. К технологиям этот вид имеет отношение достаточно отдаленное, однако применяется весьма часто.

В техническом плане можно выделить несколько протоколов, которые получили наибольшее распространение. Это PPP, L2TP, L2F, PPPoE и MPLS.

Исторически протокол PPP (Point-to-Point Protocol, RFS 1661) появился весьма давно, еще в начале 90-х годов. И использовался в основном для работы через выделенную коммутируемую линию. В качестве протокола более высокого уровня использовалась технология High-Level Data-Link Control (HDLC), которая включала поддержку IP и некоторые другие протоколы.

Спустя несколько лет был разработан более масштабируемый и технологичный PPTP (Point-to-Point Tunneling Protocol), который был поддержан большинством разработчиков. Очевидно, что в протоколе PPTP не оговариваются конкретные методы аутентификации и шифрования - это задача для более высоких уровней (по модели OSI). Но обычно их использование не вызывает трудностей, например в MS Windows включена схема шифрования DES компании RSA Data Security (Microsoft Point-to-Point Encryption - MPPE)

Следующим шагом (в 1999 году) стал L2TP (Layer-Two Tunneling Protocol, RFC 2661). Этот протокол позволяет передавать кадры второго уровня (PPP) по маршрутизируемой сети IP в виде пакетов UDP. При использовании L2TP вызовы пользователей направляются через концентратор доступа (Access Concentrator LAC) на центральный сервер (Network Server LNS), который являются конечной точкой для всех сеансов связи PPP.

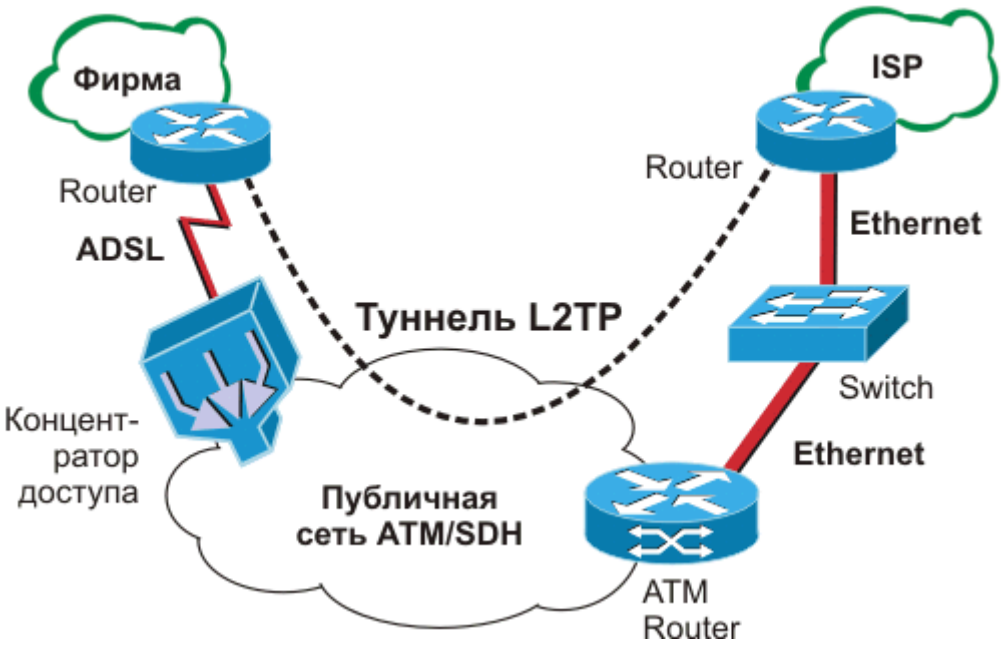

Рис. 6.4. Схема сети коммутируемого доступа с использованием L2TP

Такая схема удобна для мультисервисных сетей передачи данных, так как не зависит от особенностей ее реализации. На одном туннеле L2TP могут совместно использоваться ATM, Ethernet, Frame Relay - но это ничего не изменит в логической схеме туннеля.

Достаточно выполнения одного условия - связи на уровне IP. Соответственно, не нужно осуществлять конфигурацию адресов и выполнять аутентификацию - эти вопросы решаются на уровне IP.

Надо отметить, что как L2TP, так и PPPTP может использоваться совместно с широко распространенным средством шифрования IPSec, которое резко повышает безопасность передаваемых данных. IPSec (IP Security Protocol) обеспечивает шифрование дейтаграмм IP на третьем уровне по модели OSI. ПРи этом определены стандартные методы аутентификации пользователей (или компьютеров) при инициации тоннеля, способы шифрования данных конечными узлами, формирования и проверки цифровой подписи, а также стандартные методы обмена и управления криптографическими ключами.

С другой стороны, надежные методы шифрования имеет свою обратную сторону - высокие требования к производительности терминирующего роутера, а значит его невысокую производительность и большую стоимость. На практике, модуль шифрации IPSec начального уровня для Cisco, рассчитанный на поток данных в 5 мегабит, стоит более тысячи долларов.

Однако, для локальной сети значительно более удобен (и имеет меньшие накладные расходы) протокол PPPoE (PPP other Ethernet, RFC 2516). Название говорит само за себя. Технология эта относительно новая, стандарт выпущен а феврале 1999 года, но уже успела стать популярной.

Актуальность PPPoE для домашних (территориальных) сетей и Ethernet-провайдеров весьма высока. Получается, что через ЛВС можно работать по хорошо изученному алгоритму классического коммутируемого доступа. Можно поддерживать аутентификация пользователей по протоколам PAP и CHAP, динамическое выделение IP-адресов пользователям (по DHCP), назначение адреса шлюза, DNS-сервера и другие полезные возможности. Более того, остается старая и отработанная система биллинга (на основе TACACS или RADIUS), управления, и технической поддержки.

Так как именно технология построения сетей на основе Ethernet является основной целью данной книги, рассмотрим использование протокола PPPoE более подробно.

Логика работы следующая - два узла должны сообщить друг другу свои адреса и установить начальное соединение, а затем запустить сессию PPP.

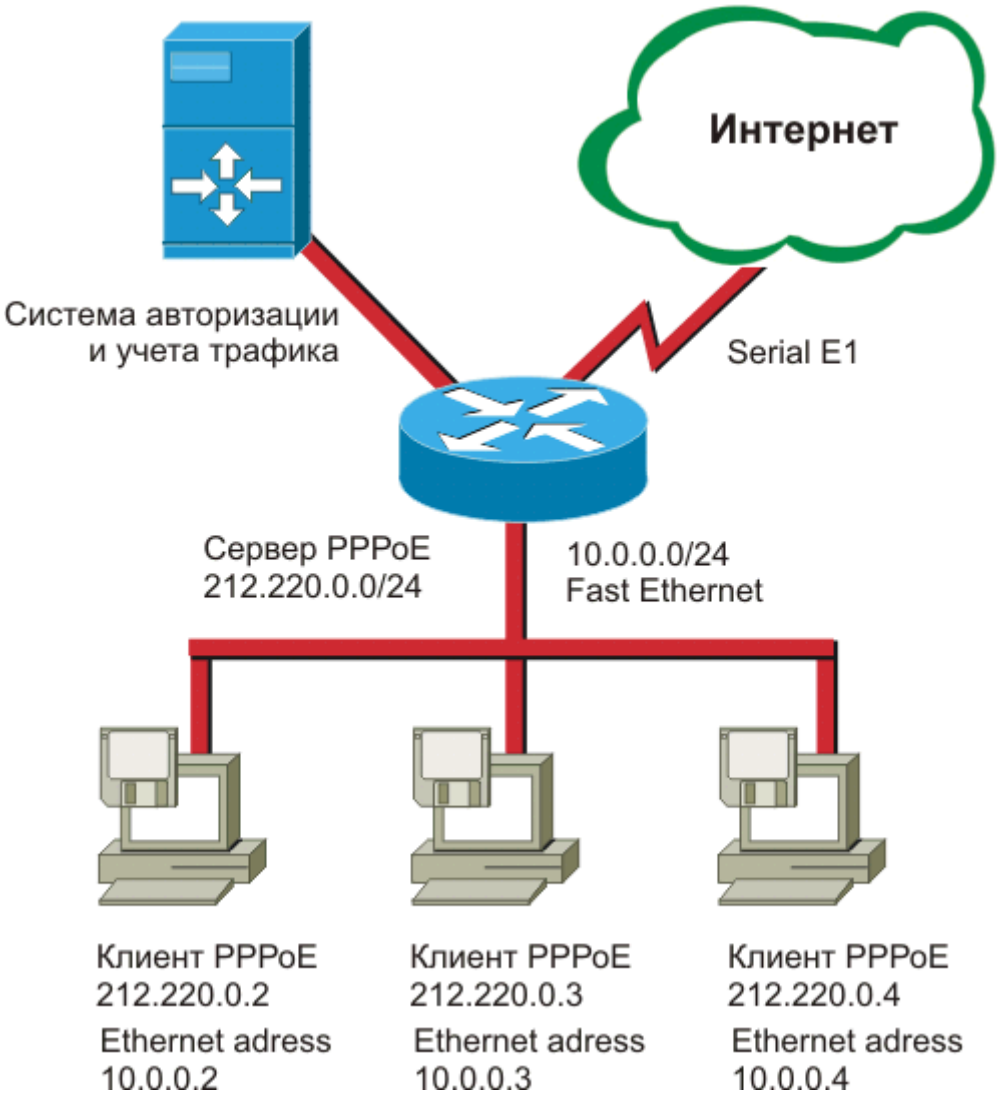

Рис. 6.5. Схема сети, ориентированной на PPPoE

В начале узел-клиент посылает широковещательный запрос Ethernet (PPPoE Active Discovery Initiation, PADI), в котором адрес назначения кадра является broadcast address, на поиск сервера со службой PPPoE. Ответ от концентратора доступа (PPPoE Active Discovery Offer, PADO) посылается клиенту (если в сети есть много устройств со службой PPPoE, то клиент получит много пакетов PADO).

Программное обеспечение клиента выбирает необходимый ему концентратор доступа и посылает ему пакет (PPPoE Active Discovery Request, PADR) с информацией о требуемой службе (класс обслуживания, имя провайдера и т.п.). После получения запроса, концентратор доступа подготавливается к началу PPP сессии и посылает клиенту пакет PADS (PPPoE Active Discovery Session-confirmation).

Если службы, запрашиваемые клиентом, доступны, в состав пакета PADS входит уникальный номер сессии, присвоенный концентратором, и этап работы по установленной сессии PPP. В противном случае клиент получает пакет PADS с указанием ошибки в запросе услуги.

В заключение рассказа о PPPoE отметим его основной недостаток - технология работает только в сети Ethernet, т.е. применение транзитных маршрутизаторов (работающих на уровне IP) недопустимо (или требует от них специального программного обеспечения).

Это сильно сужает возможности PPPoE, и, скорее всего, так и не даст этому методу завоевать рынок.

Кроме перечисленных выше, нужно отметить протокол L2F (Layer 2 Forwarding), являющийся еже одним развитием PPTP. В отличие от него, L2F может использовать для создания туннеле не только IP, но и другие протоколы сетевого уровня. Кроме этого, для удаленного доступа может быть использован не только PPP, но и другие протоколы, например, SLIP.

Можно добавить, что L2F является одним из компонентов базовой для большинства провайдеров операционной системы IOS (Internetwork Operating System) компании Cisco Systems. Но, даже не смотря на это, большого распространения (по крайней мере в России) он не получил.

Еще один одним способом создания ВЧС является технология многопротокольной коммутации с заменой меток (Multiprotocol Label Switching, MPLS). Это решение наиболее новое из перечисленных, и создает туннель уже не на 2-ом (канальном) уровне, а на 3-ем (сетевом). Если говорить упрощенно в терминологии данной главы, то это некий гибрид между локальным и телекоммуникационным способом.

Возможности технологии велики, и весьма интересны. Так, допустимо на одном физическом маршрутизаторе создать несколько виртуальных, каждый из которых будет работать по собственному набору правил.

Однако технология MPLS еще не получила статуса IEEE, и является корпоративным стандартом некоторых вендоров (в особенности Cisco). К тому же это решение на сегодня является весьма дорогим, и поэтому недоступным для небольших сетей.

В заключение, надо отметить, что развитие средств создания ВЧС сейчас переживает период бурного развития, появляются новые технологии, и производители… Поэтому нужно понимать, что кроме рассмотренных способов построения ВЧС есть много частных решений от различных компаний. Их диапазон весьма велик - от интегрированных многофункциональных и специализированных устройств до чисто программных продуктов.

Часть 3. Глава 6

Сравнение "локального" и "телекоммуникационного" метода.

Вообще говоря, оба метода могут применяться совместно. От этого безопасность работы в сети, защита от подделки учетных данных, и надежность только возрастут, поэтому противопоставлять их друг-другу не совсем правильно. Однако главным критерием в данном случае является стоимость установки и обслуживания сети, и в этом ключе имеет смысл рассмотреть основные достоинства и недостатки обоих методов.

Основная слабость телекоммуникационного способа в том, что он не дает средств контроля абонентов внутри сети Ethernet. Т.е. несколько узлов вполне могут обмениваться любой информацией, и по любому протоколу - это скорее всего будет даже не замечено

провайдером. На первый взгляд это не слишком страшно - доступ к внешнему трафику защищен, данные абонентов шифруются…

Но у пользователей остается возможность использовать сеть в своих нуждах - например обмениваться большим объемом данных (по сути бесплатно загружая сеть), или вообще сделать "пиратское" подключение к другому провайдеру и продавать трафик другим абонентам. На этом фоне взлом недостаточно защищенных компьютеров изнутри сети покажется совсем нестрашным…

Добавляет проблем и то, что сеть остается обычным Ethernet'ом, со всеми его недостатками. Так, кадр канального уровня может быть простыми методами перехвачен соседним узлом ("прослушивание" при некоммутироемой сети, либо несколько более сложные процедуры на сети, построенной на неуправляемых коммутаторах). Поэтому, нешифрованный туннель не спасает положение. Сложность "подделки" учетных данных несколько увеличивается, но "прослушивание" заметно не усложняется. Разумеется, шифрование снимает проблему, однако требует существенных вычислительных ресурсов от сервера провайдера.

Следующий практический минус - при сложной топологии сети провайдера (например, при передаче данных между сегментами сети через коммуникации стороннего оператора) появляется возможность построения несанкционированных каналов связи уже на уровне "чужих" IP адресов (без шифрации).

В то же время к несомненным плюсам данной технологии можно отнести простоту внедрения и эксплуатации, удобный биллинг (отработанный еще для коммутируемого доступа), экономию IP адресов (их можно выдавать последовательно из одного большого блока). Авторизация по паролю так же дает несколько непривычные возможности, например доступ до ресурсов сети с удаленного узла (из другого города), или dial-up в случае сбоя сети Ethernet с теми же учетными данными.

В целом, можно сказать, что на сегодня телекоммуникационный метод является необходимым минимумом, который должен обеспечить серьезный Ethernet-провайдер.

"Локальная" технология требует больших капитальных затрат - для нее (как минимум) необходимы дорогие управляемые коммутаторы. Это, пожалуй, главный и единственный минус данного пути развития.

Однако взамен технология позволяет обеспечить полную защиту (изоляцию) пользователя, и возможность четко идентифицировать узел прямо "на порту" - что позволяет полностью контролировать сеть полностью с центральной площадки оператора. Т.е. "видеть все действия" и "управлять" каждым пользователем в отдельности.

Плюс ко всему можно использовать такие дополнительные возможности оборудования, как резервирование линий (STP), подсчет трафика на порту абонента (SNMP). А в перспективе - простой переход к обеспечению разделения по качеству сервиса (QoS). Что вполне может вывести услугу на более высокий качественный (мультисервисный) уровень.

Можно сказать, что стоимость управляемых коммутаторов постоянно и быстро снижается. На сегодня уже можно приобрести модели китайских производителей в районе $200-400, в дальнейшем можно прогнозировать частичное вытеснение неуправляемых моделей в

пользу таких же по стоимости "интеллектуальных" устройств, и стирание ценовой границы между ними.

Таким образом, в долговременной перспективе "локальная" технология выглядит несколько более предпочтительно. Но окончательный вывод делать пока преждевременно - слишком быстро все меняется на этом динамичном рынке.

Глава 7. Экономика и управление Ethernet-провайдера.

Каждый народ заслуживает таких провайдеров, которых оплачивает.

Домашние сети и Ethernet-провайдинг явление во многом уникальное. Самим своим существованием подобные предприятия обязаны экономическому казусу. А точнее - резкому (и в общем неожиданному) падению стоимости оборудования из сектора SOHO/Enterprise (домашний, небольшой и средний офис).

В конце 90-х выяснилось, что оборудование, пригодное для создания районной и, тем более, внутридомовой разводки Ethernet стоит невообразимо дешево (по телекоммуникационным меркам, разумеется). Классические технологии провайдеров того времени (xDSL, V35, E1, и т.п.) уступали по стоимости в десятки, а порой даже в сотни раз.

Это положение не осталось незамеченным любителями и небольшими активными фирмами. Их не остановил даже не совсем понятный правовой статус создаваемых сетей, сложности освоения новых технологий, и прочие риски, присущие принципиально новым проектам. Не зря еще в позапрошлом столетии писал Карл Маркс:
"Капитал боится отсутствия прибыли или слишком маленькой прибыли, как природа боится пустоты. Но раз имеется в наличии достаточная прибыль, капитал становится смелым. Обеспечьте 10 процентов, и капитал согласен на всякое применение, при 20 процентах он становится оживленным, при 50 процентах положительно готов сломать себе голову, при 100 процентах он попирает все человеческие законы, при 300 процентах нет такого преступления, на которое он бы не рискнул, хотя бы под страхом виселицы."

Свою роль в становлении Ethernet-провайдинга как отрасли сыграли и монополисты телефонии. Как владельцы единственных существующих распределительных сетей они (за редким исключением) оказались неспособными эффективно распоряжаться этим "богатством". Однако, альтернативных операторов до "последней мили" они не допустили. Оставив последним невеселый выбора - либо скатиться в небольшие ведомственные и прочие узкие ниши... Либо строить свою распределительную сети на основе Ethernet.

В результате незаметно, в течении 3-4 лет, Ethernet-провайдеры через свои сети подключили многие тысячи абонентов. И захватили во многих городах (включая Москву, и прочие крупные центры) более половины (а кое-где и до 90%) рынка домашних пользователей выделенных линий. Серьезно потеснив xDSL и DialUp.

Сейчас ценовая диспропорция Ethernet с другими технологиями постепенно выравнивается, да и владельцы телефонной инфраструктуры под давлением конкуренции начали принимать меры по "самоспасению". Но мощный первоначальный экономический импульс еще далеко не исчерпан. Сети продолжают расти едва ли не в геометрической прогрессии.

Но если несколько лет назад прибыль относительно легко покрывала все издержки неуклюжей полулюбительской организации, то чем дальше, тем острее ведется конкурентная борьба. И тем большее значение придается правильной экономической и организационной части сетевой инфраструктуры. О которой, собственно, и пойдет речь в данной главе.

Глава 7. Главное – это абонент.

У провайдеров не так много источников доходов. Вернее сказать, он только один - платежи абонентов. Поэтому именно с них нужно начать рассмотрение всех экономических вопросов операторов связи вообще и Ethernet-провайдеров в частности.

Понятно, что сделать точный расчет без "привязки" к городу, времени, району, ситуации и т.п. факторам нельзя. Поэтому приведенные ниже выкладки можно рассматривать лишь как приблизительные, обзорные, показывающие скорее тенденции, а не факты.

Для начала несколько усредненных цифр по отчетам экспертного агентства J'son & Partners. В Москве порядка 3 миллионов домохозяйств, из них к концу 2004 года будет подключено к Интернет широкополосным каналом около 250 тысяч. И быстрый рост (до 80-90%) продолжится еще один год, и к 2006 году количество абонентов вырастет до 500 тысяч. Далее рост замедлится, но к 2010 году их количество достигнет 2 миллионов (если не вмешаются серьезные катаклизмы экономики или политики).

Отметим, что для других регионов России эти данные то же вполне применимы - разумеется с определенной временной поправкой.

То есть при таком быстром росте нельзя строить сеть с расчетом на сегодняшние 10% (5%, 15%) подключенных домохозяйств. Нужно рассчитывать на "завтрашние" (заметно более выгодные) финансовые показатели по 20-ти процентам подключенных квартир. И иметь в виду возможность подключения до 80% через несколько лет.

Второй важный показатель - сумма, которую пользователь готов заплатить за выделенный канал в месяц, то же известна с достаточно большой точностью. Исследования, проведенный для московского оператора ADSL (Стрима) показывают следующее:

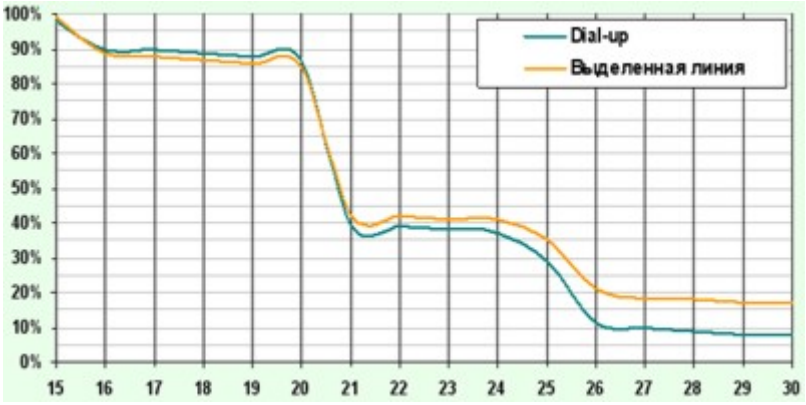

Рис. 7.1. Процент пользователей, готовых подключиться к Интернет, в процентах от опрощенных, в зависимости от суммы месячных затрат, в USD.

Конечно, сумма реальных затрат абонента может сильно отличаться от планируемых расходов. Однако уровень массового спроса вполне определен - это 20 USD в месяц (на 2004 год, для Москвы).

Интересный и важный следующий момент. Сумма средних ежемесячных трат практически не зависит от стоимости услуг (бюджетная модель потребления) - при более дорогом трафике абонент потребляет его меньший объем, при более дешевом - больший. И только при помощи принципиально иных (и конечно нужных) услуг можно получить увеличение абонентского платежа.

Например, один-два доллара с абонента можно заработать на доступе к качественно оформленному видео-аудио порталу. Или за "профессиональный" почтовый ящик с доступом по IMAP. Или за место под www сервер. В общем, так или иначе, но до 25 USD средний платеж "дотянуть" в Москве можно (в других регионах России эта величина будет меньшей - приблизительно от 10 до 20 долларов).

Что бы провайдерская фирма могла хоть как-то существовать (содержать штат, офис, платить налоги) нужно получить около 5к$ прибыли. Да еще оборудование центрального узла и лицензии - $20к разовая покупка. Учитывая, что стоимость обслуживания абонента сети около $10 (этот вопрос будет рассмотрен более подробно в следующих параграфах), то нужно подключить минимум 500 абонентов. Однако если подумать о начальных затратах, то выходит, что сети менее 1000 пользователей способны существовать только за счет внешних инвестиций (либо на иной, не коммерческой мотивации).

При себестоимости подключения абонента в $50 минимальный стартовый капитал для строительства жизнеспособной сети составляет 50 тысяч долларов. Однако, подключение процесс не одномоментный. И примерно год придется потратить на строительство при сохранении основных расходов. Это еще затраты порядка 50-100 тысяч. Таким образом, в районе с сильной конкуренцией "стартовать" без серьезных денег бессмысленно.

Конечно, часть расходов может покрыть плата за подключение. Более того, еще несколько лет назад сети начинали строительство вообще без инвестиций, поддерживая развитие за счет этого источника. Но конкуренция берет свое - приобретать новых абонентов сложнее чем удерживать, поэтому бесплатное (или дешевое) подключение становится нормой для "догоняющих" компаний.

С ростом количества абонентов растет и доход оператора. Затраты, благодаря эффекту масштаба, увеличиваются в меньшей степени. Понятно, что не нужен второй офис,

директор, бухгалтер, более эффективно используются силы системных администраторов и монтажников. Да и трафик в больших объемах стоит дешевле.

Можно предположить, что себестоимость услуг на абонента (обслуживание плюс трафик и другие покупные услуги) упадет с 15-20 долларов до 10. На оставшиеся $20-$10=$10 нужно жить и развиваться. Много это или мало?

С одной стороны вроде бы рентабельность более 100%, чего еще желать... С другой - в расчеты не включена амортизация основных фондов (т.е. инфраструктуры) и необходимость возврата инвестиций. В провайдинге, как нигде, идет быстрая смена поколений оборудования и материалов.

Предположим (упрощенно), что сеть развивалась следующим образом (в месяц добавляется 100 абонентов, себестоимость подключения $50):

Мес.	абоненты, чел.	затраты на обслужив.	доход, на абонента	прибыль на аб.	затр. на подкл.	пр. на сеть
1	100	25	20	-5	25000	-25500
2	200	25	20	-5	5000	-6000
3	300	25	20	-5	5000	-6500
4	400	25	20	-5	5000	-7000
5	500	25	20	-5	5000	-7500
6	600	25	20	-5	5000	-8000
7	700	20	20	0	5000	-5000
8	800	20	20	0	5000	-5000
9	900	20	20	0	5000	-5000
10	1000	20	20	0	5000	-5000
11	1100	20	20	0	5000	-5000
12	1200	20	20	0	5000	-5000
13	1300	15	20	5	5000	1500
14	1400	15	20	5	5000	2000
15	1500	15	20	5	5000	2500
16	1600	15	20	5	5000	3000
17	1700	15	20	5	5000	3500
18	1800	15	20	5	5000	4000
19	1900	10	20	10	5000	14000
20	2000	10	20	10	5000	15000
21	2100	10	20	10	5000	16000
22	2200	10	20	10	5000	17000
23	2300	10	20	10	5000	18000
24	2400	10	20	10	5000	19000
25	2500	10	20	10	5000	20000
26	2600	10	20	10	5000	21000
27	2700	10	20	10	5000	22000
28	2800	10	20	10	5000	23000
29	2900	10	20	10	5000	24000
30	3000	10	20	10	5000	25000
31	3100	10	20	10	5000	26000
32	3200	10	20	10	5000	27000
33	3300	10	20	10	5000	28000
34	3400	10	20	10	5000	29000
35	3500	10	20	10	5000	30000
36	3600	10	20	10	5000	31000
				Итого:	200000	331000

Рис. 7.2. Экономические показатели развития домашней сети, в USD.

Первый год, как и говорилось выше, выход на операционную окупаемость. Далее идет работа в прибыль.

Однако, через 3 года вполне может оказаться, что сеть... устарела. И нуждается в тотальной реконструкции. На первоначальное строительство было затрачено $200к, реконструкция обойдется в $150к. А прибыль получена всего $330к. Т.е. результат - около 50% за 3 года... Далеко не блестящий - а ведь в реальности затраты всегда больше, а прибыль - меньше.

Конечно, в примере очень велики погрешности. На практике в данной ситуации возможна и заметная прибыль, например если подключать не 100 абонентов в месяц, а 200 - получить "чистыми" удастся $687к. Но если выбрать слишком дорогое оборудование и тратить на подключение $100 - то в результате сеть будет стоить $370к, а прибыль - $150к. Но тут и реконструкция может понадобиться не через 3, а через 4 года.

Таким образом, экономика сетей (как и любых проектов, рассчитанных на сбор средств с большого числа абонентов) очень сильно зависит от правильных решений. 2-3 лишних доллара с клиента способны полностью переломить ситуацию в ту или иную сторону. Малый темп подключений - убытки. Быстроустаревающая схема - убытки, дорогое решение "с запасом" - опять убытки. В общем, вариантов масса, и они требуют настоящего профессионального расчета.

Кроме цифр на выбор и платежи абонента влияет еще множество субъективных факторов. Район города, время года, уровень цен конкурентов DialUp, степень телефонизации, наличие или отсутствие повременной оплаты телефона, и многое другое. Это все желательно учитывать в бизнес-плане.

Но особенное внимание нужно обратить на качество услуг - это огромный вопрос, но и он выходит за рамки экономики Ethernet-провайдеров. Для простоты нужно считать, что качество не должно подлежать обсуждению. А просто должно быть. То же самое, кстати, можно сказать и об имидже оператора.

Подводя итог, можно сказать, что провайдеру нужно взять с абонентов максимум денег, потратив на это минимум. Случаи любительских сетей, а так же полусоциальные проекты тут придется оставить в стороне - у них сосем другие, как правило неэкономические задачи. Таким образом, задача распадается на классические условия:

- Привлечь максимум пользователей (причем обязательно платежеспособных).
- Создать сеть с минимальной полной стоимостью (строительство плюс обслуживание);
- Продать пользователям наибольший возможный пакет услуг.

А вот как идти к поставленной цели - будет рассмотрено в следующих частях.
