

Теория

Глава 1 : Операторские технологии передачи данных

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 Мбит/с передавал 24 тайм-слота, а в Европе (и немного позже в Советском Союзе) - поток E1, имеющий скорость 2,048 Мбит/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 8,448 - 34,368 - 139,264 - 564,992 Мбит/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.

[Теория] 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.

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).

[Теория]

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.

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.

[Теория]

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 прозрачностью FR для протоколов более высокого уровня снискало ему популярность в кругах распределенных банковских и корпоративных сетей.

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.

[Теория]

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. Обратная 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.

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 тоже 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 заголовков), 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.

Глава 2 : Технологии локальных сетей

Незаслуженно забытый ARCnet

Attached Resource 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. А также ограничение максимального числа клиентов в пределах одной сети - не более 256 и как правило необходимость выставлять сетевые адреса на сетевых картах с помощью джамперов, соблюдая при этом их уникальность. 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 (благодаря своей надежности и большой протяженности). 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: $T = (TDP + TOBoNb) \cdot ND$, 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. Как правило сеть состояла из системы активных (до 600 метров) и пассивных (до 200 метров) хабов, связанных коаксиальными линиями. В нашей стране эти сети получили большое распространение на промышленных предприятиях в 80-ых годах, благодаря использованию дешевого и массового кабеля РК-75 (антенный) и серверов Novell Netware 2.x-3.x

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 это не могло сыграть решающую роль, и сейчас найти реально работающую сеть Token Ring практически невозможно.

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 передаче маркера.

Дополнительно предусматривалась развитая схема приоритизации 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.

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 нише. Не помогли стандарту и попытки перейти 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.

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 она 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 802.3u), а затем и "гигабитном" Ethernet 1000base-T.

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 шины 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 3 : 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.

[Теория]

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 Token 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 (switch). 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 802.3х, появляется полный дуплекс и контроль соединения для 10baseT, спецификация IEEE 802.1р 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 4 : АТМ как универсальная технология передачи данных

Описание стандарта АТМ 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 АТМ 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 АТМ (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 АТМ-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 Т3).

Если говорить в общем, то суть АТМ 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.

[Теория]

Рис. 2.4. Принцип работы АТМ

На размер минимальной порции данных (ячеек в терминологии АТМ) 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 АТМ более 622 Мбит, и резко повысило стоимость на меньших скоростях.

Второй компромисс АТМ - 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 АТМ 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 АТМ. 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 АТМ 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 АТМ на 155 Мбит/с чрезвычайно дорогим для использования в этом сегменте рынка.

Предприняв попытку определить низкоскоростные решения для настольных систем, АТМ 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), АТМ 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 АТМ на некоторое время закрепились. Таково ее положение в отрасли на сегодня. Однако, и этот вопрос будет рассмотрен еще не раз в следующих главах.

Глава 5 : 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 передается по сетям электросвязи. И именно ему они обязаны головокружительным ростом. Поэтому, их нельзя разделять ни в технических, ни в бизнес-расчетах - 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.

[Теория]

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.

[Теория]

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.

[Теория]

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.

[Теория]

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 UUСР'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, заверивший 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.

Глава 6 : Принципы построения СКС

История СКС

Примерно в середине 80-х годов в офисы (прежде всего североамериканские) быстро начала внедряться компьютерная техника. Что вызвало практически обвальным рост объема информации, передаваемой внутри здания. Требования к кабельным системам увеличились. Но хуже всего, разное оборудование требовало физически разных сетей, что по очевидным причинам было совершенно неприемлемо для потребителя.

Очевидным (но далеко не простым) выходом стала **концепция структурированной кабельной системы (СКС), которая не зависит от выбора оборудования и поддерживает абсолютное большинство существующих и перспективных приложений.**

Первая попытка была осуществлена корпорацией IBM в гордом одиночестве. Была разработана кабельная система IBM для серверов AS/400, сетей Token Ring, а так же некоторых вспомогательных устройств. Удачной технической находкой стало введение в состав сети частей, используемых под телефонию.

Используемые в сети IBM виды кабелей:

- 2 экранированные витые пары из монолитных проводников (22 AWG, 150 Ом) в общем внешнем экране
- 4 неэкранированные (22 или 24 AWG, до 1 МГц) витые пары из монолитных проводников
- Два многомодовых оптических волокна
- Коммутационный кабель. 2 экранированные витые пары из многожильных проводников (26 AWG) в общем внешнем экране
- Плоский кабель для прокладки под ковровыми покрытиями. 2 не перевитые экранированные

- пары из монолитных проводников(26 AWG)
- 2 пары из монолитных проводников (26 AWG)

Зарождающаяся монополия IBM вызвала тревогу многих разработчиков сетей, и в 1985 году Ассоциация электронной промышленности США (Electronic Industries Association - EIA) приступила к созданию стандарта кабельных систем зданий.

В 1988 году к работе по стандартизации подключилась Ассоциация телекоммуникационной промышленности США (Telecommunications Industry Association - TIA).

Первый документ, TIA/EIA-569 "Стандарт для коммерческих зданий на кабельные пути телекоммуникационных кабелей" был принят в октябре 1990. В июле 1991 одобрен краеугольный "Стандарт телекоммуникационных кабельных систем коммерческих зданий" TIA/EIA-568, который определял структуру кабельной системы, требования к кабелям и разъемам, ограничивал длины кабельных сегментов. Допускалось использование неэкранированных витых пар с волновым сопротивлением 100 Ом и экранированных витых пар с сопротивлением 150 Ом, а также коаксиальных кабелей и многомодовых волоконно-оптических кабелей.

В ноябре 1991 года появилась дополнительная спецификация TIA/EIA TSB-36, в которой впервые вводилось понятие категорий кабелей из неэкранированных витых пар, фактически предложенной в 1989 году американской исследовательской организацией Underwriters Laboratories (UL) совместно с фирмой Anixter.

- Категория 1. Цепи питания и низкоскоростной обмен данными
- Категория 2. Голосовые каналы связи и системы безопасности
- Категория 3. 16 МГц, локальные сети Token Ring и Ethernet IOBase-T
- Категория 4. До 20 МГц, локальные сети Token Ring и Ethernet IOBase-T
- Категория 5. До 100 МГц, локальные сети со скоростью передачи данных до 100 Мбит/с

Это было очень важным этапом, который покончил с разнообразием типов кабелей. Практика же быстро опередила требования, можно сказать что рынок быстро перешел на единую "Категорию 5", проигнорировав все другие типы. Особенно явно это было видно в России, интеграторы которой просто не успели использовать более младшие категории кабелей в заметном объеме.

В январе 1993 года был одобрен TIA/EIA-606 "Стандарт на администрирование телекоммуникационной инфраструктуры коммерческих зданий". Он упорядочивает маркировку, ведение записей, правила оформления схем, отчетов, и т.п.

Далее работа по стандартизации не останавливалась, достаточно, например, отметить TIA/EIA-607 (август 1994 года), регламентировавший требования к устройствам заземления, технический документ TSB-95 (сентябрь 1998), в котором приводились параметры по расширению Категории 5 для работы с приложениями Gigabit Ethernet, TIA/EIA-570-A (май 1999), устанавливающий оптический разъем SC как основной, и допускающий LC в системах нового поколения...

Параллельно с TIA/EIA работу над стандартизацией СКС вели Международная организация по стандартизации (ISO) и Международная электротехническая комиссия (IEC). В 1995 году они выпустили совместный документ - стандарт ISO/IEC 11801 "Информационные технологии. Универсальная кабельная система для зданий и территории Заказчика". В 1999 году принимается стандарт ISO/IEC 14763-1, являющийся аналогом американского стандарта TIA/EIA-606.

Не отстала Европейская организация по стандартизации CENELEC, которая в августе 1995 года подготовила свой стандарт EN50173 (EN - Europa Norm).

Все три стандарта весьма близки друг к другу, различия скорее терминологические, и выходят далеко за рамки данной статьи. Надо лишь отметить, что Российская практика построения сетей опирается большей частью на североамериканскую версию.

Общие требования к СКС

Не смотря на то, что TIA/EIA представляют собой более чем объемные документы, концепцию (можно даже сказать "философию") СКС можно свести к весьма простым требованиям:

- **Универсальность** - возможность использования однотипных каналов для передачи сигналов различных систем (данные, голос, видео);
- **Совместимость** со стандартным активным оборудованием любых производителей;
- **Избыточность** - наличие достаточного количества резервных каналов связи, необходимых для расширения системы в процессе эксплуатации;
- **Гибкость** - простота и удобство обслуживания системы при внесении изменений в ее конфигурацию;
- **Надежность** - способность системы сохранять рабочие параметры в заданных диапазонах в течение всего срока эксплуатации / гарантийного срока.

=== Структура СКС ===

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 частью среды передачи.

Нельзя упускать главный, вынесенный в название, термин - **структурированность**. По назначению, структурированную сеть принято разделять на три подсистемы. Магистраль комплекса, магистраль здания и горизонтальную подсистему.

[Теория]

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.

Кроме общей классификации, различают множество типов каждой подсистемы, оговаривается, все вплоть до максимальной нагрузки на пол от установленных телекоммуникационных шкафов. При этом нельзя сказать, что все становится просто и понятно, есть и нестыковки. Особенно когда дело доходит до конкретики. То раскладки "цветов" в разъеме разные, то проектные ограничения сильно отличаются...

Ничего удивительного нет, ведь СКС - в сущности 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.

Более того, нужно понимать, что в отличие от активного оборудования, СКС создают тысячи и десятки тысяч независимых организаций, 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.

Однако, основные принципы построения позволяют сравнительно легко обходить подводные камни частных стандартов.

Избыточность

Хотелось бы особо отметить такой признак, как **избыточность**. В отличие от других, он не слишком очевиден, более того, на первый взгляд кажется нерациональным и даже вредным. Достигается он 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.

Понятно, что это 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. Ведь 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).

Преимущества СКС

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.

Как правило, эти аргументы являются достаточными для убеждения корпоративного заказчика. И выбор, в основном, идет не между "идеями", а по вариантам исполнения (т.е. интеграторами).

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, часто достигая размеров города.
Качество услуг не нормируется.	Снижение качества услуг (или их временное прекращение) оговаривается регламентами, и должно быть минимизировано. Иначе говоря, существует нормировка качества услуги.
Обслуживание в процессе эксплуатации должно быть исключено, или, по крайней мере, минимизировано.	Обслуживание - плановый и естественный процесс, оно проводится фактически непрерывно (на разных частях сети). Есть постоянный штат специалистов, которые заняты обслуживанием инфраструктуры.

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 одновременное использование нескольких различных сетевых протоколов (в настоящее время не актуально);	Как правило, используется один протокол передачи данных. Более того, количество используемых приложений может быть ограничено (например, часто запрещен netbios).

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.

На основании вышеизложенного, можно сделать следующий вывод:

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 7 : Проблемы внедрения СКС в небольших сетях

Недостатки СКС для решения задач малых предприятий

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.

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.

Понятно, что для больших фирм потребность в высоком качестве и низкие затраты 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 20-30 человек, которая занимает 10-15 комнат в **арендованном** помещении, на 1-2 этажах? * При таком варианте ответ совсем не однозначен, и зависит от многих дополнительных факторов.

Разумеется, недорогая сеть, построенная "по потребности" - это совсем не значит свалить все активное оборудование в кучу под стол, разбросать кабеля по полу, обжать разъемы отверткой. Стойки, короба, качественные кабели 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. Преобладает подход "все или ничего" - стандартная СКС за полную стоимость, или наплевательское "кабель по плинтусу, а хаб - под стол".

- Действительно, многие производители СКС, не считают потребителями своей продукции офисы с количеством рабочих мест менее 50.

[править]

Оценка качества

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.

Попробуем забыть (не навсегда, конечно) вопрос 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.

[Теория]

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, 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. Хотя 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 то же. 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.

[править]

Оценка долговечности

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 сохранения 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 должен появиться в рабочих станциях только после 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.

Однако практика показала, что, не смотря на массовую установку гигабитных сетевых карт, переход на Gigabit идет очень неторопливо. В том числе из-за большого количества инсталлированных сетей Cat.5, которые поддерживают гигабит не полностью. Обычно проще продолжить работу на 100 мегабит, чем полностью менять кабельную систему.

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 8 : 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).

Содержание

- 1 Соединение в сеть двух компьютеров
- 2 Основные моменты настройки компьютеров
- 3 Создание сети малого офиса (5-10 рабочих мест)
- 4 Сеть небольшой фирмы (40-60 рабочих мест)

[править]

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 рассмотрены 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 (УТР)

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.

Изображение:Ch5-1.jpg

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.

[править]

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".

[Теория] 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".

[Теория] 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.

[Теория] Рис. 5.17. Протокол Интернета TCP/IP.

Некоторой настройке 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.

[править]

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:

[Теория] 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 мешают. 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. Удлинитель крайне не желательны - при уборках или перемещениях мебели они страдают в первую очередь.

Вот пример простого эскизного проекта:

[Теория] 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 годятся материалы и оборудование даже малоизвестных марок типа Genius, Surecom, Eline, Comrex, 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 кирпича) 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 конструктивно-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 выпадения 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.

[Теория] 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).

[Теория] 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 пожаробезопасность.

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.

[Теория] 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.

[править]

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 техническими особенностями 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.

[Теория] 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.

Глава 9 : Будущее СКС и его влияние на Ethernet-провайдинг

Известно, что Ethernet-провайдинг фактически паразитирует на своем старшем брате - корпоративных сетях. Из этого параллельного мира берется почти все - идеи, элементы СКС, активное оборудование... И еще цены на все перечисленное, сниженные массовыми (отнюдь не операторскими) тиражами.

Еще с конца прошлого века интеграторы бодро заявили, что СКС категории 6 (до 200 МГц) перекроют все потребности на 10 лет вперед, призвали переходить на этот стандарт, и... Замолчали.

Реальные инсталляции Cat.6 оказались весьма дорогими и малосовместимыми. Например, далеко не всякие разъемы RJ45 проходят по этому стандарту. Появились даже идеи "пропустить" Cat.6 в пользу Cat.7. И, хотя острота вопроса была снята Cat.6A - осадок остался.

С Cat.7 все еще более интересно. Тут нужно применять специальные разъемы, например TERA компании Siemon, или GG45 NEXANS. И конечно, специальный, дорогой кабель (стоимость более \$1 за метр).

[Теория] Разъем TERA компании Siemon.

С другой стороны, для гигабита более чем достаточно Cat.5e - что и устраивает большинство заказчиков до настоящего времени. Ну а про главный козырь СКС (готовность к любым приложениям на 10-15 лет вперед) предпочитают "слегка" умалчивать.

Летом 2006 года был принят 10GBase-T (802.3an) однако спецификация 10GBase-T, позволяет использовать в большинстве случаев витую пару категории 6A, в некоторых унаследованных приложениях - витую пару категории 5E и в некоторых европейских странах - витую пару класса high-end категории 7. Причем неэкранированный кабель Cat.6 поддерживает работу 10GBase-T только на 55 метров, а Cat.5e на расстояниях менее 15-20 метров.

Есть и более кардинальные предложения, для скоростей 10G просто использовать оптоволокно. Выйдет надежнее и дешевле - ведь хепрак и X2 на стекло давно в рознице (цена SM - менее \$1000), а на медь - лишь обещаны (до сих пор, на конец 2007 года, модулей 10GBase-T нет в линейке Cisco).

Кстати сказать, есть хороший пример. На сегодня гигабитные модули SFP и GBIC для оптики (SM) заметно дешевле, чем для витой пары. Очень вероятно, что для 10GBase-T это повторится.

Не отстают и аналитики - они давно пообещали, что продажи оптоволокна для СКС превысят медь (правда, в стоимостном эквиваленте): [Теория]

Там же фактически говорится о забавном отходе от принципов СКС. Не явно, но подразумевается частичная модернизация оптических линий в центре, в серверной, и при этом сохранение обычных медных линий до рабочих станций. Конечно, это вполне логично в сложившейся ситуации, но...

Складывается двойственная и не последовательная картина. Не может быть ближайшее будущее таким туманным, ведь на кону большие деньги (СКС просто обязаны жить реалиями будущих десятилетий).

На мой взгляд, вполне вероятно, что "на щит" массовых инсталляций будет поднят наиболее перспективный и универсальный вариант - а именно FTTH, волокно до рабочего места. И произойдет это ориентировочно все к тому же 2010 году.

Что для этого понадобится?

- Дальнейшее удорожание витой пары. Сейчас наиболее недорогие типы перебрались через рубеж 20 центов за метр, а качественный кабель добрался до 40 центов. И дальнейший рост цен на медь не внушает оптимизма.
- Соответствующее удешевление оптоволоконка. Хотя уже сейчас патчкордовый кабель стоит порядка 20 центов за метр. Ну а оптическая мелочевка и сейчас дешевле, чем медная 6-ой категории.
- Переход на IP-телефонию. Надеяться на аналоговые телефоны с оптическим интерфейсом явно не стоит.
- Удешевление SFP до неприличных 10-20 баксов. Что, впрочем, в Китае реально.
- Переход производителей активного оборудования на интерфейс SFP. В конце концов, это даже дешевле, чем витая пара (нужно меньше элементов), а сегодняшняя дороговизна портов SFP - чистый маркетинг, и не более того.

Достоинства FTTH:

- Оптика занимает мало места, а значит кабельные каналы могут быть почти в десяток раз тоньше. Это ощутимая экономия.
- У оптоволоконка выше пожаробезопасность (просто существенно меньше потенциально горючей изоляции).
- Можно забыть про электромагнитные наводки и грозы (оборудование в правильных СКС тоже горит без защит).
- Ну и конечно - необъятный запас по полосе и дальности (стандарты на 100 метров нервно курят). Можно строить централизованные СКС как минимум масштаба здания любого размера.

Недостатки FTTH тоже есть, можно и не спорить. Однако, надо заметить что они по большей части далеко не технического характера. И не экономического. Психология, привычки, и навыки монтажников - вот что сдерживает атаку стекла.

Что же это означает для Ethernet-провайдеров? Миграция из корпоративного мира оборудования (и, главное, навыков) может сделать оптические технологии очень недорогими и привлекательными для использования в операторской деятельности.

Волокно до пользователя в доме очень удобно. Чего стоит "отмена" ограничения длины и грозозащитных наводок? А избавление от охотников за цветметом? Легкий проход самых узких и забитых стояков? Возможность более-менее легального использования шахт силовой проводки? Недорогая негорючесть (меньше изоляции - меньше цена специальной оболочки)?

Особенно нужно выделить **возможность пассивных выносов на маленькие здания** (вплоть до хрущевок на пару подъездов), чтобы не заморачиваться там с установкой активки, проектированием, обслуживанием, питанием, и т.п. проблемами. Несложно и недорого включить абонентов при помощи сетевой карты с оптическим портом или конвертером.

Действительно, сотня метров 16-ти волоконки стоит смешные по нынешним временам \$50-60, этого вполне хватит на 16 абонентов в 40-50 квартирном доме (проникновение более 40% найти за пределами Москвы сложно). Конкурирующий на таких пролетах П-296 обойдется в те же самые деньги, если не дороже.

Разводка внутри дома оптическими патчкордами по 50-150 метров тоже не должна вызвать затруднений (в самом крайнем случае, придется разъем восстановить, пустяковые затраты на уровне пары долларов). Само же волокно, как показано выше, стоит не дороже витой пары.

Дополнительные расходы возникают только на уровне оптоволоконных трансиверов, это добавит разовых затрат порядка 80 долларов на абонента. Не такая и большая сумма за упрощение структуры и сокращение количества обслуживаемых активных узлов (официальное разрешение на подключение электропитания может обойтись дороже десятка абонентов).

Так что в некоторых случаях выгоды представляются столь впечатляющими, что разумно применять

волокну до пользователя уже сейчас. Не дожидаясь массового строительства "стеклянных" СКС. Что, собственно, некоторые операторы уже делают.

Глава 10 : XDSL

Вопрос широкополосного доступа - по сути сводится к организации высокоскоростной цифровой линии до пользователя (далее - DSL, Digital Subscriber Line). Исторически, первыми на эту роль претендовали телефонные коммуникации, которые технически представляют собой отдельную медную пару от АТС до каждого абонента. Связь между АТС к началу "компьютерной" эры уже строилась при помощи цифровых каналов SDH (E1, STM).

Длительное время было принято передавать данные по телефонной сети "поверх" голоса, в частотном диапазоне голосовой связи (300 Гц - 3400 Гц), с помощью голосовых "модемов" (от слов модулятор-демодулятор). Т.е. данные преобразовывались в звук и воспроизводились в линию, с обратным преобразованием на принимающей стороне. Изначально модемы вообще представляли собой приставку с микрофоном и динамика, на которую "клали" обычную телефонную трубку.

Первым модемом для персональных компьютеров стало устройство компании Hayes Microcomputer Products, которая в 1979 году выпустила Micromodem II для персонального компьютера Apple II. Модем стоил 380 долл. и работал со скоростью 110/300 бит/сек. В 1981 году фирма Hayes выпустила модем Smartmodem 300 бит/сек, система команд которого стала стандартом де-факто.

Следующие 20 лет технологии совершенствовались, но уже в конце 90-х годов был достигнут теоретический предел скорости передачи данных - 56 кбит/сек, протокол V.90. Более в голосовом диапазоне достичь невозможно.

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, так как нужно поставить оборудование уплотнения на каждом узле, и подвести к нему высокоскоростной канал интернет. Но преимущества в скорости оказались слишком велики, и технология начала бурно развиваться.

xDSL

Буквально за несколько лет было разработано несколько десятков видов DSL, отличающихся методами модуляции, используемых для кодирования данных. На сегодня можно выделить следующие основные стандарты:

- ADSL (ADSL2) - 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 многие системы ADSL (особенно ранние версии) при передаче данных имеют большую задержку (до 20 мсек, что почти в 10 раз больше чем у систем SDSL или HDSL).

Известно более десятка разновидностей ADSL - ANSI T1.413-1998 (Issue 2 ADSL), ITU G.992.1 (G.DMT), ITU G.992.2 (G.Lite), ITU G.992.3/4 (ADSL2), ITU G.992.3/4 Annex L (RE-ADSL2), ITU G.992.5 (ADSL2+), ITU G.992.5 Annex L (RE-ADSL2+)... Эта технология - одна из самых технически совершенных в проводной связи, изворотливость инженеров, добивающихся максимальной скорости на сложных линиях, поражает воображение и заслуживает, как минимум, отдельной книги.

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 и 24 Мбит/с для ADSL2+, частоты 138...2208 кГц), чем в противоположном направлении ("восходящий" поток данных от 640 Кбит/с до 1,5 Мбит/с, частоты 26...138 кГц). Наибольшая скорость достигается на расстоянии до 3 км, а максимальное расстояние для устойчивой связи на минимальной скорости около 5-6 км.

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.

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:

[Теория] Частоты ADSL.

Для того, что бы телефон и ADSL не мешали друг другу на одной линии используют сплиттер (POTS Splitter) - пассивное устройство (обычно встроенное в ADSL-модем), 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.

С другой стороны, 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;

Тем не менее, ADSL широко используется телефонными монополистами в качестве недорогой услуги подключения к сети Интернет, поэтому часто у "домашних" и корпоративных 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 часто применяется для связи точка-точка, используемое оборудование обычно одинаково для обеих сторон канала. Но встречаются и варианты модулей для многопортовых DSLAM, специально для организации корпоративных сетей. Из-за в порядке меньшей популярности стоимость устройств SDSL заметно больше, чем ADSL.

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 сплиттеров 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.

VDSL.

Технология VDSL является наиболее современной и "быстрой" технологией xDSL. Скорость передачи данных "нисходящего" потока составляет от 11 до 100 Мбит/с (для VDSL2), (138...3750 5200...8500 кГц), "восходящего" - в пределах от 1,5 до 2,3 Мбит/с (26...138 3750...5200 8500...12000 кГц).

VDSL можно рассматривать как высокоскоростной ADSL, рассчитанный на небольшие расстояния (до 1,0-1,5 км.) и, желательно, новые кабели с хорошими волновыми свойствами. Устройства просты, весьма недороги, и получают последнее время все большее распространение на небольших кампусных сетях. Он позиционируется скорее как удлинитель Ethernet, появляются комбинированные коммутаторы Ethernet - VDSL, в которых последний играет ту же роль, которую обычно предназначали оптоволокну.

Более того, VDSL последнее время часто используют для замены ADSL, для этого с АТС делают "выносы" в микрорайон или даже отдельный многоквартирный дом, и запускают VDSL по старой или вновь построенной телефонной разводке.

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.

В перспективе можно ожидать появление единого стандарта, сочетающего достоинства всех рассмотренных технологий. Предпосылки к этому уже есть сейчас, но все же практическое внедрение - дело будущего.

HomePNA

Если технологии xDSL пришли 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.

[Теория] 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 сплиттером). 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, в том числе "шине" и "дереве" (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. Но при этом была утрачена "топологическая всеядность" - система может работать только как "точка-точка".

Дальнейшее развитие было вполне предсказуемым. Квартирное (по сути) решение попытались использовать операторы "последней мили". Появились многопортовые устройства HomePNA, предназначенные для оказания услуг передачи данных в многоквартирном доме или кампусе, а так же дальнобойные системы (до 1-1,5 км).

Однако, результаты внедрения были весьма неоднозначными. Нестабильная работа устройств и отсутствие методов и способов контроля "убила" немногочисленные попытки внедрения, и на сегодня HomePNA в России практически не используется. Рожденная для среднего американского коттеджа, технология так и не смогла закрепиться в провайдинге.

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, вероятно, 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 превосходили xDSL и HomePNA. В техническом плане Cisco LRE совпадает с VDSL, более того, многие современные VDSL модемы совместимы с устройствами LRE.

- 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). 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.
- Фактическая неработоспособность в многопарных телефонных кабелях.

Все вышеперечисленное привело к фактической стагнации LRE-проекта, 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.

Глава 11 : Беспроводные сети

Шумоподобные сигналы

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.

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 = $1/t_i$, где t_i - 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.

[Теория] 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 обеспечения 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 семейства 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 Ethernet 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 разрабатывались (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	802.11n
Частоты	2,4-2,483 ГГц	2,4-2,483 ГГц	5,15-5,25 ГГц 5,25-5,35 ГГц 5,725-5,850 ГГц	2,4-2,483 ГГц	5 ГГц 2,4 ГГц
Метод передачи	DSSS, FHSS	DSSS	DSSS	DSSS	
Скорость	1,2 Мб/с	1,2, 5,5, 11 Мб/с	6, 9, 12, 18, 24, 36, 48, 54 Мб/с	6, 9, 12, 18, 24, 36, 48, 54 Мб/с	До 248 Мб/с

Метод модуляции	BPSK, QPSK	BPSK, QPSK, CCK	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).

[Теория] 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 линии 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.

Для работы радиоканала кроме качественного активного устройства потребуется пассивная часть - антенна и подводный 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 кабели:

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 радиоэзертнет 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).

[Теория] 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).

[Теория] 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.

Антенна типа двойной биквадрат. Проста в изготовлении. Хорошая диаграмма направленности и усиление которое никто не мерял ввиду кустарности изготовления.

[Теория] Самодельная антенна типа двойной биквадрат.

В заключение можно упомянуть еще один экзотический тип антенн, которые часто используются в кустарных сетях. Это "баночная" антенна.

[Теория] 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.

Глава 12 : 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 непригоден.

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:

[Теория] 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:

[Теория] 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 x 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 SNMP 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 знания 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 для его вхождения в имеющуюся сеть. Однако никто не мешает энтузиастам самостоятельно строить параллельные сети на той же проводке, забирая себе часть полосы пропускания, что неминуемо сказывается и на уже имеющихся сетях, в том числе сети оператора.

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".

Глава 13 : 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. Для управления телевизионными сетями (например, линейными усилителями) требовался обратный канал. И он 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 (если они имеют не модульные дуплексоры в магистральных и домовых усилителях) 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. (дополнительно в квартире абонента устанавливается фильтр обратного канала на отвод к ТВ приемнику, а перед кабель-модемом изолятор земли)

Вполне работоспособная схема, только головная станция для передачи данных не дешевая (\$5000-\$20000), и скорость ограничена несколькими десятками мегабит "на всех" в одном TV канале (правда каналов таких в широкополосной сети несколько десятков) на одном физическом направлении.

Однако, на эту внешне безоблачную картину наложилась Российская реальность.

Сети КТВ появились и выросли очень похоже на современные "домашние" Ethernet-сети, на энтузиазме и небольших деньгах. 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, услуга массово востребованная 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.

Если привечь статистику, то на конец 2006 года можно видеть следующую картину:

СКПТ (системы коллективного приема телевидения, т.е. антенна на подъезд) 40%

КСКПТ (крупные системы приема телевидения) 15%

ГВКС (гибридные волоконно-коаксиальные сети) HFCN (500-3500) 20%

ГВКС (гибридные волоконно-коаксиальные сети) HFCB (50-150) 5%

IPTV 1%

MMDS 5%

Спутниковое TV 1-2%

Эфирные антенны 5%

Очевидно, что использовать сети СКПТ, КСКПТ, просто антенны (а это в сумме 60%) для высокоскоростной передачи данных невозможно без коренной реконструкции, которая может вылиться в полную замену всей головной и магистральной части. Да и ранние гибридные сети способны к существованию на широкополосном рынке с большими оговорками. К счастью, каждые 10-12 лет сети КТВ полностью амортизируются и вынуждены проходить капремонт и реконструкцию с заменой выработавшего ресурс коаксиала и усилителей. Другого способа обеспечить телевидение в каждой квартире пока не существует (если, конечно, не считать IPTV), а усилителей и пассивного оборудования без возможности обратного канала уже просто не производят.

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. Технология действительно не может эффективно использоваться в режиме "группового кабель-модема" со строительством параллельного стояка изернет сети, она успешна только в случае индивидуального кабель-модема у каждого абонента.

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 сногшибательными.

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 вырождаться 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 нужды 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 закрыты.

В заключение, 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 (строго говоря, это просто модификация популярной модели Cisco 7200VXR).

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 одного обратного канала, их на плате от 1го до 8 на каждый нисходящий канал).

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).

Существует обоснованное мнение, что установка группового кабель-модема является существенной ошибкой в проектировании сети, поскольку ведет к необходимости обслуживать оператором КТВ второго подъездного стояка. Так же автоматически пропадает преимущество кабельного модема в технологии деления полосы пропускания и безопасностью по сравнению с изернет сетями.

Строительство слаботочного стояка это неизбежный этап развития сети КТВ, однако оправдано оно только при достижении проникновения услуги передачи данных в конкретном доме до уровня в 20-30%. По времени это совпадает с переходом на оптический домовый усилитель.

В заключение можно сказать, что на практике DOCSIS и Ethernet редко конкурируют, чаще а дополняют друг друга: до 25% проникновения выгоден DOCSIS, выше - Ethernet.

Глава 14 : Экзотические способы передачи данных

Атмосферные лазеры

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.

Можно выделить два типа аппаратуры: с узким лучом (угол излучения 0,5–5 мрад) и с широким (угол излучения 8–12 мрад). Первые можно отнести к дорогим, дальнобойным системам (часто с автоподстройкой луча), вторые - напротив, недорогие, с дальностью работы менее 1 километра.

Как в России, так и зарубежом появились монстрообразные установки с узким лучом, предназначенные для работы на расстояние до нескольких километров с приемлемым уровнем надежности. Как классический пример можно привести серию "МОСТ" государственного Рязанского Приборостроительного Завода.

[Теория] 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 ряд 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 истории использования подобных мощных систем есть отчетливый кризис (в районе 2002 года). Согласно Telford M. Free Space optics takes off (Lightwave Europe. April 2003), сумма продаж аппаратуры в США и Западной Европе в 2000 г. ставила 100 миллионов долларов, и ожидалось что к 2005 г. она увеличится до 200–400 млн. долларов.

Однако, технология оказалась сильно переоцененной. Причин было несколько.

- Технологическая - систем с автоматической подстройкой наведения не было вообще, или они были несовершенны.
- Рекламная. Производители дали много "обещаний" (например, заявляли дальность работы существенно больше реальной).
- Проблемы проектирования. Понятно, что грамотно разместить и эксплуатировать оптические системы было не просто.

Все это вызвало многочисленные отказы, и общее недоверие лазерным линиям связи. Поэтому серьезные, мощные системы использовались (и используются сейчас) в очень узком сегменте рынка, и особого интереса для Ethernet-провайдеров явно не представляют.

Второй волной были любительские системы (понятно, то там использовался "широкий" лу). 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".

[Теория] 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 2004 г. появился новый тип аппаратуры – пассивный приемопередатчик. Из лазерной "головки" убрана вся электроника, по оптическому кабелю подается сигнал (уже модулированный), которое вводится в антенну (систему линз). По сути, если говорить упрощенно, это атмосферный преобразователь на обычный оптоволоконные медиаконвертер. Вся электронная часть такой линии устанавливается в помещении.

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 мало, можно привести примеры: MRV, Англия (Terescope 1, или TS1), НПП «Лазерные технологии», Екатеринбург (ОСС-2005). Кроме этого, ГРПЗ (Рязань) подготовил к производству аппаратуру Artolink-1Гб/с с пассивной оптикой и активным наведением.

[править]

Модификации Ethernet

Следующие устройства передачи данных по сути являются модификацией обычного Ethernet, и предназначены для решения каких-либо узких задач (как правило увеличения дальности работы).

100С5

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 длине (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.

[Теория] 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 вполне 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.

[Теория] Рис. 5.14. Downgrade 10base-TX

На карточке просто перепаяется 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.

[править]

AuDSL

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. ;-)

[править]

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.

[Теория] 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 15 : Место Ethernet в провайдинге

Не важно, как поставлена сеть, важен улов

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.

[Теория]

Сетевой адаптер 10/100 стоимостью \$3. 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).

Еще десять лет назад 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 приоритизации:

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 приоритизацию (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 установленных 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 16 : Сравнение TDM, ATM, и Ethernet

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

[Теория]

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 (потокowego 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 17 : 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 конъюнктуры. 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 отечественные разработки типа Гранчей, экзотические соединения 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, отсекает 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 окончное 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 18 : 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 невероятно 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.

[Теория]

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 Comrex 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 19 : 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.*

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.

Сложно сказать, кто первый объединил технологии этих двух "миров". Скорее всего процесс шел почти незаметно, одновременно в разных местах (и даже разных странах). **Так возник Ethernet-провайдинг - массовое коммерческое оказание телематических услуг с использованием технологии Ethernet.**

Большинство Ethernet-провайдеров (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.

[Теория] 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. Междомовая разводка. Служит для объединения активного оборудования абонентских систем здания в единую инфраструктуру, с последующим присоединением к магистральной сети (или сразу к Интернет).
3. Магистральная сеть. Используется для объединения междомовых сетей.

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

Глава 20 : 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 21 : 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 22 : 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.

[Теория] 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 кабели 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 5е (до 125 МГц), в разработке Категория 6 (до 200 МГц) и Категория 7 (до 600 МГц).

[Теория] 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 кабели имеют изоляцию из вспененного (ячеистого) полиэтилена, которые обеспечивают низкие диэлектрические потери, или тефлона, который обеспечивает уникальный рабочий диапазон температур.

Разрывная нить (обычно капрон) используется для облегчения разделки внешней оболочки - при вытягивании она делает на оболочке продольный разрез, который 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 кабели 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 защита 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 оболочкой, 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 .

[Теория] 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.

[Теория] Рис. 7.7. Частотная зависимость электрических свойств витой пары

На основании перечисленных электрических параметров, может быть рассчитано волновое сопротивление. Сделать это можно по формуле $Z = \sqrt{(R + j\omega L) / (G + j\omega C)}$, которую для высоких частот Ethernet можно упростить до $Z = \sqrt{L/C}$. В рабочем диапазоне кабеля эта величина должна составлять $100 \pm 15\%$ Ом.

Волновое сопротивление хорошо характеризует однородность тракта передачи электромагнитной энергии. Его неоднородности неизбежно вызывают отражения части сигнала, и ухудшение качества линии. Поэтому, 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 рефлектометрии.

Глава 23 : 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, чтобы 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: $X(\text{дБ}) = 20 \cdot \log_{10}(P_1/P_2)$, где P_1 и P_2 - 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.

$$A = 20 \cdot \log_{10} (P_{\text{передатчика}} / P_{\text{приемника}})$$

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

$$\alpha(\text{дБ/метр}) = A(\text{дБ}) / L(\text{м}), \text{ где } L - \text{длина кабеля.}$$

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.

[Теория] 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: $NEXT (FEXT) = 20 \cdot \log_{10} (P_c/P_n)$, где P_c - мощность сигнала, а P_n - 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 параметра, 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:

$NEXT(f) = NEXT(0,772) - 15 \cdot \log_{10}(f/0,772)$, 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 передаче 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.

[Теория] 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 Velocity 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 24 : 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 длины 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.

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 прорежут изоляцию и часть проводника, обеспечивая тем самым электрический контакт.

Для уменьшения разбалансировки, вызванной нарушением скрутки витых пар, разработчики используют конструкцию, позволяющую расплести 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 отдельно.

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.

[Теория] 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.

[Теория] 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.

[Теория] 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.

[Теория] 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 кабели 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.

[Теория] 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 проволокой. 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 25 : Измерение параметров среды передачи

Как уже говорилось выше, для определения качества линий используют величины, измеряемые 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 разрешения 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 сертификации кабельной системы на соответствие определенным классам приложений.

[Теория] 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 С (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 задержка 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.

[Теория] Рис. 7.17. Типовые ошибки при монтаже разъемов

- 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).
- Перестановка пар (Transposed Pairs). Подключение любой из пар к контактам другой пары на противоположной стороне линии. Практически всегда приводит к потере связи (исключение - активное оборудование, имеющее автоопределение перекрещенных линий).
- 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 испытаний).

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 26 : 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. Больше 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 кабели 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 оптоволокон, вполне реальны и лишь слегка экзотичны.

Основными достоинствами оптоволокон является практически неограниченная 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 оптоволокон 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 27 : Конструкция оптических волокон

Основным элементом оптоволоконных кабелей является оптическое волокно (световод), изготовленный из кварцевого стекла. Показатель преломления 1,46, коэффициент теплопроводности 1,4 Вт/мк, плотность 2203 кг/м. По нему можно передавать световые сигналы с длинами волны 0,85-1,6 мкм, что соответствует диапазону частот $(2,3-1,2) \cdot 10^{14}$ Гц. Собственно, именно этот параметр особо привлекателен для высокоскоростной передачи данных.

Действительно, даже использовать одну сотую часть этого диапазона, то через оптоволоконно можно передать до миллиарда телефонных разговоров или сотню тысяч телевизионных каналов.

[править]

Конструкция оптического волокна

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

[Теория]

Конструкция оптического волокна

Сложность конструкции скорее кажущаяся, чем реальная. Внешний диаметр отражающей оболочки (клядинга) унифицирован для всех типов кабелей и составляет 125 ± 2 мкм. В этот размер входит и 2-3 мкм. слой полимерного лака, который служит защитой от влаги и диффузии водорода.

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.

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

[править]

Мультимодовое и Одномодовое волокно

По типу конструкции, вернее по размеру сердцевины, 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.

[Теория]

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, фактически никогда массово

не использовался из-за большой модовой дисперсии (а значит, невозможностью работы на высоких скоростях передачи данных).

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.

Из-за небольшого диаметра сердечника, при использовании одномодового волокна требуется большая точность работ. Как сварка, так и соединение на разъемах требует существенно меньших допусков, чем в случае с многомодовым волокном. Это существенно осложняло работы еще несколько лет назад, поэтому много "старых" сетей сделаны на "мультимоде".

Однако в настоящее время технические проблемы применения одномодового волокна решены окончательно. А так как волокно MM примерно в полтора-два раза дороже, чем SM, по всей вероятности, "мультимод" скоро вообще исчезнет из практики (провайдеры его уже не используют).

Вторым ограничителем использования одномодовых кабелей было дорогое активное оборудование. Еще лет 5-7 назад, стоимость конвертера SM доходила до \$1000. Однако на сегодня ценовое различие уже трудноуловимо, и им можно пренебречь. Более того, массовое применения одноволоконного оборудования (WDM) вообще отбрасывает "мультимод" в разряд ретро-экзотики.

[править]

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.	8-9 мкм	50 или 62,5 мкм
Стоимость волокон и кабелей.	Около 70% от многомодового	-
Средняя стоимость конвертера в витую пару Fast Ethernet.	\$60	\$50

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
Историческая область применения.	телекоммуникации	локальные сети

Глава 28 : 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 кабели (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 кабели 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 достигать до 450м.
- Подводные.

Рассмотрим подробнее конструкцию кабелей. Ее выбор для построения сети "последней мили" достаточно ограничен. Это должны быть недорогие кабели 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, многотрубный кабель).

[Теория] 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 наполнитель (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 прут, 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 оболочку 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°C до +50°C;
- температурный диапазон эксплуатации - от -40°C до +60°C;
- 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 оптоволокон.

Примерно то же самое относится к вариантам кабелей, предназначенных для прокладки внутри помещений, у которых волокно находится внутри монолита из пластика (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-МНП-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 кабели легко крепить даже с помощью подручных материалов.

Глава 29 : Устройство приемопередатчиков

Открытие светодиодов и лазеров

Кроме световодов с малым затуханием для высокоскоростной передачи данных нужны быстродействующие излучатели света. Причем малогабаритные, и с низким энергопотреблением.

Принцип работы таких устройств был открыт в разрушенной гражданской войной России, в 1923 году, Олегом Владимировичем Лосевым. Занимаясь исследованиями кристадина в Нижегородской радиотехнической лаборатории, он обнаружил, что полупроводниковые детекторы при пропускании тока испускают свет. Особенно хорошо явление было заметно в карбиде кремния (SiC, карборунде). Применяя метод шлифов и зондовой микроскопии удалось выяснить, что эффект фотоэлектродвижущую природу и возникает в части активного слоя толщиной 1

Практическая ценность открытия уже тогда была высоко оценена - быстродействующие, не требовавшие вакуума, источники света с низким (около 10 Вольт) напряжением питания были более чем интересны промышленности. В двадцатые годы само явление электролюминесценции называли "светом Лосева" (Losev light, Lossew Licht). За исследование свечения Лосеву (вообще не получившего высшего образования) в 1938 г. без защиты диссертации была присуждена степень кандидата физико-математических наук.

Интересно, что Лосев видел большие перспективы за таким материалом, как кремний. В начале 1941 г. он начал работу по новой теме "Метод электролитных фотосопровитлений, фоточувствительность некоторых сплавов кремния". Результат, к сожалению, неизвестен, так как работа была закончена в блокадном Ленинграде.

Надо сказать, что исследования полупроводников шли в то время очень активно. Например, в 1932 году А.Ф. Иоффе и Я.И. Френкель создали теорию выпрямления тока на контакте металл-полупроводник, основанную на явлении туннелирования. Так же Френкель ввел понятие экситона в полупроводниках. Первая диффузионная теория выпрямляющего p-n-перехода, ставшая основой

теории р-п-перехода В. Шокли, была опубликована Б.И. Давыдовым в 1939 г.

Но только спустя 30 лет после открытия О. Лосева, в 1951 г., К. Lehovec с сотрудниками показал, что детектирование и электролюминесценция имеют единую природу, связанную с поведением носителей тока в р

Так появились и вошли в широкую практику светодиоды (Light Emitting Diodes). По сравнению в нитью накаливания это был огромный прорыв, однако, для нужд связи они были пригодны не более, чем световоды в виде стеклянных трубок. Однако, новый комплекс научных открытий не заставил себя долго ждать, хотя и пришел с совершенно неожиданной стороны - от радиофизиков.

В апреле 1954-го Таунс и Гордон запустили микроволновой квантовый генератор на парах аммиака, мазер (MASER – Microwave Amplification by Stimulated Emission of Radiation). В 1954 году, вскоре после выхода работы Таунса, Гордона и Цайгера, Прохоров и Басов опубликовали статью, где были приведены теоретические обоснования работы этого прибора (в 1964 году Таунс, Басов и Прохоров за эти исследования были удостоены Нобелевской премии).

"Перенести" открытие в оптическую среду первым решился американский физик Роберт Дике, который в мае 1956 года оформил соответствующую патентную заявку. Термин "Лазер" (Light Amplification by Stimulated Emission of Radiation) придумал аспирант Колумбийского университета Гордон Гулд. Принципиальным отличием лазеров от любых других источников света, представляющих собой по сути источники оптического шума, является высокая степень когерентности излучения, а так же направленность, низкий уровень шумов, концентрации энергии во времени и т.д.

Далее открытый принцип был применен практически для всех типов сред. Твердотельный рубиновый лазер запустил в 1960 Теодор Мейман в корпорации Hughes Aircraft. В 1961 году появился лазер на неодимовом стекле, затем в течение нескольких лет были разработаны полупроводниковые лазерные диоды, лазеры на органических красителях, химические лазеры, лазеры на двуокиси углерода.

[править]

История создания полупроводникового лазера

Развитие полупроводниковой электроники взяло старт в начале 50-х, и к 60-м оно уже превратилось в мощную отрасль, работающую, как правило, на практические заказы (в том числе военного назначения). Так, германиевые вентили, разработанные Ж.И.Алфёровым, уже в октябре 1958 г. устройства стояли на подводной лодке (а ученый, тогда еще младший научный сотрудник, получил первый орден).

Магистральным направлением было исследование монокристаллических структур на основе германия, кремния, полупроводниковых соединений типа $A^{III}B^V$ (элементов III и V групп таблицы Менделеева). Совершенствовались методы формирования р-п-переходов, замена германия кремнием позволила поднять рабочую температуру приборов и создать высоковольтные диоды и тиристоры. Работа с арсенидом галлия привела к созданию полупроводниковых лазеров, светодиодов и фотоэлементов. Электровакуумные лампы мгновенно остались в прошлом.

Но ситуация с мощным быстродействующим источником излучения оставалась не решенной. Даже наиболее подходящие по параметрам, лазеры на гомопереходах (т.е. материал был одинаков, менялся лишь тип проводимости) арсенида галлия (GaAs) имели столь высокие пороговые и рабочие токи (порядка 50 000 А/см²), и практически не могли успешно работать при комнатной температуре. Их быстродействие то же оставляло желать лучшего.

Следующий прорыв, так необходимый для оптоволоконных технологий, был сделан в 1963 году, когда Жорес Алфёров при защите кандидатской диссертации сделал вывод, что р-п-переход в гомогенном по составу полупроводнике не может обеспечить оптимальные параметры многих приборов, и выдвинул идею использования гетероструктур. Предсказывалась, что такие лазеры могут обеспечить "непрерывный режим генерации при высоких температурах", или, говоря упрощенно, работать на несколько порядков эффективнее.

Однако, после этого долгое время теория заметно опережала практику. Более того, существовал всеобщий скептицизм по поводу создания "идеального" гетероперехода. Многочисленные попытки его реализации оканчивались неудачей - материалы должны были иметь близкие тепловые, электрические, кристаллохимические свойства, а так же иметь одинаковые размеры ячеек кристаллических решёток. Неудивительно, что такую гетеропару найти не удавалось.

Нужный гетеропереход можно было формировать путём эпитаксиального выращивания, когда пленка одного монокристалла наращивалась на поверхности другого монокристалла послойно. Для

идеального гетероперехода хорошо подходили арсенид галлия (GaAs) и арсенид алюминия (AlAs), но последний мгновенно окислялся на воздухе, и его использование было очень трудной задачей.

Первоначально Ж.И.Алфёровым была предпринята попытка создать двойную гетероструктуру $\text{GaP}_{0,15}\text{As}_{0,85}\text{-GaAs}$. И она была выращена методом газовой эпитаксии, а на ней был сформирован лазер. Однако из-за небольшого несоответствия постоянных решётки он, как и лазеры на гомопереходах, мог работать только при температуре жидкого азота. Ж.И.Алфёрову стало ясно, что таким путём реализовать потенциальные преимущества двойных гетероструктур не удастся.

Помог случай - Дмитрий Третьяков (работавший с Жоресом Алфёровым) обратил внимание, что неустойчивый арсенид алюминия абсолютно стабилен в тройном соединении AlGaAs (так называемом твёрдом растворе). Так примерно в 1967 г. была найдена классическая гетеропара GaAs-AlGaAs. Накал работ по этой тематике хорошо иллюстрирует тот факт, что почти одновременно, с отставанием всего на месяц, гетероструктура $\text{Al}_x\text{Ga}_{1-x}\text{As-GaAs}$ была независимо получена в США сотрудниками фирмы IBM.

Первый в мире гетеролазер заработал в 1968 году, произошло это на Физтехе. Это было низкопороговое, работающее при комнатной температуре устройство. Доклад Ж.И.Алфёрова по этой теме на Международной конференции по люминесценции в Ньюарке (США) в августе 1969 г., произвёл огромное впечатление на коллег (в первую очередь американских).

[Теория] *Схема первого полупроводникового гетеролазера.*

В этом же году началось негласное соревнование с лабораториями Bell Telephone, IBM и RCA. Однако и в достижении непрерывного режима работы при комнатной температуре (использовалась фотолитография, лазеры устанавливались на медных теплоотводах, покрытых серебром) первыми были Ж.И.Алфёров с сотрудниками (1970 год), опередив на месяц группу М.Паниша из Bell Telephone.

Пороговые плотности тока уменьшились (по сравнению с гомогенной структурой) на два порядка, т. е. до $500\text{-}1000\text{ А/см}^2$. В результате удалось получить компактные лазеры, работающие в непрерывном режиме с высокой яркостью и выходной мощностью, которая могла быть непосредственно, с того же полупроводникового элемента (!), промодулирована с частотой до сотен и тысяч мегагерц.

Далее в процесс включились технологи, инженеры и коммерсанты. В 1975 году появился первый коммерческий полупроводниковый лазер, работающий при комнатной температуре, через год построена первая оптическая линия в Атланте; а срок службы лазеров увеличен до 100000 часов (10 лет). Уже в 1977 году срок службы лазеров был увеличен до 1 млн. часов (100 лет).

[править]

Светодиоды (Light-Emitting Diode, LED)

Светодиодом, или излучающим диодом, называют полупроводниковый прибор (p-n переход), излучающий кванты света при протекании через него прямого тока.

Принцип работы светодиода основан на излучательной рекомбинации носителей заряда в активной области гетерогенной структуры при пропускании через нее тока. Носители заряда (электроны и дырки) проникают в активный слой из прилегающих пассивных слоев (p- и n-слоя) вследствие подачи напряжения на p-n структуру, и затем испытывают спонтанную рекомбинацию, сопровождающуюся излучением света.

[Теория] *Принцип действия светодиода*

В оптических линиях связи применяются инфракрасные светодиоды, в основном на основе GaAs. Он обладает высокой эффективностью электролюминесценции, и хорошо технологически освоен. По сравнению с полупроводниковыми лазерами, светодиоды имеют большую спектральную ширину излучения, типичное значение которой составляет 20-50 нм, против 1-4 нм у лазеров. Но этот недостаток компенсируется их невысокой стоимостью.

Различают два основных типа светодиодов, применяемых в оптоволоконных системах: светодиоды с излучающей поверхностью, и с излучающей гранью (поверхностные и торцевые).

[Теория][Теория] *Виды светодиодов*

Вывод излучения в светодиодах поверхностного типа на GaAs осуществляют через круглое отверстие, вытравленное в обложке. Такую конструкцию светодиода называют диодом Баррасса. Известны также конструкции поверхностных светодиодов с выводом излучения непосредственно через подложку (на четырехкомпонентном соединении GaInAsP , подложка из InP является прозрачным окном).

В торцевых светодиодах вывод излучения активного слоя осуществляют с торца, как и в "классических" лазерных диодах. Благодаря полному внутреннему отражению оптическое излучение распространяется вдоль перехода. С помощью полосковой конструкции нижнего омического контакта, ограничения активной области, можно избежать лазерной генерации.

Передачики на основе светодиодов используются преимущественно в мультимодовых низкоскоростных системах, и на небольшие расстояния. Основными недостатками светодиодов являются малая скорость (**менее 200 МГц**), малая выходная мощность, широкая полоса спектра и большая расходимость излучения. Поэтому в одномодовых сетях они практически полностью вытеснены лазерными диодами.

[править]

Полупроводниковые лазеры (Laser Diode, LD)

По сравнению с обычными "большими" лазерами, полупроводниковые имеют целый ряд существенных отличий:

- Квантовые переходы в полупроводниковых лазерах обусловлены зонной структурой материала.
- Имеют очень малые размеры (~0,1 мм в длину), и еще меньшую активную область (~1 мкм и меньше), поэтому расхождение луча значительно больше, чем у обычного лазера.
- Пространственные и спектральные характеристики излучения полупроводникового лазера сильно зависят от свойств материала, из которого сделан переход (структура запрещенной зоны и коэффициент преломления).
- Лазерное излучение возникает непосредственно под действием тока, протекающего через прямосмещенный диод. В результате получается чрезвычайно эффективная система, поскольку **модуляция излучения происходит за счет модуляции тока**.

Принципиальным отличием лазерного диода (LD) является наличие встроенного оптического резонатора, что позволяет получить режим индуцированного излучения, которое характеризуется высокой степенью когерентности.

Энергетическая зонная диаграмма лазера в присутствии внешнего напряжения U:

[Теория][Теория] *Энергетическая зонная диаграмма лазера*

Лазерный эффект достигается при определённых пороговых значениях тока через переход. Начиная с этих значений тока спектральная полоса излучения значительно сужается. Для уменьшения рабочих токов и ослабления нагрева активный слой часто сокращают до полоски шириной 5-20 мкм, идущей от одной отражающей поверхности до другой (отсюда происходит часто встречающееся название "полосковые" лазеры). Этого достигают применением узкого металлического электрода (верхнего на рисунке). У подобных устройств снижается как пороговый ток (примерно до 100 мА при комнатной температуре), так и инерционность вследствие уменьшения ёмкости переходов.

Мощность излучения лазеров, работающих в непрерывном режиме, составляет около 0.1 Вт. В случае импульсного возбуждения мощность может быть значительно повышена, т.к. нагрев будет ослаблен. КПД инжекционных лазеров достигает 50%, инерционность составляет 1 - 10⁻⁹ с, напряжение питания не превышает 3В, а размеры нескольких миллиметров. Модуляция светового тока может осуществляться изменением напряжения (тока).

Наиболее часто в качестве оптического резонатора используют следующие системы:

1. Лазер с резонатором Фабри-Перо (FP лазер), Fabry-Perot laser (FP laser). Имеет в качестве резонатора два плоских зеркала и допускающий как одномодовый, так и многомодовый режим излучения.

[Теория] *Лазер с резонатором Фабри-Перо*

Используется в системах связи со скоростью менее 2,5 Гбит/с. Далее большую роль начинают играть динамические свойства лазерных диодов, которые проявляются в зависимости спектральной характеристики от скорости передачи при непосредственной модуляции мощности излучения путем изменения тока накачки. У одномодового лазерного диода с резонатором Фабри - Перо увеличение скорости передачи сопровождается изменением модового состава, что характеризуется динамическим расширением спектра до 10 нм при модуляции с частотой порядка 1-2 ГГц

2. Лазер с распределенной обратной связью (РОС-резонатор), Distributed feedback laser (DFB laser), образуется путем периодической пространственной модуляции параметров структуры, влияющих на условия распространения излучения. Как правило, работает на длине волны 1550 нм. Доступен стандарт CWDM с шагом 20 нм в диапазоне длин от 1310 до 1610 нм.

[Теория] *Лазер с распределенной обратной связью*

Используются преимущественно при скоростях передачи информации более 2,5 Гбит/с (и даже более 10 Гбит/с). При модуляции в диапазоне 0,25-2 ГГц имеет место лишь незначительный сдвиг (порядка 0,2 нм) при сохранении высокой степени подавления побочных мод. Поэтому эти лазерные диоды часто называют динамически одномодовыми.

3. Инжекционный лазерный диод с отражательной брэгговской решеткой, (РБО-резонатор), Distributed Bragg Reflector. По сути это разновидность лазера с распределенной обратной связью.

[Теория] *Инжекционный лазерный диод с отражательной брэгговской решеткой*

Минимальная ширина спектра достигается в лазерных диодах с внешними резонаторами, у которых она в зависимости от типа резонатора лежит в пределах 1...1500 кГц.

4. Лазеры с вертикальным объемным резонатором, (VCSEL лазер), Vertical Cavity Surface Emitting Laser (VCSEL laser). Как правило, работает на длине волны 850 нм.

[Теория] *Лазер с вертикальным объемным резонатором*

По сравнению с поперечными излучателями лазеры VCSEL имеют ряд преимуществ – они гораздо проще в изготовлении, так как допускают массовую обработку множества элементов на одной подложке, и потребляют меньше энергии. Кроме этого, они допускают высокоскоростную модуляцию, благодаря чему позволяют генерировать сигналы со скоростью 1 Gbps и более.

Доступные сегодня VCSEL изготавливаются из арсенида галлия (GaAs) и излучают свет в диапазоне от 750 до 1000 нм. Длины волн этого диапазона слишком коротки, чтобы передавать сигналы на большие расстояния, поэтому VCSEL применяются на мультимодовых кабелях (которые последнее время не слишком популярны).

[править]

Способы модуляции

В работе полупроводниковых лазеров (и светодиодов) возможны два вида модуляции: внутренняя (непосредственная) и внешняя. При внутренней модуляции электрический сигнал непосредственно воздействует на излучение источника, обеспечивая соответствующую выходную мощность и форму сигнала. Практически все системы на частотах до 1 ГГц используют этот способ, но при больших скоростях начинаются трудности - низкий уровень выходной мощности, невысокая скорость модуляции, значительные нелинейные эффекты. При внешней модуляции используется специальное модулирующее устройство, с помощью которого осуществляется воздействие на лазер, излучающий в непрерывном режиме. Эта технология используется для высокоскоростных передатчиков.

Для внешней модуляции используется (в основном) два типа устройств: интерферометры Маха-Цендера (MZI) и электроабсорбционные (EA).

Принцип действия MZI основан на электрооптическом эффекте, суть которого заключается в изменении показателя преломления под воздействием прикладываемого к материалу электрического поля – уменьшение n повышает скорость распространения света, а увеличение – снижает (фазосдвигающая схема на базе МОП-конденсатора).

[Теория] *интерферометр Маха-Цендера*

Свет в модуляторе расщепляется в двух волноводах в кристалле ниобата лития (LiNbO₃). Если необходимо послать единицу, то напряжение, прикладываемое к обоим из них, должно быть одинаковым, если ноль, – то оно прикладывается таким образом, чтобы получить смещение фаз на 180° и, соответственно, взаимное вычитание сигналов в выходном канале, объединяющем оба луча.

Устройства могут работать на частотах 20 ГГц и более, и достаточно популярны (серийно изготавливаются, например, фирмами Ramar и Laser2000)

Следующий распространенный способ - EA-модуляторы. Они базируются на эффекте сдвига запрещенной зоны в полупроводнике, который появляется в результате прикладываемого напряжения, что приводит к поглощению генерируемого лазером излучения.

Они изготавливаются из сложных полупроводников с множеством квантовых ям, где используется локализованный эффект Штарка (расщепление спектральных линий атома под действием внешнего электрического поля) или эффект электроабсорбции. Преимущество этого вида устройства в высоком быстродействии (до 40 ГГц), а так же хорошей интеграцией с лазерными диодами на фосфиде индия.

Описанные варианты модуляции не единственные, разработано много других способов управления

световым потоком. Как пример, можно привести модулятор на эффекте Поккельса, который проявляется во вращении плоскости поляризации входной световой волны при приложении напряжения. Для некоторых кристаллов (например, ниобата лития) этот поворот может достигать 90 градусов. Если поместить такой кристалл (называемый ячейкой Поккельса - ЯП) между двумя поляризационными фильтрами получится модулятор.

Ячейка Поккельса позволяет модулировать световую волну по интенсивности путем амплитудной модуляции напряжения. Частота может превышать 10 ГГц, глубина модуляции достигает 99,9%.

[править]

Оптические усилители

Оптическим усилителем (Optical amplifier) называется устройство, которое усиливает оптический сигнал прямо, без преобразования его в электрический сигнал, усиления последнего и обратного преобразования в оптический.

Полупроводниковые оптические усилители основаны на использовании возбуждаемой эмиссии, возникающей благодаря взаимодействию фотонов входного возбуждающего излучения с электронами на возбужденном уровне в зоне проводимости.

Входной сигнал служит таким источником возбуждения, энергия которого должна быть достаточна, чтобы сбросить электроны с верхнего уровня на нижний, где электрон и дырка рекомбинируют, вызывая появление вторичных фотонов. Инверсия же электронов создается за счет накачки (ввода тока в полупроводник).

Самый простой вариант базируется на той же технологии, что и лазерные диоды Фабри-Перо, которые представляют собой пару параллельных полупрозрачных зеркал, закрепляемых на входе и выходе усилителя, между которыми в процессе многократного отражения оптической волны и происходит усиление интенсивности оптического сигнала (за счет преобразования энергии накачки в энергию сигнала).

Реализуемые коэффициенты усиления составляют -22-25 дБ. Максимум коэффициента усиления зависит от величины тока через полупроводник и лежит в диапазоне 1520 - 1460 нм, смещаясь в сторону меньших длин волн при большей величине тока.

Устройства используются:

- Как усилители в качестве предусилителей перед детектированием оптического сигнала, а также для компенсации распределенных потерь в линии, позволяющих увеличить длину регенерационного участка.
- Как компенсаторы дисперсии в оптоволокне, учитывая, что они вызывают увеличение крутизны переднего и уменьшение крутизны заднего фронтов импульсов, т.е. фактически к изменению знака дисперсии.
- в качестве оптических коммутаторов для разделения по длинам волн.
- Намного большее распространение в коммуникационных системах получили усилители на легированных редкоземельными элементами оптических волокнах, основывающиеся на эффекте Рамана (комбинационного рассеяния света).

Для этого используются:

- неодим (Nd) и празеодим (Pr) - для усиления сигналов в окне 1300 нм
- эрбий (Er) - для усиления сигналов в окне 1550 нм
- иттербий (Yb), применяемый совместно с Er для расширения спектра поглощения в области 700-1100 нм, что позволяет использовать новые более мощные источники накачки.

[Теория]

Упрощенный принцип действия оптического усилителя

Редкоземельный элемент добавляют в незначительных количествах в центральный световод на небольшой длине волокна (несколько метров). В оптоволокно лазером накачки вводится световой пучок с несколько меньшей длиной волны (нужно избежать интерференции).

Во время прохождения по легированному участку ослабленного сигнала, в результате взаимодействия с квантами светового пучка накачки, электроны в ионах редкоземельных элементов

переходят на более высокий квазистационарный энергетический уровень. Возникает индуцированное излучение с равной или очень близкой длиной волны.

Оптический усилитель на оптоволокне, легированном неодимом ОУЛН (NDFA), работает на длине волны порядка 1340 нм и может быть использован для получения существенного усиления на рабочей длине волны систем связи 1310 нм только в лабораторных условиях. Более удачным в этом плане можно считать празеодим. Основными особенностями усилителей этого диапазона является то, что материалом для легирования обычно является флюоритовое, а не кварцевое стекло, а также низкая эффективность накачки (не выше 4 дБм/мВт). Опытные результаты дают усиление около 34 дБм при мощности насыщения порядка 200 мВт.

Широкое распространение получили усилители на оптоволокне, легированном эрбием. Ионы эрбия имеют пики поглощения в районе длин волн 980 и 1480 нм. Из этого следует, что источником накачки могут служить известные типы лазеров с длинами волн 797/800, 980 и 1480 нм. Из них лазеры на 800 и 980 нм соответствуют трехуровневой модели взаимодействия, а на 1480 нм - двухуровневой модели, причем более эффективно использовать лазер на 980 нм, учитывая их возможность (благодаря трехуровневой модели взаимодействия) реализовать очень низкий уровень шумов (порядка 3-5 дБ).

Однако лазеры на 1480 нм, хотя и являются менее эффективными (70% от эффективности лазеров на 980 нм), считаются более предпочтительными (как более надежные), позволяющими вместе с тем реализовать достаточно низкий уровень шума (порядка 5 дБ).

При использовании иттербия в качестве дополнительного легирующего элемента, можно воспользоваться лазерными диодами накачки, работающими на длине волны 1053 нм (так называемые DPSS-лазеры). Это позволяет получить более мощный источник накачки, что повышает усиление или увеличивает срок службы.

В зависимости от применения различают:

- *Предварительные усилители (предусилители)* устанавливаются непосредственно перед приемником регенератора и способствуют увеличению отношения сигнал/шум на выходе электронного каскада усиления в оптоэлектронном приемнике. Оптические предусилители часто используются в качестве замены сложных и обычно дорогих когерентных оптических приемников.
- *Линейные усилители* устанавливаются в промежуточных точках протяженных линий связи между регенераторами или на выходе оптических разветвителей с целью компенсации ослабления сигнала, которое происходит из-за затухания в оптическом волокне или из-за разветвления в оптических разветвителях, ответвителях, мультиплексорах WDM. Линейные усилители заменяют оптоэлектронные повторители и регенераторы в тех случаях, когда нет необходимости в точном восстановлении сигнала.
- *Усилители мощности (бустеры)* устанавливаются непосредственно после лазерных передатчиков и предназначены для дополнительного усиления сигнала до уровня, который не может быть достигнут на основ лазерного диода. Бустеры могут также устанавливаться перед оптическим разветвителем, например при передаче нисходящего трафика в гибридных волоконно-коаксиальных архитектурах кабельного телевидения.

[править]

Детекторы света

Функции фотодетекторов заключаются в преобразовании оптического сигнала в электрический. Обычно это фотодиоды на базе p-i-n перехода или лавинного эффекта.

Для работы фотодиода p-i-n между слоями с n- и p- проводимостью создается слой с собственной проводимостью (intrinsic area). При подаче обратного напряжения смещения он обедняется свободными носителями, и создаются два перехода: типа p-i и типа n-i. При поглощении света в этом слое образуются носители, которые затем ускоряются посредством сильного электрического поля. Такие приборы имеют хорошие частотные характеристики (граничная частота – около 10 ГГц).

В лавинном фотодиоде физические процессы отличаются дополнительным лавинным размножением носителей. В результате ток во внешней цепи фотодиода существенно увеличивается.

Схема сечения фотодетектора на световодах из SiGe (слой расположен на вершине кремниевого напыла световода).

[Теория] *Схема сечения фотодетектора*

Спектральный диапазон фотоприемника определяется материалом. Например, кремний и арсенид галлия подходят для волн 400–1100 нм. Однако для волн, применяемых в оптоволоконных устройствах (850, 1310 и 1550 нм) кремний является прозрачным, т.е. плохим детектором. Поэтому самым распространенным материалом является германий.

Ключевыми параметрами фотодиодов являются время отклика, линейность, уровень шумов и чувствительность.

Глава 30 : 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 высококвалифицированного 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.

[Теория] Рис. 8.5. Принцип сварки оптического волокна.

Такое соединение надежно, долговечно, и вносит ничтожно малое затухание в оптический тракт. Но для сварки нужна 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 - пороссячий 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 фиксации 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 всех вариантов конструкций проста и достаточно очевидна. Необходимо точно совместить оси волокон, и плотно прижать их торцы друг к другу (создать контакт).

[Теория] 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).

[Теория] 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.
[Теория]

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. При использовании двухволоконных SFP используется только LC, так как 2xSC в SFP просто не разместить.
[Теория]

Глава 31 : Спектральное уплотнение каналов (WDM, CWDM, DWDM)

Технологии (де)мультиплексирования

До 1996-1998 годов для мультиплексирования использовалась дискретная оптика. Но с ее помощью не удавалось добиться шага каналов менее 20 нм, и потерь менее 2-4 дБ. Это уже позволяло использовать около четырех каналов (в окне прозрачности оптических волокон того времени), но для массового "прорыва" возможностей не было.

Но в конце 20-го века прошел переход к интегральным оптическим технологиям, кроме того удалось существенно улучшить качество изготовления элементов традиционной дискретной оптики.

В настоящее время используются следующие технологии.

- На основе интегральной оптики, выделение несущих с использованием дифракционной решетки на массиве волноводов – AWG (Arrayed Waveguide Grating)

Представляет собой дифракционную решетку на поверхности или в объеме оптического планарного оптического волновода. Основан на возникновении разности фаз для различных длин волн сигнала на входе и выходе.

[Теория] *Принцип работы дифракционной решетки на массиве волноводов*

Приходящий сигнал проходит через волновод-пластину и распределяется по множеству волноводов, фактически представляющих собой дифракционную структуру AWG (arrayed waveguide grating). При этом в каждом волноводе по-прежнему присутствуют все длины волн, т.е. сигнал остается мультиплексным, только распараллеленным.

Так как длины волноводов отличаются друг от друга на фиксированную величину, потоки проходят разный по длине путь. Физически это практически не отличается от обычной дифракционной решетки (что и дало название технологии). В итоге световые потоки собираются в волноводе-пластине, где происходит их фокусировка, и создаются пространственно разнесенные максимумы, под которые и рассчитываются выходные полюса. Мультиплексирование происходит обратным путем.

Размер элемента порядка 0,2-0,5 мм, волноводы реализуются в виде планарных оптоволоконных световодов (диоксид кремния, легированный Ge или Ta), сформированных на общей подложке. Для сокращения размеров мультиплексора вдвое и экономии компонентов можно "разрезать" схему пополам, и поместить в плоскости разреза зеркало (схема Литтроу).

Так как эта технология хорошо масштабируется (т.е. можно работать с сотнями каналов), она основным используется для DWDM. Основной недостаток - высокий температурный коэффициент (0,01 нм/°C), что требует использования стабилизаторов температуры.

- На основе явления угловой дисперсии, с использованием вогнутой дифракционной решетки – CG (Concave Grating). Эта классическая схема самофокусировки хорошо известна, и применялась еще в "астрономические" времена.

[Теория] *Принцип работы вогнутой дифракционной решетки*

Поток из входного волокна попадает на вогнутую в одной плоскости дифракционную решетку, и, отражаясь от нее, фокусируется в определенных точках, в которых располагают приемные порты волокон.

Вогнутая дифракционная решетка весьма трудоемка в изготовлении, поэтому 3-D Optics используется значительно чаще.

- Модификация предыдущего метода, на основе технологии трехмерного оптического мультиплексирования – 3DO (3-D Optics WDM). Использует для коллимирования и самофокусировки вогнутое зеркало и плоскую дифракционную решетку.

[Теория] *Принцип работы 3-D Optics WDM*

Мультиплексированный поток из входного волокна отражается от вогнутого зеркала и падает на плоскую дифракционную решетку, отражающую под разными углами свет разной длины волны. Эти дифрагированные лучи, в свою очередь, отражаясь от зеркала, фокусируются в определенных точках, где должны быть расположены приемные порты массива выходных волокон.

Все элементы конструкции собраны в монолитном кварцевом блоке, что позволяет получать высокоточную и надежную конструкцию.

- Традиционная дискретная оптика, на многослойных диэлектрических тонких пленках (DTF).

Фильтр состоит из нескольких последовательно нанесенных слоев прозрачного диэлектрического материала с различными показателями преломления. На каждой границе раздела часть падающего светового пучка отражается обратно, и за счет интерференции, в зависимости от длины волны, усиливает или ослабляет падающий поток.

В результате можно получить фильтр, который будет пропускать любой заданный диапазон, и отражать все остальные.

[Теория] *Принцип работы тонкопленочных фильтров*

Для обработки многоволновых сигналов можно использовать многоступенчатые системы фильтров, в которых свет, отраженный от каждого фильтра, попадает на вход следующего... Но при этом неизбежно большое затухание, и в настоящее время такие системы на практике по сути не используются.

Прочие технологии, не нашедшие широкого применения.

- Волоконные брэгговские решетки (FBG). Волокно, легированное германием, может изменять показатель преломления под действием ультрафиолета, что дает возможность создать в нем пространственную периодическую структуру, похожую по свойствам на дифракционную решетку.

Такое волокно будет работать как фильтр, отражающий одну длину волны, и пропускающий все остальные. В настоящее время эта технология часто используется для компенсации хроматической дисперсии.

- Сварные биконические разветвители FBT (Fused Biconic Tapered). Представляют собой два сваренных друг с другом на определенной длине одномодовых оптических волокна. Если расположить два таких соединения последовательно, комбинация действует подобно интерферометру Маха-Цендера. И при подборе параметров можно получить, что волны разной длины будут в разных волокнах. Метод хорош малыми потерями, но сложен и немасштабируем.

Сравнение основных технологий мультиплексирования:

Технология	I/O AWG	I/O CG	3-D Optics WDM
Максимальное число каналов	32	78	262
Разнос каналов [нм]	0,1 – 15	1 – 4	0,4 – 250
Вносимые потери [дБ]	6 – 8	10 – 16	2 – 6

Переходное затухание [дБ]	-5 – -29	-7 – -30	-30 – -55
Чувствительность к поляризации, %	2	2 – 50	0

Технология 3-D Optics WDM имеет преимущество по четырем из пяти параметров и может быть использована в системах WDM до уровня HDWDM с разносом каналов не меньше 0,4 нм.

[править]

WDM (Bi-Directional)

Для первых вариантов мультиплексирования применялись две стандартные длины волны 1310 нм и 1550 нм. Большое "расстояние" (240 нм) позволяет реализацию без каких-либо специальных фильтров. Поэтому смысл данной технологии весьма прост - для создания канала в классическом решении используется два волокна (к одному подключен излучатель, а другому - приемник, в противоположной стороны линии - наоборот). В схеме WDM (Bi-Directional) - достаточно одного волокна.

[Теория] *Схема Bi-Directional*

Принцип работы Bi-Di легко понять из схемы. Передача проходит через полупрозрачное зеркало-отражатель, обратный сигнал отражается на приемник. При этом из-за разной длины волны не происходит "засветки" приемника отражениями передачи (которая бы неизбежно возникла при работе на одной длине волны).

В реальности это выглядит следующим образом:

[Теория] *Bi-Directional приемопередатчик*

"Уплотнение" в два раза явно недостаточно для магистральных линий, но на уровне локальных корпоративных и операторских сетей это давало быстрый и явный выигрыш. Так что недорогой WDM в настоящий момент (по крайней мере в ISP) практически полностью вытеснил традиционные, двухволоконные решения.

Внешний вид модулей Gigabit SFP WDM:

[Теория] *Модуль SFP WDM*

Приемник и передатчик смонтированы в одном моноблочном модуле. Но передатчик находится по оси устройства, а приемник - сбоку.

Так как это произошло в последние несколько лет (до этого WDM был слишком дорог), в большинстве учебников и пособий эта технология просто не упоминается. Однако, **использовать при строительстве сети старые двухволоконные решения - совершенно недопустимо.**

[править]

CWDM

Грубые WDM (Coarse WDM — CWDM) — системы с частотным разносом каналов не менее 200 ГГц (20 нм). При этом демультиплексирование (разделение) несущих не составляет проблем при использовании даже традиционных методов оптической фильтрации, например многослойных фильтров на тонких пленках.

Расстояние между длинами волн в системах CWDM недавно было стандартизировано ITU (Международный телекоммуникационный союз). Новый стандарт ITU G.694.2 определяет интервал между каналами в 20 нм в диапазоне от 1270 до 1610 нм.

[Теория] *Длины волн CWDM*

Изначально CWDM разрабатывался для магистрального сегмента, но несовместимость с оптическими усилителями и разработка стандарта DWDM (который лишен этого недостатка) поставили крест на этом направлении развития. Однако, сегодня CWDM весьма интересен для Ethernet-провайдеров.

Для начала, возьмем хрестоматийную схему применения:

[Теория] *Транк*

Отличительные «черты»: два волокна, узкий (из-за гидроксильного пика старых типов волокон) диапазон из 8-ми длин волн (с 1470 до 1610, через каждые 20 нм), транковая архитектура,

ориентированная лишь на повышение пропускной способности между двумя узлами локальной сети.

Однако, эти «фамильные» недостатки — давно пройденный этап. К сожалению, большинство провайдеров не следит за темой, считая ее малоприменимой к суровым реалиям отечественного Ethernet-провайдинга. Зря.

Во-первых, относительно новый стандарт ITU G.694.2 определяет диапазон от 1270 до 1610 нм, что дает целых 18 длин волн. Использовать его можно только на оптике без гидроксильных потерь, но сегодня других волокон просто не делают.

Во-вторых, два волокна на CWDM давно в прошлом, одноволоконные решения (с расстоянием между лямбдами в 60 нм) вполне доступны. Важный момент - для bi-di систем используются обычные двухволоконные SFP или GBIC, разделение происходит в одноволоконных MUX/DeMUX. Причем «цветной» SFP стоит около \$120-130. Примечание. Иногда в продаже встречаются одноволоконные SFP CWDM. Эта экзотика используется как решение точка-точка, и в рассматриваемых системах мультиплексирования неприменима.

И в-третьих (и это главное), архитектурные варианты построения сетей CWDM куда разнообразнее привычного представления:

[Теория] *Звезда*

Знакомая картина? Соблазнительно полностью «выкинуть» активный уровень агрегации из сети, т.е. пустить отдельную лямбду до каждого дома. С одной стороны, это дороговато, с другой — защищенный ящик и бесперебойное питание порой просто негде размещать. А MUX/DeMUX прекрасно влезут даже в муфту на столбе освещения.

[Теория] *Цепочка*

Устройство, позволяющее «вытаскивать» нужную длину волны в любой точке, называется OADM (optical add-drop multiplexer). Оно позволяет буквально «кроить» лямбды вдоль и поперек. Например, можно легко исключить «цепочки» на активном оборудовании, что резко повысит пропускную способность и полностью снимет зависимость от электропитания.

Учитывая, что потери на ввод (вывод) лямбды на OADM составляют около 1,1-1,2 Дб, а на «проход» - 1,5Дб, таких устройств на одном волокне может быть много (в разумных пределах, конечно) без особого ущерба для оптического бюджета.

[Теория] *Кольцо*

Частный случай — транковая линия, с разрывом одной из лямбд на активное оборудование. Так можно, при желании, сделать кольцо не по физической линии, а для одной длины волны. Хотя сложно представить реальную ситуацию, где это может быть необходимо, схема хорошо показывает, что с CWDM можно работать практически также, как с обычными физическими волокнами. Было бы только желание (и деньги) это делать.

Рассмотрим экономику. MUX/DeMUX на 8 одноволоконных каналов стоит менее \$1400, или \$175 на лямбду. OADM - \$350. Если брать в миниатюрных коробочках, а не полноразмерном 19-ти дюймовом конструктиве - практически вдвое дешевле. Цветные модули SFP/GBIC дороже привычного одноволоконного всего-то на \$100 (за пару). Итого, удорожание волнового уплотнения по сравнению с прямым волокном составит около \$400-600.

С другой стороны, километр «лишнего» волокна в кабеле стоит не более \$50, и то, если учесть лишние сплайс-пластины в муфтах, патчкорды, разъемы, работу по сварке, и прочее.

Таким образом, при строительстве новой сети CWDM оправдан на пролетах не менее 10 километров. На меньших расстояниях дешевле взять кабель с большим числом волокон. Для внутриквартальной разводки такие расстояния — большая редкость, но уже на уровне городской инфраструктуры — весьма обычное дело.

Как правило, самое узкое место — линии от ядра (либо арендованной инфраструктуры) до узлов агрегации микрорайона. Строились они давно, многим более 10 лет, поэтому 4-8 волокон там не редкость. Только последние несколько лет модно «на всякий случай» использовать 36 или 48 «жил».

Замена таких линий стоит в 2-3 раза дороже самого кабеля, на уровне \$3-5к за километр. Тут CWDM вне конкуренции, он просто «предназначен» для раздельного включения узлов агрегации в ядро при недостаточном количестве волокон. Таким образом, вырисовывается следующее применение технологии:

1. Строительство новых магистралей масштаба города; 2. Модернизация существующей сети, в основном от ядра до уровня агрегации.

Вместе с тем использовать CWDM на доступе, «до дома», все еще нерационально, прямые волокна более чем на порядок (!) дешевле уплотнения.

Достоинства CWDM — полная протокольная прозрачность, стандартное Ethernet-оборудование. Нет никакой проблемы включить на одну лямбду, например, любимые мультиплексоры E1 1995 года выпуска (нужно только заменить старый оптический трансивер на «цветной»), на вторую — 10G (если хватит денег на интерфейсы), а по третьей передать КТВ (тут можно даже заметно сэкономить, и обойтись вдвое более дешевыми однонаправленными MUX'ом и OADM).

[править]

DWDM

"Плотные" WDM (Dense WDM — DWDM) — системы с разносом каналов не менее 100 ГГц (или 0,8 нм), позволяющие мультиплексировать не более 32 каналов. Частотный план для DWDM систем определяется стандартом ITU G.694.1, его можно видеть на следующей иллюстрации:

[Теория] *Длины волн DWDM*

Этот вид WDM систем предъявляет более высокие требования к компонентам, чем CWDM (ширина спектра источника излучения, температурная стабилизация источника и т. д.). Поэтому, область применения — магистральные сети, для инфраструктуры масштаба города это пока слишком дорого.

Толчок к бурному развитию DWDM сетей дало появление недорогих и эффективных волоконных эрбиевых усилителей (EDFA), работающих в промежутке от 1525 до 1565 нм (третье окно прозрачности кварцевого волокна), поэтому системы WDM на эти частоты оказались более чем востребованы для дальней связи.

Действительно, обычный пролет для передачи сигналов в оптоволокне составляет на сегодня 90-150 километров. Совместное использование усилителя мощности и предусилителя (на стороне приемника) позволяет довести длину пролета до 250 км, а применение дополнительных рамановских усилителей со встречной накачкой – до 300 км.

Более того, при применении каскада оптических усилителей длина регенерационного участка может быть увеличена до 2000 км. И это на серийном (а значит, не слишком дорогим) оборудовании. Прецизионные системы позволяют достигать длин до 10 000 км, и более.

Структурно DWDM похож на подробно рассмотренный выше CWDM, только (в среднем) на 1-2 порядка дороже. Кроме того, длинные пролеты не предполагают сложных архитектурных решений (которые неизбежно вносят потери мощности). Однако более подробное рассмотрение технологии лежит далеко за рамками данного материала...

[править]

HDWDM

HDWDM - High-Density Wavelength Division Multiplexer. "Высокоплотные" системы с разносом каналов 50 ГГц и менее, позволяющие мультиплексировать не менее 64 каналов. Структурно мало отличается от простого DWDM, поэтому иногда их даже не выделяют в отдельную классификацию, считая "разновидностью" DWDM.

Глава 32 : Интерфейсы 10 Gigabit

Особенности работы оптического 10G

Деятельность по разработке стандарта 10 GE началась в 1999 году, но датой рождения 10-ти гигабитного Ethernet можно считать 13 июня 2002 г., именно тогда IEEE одобрил окончательную версию проекта стандарта 802.3ae. Первая экспериментальная сеть на его основе была построена в 2002 году в Лас Вегасе (США). Цена за порт в то время составляла около \$100 тыс.

Технология 10 Gigabit Ethernet мало отличается от первоначального варианта Роберта Меткалфа почти четвертьвековой давности. Используется прежний формат заголовка, 8-байтовая преамбула, минимальный размер кадра в 64 байта... Самым большим изменением можно считать свершившийся наконец де-юре полный отказ от протокола CSMA/CD. Тогда подразумевалось, что 10 Gig будет работать только по оптоволокну, а значит неизбежно в дуплексном режиме, а от использования концентраторов (хабов) полностью отказались еще в гигабитных сетях.

Строение физического интерфейса вполне типично, он состоит из трех уровней: PCS (Physical Coding Sublayer), отвечающий за управление передаваемыми битовыми последовательностями, PMA (Physical Medium Attachment) преобразование группы кодов в последовательный поток бит и обратно, плюс синхронизация, и PMD (Physical Media Dependent), преобразующий биты в оптические сигналы. Традиционно, они выполнены логически независимыми друг от друга частями.

[Теория] *Физический интерфейс 10G.*

Со стандартами физических интерфейсов (PHY) история получилась не слишком простая.

Сначала на каждую из длин волн был предложен свой PMD - 10GBASE-S для 850нм (от short), 10GBASE-L для 1310нм (long) и 10GBASE-E для 1550нм (extra long). Это весьма похоже на уже привычные гигабитные интерфейсы как по смыслу, так и по буквенным сокращениям.

Но затем началось "расширение" стандартизации, потому что в то время IEEE "болел" переходом от локальных (LAN) и распределенных (WAN) сетей. Более того, момент получился удачный - пропускная способность SONET/SDH канала OC-192 очень близка к 10 Гбит/сек. Были предложены отдельные LAN PHY ("R") и WAN PHY ("W"), что в сочетании с тремя основными интерфейсами дало многообразие из шести вариантов.

- 10GBASE-SR (10GBASE-SW)
- 10GBASE-LR (10GBASE-LW)
- 10GBASE-ER (10GBASE-EW)

Технически WAN-расширение выглядело как добавление специального WAN Interface Sublayer (WIS) между уровнями PCS и PMA. В результате, при одном и том же MAC-уровне на передачу "в лазер" могли идти как кадры Ethernet (10,3125 гигабит, 16*644 Mb/s), так и SONET/SDH (9,95 гигабит, 16*622 Mb/s).

Важно отметить, что предлагался единый интерфейс именно на MAC-уровне, формат XGMII. Различие Ethernet/SDH уже было заложено аппаратно в сам оптический интерфейс. Практика показала, что это было не слишком удобное решение (и оно было позже исправлено в формате XFP), но об этом ниже.

Стремление "подружить" WAN и LAN версии окончилось не слишком успешно. Оптические спецификации (синхронизация, задержки, и т.п.) остались различными. Несмотря на то, что Ethernet успешно упаковывается в полезную нагрузку фрейма SONET/SDH, соединение с L3 интерфейсами, основанными на стеке протоколов PPP/HDLC невозможно. Так что WAN-версия 10G используется в основном для соединения с OC-192, например транспондером DWDM.

На этом сложности стандартизации оптических интерфейсов 10G не закончились. Выяснилось, что для мультимодового кабеля характерно сильное рассеивающее действие на лазерное излучение со стороны неоднородностей, сконцентрированных на оси сердцевины многомодового волокна. Как следствие - большая дифференциальная модовая задержка DMD, сокращающая дальность работы линий на старом волокне с сердцевиной 65,5нм буквально до 20-30 метров.

"Новое" 50-ти нанометровое волокно ситуацию улучшало, но даже до 100 метров дотянуть параметры не удавалось. Было разработано специальное мультимодовое волокно (TIA-492AAAC) с улучшенным DMD, на нем линия "удлинялась" до 300 метров.

Поэтому был разработан специальный тип 10GBASE-LX4, который работал на одном физическом канале как 4 параллельные линии на скорости 3,125 Гб/с, 1310нм с технологией спектрального уплотнения WWDM. Это позволило работать на 300 метров при использовании обычного мультимодового волокна, и до 10 км. на одномодовом. Но достигнуто это было путем существенного удорожания приемопередатчиков.

Важно отметить, что этот стандарт не имеет своего WAN-аналога, так как для сетей Sonet/SDH мультимодовый кабель давно не применяется. Более того, мультимод в настоящее время практически вышел из употребления и в Ethernet-сетях, поэтому стандарт 10GBASE-LX4 представляет собой скорее исторический интерес, нежели практический. И в дальнейшем, ниже по тексту, упоминаться не будет совсем.

Следующий "стандартизационный" рывок был сделан относительно недавно, и похоже, на этом все не прекратится. Помимо IEEE был введен тип XENPAK 10GBASE-ZR с дальностью до 80 км. В тоже время, был практически отвергнут 10GBASE-LRM (работает на 300 метров по мультимоду на одной

длине волны за счет электронной компенсации дисперсии, EDC), который ожидался к принятию в 2006 году.

[править]

Дальность работы

По рабочему расстоянию удобно свести стандарты в следующую таблицу:

Стандарт LAN	Тип волокна	Бюджет, дБ	Дальность, м	Длина волны, нм	Тип излучателя	Стандарт WAN
10GBASE-SR	ММ, сердечник 62нм		26	850нм	VCSEL	10GBASE-SW
	ММ, сердечник 50нм		82	850нм	VCSEL	
	ММ, с улучшенным DMD		300	850нм	VCSEL	
10GBASE-LX4	ММ		300	1310нм	4*DFB	неприменим
	SM	9,4	10 000	1310нм	4*DFB	
10GBASE-LR	SM	9,4	10 000	1310нм	DFB	10GBASE-LR
10GBASE-ER	SM	15	40 000	1550нм	EML	10GBASE-ER
10GBASE-ZR	SM	23	80 000	1550нм	EML	не IEEE
10GBASE-LXM	ММ		300	1310нм	DFB с EDC	неприменим

Цветом выделены стандарты, наиболее актуальные для Ethernet-провайдеров.

[править]

ХЕНПАК

Этот формат стал первым универсальным модулем. Хотя до этого существовали устройства с оптическими интерфейсами, например модуль для Cisco Catalist 6500 WS-x6502-10GE имел возможность использования сменных вставок WS-G6483 (10GBASE-ER) или WS-G6488 (10GBASE-LR). Громоздкая и неудобная конструкция, понятно, почему появилась необходимость в 10-ти гигабитном аналоге модулей GBIC|SFP.

Работа над MSA XENPAK (Multi-Source Agreement, соглашение о спецификациях, которые поставщики заключают для продвижения технологии) было инициировано 12 марта 2001 г. компаниями Agilent Technologies и Agere Systems (бывшая Microelectronics Group Lucent Technologies), и сегодня оно является открытым для любой организации. Декларировалась полная поддержка стандарта IEEE 802.3ae. Официальный сайт проекта Xenpak - xenpak.org, но особой информации на нем нет - проект предназначен в основном разработчикам.

Модули Xenpak подключаются через 70-ти контактный интерфейс XAUI (10 Gigabit Attachment Unit Interface), в котором реализуются четыре параллельных канала по 3,125 Гбит/с. Подробнее принцип работы можно видеть на следующей схеме:

[Теория] *Схема Xenpak 10G.*

Итогом работ стали массово выпускаемые рядом производителей (Agilent, Intel, Molex, другие) модули следующего вида:

[Теория] *Внешний вид Xenpak 10G.*

Интересные технические особенности:

- Интерфейс XAUI 4*3,125G
- Размер устройства - 126*36*17 мм
- Потребление электроэнергии 8-10 Вт
- Коннектор 70 pin
- Оптический разъем SC.
- Используется, к примеру, в Cisco серии 6500, CRS-1.
- Не поддерживает скорости, отличные от 10GB.

В настоящее время Xenpak постепенно теряют популярность, и вытесняются форматами X2 и XFP. Причиной этого являются большие габариты и существенное тепловыделение.

[править]

X2 и XPAK

Модули X2 сразу позиционировались лишь как косметическое развитие Xenpak. Проект официально стартовал 22 июля 2002 (сайт, весьма похожий на Xenpak.org по дизайну - x2msa.org) при поддержке Agere Systems, Agilent Technologies, JDS Uniphase, Mitsubishi Electric, NEC, OpNext, Optillion и Tyco Electronics.

X2 в полтора раза меньше XENPAK, и полностью поддерживает спецификации XENPAK MSA, включая электрические параметры интерфейса ввода/вывода, 70-ти контактный разъем, тепловые режимы и параметры электромагнитной совместимости. Однако, его энергопотребление более чем в два раза меньше (4 Вт против 8-10), что очень важно для многопортовых устройств.

Второе важное отличие - X2 унифицированы с модулями XPAK, которые никогда не использовались в оборудовании Ethernet, и применялись в сетевых адаптерах и дисковых массивах. Поэтому X2 получил поддержку скоростей 10G Fiber Channel, 10,5 Gb/c.

И третье изменение - смена способа крепления, в отличие от Xenpak, который крепится за корпус устройства внешними болтами, X2 крепится за сам разъем, установленный на печатной плате (подобно GBIC и SFP). Это значительно более удобно и просто.

[Теория] *Внешний вид X2.*

[Теория] *Внешний вид XPAK.*

Интересные технические особенности X2:

- Интерфейс XAUI 4*3,125G
- Размер устройства - 100*36*12 мм
- Потребление электроэнергии 4 Вт
- Коннектор 70 pin
- Оптический разъем SC.
- Используется, к примеру, в Cisco серии 4500, 3750E.
- Поддерживает скорости, отличные от 10GB, - 10G FC 10,5 Gb/c.

[править]

XFP

Разработка этих модулей стартовала 4 Марта 2002 и явно проходила под влиянием гигабитного стандарта SFP, и, по сути, это было предложение новой, совершенно отличной от XENPAK, концепции миниатюрных модулей. Инициаторами MSA (xfpmsa.org) выступили Broadcom Corporation, Brocade, Emulex Corporation, Finisar, JDS Uniphase, Maxim Integrated Products, ONI Systems, ICS (a Sumitomo Electric company), Tyco Electronics и Velio.

Основными достоинствами разработки считаются большой список поддерживаемых скоростей (практически все возможные "около" 10 гигабит), и миниатюрные размеры.

Эти возможности легко понять, рассмотрев схему модулей XFP:

[Теория] *Схема XFP 10G.*

Кодирование битовой последовательности (PCS) вынесено из модуля на основное устройство, и сам

XFP является по сути универсальным последовательным преобразователем, которому "все равно" что передавать в линию (что очень похоже на привычные гигабитные SFP).

Внешний вид модуля:

[Теория] *Внешний вид XFP.*

Интересные технические особенности:

- Интерфейс XFI 1*10G
- Размер устройства - 78*18*10 мм.
- Не поддерживает стандарт 10GBASE-LX4.
- Потребление электроэнергии 3,5 Вт
- Коннектор 30 pin
- Оптический разъем LC.
- Используется, к примеру, в Cisco серии 12000.
- Поддерживает скорости, отличные от 10GB (10.3 Gb/s), - OC-192/STM-64 9,95 Gb/c, 10G FC 10,5 Gb/c, G.709 10,709 Gb/c.

[править]

10GB твинаксиал (10GBase-CX4)

Хотя этот вариант 10-ти гигабитного Ethernet не является оптическим, он так же далеко от "витой пары", как и от "стекла". Частотные возможности твинаксиального (twin-axial) кабеля близки к оптическому, соответственно, используются похожие технические решения.

[Теория] *твинаксиальный кабель*

Разработка 10GBase-CX4 была начата рабочей группой IEEE 802.3ак в 2002 году. Он обеспечивает соединение 10G на расстояние до 15 метров на базе твинаксиальных кабелей. Ориентирован этот вид на внутриузловые соединения, и для Ethernet-провайдеров малоинтересен.

Разработчики пошли примерно по тому же пути, как в вышеописанном 10GBASE-LX4. А именно, применили четырех дифференциальных передатчика и приемника на каждую линию. В каждом канале скорость 2,5 Гбит/с, тактовая частота 3,125 ГГц и кодированием по стандарту 8B10B (т.е. тому же, что и в LX4). Для этого требуются четыре дифференциальные пары, работающие в каждом направлении, и, соответственно, общее число твинаксиальных каналов в соединительном кабеле равно восьми.

[Теория] *Модуль XFP 10GBase-cx4*

Сейчас 10GBase-cx4 практически не применяется на практике (по крайней мере в России). причина - так как оптические варианты 10G быстро стали дешевле и проще твинаксиальных (которые первоначально позиционировались как "экономичный" вариант). Более того, твинаксиальные кабельные сборки (infiband 4x) сами по себе весьма неудобны, не дешевы (\$200-500), и не могут быть изготовлены в "полевых" условиях (в отличие от оптоволоконных патчкордов).

[править]

SFP+

Стандарт SFP+ был принят в 2008 году, а первое оборудование его использующее появилось в начале 2009. Причиной появления послужило желание применить выгоды формата SFP для 10-гигабитных потоков, в частности необходимость увеличения плотности портов коммутаторов. SFP+ является логическим продолжением формата XFP. Для уменьшения размера и энергопотребления часть электроники была вынесена из модуля на устройство-носитель.

- Cisco 10GBASE SFP+ Modules
- SFP+ compliance testing

Существуют модули SFP+, предназначенные не только для оптоволоконных каналов, но и рассчитанные на медный кабель. Эти модули обычно жестко связаны с кабелем, и по сути являются его неотделяемыми разъемами, как у патчкорда. Длина кабеля обычно варьируется от 1 до 15 м.

Глава 33 : Конструкционные элементы (шкафы и муфты)

Как правило, оптоволоконные кабеля разделяются 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, чтобы 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.

[Теория] Рис. 8.8. Конструкция настенного оптического шкафа

Шкаф представляет собой устанавливаемый на стене или на любой стойке универсальный металлический корпус, в котором имеется разъемно-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 внутреннее 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 (сплайн-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.

[Теория] Рис. 8.9. Конструкция муфты.

Конструкция муфт достаточно проста. Это герметически закрытый корпус, в котором размещен организатор световодов (сплайн-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 термоусаживающегося 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. Большей частью выбор конструктива определяется условиями эксплуатации. Шкафы принадлежат к конструкциям, предназначенным для размещения в относительно чистых зонах с возможностью быстрого доступа к волоконным соединениям. Если же нужно обеспечить повышенный уровень защиты волокон или коннекторов от неблагоприятных условий - применяют муфты. Например, в запыленных, загазованных условиях; при вероятном воздействии водяного пара или конденсата; на линиях связи под открытым небом или проложенных под водой/землей.

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

Глава 34 : Расчет оптического бюджета

Оптический бюджет – разность между оптической мощностью передатчика и чувствительностью приемника, выраженная в дБ. Это паспортная информация, которую производитель (по идее) должен прикладывать ко всем приемопередатчикам.

Если суммарное затухание линии больше оптического бюджета - работать ничего не будет. Поэтому часто бывает нужно сделать оценку заранее, учитывая каждый компонент линии.

Упрощенно это можно представить себе в виде следующей схемы:

[Теория] *Оценка работоспособности оптоволоконной линии*

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.

Типичный бюджет оптических приемопередатчиков:

- 100BASE-FX, 1310 нм, 12 дБ
- 1000BASE-SX, 850 нм, 7 дБ
- 1000BASE-LX, 1310 нм, 7 дБ
- 1000BASE-ZX, 1550 нм, 22 дБ

Типичные потери:

- затухание в мультимодовом кабеле (850 нм) - 2,7 дБ/км
- затухание в мультимодовом кабеле (1310 нм) - 0,75 дБ/км
- затухание в одномодовом кабеле (1310 нм) - 0,35 дБ/км.
- затухание в одномодовом кабеле (1550 нм) - 0,2 дБ/км.
- коннекторы, MM - 0,5 дБ
- коннекторы, SM - 0,3 дБ
- на сплайсе - 0,1 дБ
- на сварке - 0,02 дБ

Так же рекомендуется учитывать, что мощность лазера (светодиода) несколько уменьшается с течением времени. Обычно на ремонт и старение эмиттера отводится около 2-3 дБ.

Глава 35 : Модели коммуникации (OSI)

Связь между моделью OSI и стеком TCP/IP

Модель OSI	Протоколы информационного обмена	Стек TCP/IP

7	HTTP, SNMP, FTP, Telnet, SSH, и много других	I
6		
5	TCP, UDP, DNS, NetBios	II
4		
3	IP, ARP(RARP), ICMP, RIP, DHCP	III
2	Ethernet, ATM, Frame Relay, SDH (Для стека TCP/IP не регламентируется)	IV
1		

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.

[править]

Физический уровень модели OSI

[Теория] 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 способах 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).

[править]

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 поддерживающее Auto-negotiation, воспринимает 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-negotiation, 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.

[править]

Присоединение к физической среде (PMA)

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.

[Теория] 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:

[Теория] Рис. 9.3. Реализация повторения передачи (отката) при коллизии в сетях Ethernet.

Ключевым моментом является выбор задержки (Т) передачи перед повтором, которая равна случайно выбранному из заданного диапазона количеству интервалов (N) времени (t). Иначе говоря, $T = N \cdot t$, 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.

[Теория] 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 (3×10^8 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.

[Теория] 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%.

Принципы кодирования 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, наравне 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 монополюно 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 различать кодирование битовой последовательности в электрический сигнал, и кодирование данных, которое преобразует одну последовательность битов в другую.

Передача битовой последовательности в Ethernet производится обычным способом.

Тактовая частота приемника и передатчика синхронизируется. Далее, на стороне передатчика последовательность битов-импульсов представляется суммой синусоидальных электрических сигналов принятого уровня напряжения, после чего гармоники (кроме первой, нужной для восстановления формы сигнала) фильтруются.

Приемник усиливает полученное, восстанавливает его форму, и производит 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).

[Теория] 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 оптоволоконна 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.

[Теория] 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 удастся 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 связано 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-битная 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 36 : Модификации Ethernet

Краткая история

Принято считать, что Ethernet был разработан 22 мая 1973 года. Именно тогда Роберт Меткалф (Robert Metcalfe) составил докладную записку главе Xerox PARC. Законное право на технологию было получено позже, в 1976 году Меткалф и его ассистент Дэвид Боггс (David Boggs) издали брошюру под названием «Ethernet: Distributed Packet-Switching For Local Computer Networks». Новая технология получила имя Ethernet (эфирная сеть), в честь радиосети Гавайского университета ALOHA, в которой был использован схожий механизм разделения среды передачи (радиоэфира).

Позже, в 1973 году, Меткалф ушёл из Xerox и основал компанию 3Com. Ему удалось убедить DEC, Intel и Xerox совместно разработать стандарт Ethernet (DIX). В феврале 1980 г. результаты были представлены в IEEE, где была сформирована группа 802 для работы над проектом. Впервые он был опубликован 30 сентября 1980 года.

Для успешного внедрения технологии группа разработчиков Digital представила чип Ethernet и исходные тексты его программного обеспечения компаниям Advanced Micro Devices (AMD) и Mostek. В результате возможность производить совместимые чипсеты Ethernet получили и другие компании. Это сказалось на качестве железа и снижении его стоимости.

За прошедшие 30 лет (фантастическое для индустрии телекома время) сменилось много модификаций протокола, однако его основа, формат, практически не претерпел изменений до настоящего времени.

[править]

Устаревшие протоколы

- Xerox Ethernet — первоначальная технология, скорость 2,94 Мбит/с, коаксиальный кабель, существовала в двух вариантах Version 1 и Version 2 (формат кадра применяется до сих пор).
- 10BROAD36 — "дальнобойная" модификация, не получила распространения. Была применена технология широкополосной модуляции (подобно тому, что используется в кабельных модемах KTB). Коаксиальный кабель 75 Ом, сегмент до 3,6 км, скорость 10 мегабит.
- 1BASE5 (StarLAN) — первая модификация Ethernet, использующая витую пару. Скорость 1 Мбит/с, коммерческого применения не получил. Упомянется, в основном, как часть не менее экзотической UltraNet.
- 10BASE-5, IEEE 802.3, принят в июне 1983 г. Так называемый "Толстый Ethernet", поддерживал скорость до 10 мегабит по кабелю типа RG-8X (50 Ом, диаметр около 9 мм). Максимальная длина сегмента до 500 метров. Подключение делалось "протыканием" оболочки кабеля до центральной жилы специальным устройством "вампириком" (vampire tap).
- 10BASE2, IEEE 802.3a, принят в июне 1983 г, скорость 10 мегабит. Получил название "Тонкий Ethernet" — используется кабель RG-58, с максимальной длиной сегмента 185 метров. Компьютеры присоединялись последовательно один к другому через T-образный BNC-коннектор. На каждом конце был необходим терминатор (сопротивление 50 Ом). Долгое время эта технология была основной, и широко применялась во всем мире.
- StarLAN 10 — Первая разработка, использующая витую пару для передачи данных на скорости 10 Мбит/с. В дальнейшем эволюционировал в стандарт 10BASE-T.
- 10BASE-T, IEEE 802.3i, принят в 1991 г. Для передачи данных используется 4 провода кабеля витой пары (две скрученные пары) категории-3 или категории-5. Максимальная длина сегмента 100 метров. Важный момент - для соединения компьютеров использовались специальные устройства-разветвители - хабы (hub), соответственно топология - звезда.
- FOIRL — (англ. Fiber-optic inter-repeater link). Базовый стандарт для технологии Ethernet, использующий для передачи данных оптический кабель. Максимальное расстояние передачи данных без повторителя 1 км. Не получил распространения.
- 10BASE-F, IEEE 802.3j — основной термин для обозначения семейства 10 Мбит/с ethernet-стандартов, использующих оптоволоконный кабель на расстоянии до 2 километров: 10BASE-FL, 10BASE-FB и 10BASE-FP. Из перечисленного только 10BASE-FL получил широкое распространение.
 - 10BASE-FL (Fiber Link) — Улучшенная версия стандарта FOIRL. Улучшение коснулось увеличения длины сегмента до 2 км.
 - 10BASE-FB (Fiber Backbone) — Сейчас неиспользуемый стандарт, предназначался для объединения повторителей в магистраль.
 - 10BASE-FP (Fiber Passive)- Топология «пассивная звезда», в которой не нужны повторители — никогда не применялся.

[править]

Протоколы 100 мегабит

- 100BASE-T — общий термин для обозначения стандартов, использующих в качестве среды передачи данных витую пару (коаксиальный кабель более не используется). Длина сегмента до 100 метров. Включает в себя стандарты 100BASE-TX, 100BASE-T4 и 100BASE-T2.

- 100BASE-TX, IEEE 802.3u (утвержден в 1995 году) — развитие стандарта 10BASE-T для использования в сетях топологии "звезда". Задействована витая пара категории 5, фактически используются только две пары проводников. Длина линии - до 100 метров.
- 100BASE-T4 — стандарт, использующий витую пару категории 3. Задействованы все четыре пары проводников, передача данных идёт в полудуплексе. Практически не используется.
- 100BASE-T2 — стандарт, использующий витую пару категории 3. Задействованы только две пары проводников. Поддерживается полный дуплекс, когда сигналы распространяются в противоположных направлениях по каждой паре. Скорость передачи в одном направлении — 50 Мбит/с. Не используется.
- 100BASE-FX — стандарт, использующий многомодовое оптоволокно. Максимальная длина сегмента 400 метров в полудуплексе (для гарантированного обнаружения коллизий) или 2 километра в полном дуплексе.
- 100BASE-LX — стандарт, использующий одномодовое оптоволокно. Максимальная длина сегмента 15 километров в полном дуплексе на длине волны 1310 нм.
- 100BASE-LX WDM — стандарт, использующий одномодовое оптоволокно. Максимальная длина сегмента 15 километров в полнодуплексном режиме на длине волны 1310 нм и 1550 нм. Интерфейсы бывают двух видов, отличаются длиной волны передатчика и маркируются либо цифрами (длина волны) либо одной латинской буквой A(1310) или B(1550). В паре могут работать только парные интерфейсы: с одной стороны передатчик на 1310 нм, а с другой — на 1550 нм.

[править]

Гигабит Ethernet (Gigabit Ethernet, 1 Гбит/с)

В 1996 г. начались работы по стандартизации сетей Ethernet со скоростью передачи данных 1000 Мбит/с, которые называют Gigabit Ethernet. Был образован Gigabit Ethernet Alliance, в который вошли 11 компаний: 3Com, Bay Networks, Cisco, Compaq, Granite Systems, Intel, LSI Logic, Packet Engines, Sun, UB Networks и VLSI Technology.

К началу 1998 года в Альянс входило уже более 100 компаний. В июне 1998 г. принимается стандарт IEEE 802.3z, использующий одномодовые и многомодовые оптоволоконные кабели, а также STP категории 5 на короткие расстояния (до 25 м). Столь малое допустимое расстояние в случае применения UTP обуславливало сомнительную возможность практического применения такого варианта.

Положение изменилось с принятием в июне 1999 г. стандарта IEEE 802.3ab для передачи 1000 Мбит/с по неэкранированной витой паре на расстояния до 100 м.

- 1000BASE-T, IEEE 802.3ab — стандарт, использующий витую пару категорий 5е или 6. В передаче данных участвуют все 4 пары. Скорость передачи данных — 250 Мбит/с по одной паре.
- 1000BASE-TX был создан Ассоциацией Телекоммуникационной Промышленности (TIA) и опубликован в марте 2001 года как «Спецификация физического уровня дуплексного Ethernet 1000 Мб/с (1000BASE-TX) симметричных кабельных систем категории 6 (ANSI/TIA/EIA-854-2001). Использует раздельную приёмо-передачу (2 пары на передачу, 2 пары на приём, по каждой паре данные передаются со скоростью 500 Мбит/с), что существенно упрощает конструкцию приёмопередающих устройств. Но, как следствие, для стабильной работы по такой технологии требуется кабельная система высокого качества, поэтому 1000BASE-TX может использовать только кабель 6 категории. Ещё одним существенным отличием 1000BASE-TX является отсутствие схемы цифровой компенсации наводок и возвратных помех, в результате чего сложность, уровень энергопотребления и цена процессоров становится ниже, чем у процессоров стандарта 1000BASE-T. На основе данного стандарта практически не было создано продуктов, хотя 1000BASE-TX использует более простой протокол, чем стандарт 1000BASE-T, и поэтому может использовать более простую электронику.
- 1000BASE-X — общий термин для обозначения стандартов со сменными приёмопередатчиками GBIC или SFP.
 - 1000BASE-SX, IEEE 802.3z — стандарт, использующий многомодовое оптоволокно. Дальность прохождения сигнала без повторителя до 550 метров.
 - 1000BASE-LX, IEEE 802.3z — стандарт, использующий одномодовое оптоволокно. Дальность прохождения сигнала без повторителя до 80 километров.[источник?]
 - 1000BASE-CX — стандарт для коротких расстояний (до 25 метров), использующий экранированную витую пару (STP) с волновым сопротивлением 150 Ом. Сейчас не используется.
 - 1000BASE-LH (Long Haul) — стандарт, использующий одномодовое оптоволокно. Дальность прохождения сигнала без повторителя до 100 километров.

[править]

10 Гигабит Ethernet

В начале 2000 г. 3Com, Cisco Systems, Extreme Networks, Intel, Nortel Networks, Sun Microsystems и Worldwide Packets основали 10 Gigabit Alliance. Стандарт 10 Гигабит Ethernet включает в себя семь стандартов физической среды для LAN, MAN и WAN.

- 10GBASE-CX4 — Технология 10 Гигабит Ethernet для коротких расстояний (до 15 метров), используется медный кабель CX4 и коннекторы InfiniBand.
- 10GBASE-SR — Технология 10 Гигабит Ethernet для коротких расстояний (до 26 или 82 метров, в зависимости от типа кабеля), используется многомодовое оптоволокно. Он также поддерживает расстояния до 300 метров с использованием нового многомодового оптоволокна (2000 МГц/км).
- 10GBASE-LX4 — использует уплотнение по длине волны для поддержки расстояний от 240 до 300 метров по многомодовому оптоволокну. Также поддерживает расстояния до 10 километров при использовании одномодового оптоволокна.
- 10GBASE-LR и 10GBASE-ER — эти стандарты поддерживают расстояния до 10 и 40 километров соответственно.
- 10GBASE-SW, 10GBASE-LW и 10GBASE-EW — Эти стандарты используют физический интерфейс, совместимый по скорости и формату данных с интерфейсом OC-192 / STM-64 SONET/SDH. Они подобны стандартам 10GBASE-SR, 10GBASE-LR и 10GBASE-ER соответственно, так как используют те же самые типы кабелей и расстояния передачи.
- 10GBASE-T, IEEE 802.3ap-2006 — принят в июне 2006 года после 4 лет разработки. Использует экранированную витую пару. Расстояния — до 100 метров.

Глава 37 : 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 заданы 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 опрaвлен 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).

[Теория] 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

Версия	Длина	Тип сервиса	Общий размер	
Идентификация			Флаги	Смещение фрагмента
Время жизни		Протокол	Контрольная сумма заголовка	
Адрес отправителя				
Адрес получателя				
Опции и заполнение				
Данные				

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 (Service 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 смещение 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 Интернет, 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 Интернет 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	Диапазон значений первого октета	Значения адреса в десятичной записи	Возможное кол-во сетей	Возможное кол-во узлов
A	от 00000001-... до 01111110-...	от 1.xxx.xxx.xxx до 126.xxx.xxx.xxx	126	16777214
B	от 10000000-00000000-... до 10111111-11111111-...	от 128.0.xxx.xxx до 191.255.xxx.xxx	16382	65534
C	от 11000000-00000000-00000000-... до 11011111-11111111-11111111-...	от 192.0.0.xxx до 223.255.255.xxx	2097150	254
D	от 1110000-... до 1110111-...	от 224.xxx.xxx.xxx до 239.xxx.xxx.xxx	-	268435456
E	от 1111000-... до 1111111-...	от 240.xxx.xxx.xxx до 255.xxx.xxx.xxx	-	134217728

Понятно, что адреса класса А предназначены для использования в очень больших сетях общего пользования (например, национальных). Класс В 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 С, которые позволяют адресовать 254 узла. Адреса класса D используются при обращениях к группам машин, а адреса класса Е зарезервированы для использования в экспериментальных 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 С можно адресовать не 256, а только 254 узла.

Кроме этого, зарезервировано несколько групп адресов специального назначения. Так, сеть класса А 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 А), 172.16.0.0-172.31.255.255 (16 сетей класса В), 192.168.0.0-192.168.255.255 (255 сетей класса С). Такие адреса часто используются для маскарadingа, 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 А. 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, была 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 C, 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 C 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 "C" 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

Тип оборудования (для Ethernet - 1)		Тип протокола (для IP-0800)
Длина MAC-адреса	Длина IP-адреса	Операция. 1-ARP (запрос), 2-ARP (ответ), 3-RARP (запрос), 4-RARP (ответ)
Аппаратный адрес (для Ethernet MAC) отправителя (байты 9-14)		
IP-адрес отправителя (байты 15-18)		
Аппаратный адрес (для Ethernet MAC) получателя (байты 19-24)		
IP-адрес получателя (байты 25-28)		

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 перепривить 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:

Метка	CoS	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, и 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 38 : 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.

[Теория] 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 используются 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.

[Теория] 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 концентраторы 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 39 : 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 коллизийный домен, или, вдобавок, территориально удалены друг от друга?

Для решения этой задачи применяют мосты (Bridge). Как и повторители, они принимают данные на входящий порт, и передают на исходящий с восстановленным уровнем и формой сигнала. Но на этом сходство заканчивается, и начинаются различия.

[Теория] 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 разделяют 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 40 : Маршрутизаторы

Можно сказать, что маршрутизаторы (роутеры, routers) - это следующая ступень сетевой иерархии. Упрощенно 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).

[Теория] Рис. 10.4. Применение маршрутизатора в корпоративной сети

Подобно повторителям, маршрутизаторы восстанавливают уровень и форму передаваемого 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. Обратной 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:

$$\text{Скорость} = N/(K) * 8 * S ,$$

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 $40000/5 \cdot 500 \cdot 8 = 32$ Mbit/s

Однако нужно учитывать, что access листы, роутмапы, firewalls, 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 41 : 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 основывалась 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, который 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 широкоэмитательными (бродкастовыми) кадрами. Однако, во-первых, это возможно только в больших 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 буферизацией (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 буферизоваться.

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;
- многоходовая 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) попадает в двумерную 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).

Многоходовая 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.

[Теория] 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 АТМ. 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 АТМ 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 Comrex 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 группы 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 замену 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 42 : 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 (САМ-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 САМ-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 замедлится 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 дополнительные условия 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 компьютера), 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 Ethernet 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 43 : 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.

[Теория] 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 вернуться 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 коллизийные 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 остальной сети 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 позволяют

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 вианами, 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 вианами, 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 44 : Термины по "ПУЭ"

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). Хотя 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 законодательстве 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 пострададут только предохранители.
3. Обратная 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 пришить 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...

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:

[Теория] Рис. 4.1. Сеть 220/380 Вольт.

Три фазы (А, В, С) 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. "Т" - 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): "Т" - 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 отдельными 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.

[Теория] [Теория] [Теория] 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:

[Теория] 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 комбинированные 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.

[Теория] 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 (временки, 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 провайдера просто нет задач, на которых сказывается дешевизна алюминиевых проводов.

Глава 45 : 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 сигналов частоты 50 Гц способна ввергнуть любого неопытного 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 электробезопасности".

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 металлических

- 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 (РЕ) 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.

[Теория] 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 "забатаривания" - 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, чтобы 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. Хотя 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 "заземленного" 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, электрополотенц и т.п.) к нулевому защитному проводнику.

Вообще, это проще представить следующей иллюстрацией:

[Теория] Рис. 4.6. Схема заземления.

Картина довольно 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 совершенно 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.

Глава 46 : 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 микросекунд, или 0,06 секунды). Сечение проводников витой пары - 0,4 мм. соответственно, для заноса большой энергии потребуются 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 кабели 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:

[Теория] Рис. 4.7. Заземление экранов кабелей, грозозащит и активного оборудования по новой редакции ПУЭ.

В то время как старая редакция предусматривала такую схему:

[Теория] 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, чтобы 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 большой 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 кабели 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 выше 60 МГц очень мал, но очень важен для восстановления формы сигнала. Однако, даже при наличии помех на частоте выше 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 кабели 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:

[Теория] Рис. 4.9. Заземление экрана кабеля.

С одной стороны выполняется "глухое" заземление. С другой - через гальваническую развязку (разрядник, конденсатор, искровой промежутки). 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.

Глава 47 : Использование грозозащит

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).

[Теория] [Теория] Рис. 4.10. Сетевая карта.

Один из самых распространенных 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 карточке "только ТР" 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) Вольт.

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 к 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 хамам 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.

[Теория] Рис. 4.11. Явления при наводке на витую пару.

Результат будет все равно один. Через первичную обмотку трансформатора активного устройства будет течь ток ($I_{ж}$), и вместе с тем эта же обмотка получит напряжение ($U_{п}$). Других заметных физических результатов не сможет добиться ни одна наводка.

Поражение активного устройство может пройти следующими способами:

[Теория] Рис. 4.12. Поражение устройства наводкой на витую пару.

Во-первых, это пробой на землю сетевой карты или коммутатора ($I_{пп}$).

В этом случае напряжение $U_{п}$ 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 перепаявается 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:

[Теория] 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 магистральной. 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:

[Теория] 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 APC 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 спасти 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 незначительна. 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. :-)