Министерство образования и науки Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

Е.А. Чернецова

СИСТЕМЫ И СЕТИ ПЕРЕДАЧИ ИНФОРМАЦИИ

Часть 1

Телекоммуникационные сети

Монография

РГГМУ
Санкт-Петербург
2013

УДК 681.3.07

Чернецова Е.А. Системы и сети передачи информации. Часть 1. Телекоммуникационные сети. – СПб.: РГГМУ, 2013. – 244 с.

ISBN 978-5-86813-347-3

Рецензент: И.В. Алешин, д-р техн. наук, проф., Санкт-Петербургский государственный морской технический университет

В монографии изложены основные принципы, на которых основана работа систем связи. Представлены принципы построения информационно-телекоммуникационных сетей и систем различного назначения, а также основные сведения о процессах передачи и преобразованиях информации в сетях и системах связи.

Монография состоит из трех частей: часть 1 – «Телекоммуникационные сети», часть 2 – «Цифровые технологии передачи данных», часть 3 – «Системы цифровой связи».

Монография рассчитана на специалистов в области телекоммуникационных систем, а также для самостоятельного продолжения изучения систем связи.

Chernetsova, E.A. Systems and networks of information transfer. Part 1. Telecommunication networks. – St Petersburg: RSHU Publishers, 2013. – 244 pp.

This monograph describes the basic principles on which the work of the communication systems is based. There are the principles of construction of information-telecommunication networks and systems of various purpose, as well as basic information about the processes of transfer and transformation of the information in networks and communication systems presented. The monograph consists of three parts: part 1 – «Telecommunication networks», part 2 – «Digital technologies of data transmission», part 3 – «the System of digital communication».

The monograph is intended for specialists in the field of telecommunication systems, and also will allow the reader to independently continue the study of communication systems.

ISBN 978-5-86813-347-3

Введение

С изобретением в 1835 г. электрического телеграфа в истории человечества началась новая эпоха – эпоха электросвязи. Менее чем за 200 лет телекоммуникационные технологии прошли огромный путь – от громоздких и неуклюжих устройств, которыми могли пользоваться лишь государственные организации и немногие наиболее обеспеченные частные лица, до глобальной инфраструктуры, обеспечивающей связь на всем земном шаре между самыми отдаленными его уголками. Огромная скорость, с которой распространяются электромагнитные волны, позволяет за ничтожные доли секунды преодолевать расстояния в десятки тысяч километров, передавая все виды информации: звук, неподвижные и подвижные изображения, компьютерные данные и т. д.

Изначально электрическая связь была проводной. Лишь в конце XIX в. была открыта и использована возможность связи без проводов, посредством электромагнитных волн, распространяющихся в свободном пространстве. К настоящему времени беспроводные технологии получили исключительно широкое распространение. Применение радиотехнологий в системах связи становится все более распространенным из-за таких очевидных преимуществ, как невысокая стоимость внедрения, мобильность, быстрота развертывания и низкие эксплуатационные расходы.

Однако, несмотря на использование самых современных средств и методов обработки сигналов, беспроводные средства связи проигрывают по пропускной способности кабельным линиям. Это связано с тем, что электромагнитный сигнал, распространяющийся в закрытой направляющей системе (в кабеле), находится в гораздо более выгодных условиях, чем радиосигнал в открытом пространстве. Вместе с тем, оборудование кабельной линии связи – чрезвычайно трудоемкое и дорогостоящее мероприятие.

Все эти проблемы уже на самых ранних этапах развития средств проводной связи привели к необходимости повышать эффективность использования линейно-кабельных сооружений за счет передачи одновременно нескольких сигналов по одной паре проводов. Разработка таких способов положила начало созданию

аппаратуры уплотнения, или мультиплексирования. Технологии уплотнения в ходе своего развития прошли несколько этапов и к настоящему времени обеспечили создание мощной глобальной сети типовых каналов и трактов, то есть так называемой первичной, или транспортной сети.

Развитие современной экономики, а также территориальная распределенность офисов компаний обусловливают развитие в настоящее время мультисервисных сетей, интегрирующих воедино локальные вычислительные сети, телефонную сеть и другие средства телекоммуникаций. Основные требования к сетям заключаются в возможности гибко использовать и наращивать в будущем имеющиеся каналы связи без серьезных дополнительных инвестиций, а также в способности передавать большие объемы разнородного трафика. Сетевая безопасность является неотъемлемой частью системы информационной безопасности предприятия и обеспечивает защищенность информационной системы на уровне сетевой инфраструктуры.

Монография «Сети и системы передачи информации» имеет целью изложить принципы построения информационно-телекоммуникационных сетей и систем различного назначения. В ней изложены основные представления о процессах передачи и преобразования информации в сетах и системах связи.

1. ОБЩИЕ СВЕДЕНИЯ О СЕТЯХ И СИСТЕМАХ ПЕРЕДАЧИ ИНФОРМАЦИИ

1.1. Основные понятия и определения

Информация – это сведения о каких-либо процессах, событиях, фактах или предметах. Известно, что 80...90 % информации человек получает через органы зрения и 10...20 % – через органы слуха. Другие органы чувств дают в сумме 1...2 % информации. Физиологические возможности человека не позволяют обеспечить передачу больших объемов информации на значительные расстояния [1].

Связь – техническая база, обеспечивающая передачу и прием информации между удаленными друг от друга людьми или устройствами. Аналогия между связью и информацией такая же, как у транспорта и перевозимого груза. Средства связи не нужны, если нет информации, как не нужны транспортные средства при отсутствии груза.

Сообщение – форма выражения (представления) информации, удобная для передачи на расстояние. Различают оптические (телеграмма, письмо, фотография) и звуковые (речь, музыка) сообщения. Документальные сообщения наносятся на определенные носители (чаще всего на бумагу) и там же хранятся. Сообщения, предназначенные для обработки в компьютерных информационных системах, принято называть данными.

Информационный параметр сообщения – параметр, в изменении которого «заложена» информация. Для звуковых сообщений информационным параметром является мгновенное значение звукового давления, для неподвижных изображений – коэффициент отражения, для подвижных – яркость свечения участков экрана. По характеру изменения информационных параметров различают непрерывные и дискретные сообщения.

Сигнал – физический процесс, отображающий передаваемое сообщение. Отображение сообщения обеспечивается изменением какой-либо физической величины, характеризующей процесс. Эта

величина является информационным параметром сигнала.

Сигналы, как и сообщения, могут быть непрерывными и дискретными. Информационный параметр непрерывного сигнала с течением времени может принимать любые мгновенные значения в определенных пределах. Непрерывный сигнал часто называют аналоговым. Дискретный сигнал характеризуется конечным числом значений информационного параметра. Часто этот параметр принимает всего два значения.

В дальнейшем будем рассматривать принципы и средства связи, основанные на использовании электрической энергии в качестве переносчиков сообщений, т.е. электрических сигналов. Выбор электрических сигналов для переноса сообщений на расстояние обусловлен их высокой скоростью распространения (около 300 км/мс).

Основным преимуществом цифровой связи является легкость восстановления цифровых сигналов по сравнению с аналоговыми. Рассмотрим рис. 1.1, на котором представлен идеальный двоичный цифровой импульс, распространяющийся по каналу передачи данных. На форму сигнала влияют два основных механизма:

1. Поскольку все каналы и линии передачи имеют неидеальную частотную характеристику, идеальный импульс искажается.

2. Нежелательные электрические шумы или другое воздействие со стороны еще больше искажает форму импульса. Чем протяженнее канал, тем существеннее эти механизмы искажают импульс (рис. 1.1). В тот момент, когда переданный импульс все еще может быть достоверно определен (прежде чем он ухудшится до неоднозначного состояния), импульс усиливается цифровым усилителем, восстанавливающим его первоначальную идеальную форму. Импульс “возрождается” или восстанавливается. За восстановление сигнала отвечают регенеративные ретрансляторы, расположенные в канале связи на определенном расстоянии друг от друга.

Цифровые каналы менее подвержены искажению и интерференции, чем аналоговые. Поскольку двоичные цифровые каналы дают значимый сигнал только при работе в одном из двух состояний – включенном или выключенном возмущение должно быть достаточно большим, чтобы перевести операционную точку кана-

ла из одного состояния в другое. Наличие всего двух состояний облегчает восстановление сигнала и, следовательно, предотвращает накопление в процессе передачи шумов или других возмущений. Аналоговые сигналы, наоборот, не являются сигналами с двумя состояниями; они могут принимать бесконечное множество форм. В аналоговых каналах даже небольшое возмущение может неузнаваемо исказить сигнал. После искажения аналогового сигнала возмущение нельзя убрать путем усиления. Поскольку накопление шума неразрывно связано с аналоговыми сигналами, как следствие, они не могут воспроизводиться идеально. При использовании цифровых технологий очень низкая частота возникновения ошибок плюс применение процедур выявления и коррекции ошибок делают возможным высокую точность сигнала. Остается только отметить, что с аналоговыми технологиями подобные процедуры недоступны.

Рис. 1.1. Передача цифрового импульса по каналу связи [2]

Существуют и другие в преимущества цифровой связи. Цифровые каналы надежнее и могут производиться по более низким ценам, чем аналоговые. Кроме того, цифровое программное обеспечение позволяет более гибкую реализацию, чем аналоговое (например, микропроцессоры, цифровая коммутация и большие интегральные схемы. Использование цифровых сигналов и уплотнения с временным разделением (time-division multiplexing – TDM) проще применения аналоговых сигналов и уплотнения с частотным разделением (frequency-division multiplexing – FDM). При передаче и коммутации различные типы цифровых сигналов (данные, телеграф, телефон, телевидение) могут рассматриваться как

идентичные: ведь бит — это и есть бит. Кроме того, для удобства коммутации и обработки цифровые сообщения могут группироваться в автономные единицы, называемые пакетами. В цифровые технологии естественным образом внедряются функции, защищающие от интерференции и подавления сигнала либо обеспечивающие шифрование или секретность. Кроме того, обмен данными в основном производится между двумя компьютерами или между компьютером и цифровыми устройствами или терминалом. Подобные цифровые оконечные устройства лучше (и естественнее!) обслуживаются цифровыми каналами связи.

Чем же мы платим за преимущества систем цифровой связи? Цифровые системы требуют более интенсивной обработки, чем аналоговые. Кроме того, для цифровых необходимо выделение значительной части ресурсов для синхронизации на личных уровнях. Аналоговые системы, наоборот, легче синхронизировать. Еще одним недостатком систем цифровой связи является то, что ухудшение качества носит пороговый характер. Если отношение сигнал/шум падает ниже некоторого порога, качество обслуживания может внезапно измениться от очень хорошего до очень плохого. В аналоговых же системах ухудшение качества происходит более плавно.

Главным же преимуществом цифровой связи по сравнению с аналоговой является то, что цифровая связь позволяет реализовать любое, априорно заданное качество связи, выражающееся в вероятности битовой ошибки.

1.2. Обобщенная структурная схема системы электросвязи

Система электросвязи – это совокупность технических средств и среды распространения, обеспечивающая передачу сообщений [1]. Обобщенная структурная схема систем электросвязи показана на рис. 1.2. Сообщение с выхода источника сообщения (ИС) при помощи преобразователя сообщение – сигнал (Пр. С-С) преобразуется в первичный электрический сигнал, которые не всегда удобно (а иногда невозможно) непосредственно передавать по линии связи.

Поэтому первичные сигналы при помощи передатчика (ПРД) преобразуются в так называемые вторичные сигналы, характери-

стики которых хорошо согласуются с характеристиками линии связи. С вызова линии связи сигналы поступают на вход приемника (ПРМ) и через (Пр. С-С) – потребителю сообщения (ПС).

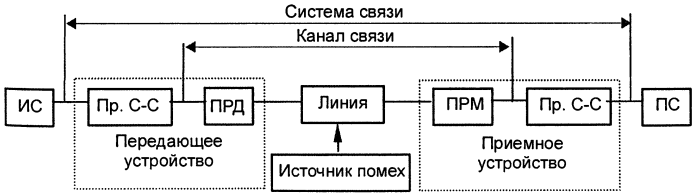


Рис. 1.2. Обобщенная структурная схема системы электросвязи [1]

Канал связи – совокупность технических устройств (преобразователей) и среды распространения, обеспечивающих передачу сигналов на расстояние.

Каналы и системы связи, использующие искусственную среду распространения (металлические провода, оптическое волокно), называются проводными, а каналы и системы связи, в которых сигналы передаются через открытое пространство – радиоканалами и радиосистемами.

1.3. Классификация видов электросвязи

Условная классификация современных видов электросвязи по критерию реального времени и отложенной доставки показана на рис. 1.3. Классификация систем электросвязи по видам передаваемых сообщений и среды распространения приведена на рис. 1.4. Все виды электросвязи по типу передаваемых сообщений могут быть разделены на предназначенные для передачи звуковых и оптических сообщений. В зависимости от назначения сообщений виды электросвязи могут быть классифицированы на предназначенные для передачи сообщений индивидуального и массового характера. В зависимости от временного режима доставки сообщений виды электросвязи могут быть разделены на предназначенные для работы в реальном времени и осуществляющие отложенную доставку сообщений.

Приведенные на рис. 1.3 и 1.4 классификации достаточно условны, поскольку в последнее время наметилась тенденция объединения видов электросвязи в единую интегральную систему на

основе цифровых методов передачи и коммутации для передачи всех видов сообщений.

Рис. 1.3. Классификация видов электросвязи по критерию реального времени и отложенной доставки [1]

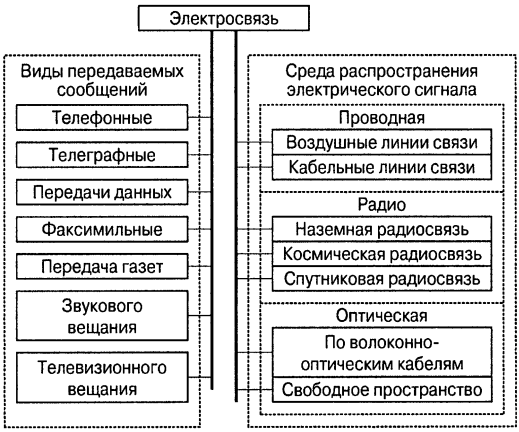


Рис. 1.4. Классификация систем электросвязи по видам передаваемых сообщений и среды распространения [5]

1.4. Архитектура сетей электросвязи

Сеть связи – это совокупность технических средств, обеспечивающих передачу и распределение сообщений. Принципы построения сетей связи зависят от вида передаваемых и распределяемых сообщений.

В сетях с небольшим количеством компьютеров (10–30) чаще всего используется одна из типовых топологий, представленных на рис. 1.5, т.е. физического расположения компьютеров, кабелей и других компонентов – шина, звезда или кольцо. В табл. 1.1 показаны преимущества и недостатки основных сетевых топологий. Все перечисленные топологии обладают свойством однородности, т.е. все компьютеры в такой сети имеют одинаковые права в отношении доступа к другим компьютерам. Это упрощает процедуру наращивания числа компьютеров, облегчает обслуживание и эксплуатацию сети.

Шина (bus) – компьютеры подключены вдоль одного кабеля (сегмента)

Звезда (star) – компьютеры подключены к сегментам кабеля, исходящим из одной точки, или концентратора (hub)

Кольцо (ring) – компьютеры подключены к кабелю, замкнутому

Рис. 1.5. Основные сетевые топологии

Под физической топологией понимается конфигурация связей, образованных отдельными частями кабеля, под логической топологией понимается конфигурация информационных потоков между компьютерами в сети. Во многих случаях физическая и логическая топология сети совпадают. На рис. 1.6 показано несовпадение физической и логической топологий. Сеть, представленная на рис. 1.6, *а* имеет физическую топологию «кольцо». Сеть,

представленная на рис. 1.6, *б* имеет физическую топологию «шина», но логическую топологию «кольцо», так как доступ информационного потока каждого компьютера к шине организован по кольцевому принципу.

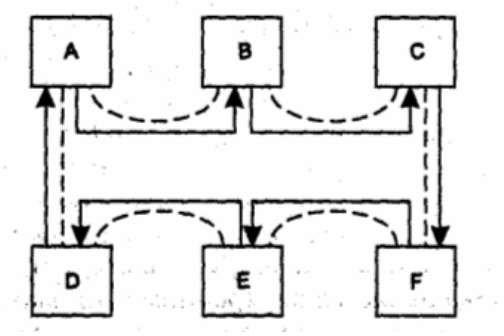
Таблица 1.1

Преимущества и недостатки основных сетевых топологий

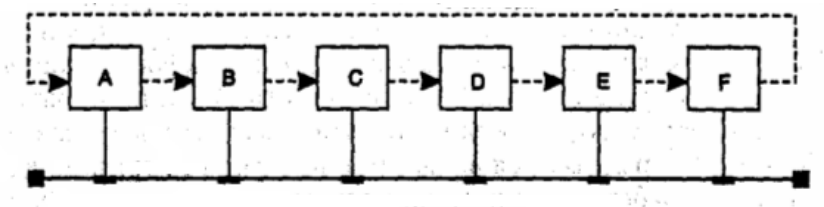
Топология	Преимущества	Недостатки
Шина	Экономный расход кабеля. Сравнительно недорогая и несложная в использовании среда передачи данных. Простота построения. Сеть легко расширяется	При значительных объемах трафика уменьшается пропускная способность сети. Трудно локализовать проблемы. Выход из строя кабеля останавливает работу многих пользователей
Звезда	Легко модифицировать сеть, добавляя новые компьютеры. Централизованный контроль и управление. Выход из строя одного компьютера не влияет на работоспособность сети	Выход из строя центрального узла выводит из строя всю сеть
Кольцо	Все компьютеры имеют равный доступ. Количество пользователей не оказывает значительного влияния на производительность	Выход из строя одного компьютера может вывести из строя всю сеть. Трудно локализовать проблемы. Изменение конфигурации сети требует остановки всей сети

Логическая топология сети определяется методом доступа сетевых устройств к каналу связи. Чаще всего используются три основных метода доступа сетевых устройств к каналу связи: конкурентный, опроса и маркерный.

Конкурентный метод доступа состоит в том, что точка передает данные, как только ей это становится необходимым. При этом необходимо, чтобы все остальные сетевые устройства не передавали никакой информации в этом промежутке времени. К сожалению, выяснилось, что такая ситуация практически невозможна, и система, работающая по этому принципу не достигает максимальной скорости передачи в канале связи. Происходит это потому, что очень часто две или более точек сети передают пакеты почти одновременно. Результатом этого становится столкновение пакетов и искажение передаваемой информации, называемое коллизией. Для предотвращения этой ситуации были разработаны методы регулирования доступа в конкурентных системах.



а



б

Рис. 1.6. Физическая и логическая топология сети [3]

Одним из таких современных методов является метод CSMA/CA (Carrier Sence, Multiple Access/Collision Avoid – анализ несущей, множественный доступ, предотвращение коллизий). Этот метод требует, чтобы каждая станция, желающая передать информацию в канал, предварительно проверила, свободен ли он. Если канал занят, станция обязана выжидать не передавая информации. Если канал свободен, она передает короткое проверочное сообщение, выполняющее функцию детектора коллизии.

Другим широко распространенным методом конкурентного доступа является метод CSMA/CD (Carrier Sence, Multiple Access/Collision Detection – анализ несущей, множественный доступ, обнаружение коллизий), позволяющий быстро обнаружить коллизию. Высокая скорость обнаружения коллизии обеспечивает этому методу наибольшую скорость передачи из всех конкурентных методов доступа.

Метод опроса (поллинга) требует, чтобы из всех точек сети была выделена одна, называемая первичным контроллером, веду-

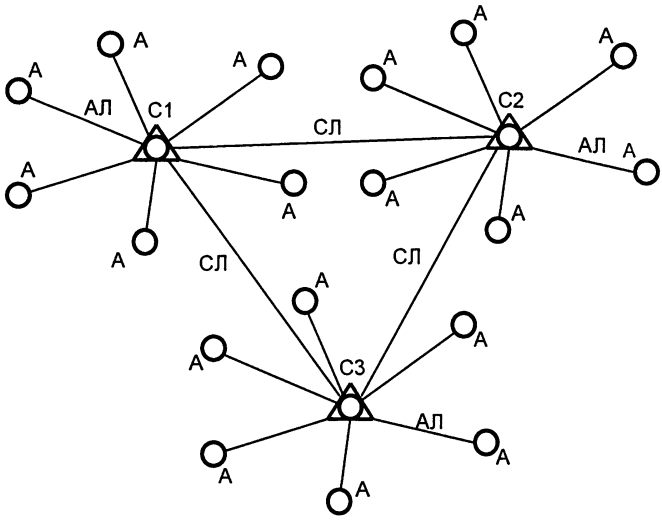
щим устройством или канальным арбитром. Все остальные устройства в сети объявляются вторичными. Арбитр опрашивает в заранее установленном порядке все сетевые устройства на предмет наличия у них информации для передачи. Если потребность в передаче у устройства есть, арбитр предоставляет ему некоторое время для доступа к каналу и обмена информацией. Метод поллинга полностью исключает коллизии, но перегружает канал связи дополнительной информацией и ограничивает вторичные устройства во времени доступа. Наилучшие характеристики этот метод показывает, если все станции через регулярные промежутки времени передают информацию. Сетевая топология типа “звезда” как будто специально создавалась для метода поллинга.

Маркерный метод (Token passing) доступа очень похож на метод поллинга, но без арбитра. Системы с маркером считают активным (т.е. способным передавать информацию) устройство, владеющее маркером (token), который представляет собой некое специальное информационное сообщение и передается от одного устройства к другому. Таким образом все устройства по очереди становятся активными.

Устройства не владеющие маркером, считаются пассивными и передавать информацию в канал связи не могут. Правила передачи токена определяют, от кого устройство может получить токен, сколько времени оно может им владеть и кому должно его передать. Преимущества и недостатки маркерного метода, такие же, как и у метода поллинга. Но маркерный метод имеет важное преимущество, заключающееся в отсутствии центрального арбитра. Поэтому отказ любого сетевого устройства не обязательно приведет к отказу всей сети. Дополнительным его недостатком является относительное усложнение каждого устройства.

Структура телефонных сетей может иметь следующую топологию:

- радиально-узловую (рис. 1.7): такую структуру имеют городские телефонные сети, если емкость сети не превышает 80...90 тыс. абонентов;
- радиально-узловую с узловыми районами (рис. 1.8). Используется при построении телефонных сетей крупных городов.



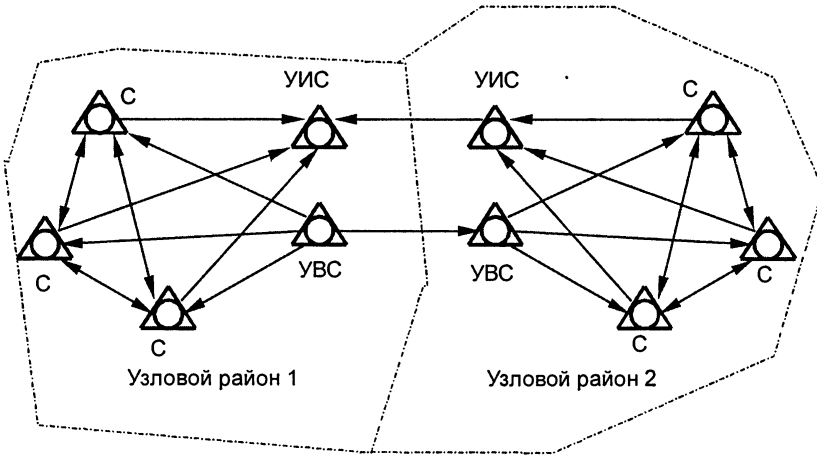


Рис. 1.8 .Топология радиально-узловой сети с узловыми районами [1].
УВС – узел входящих сообщений; УИС – узел исходящих сообщений

Для обеспечения передачи индивидуальных сообщений необходимо связать (соединить) оконечные аппараты абонентов. Электрическая цепь (канал), состоящая из нескольких участков и обеспечивающая передачу сигналов между абонентами, называется

соединительным трактом. Процесс поиска и соединения электрических цепей называется коммутацией каналов. Сеть, обеспечивающая коммутацию каналов, называется сетью с коммутацией каналов (СКК). Узловые станции сети СКК называются станциями коммутации.

При передаче документальных сообщений кроме организации связи с коммутацией каналов возможно осуществлять поэтапную передачу сообщения от узла к узлу. Такой способ передачи получил название коммутации сообщений. Соответственно, сеть, обеспечивающая коммутацию сообщений, называется сетью с коммутацией сообщений (СКС).

Разновидностью СКС является сеть с коммутацией пакетов (СКП). В этом случае полученное от передающего абонента сообщение разбивается на блоки (пакеты) фиксированной длины. Пакеты передаются по сети (необязательно по одному и тому же маршруту) и объединяются в сообщение перед выдачей принимающему абоненту. В свою очередь, СКП подразделяются на дейтаграммные (от англ. *datagram*) и сети виртуальных каналов. В дейтаграммных сетях каждый из пакетов рассматривается как независимый информационный блок, причем пакеты могут проходить через сеть по различным маршрутам. В сетях виртуальных каналов до передачи пакетов через сеть выбирается оптимальный в некотором смысле маршрут, по которому затем передаются пакеты. Последовательность узлов, входящих в выбранный маршрут, образуют собственно виртуальный канал. Узловые станции СКС и СКП называются центрами коммутации сообщений (ЦКС) и пакетов (ЦКП) соответственно.

На практике наиболее широко применяются метод коммутации каналов и метод коммутации пакетов. Телеграфные сети строятся по радиально-узловому принципу с учетом административно-территориального деления страны. Оконечными пунктами телеграфной сети являются либо отделения связи, либо телеграфные абоненты, обладающие телеграфной аппаратурой. Сеть имеет три уровня узловых пунктов: районные, областные и главные. Сеть передачи данных имеет схожую структуру. Сеть факсимильной связи строится на базе телефонной сети. Важнейшими сетями передачи массовых сообщений являются сети вещания. Вещание –

процесс одновременной передачи сообщений общего назначения широкому кругу абонентов при помощи технических средств связи. Вещательная программа – последовательность передачи во времени различных сообщений. Организация вещания включает в себя две задачи: подготовку вещательных программ и доведение программ до абонентов. Основными требованиями к сетям вещания являются: охват вещанием всего населения страны, высокое качество передаваемых программ, надежность и экономичность.

Распределение программ в сети звукового вещания производится по каналам связи, разветвление - на специальных узлах. Сеть каналов звукового вещания строится по радиально-узловому принципу. По способу доведения различают радиовещание и проводное вещание (по специальным проводным линиям или линиям телефонной связи). Распределение программ в сети телевизионного вещания производится по каналам связи, разветвление – на специальных узлах. Сеть ТВ вещания строится по радиально-узловому принципу. Используется два способа доведения ТВ программ: радиовещание с помощью радиотелевизионных передающих станций (РТПС) (эфирное ТВ) и проводное вещание (кабельное ТВ).

Современной разновидностью эфирного ТВ является спутниковое телевизионное вещание с непосредственным приемом на установки, расположенные у абонентов. Закономерность распространения радиоволн метрового и дециметрового диапазона ограничивает зону уверенного приема сигналов.

РПТС пределами оптической (прямой) видимости. Для увеличения зоны уверенного приема необходимо поднимать передающую и приемную антенны. Для типовых РТПС с опорами для антенн высотой 200...350 м радиус зоны обслуживания составляет 60...100 км. Останкинская телебашня при высоте 536 м обеспечивает радиус зоны обслуживания 120...130 км. Передача газет в сети передачи газет обеспечивается факсимильным способом с использованием аналоговой аппаратуры «Газета-2», находящейся в эксплуатации более 20 лет. На территории России имеются 32 пункта приема газет, обычно расположенные непосредственно в типографиях. Пункт разветвления каналов находится на центральной междугородной телефонной станции, поскольку для передачи газет используются телефонные каналы. Газеты передаются еже-

дневно, по 4...5 ч в сутки. В настоящее время происходит спад нагрузки на данную сеть, поскольку применение аналогового способа передачи не удовлетворяет в полной мере требования, предъявляемые полиграфистами. Для передачи газет используются иные сети (Internet и т.п.)

1.5. Системы распределения информации

Одним из важнейших направлений интеграции сетевых технологий является распределенная обработка данных, позволяющая повысить эффективность удовлетворения информационной потребности пользователя и обеспечить гибкость и оперативность принимаемых им решений. Под распределенной обработкой информации понимается комплекс операций с информацией (традиционно описываемый термином «обработка информации»), проводимый на независимых, но связанных между собой вычислительных машинах, предназначенных для выполнения общих задач. Системы распределенной обработки информации (или распределенные вычислительные системы) в виде многомашинных вычислительных комплексов и компьютерных сетей представляют собой одну из наиболее прогрессивных форм организации средств вычислительной техники.

Для достижения целей реальной и эффективной распределенной обработки информации вычислительные системы должны обладать рядом важнейших свойств (атрибутов), основными из которых являются прозрачность, открытость, переносимость приложений, гибкость, масштабируемость, безопасность.

Под *прозрачностью* (transparency) понимают «незаметность» для пользователя внутренней работы системы, что достигается путем сокрытия от пользователя аспектов организации и реализации распределенной обработки информации. Пользователи распределенной системы должны обладать доступом к ресурсам, не задаваясь вопросами о взаимодействии между процессами, о физическом месте размещения ресурсов, о том, какой именно процесс обслуживает тот или иной запрос пользователя.

Под *открытостью* понимают использование синтаксических и семантических правил, основанных на стандартах. Правильный интерфейс обеспечивает возможность правильной совместной рабо-

ты одного произвольного процесса, нуждающегося в интерфейсе, с другим произвольным процессом, представляющим интерфейс.

Переносимость приложений характеризует возможность приложения, выполненного для одной системы, работать в составе другой системы.

Гибкость характеризует легкость конфигурирования системы при изменении состава компонентов.

Масштабируемость, или расширяемость (scalability), означает способность распределенной системы увеличиваться в масштабах (возможность подключения к системе дополнительных компонентов) без влияния на работу существующих приложений и пользователей. Масштабируемость рассматривается по отношению к размеру (подключение дополнительных пользователей и ресурсов), к географическому положению (пространственное расположение пользователей и ресурсов), к административному устройству (управление в административно независимых организациях). Проблемы масштабируемости обычно связаны с «узкими» местами по обслуживанию (один сервер для множества клиентов), по данным (один файл с общей информацией), по алгоритмам (централизованный алгоритм и перегрузка коммуникационной сети).

Применение децентрализованных алгоритмов придает распределенной системе следующие характерные черты:

- никто не обладает полной информацией о системе;
- решения принимаются на основе локальной информации;
- сбой в одном месте не вызывает нарушения работы алгоритма;
- существования единого времени не требуется.

Требование масштабируемости является существенным препятствием на пути распространения систем, реализованных на базе локальных сетей, на уровень сетей глобальных.

Безопасность распределенных систем связана с обеспечением защиты ресурсов от атак со стороны враждебно настроенных пользователей. С целью повышения безопасности распределенные системы должны использовать защищенные каналы передачи данных, разрешать доступ к ресурсам только для авторизованных пользователей и допускать чтение передаваемых по сети данных только получателем.

Прикладное программное обеспечение (ПО) может быть представлено в виде набора из трех частей, обычно называемых слоями (или уровнями):

1) слой (уровень) логики (алгоритмов) представления, или презентационный слой;

2) слой (уровень) бизнес-логики (вычислительных и управляющих алгоритмов), или слой прикладной логики;

3) слой (уровень) логики доступа к данным, или слой управления ресурсами.

Появление классов мини- и микроЭВМ, особенно класса персональных компьютеров (ПК) привело к разработке архитектур с децентрализованной обработкой информации, функционирующих в рамках парадигмы построения сетей, называемой моделью клиент/сервер (client/server model). Клиентами (client) в данном случае считаются вычислительные машины, нуждающиеся в получении тех или иных услуг, а серверами (server) – вычислительные машины, которые эти услуги предоставляют.

Стремление повысить гибкость и масштабируемость многопользовательской распределенной системы привело к архитектурным решениям с тремя звеньями. С середины 1990-х гг. интенсивное практическое внедрение получила трехзвенная архитектура, которая поддерживает концепцию «клиент/сервер», но разделяет систему по функциональным границам между тремя слоями: логикой представления, бизнес-логикой и логикой доступа к данным (рис. 1.9). В 3-звенной архитектуре появилось дополнительное звено (так называемый «сервер приложений»), целиком предназначенное для реализации бизнес-логики. Трехзвенная архитектура позволила более явно отделить прикладную логику от пользовательского интерфейса и уровня баз данных. Так как в трехзвенной архитектуре под бизнес-логику обычно выделяется отдельная машина-сервер, то это повышает гибкость распределенной системы (поскольку все три слоя отделены друг от друга, то становится возможным относительно легкое изменение либо перемещение любого из них без существенного влияния на остальные слои).

Характерным примером использования трехзвенной архитектуры являются веб-приложения, которые реализуются посредством трех компонентов: веб-браузера клиента, веб-сервера и ре-

ляционной базы данных. Клиенты в этом случае не поддерживают постоянного соединения с базой данных, а обмениваются информацией со средним звеном только тогда, когда это необходимо. В то же время процесс среднего звена поддерживает всего несколько активных соединений с базой данных, но использует их многократно. Поэтому процессы в среднем звене могут предоставлять обслуживание теоретически неограниченному числу клиентов.

Рис. 1.9. Вариант построения 3-звенной архитектуры клиент/сервер

Дальнейшее увеличение гибкости и масштабируемости распределенных систем достигается переходом к многозвенным архитектурам, включающим более чем три звена, и соответствующим распределением слоев прикладного программного обеспечения (и их частей) по разным машинам. Например, слой логики доступа к данным может быть разделен на СУБД и собственно базу данных, хранимую на отдельном устройстве (или группе устройств). Такая конфигурация отражает реализацию распределенной СУБД (рис. 1.10).

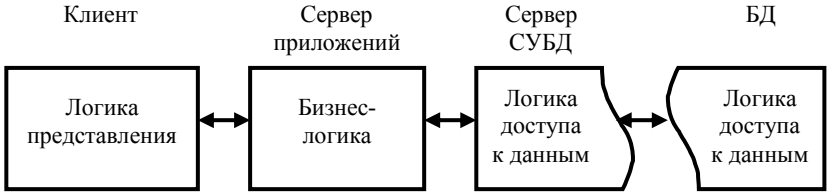


Рис. 1.10. Вариант построения 4-звенной архитектуры клиент/сервер

Перенос основных операций приложения на отдельный уровень позволяет с максимальной эффективностью распределить нагрузку на аппаратные устройства (трехзвенная модель на самом деле может быть многозвенной с разделением нагрузки на несколько серверов приложений) и обеспечивает безболезненное наращивание как функциональности приложения, так и числа обслуживаемых пользователей.

Синхронный режим коммуникаций между двумя прикладными модулями (клиентом и сервером) поддерживает спецификация удаленного вызова процедур (remote procedure call – RPC). Для установки связи, передачи вызова и возврата результата клиентский и серверный процессы обращаются к специальным компонентам – клиентскому и серверному переходникам, или заглушкам (от англ. *stub* – заглушка, переходник). Эти stub-процедуры не реализуют никакой прикладной логики и предназначены только для организации взаимодействия удаленных (в общем случае) прикладных модулей. Каждая функция на сервере, которая может быть вызвана удаленным клиентом, должна иметь такой процесс.

При вызове клиентом удаленной процедуры вначале выполняется локальный вызов процедуры, являющейся частью клиентского переходника. Локальный вызов вместе с параметрами передается клиентскому переходнику. При этом с помощью специального языка описания интерфейсов (Interface Definition Language – IDL) производится определение интерфейса процедуры, то есть описание параметров процедуры, передаваемых ей до выполнения RPC и возвращаемых после завершения RPC. Затем это описание транслируется и производится упаковка данных в формат сообщения – маршалинг (marshaling). Клиентский переходник вызывает локальную операционную систему, которая пересылает сообщение удаленной операционной системе сервера. Удаленная операционная система передает сообщение серверному переходнику, реализующему серверную часть вызова и состоящему из программ получения запроса от клиента, форматирования данных (демаршалинг), вызова реальной процедуры (реализованной на сервере) и возврата результатов клиенту. Клиент блокируется и ждет ответа, а на сервере запускается серверный переходник, преобразующий сообщение в параметры локальной процедуры. Сервер видит вызов как прямое обращение к его локальной процедуре с нужными параметрами, выполняет вызов и передает результаты серверному переходнику. Серверный переходник форматирует результаты работы процедуры в сообщение для клиента и вызывает локальную операционную систему сервера. Операционная система сервера пересылает сообщение операционной системе клиента. Клиент выводится из состояния ожидания, его операционная система при-

нимает сообщение и направляет его клиентскому переходнику, который извлекает результаты из сообщения, передает их клиенту и возвращает клиенту управление.

Принципиальная схема организации удаленного вызова процедур представлена на рис. 1.11.

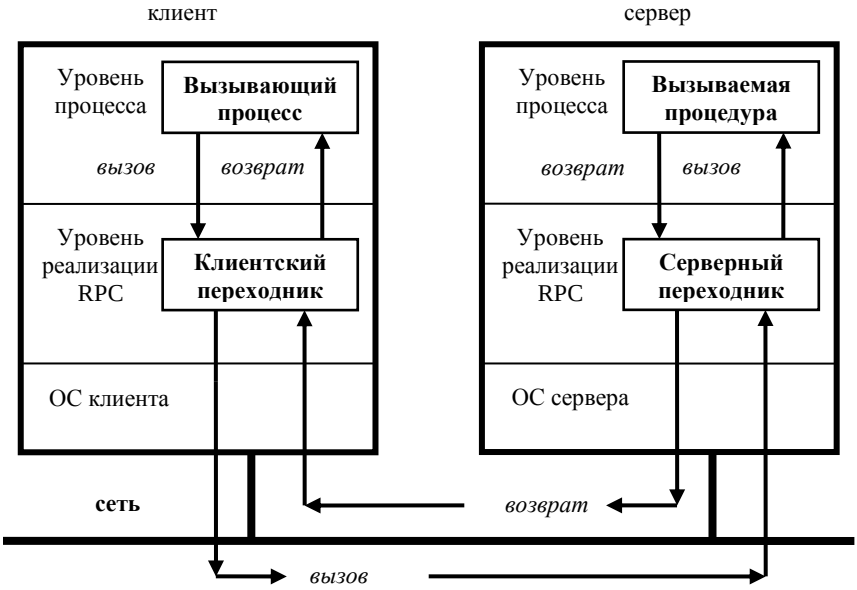


Рис. 1.11. Принципиальная схема организации удаленного вызова процедур

Объектно-ориентированный подход к организации распределенной обработки информации способствует значительному усовершенствованию механизмов организации распределенной обработки информации. Важнейшим свойством объектов (object) является то, что они позволяют скрыть свое внутреннее строение посредством наличия строго определенного интерфейса. Поэтому при замене или изменении объектов интерфейс может оставаться неизмененным. Вследствие этого возможно относительно легкое распространение и применение принципов RPC к удаленным объектам.

Объекты инкапсулируют данные, называемые состоянием (state), и операции над этими данными, называемые методами (method). Для доступа или манипулирования состоянием объекта

нужно использовать методы, обращение к которым осуществляется через интерфейсы. Объект может реализовывать множество интерфейсов, а для данного описания интерфейса может существовать несколько объектов, предоставляющих его реализацию.

Для распределенных систем разделение на интерфейсы и объекты позволяет помещать интерфейсы на одну вычислительную машину, а сами объекты – на другую. Принципиальная схема организации механизма удаленных объектов представлена на рис. 1.12. При выполнении клиентом «привязки» к распределенному объекту в адресное пространство клиента загружается реализация интерфейса объекта, называемая заместителем (proxy). Заместитель клиента аналогичен клиентскому переходнику в механизме RPC. Он выполняет маршалинг[1] параметров в сообщения при обращении к методам, демаршалинг данных из ответных сообщений с результатами обращения к методам, передачу результатов клиенту. Сами же объекты находятся на сервере и предоставляют необходимые клиентской системе интерфейсы.

Входящий запрос на обращение к методу сначала попадают в так называемый серверный каркас, или скелетон (skeleton), аналогичный серверному переходнику в RPC. Серверный каркас преобразует входящий запрос в обращение к методу через интерфейс объекта, находящегося на сервере. Каркас также отвечает за маршалинг параметров в ответных сообщениях и их пересылку заместителю клиента. Если объект физически распределен по нескольким вычислительным машинам, то это скрывается от клиентов за интерфейсами объектов.

Форма существования объектов в распределенных системах чаще всего соответствует объектам выбранного объектно-ориентированного языка программирования. Такие объекты представляют собой так называемые объекты времени компиляции. Использование этих объектов в распределенных системах обычно значительно упрощает создание распределенных приложений. Недостатком использования таких объектов является их зависимость от конкретного языка программирования. Альтернатива состоит в создании распределенных объектов непосредственно во время выпол-

[1] Маршалинг – процесс преобразования представления объекта в памяти в формат данных, пригодный для хранения или передачи.

нения. При этом подходе распределенные приложения не зависят от конкретного языка программирования и они могут быть созданы из объектов, написанных на различных языках. При работе с такими объектами времени исполнения для превращения конкретной программной реализации в объект, методы которого будут доступны с удаленной вычислительной системы, используется адаптер объектов, служащий оболочкой этой реализации с целью придания ей реализации видимости объекта.

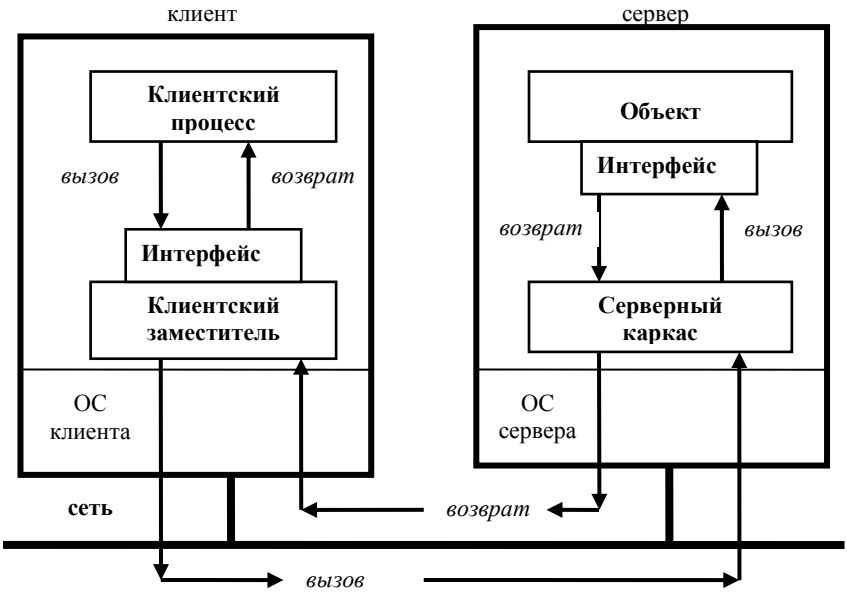


Рис. 1.12. Принципиальная схема организации механизма удаленных объектов

Объекты подразделяются на сохранные (persistent) и транзитные, или нерезидентные (transient). Сохранный объект не зависит от своего текущего сервера и продолжает существовать, даже не находясь постоянно в адресном пространстве серверного процесса. Сервер, управляющий таким объектом, может сохранить состояние объекта во вспомогательном запоминающем устройстве и прекратить свою работу, а затем после запуска снова прочитать состояние сохранного объекта из запоминающего устройства в свое адресное пространство и приступить к обработке обращений к объ-

екту. Нерезидентный объект существует, пока им управляет сервер. Если сервер завершает работу, то такой объект прекращает существовать.

Системы, поддерживающие распределенные объекты, обычно предоставляют ссылки на объекты, уникальные в пределах системы. Такие ссылки могут свободно передаваться между процессами, запущенными на различных вычислительных машинах, например, как параметры обращения к методу. Перед обращением к методу объекта по его ссылке сначала выполняется привязка (явная или неявная), в результате создается заместитель объекта, реализующий интерфейс с методами, к которым обращается процесс. Для выполнения привязки система находит сервер, управляющий объектом, и помещает заместитель объекта в адресное пространство клиента. В результате обеспечения таким образом непрозрачности реализации ссылок на объекты (сокрытия истинной реализации ссылок) достигается повышенная прозрачность распределения по сравнению с традиционным механизмом RPC.

Клиент, осуществив связь с объектом, может через заместителя объекта обратиться к методам объекта. Таким образом при объектно-ориентированном подходе к распределенной обработке информации реализуется механизм так называемого удаленного обращения к методам (Remote Method Invocation – RMI).

Обращение к методу может быть статическим (интерфейсы известны при разработке) или динамическим (параметры собираются перед обращением к методу). На основе механизма RMI разработаны множество стандартов и программных реализаций объектно-ориентированных платформ промежуточного ПО, поддерживающих эффективную распределенную обработку информации.

Для реализации распределенной обработки информации на основе транзакционного взаимодействия применяются мониторы обработки транзакций TPM (Transaction Processing Monitor), или транзакционные мониторы, разработанные для обеспечения надежного мультиплексного доступа к большому количеству ресурсов для большого количества параллельных пользователей. Механизм TPM – наиболее старая технология реализации распределенных систем, которая появилась в 1970-х гг. в среде больших универсальных вычислительных машин для выполнения банков-

ских, страховых и других высококритичных вычислений. Транзакционные мониторы представляют одну из самых сложных и многофункциональных технологий в мире промежуточного ПО. Они предназначены для автоматизированной поддержки приложений, оформленных в виде последовательности транзакций. Каждая транзакция представляет собой законченный блок обращений к ресурсу (чаще всего – к базе данных) и некоторых действий над ним. Корректное выполнение транзакции должно гарантировать выполнение четырех условий – так называемых свойств ACID (Atomicity, Consistency, Isolation, Durability):

• Atomicity (атомарность) – операции транзакции образуют неразделимый, атомарный блок («unit of work» – «единица работы») с определенным началом и концом. Этот блок либо выполняется от начала до конца, либо не выполняется вообще. Если в процессе выполнения транзакции произошел сбой, происходит откат к исходному состоянию.

• Consistency (согласованность) – по завершении транзакции все задействованные ресурсы находятся в согласованном состоянии.

• Isolation (изолированность) – одновременный доступ транзакций различных приложений к разделяемым ресурсам координируется таким образом, чтобы эти транзакции не влияли друг на друга.

• Durability (долговременность) – все модификации ресурсов в процессе выполнения транзакции будут долговременными.

В системе без TPM обеспечение свойств ACID берут на себя серверы распределенной базы данных на основе протокола 2PC – (two-Phase Commit – двухфазное подтверждение). Протокол 2PC описывает двухфазный процесс, в котором перед началом распределенной транзакции все системы опрашиваются о готовности выполнить необходимые действия. Если каждый из серверов баз данных дает утвердительный ответ, транзакция выполняется на всех задействованных источниках данных. Если хотя бы в одном месте происходит какой-либо сбой, будет выполнен откат всех частей транзакции. Однако в системе с распределенными базами данных выполнение протокола 2PC можно гарантировать только в том случае, если все источники данных принадлежат одному поставщику. Поэтому для сложной распределенной среды, которая обслуживает тысячи клиентских мест и работает с десятками раз-

нородных источников данных, требуется использование механизма монитора обработки транзакций. Транзакционные мониторы способны координировать и управлять транзакциями, которые обращаются к серверам баз данных от различных поставщиков благодаря тому, что большинство этих продуктов помимо протокола 2PC поддерживают транзакционную архитектуру общего стандарта распределенной обработки транзакций DTP (Distributed Transaction Processing) для данной категории промежуточного программного обеспечения MW (middleware). Архитектура DTP поддерживает совместное использование ресурсов (файлов или баз данных) множеством программ, обеспечивая управление доступом, гарантирующее согласованность системы в целом. Транзакционный монитор поддерживает выполнение распределенных транзакций на основе транзакционного RPC. Традиционные вызовы удаленных процедур независимы. Если вызывается сервер, который, выполняя удаленную процедуру, вызывает другой сервер, нет способа отличить, где произошла ошибка – в первом или втором сервере. Семантика же транзакционного вызова такова: если группа вызовов процедур внутри транзакции подтверждается (успешно завершается), имеются гарантии, что каждый из вызовов завершился успешно. Если возникло прерывание выполнения группы вызовов, общий эффект будет таким, как если бы ни один из вызовов не выполнялся. Процедурные вызовы, заключенные в транзакционные скобки, рассматриваются как единое целое, а инфраструктура RPC гарантирует их атомарность.

Функциональность транзакционных мониторов достаточна для разработки, выполнения, управления и сопровождения транзакционных информационных распределенных систем. Эта функциональность включает в себя язык IDL, именование, безопасность и аутентификацию, компиляторы переходников, поддержку работы с транзакционными вызовами (транзакционные скобки, обратные вызовы), ведение журнальных записей, восстановление, блокировку, управление процессами и приоритетами, балансировку нагрузки, репликацию, управление ресурсами.

Архитектура транзакционных мониторов включает клиентский интерфейсный компонент и поддержку прямого доступа через терминал. Программный поток исполняет процедуры, напи-

санные на языке данного монитора, которые содержат операции над именованными логическими ресурсами. Маршрутизатор сопоставляет операции и вызовы, которые могут относиться к ресурсам (например, базе данных) или локальным службам самого монитора. В состав маршрутизатора входит специализированная база данных, содержащая определения соответствий между именами логических ресурсов и физическими устройствами. При изменении системы администратор исправляет это соответствие: клиентское приложение модифицировать не требуется – клиент знает только логические имена. Взаимодействие с ресурсами осуществляется через менеджера взаимодействия (например, систему сообщений, обеспечивающую откат и гарантию доставки). Разнородность ресурсов, связанных с монитором, скрывают оболочки. Выполнение транзакции проводит менеджер транзакций, исполняющий протокол 2PC и гарантирующий транзакционные свойства процедур, исполняемых транзакционным монитором.

Примитивы транзакционных скобок есть обращения к клиентскому или серверному переходнику. При работе клиентский переходник, открывающей скобки, получает от менеджера транзакций имя транзакции и создает контекст последовательности вызовов. При обращении клиента к одному из серверов серверный переходник извлечет контекст, уведомит менеджера транзакций, что стал участником транзакции и преобразует удаленный вызов в локальный. При выполнении закрывающей скобки клиент обращается к менеджеру транзакций, тот инициирует протокол 2PC со всеми серверами и принимает решение о завершении транзакции или об отказе. После завершения 2PC менеджер транзакций сообщает об этом клиентскому переходнику, который возвращает управление программе клиента, показывая, как завершилась транзакция. Полезность транзакционных мониторов и последующее появление брокеров объектов привело к построению объектно-ориентированных транзакционных мониторов или объектных мониторов транзакций OTM (object transaction monitor). Системы OTM берут лучшее из двух технологий. Они поддерживают объектную модель и при этом обеспечивают целостность распределенных транзакций на множестве разнородных источников данных, масштабируемость, надежность и высокую производительность – основные ка-

чества, присущие транзакционным мониторам. Кроме того, ORB сами по себе, как правило, не реализуют возможностей оптимального распределения нагрузки и восстановления при сбоях. Эти важнейшие службы высококритичной распределенной среды добавляются путем интеграции с технологией транзакционных мониторов. При этом OTM способны упростить развертывание транзакционных приложений. TPM – одна из самых сложных в реализации категория MW, а строгая объектная архитектурная надстройка позволяет скрыть ее сложности от разработчика. Многие OTM также интегрируются с сервисами очередей сообщений, поддерживая тем самым асинхронную модель коммуникаций.

Системы OTM отличаются от других средств интеграции разных категорий MW тем, что все необходимые свойства TPM и ORB предоставляются в одном продукте. Многие представители категории OTM базируются на компонентной модели CORBA/Java (эти две технологии построения распределенных компонентных сред все более тесно интегрируются друг с другом) и стандартной транзакционной архитектуре DTP, поддерживая при необходимости работу с объектами компонентной объектной модели DCOM (Distributed Component Object Model).

Так, консорциумом OMG была разработана спецификация объектного сервера транзакций OTS (Object Transaction Server), цель которой – унифицировать объединенную функциональность мониторов транзакций и брокеров объектных запросов. Это расширение CORBA нашло свое отражение в спецификации JTS для Java (Java Transaction Service – служба транзакций Java).

Рассмотрим распределенную обработку информации на основе технологий обмена сообщениями. Промежуточное ПО, ориентированное на обмен сообщениями (Message Oriented Middleware – MOM), относительно молодая и динамично развивающаяся категория систем промежуточного слоя. Согласно этой модели приложения обмениваются байтовыми строками – сообщениями, обращаясь к API-интерфейсу системы MOM, который изолирует их от непосредственного взаимодействия с ОС и сетевыми протоколами. В отличие от ранее рассмотренных моделей промежуточного ПО, MOM реализует, скорее, равноправные (peer-to-peer), чем подчиненные (клиент-сервер) отношения между модулями приложений. MOM можно считать и наиболее гибкой категорией MW, поскольк-

ку системы этого типа поддерживают как синхронные, так и асинхронные коммуникации на базе сетевых протоколов с установлением и без установления соединения. По способу обмена сообщениями все продукты МОМ могут быть разделены на три подгруппы систем: 1) с передачей сообщений, 2) с очередями сообщений, 3) типа публикация/подписка.

Системы с передачей сообщений (Message Passing – MP) обеспечивают непосредственное взаимодействие приложений друг с другом путем отправки и получения сообщения. Для этого между программными модулями устанавливается логическое соединение. Отсюда следует, что данное решение не подходит для слабо связанных программ, работающих в независимом временном режиме, например, приложений, определенные компоненты которых обслуживают мобильных пользователей. Обмен сообщениями может происходить в синхронном и асинхронном режиме. Кроме средства непосредственных коммуникаций, системы этого типа могут обеспечивать дополнительные службы промежуточного слоя, например, службу каталогов.

Многочисленная часть МОМ-систем реализует асинхронный механизм очередей сообщений (Message Queuing – MQ). В отличие от передачи сообщений, эта модель межпрограммного взаимодействия не требует поддержки непосредственного соединения одного прикладного модуля с другим, но гарантирует доставку сообщения даже в том случае, если программа-адресат в данный момент не доступна. Программа-отправитель передает сообщение MQ-системе и продолжает выполнение. Сообщение помещается в локальное промежуточное хранилище – очередь сообщений, размещенную в оперативной памяти или на диске, откуда оно может быть немедленно или через какое-то время передано программе-получателю. Таким образом, приложения, которые используют эту модель связи, могут работать практически независимо друг от друга без временной синхронизации. Поэтому механизм очередей сообщений является удачным решением для приложений, предназначенных мобильным пользователям, для реализации потоков работ и поддержки приложений в глобальных сетях с медленными и не очень надежными соединениями.

Большинство MQ-систем включает менеджер очереди (Queue Manager), который управляет локальными очередями, гарантирует передачу сообщений нужному адресату и, взаимодействуя с менеджерами на других узлах, следит за сетевым маршрутом передачи сообщения, выбирая альтернативный путь, если по тем или иным причинам основной оказывается недоступен. Принципиальная схема организации механизма очередей сообщений представлена на рис. 1.13.

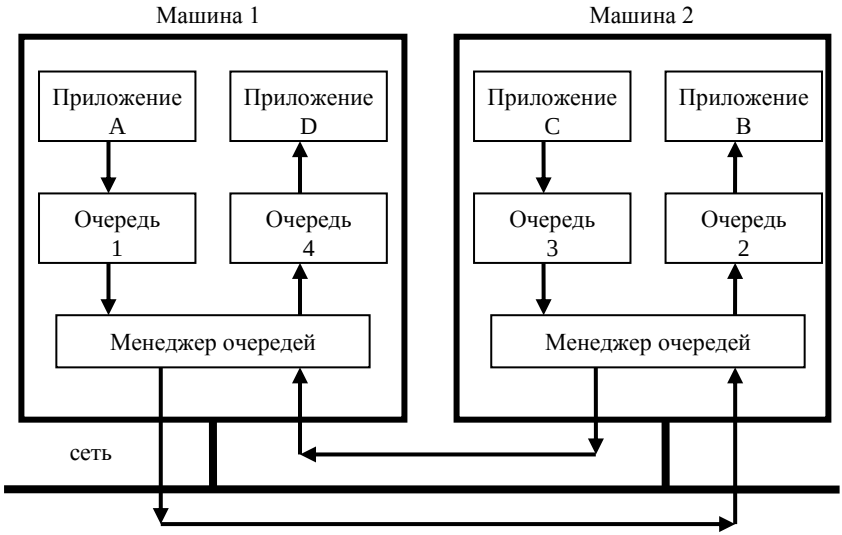


Рис. 1.13. Принципиальная схема организации механизма очередей сообщений

Очереди сообщений могут быть долговременными (persistent) или нет. В последнем случае, если произойдет сбой в работе менеджера очередей, то сообщения в очереди будут потеряны. Если поддерживается долговременная очередь, сообщения будут восстановлены после перезапуска менеджера. Этот вариант, безусловно, является предпочтительным для большинства ответственных приложений. Еще одной отличительной чертой промежуточных систем на основе очередей сообщений является обеспечение одного из трех уровней «качества обслуживания»:

• надежная доставка сообщений (reliable message delivery) – система гарантирует, что в процессе обмена сообщениями ни один сетевой пакет не будет потерян;

• гарантированная доставка сообщений (guaranteed message delivery) – сообщение доставляется адресату немедленно или через заданный промежуток времени, не превышающий определенного значения (в случае, если сеть в данный момент не доступна);

• застрахованная доставка сообщений (assured message delivery) – каждое сообщение доставляется только один раз.

Промежуточные системы на базе очередей сообщений могут поддерживать обработку транзакций, разбивая большие синхронные транзакции, которые модифицируют несколько распределенных, разнородных баз данных, на меньшие асинхронные транзакции, взаимодействующие друг с другом посредством очередей. Таким образом MOM-системы могут использоваться как более производительный асинхронный коммуникационный уровень для мониторов обработки транзакций TPM. Очереди сообщений представляют собой мощный, гибкий и в то же время простой механизм межпрограммного взаимодействия. По существу, этот механизм близок к другой парадигме разработки приложений – созданию программ, управляемых событиями. Событие одного приложения (представленное сообщением) вызывает определенное действие в другом. И такая модель наиболее близка к реальному взаимодействию процессов в бизнесе реальных компаний. Представителями программных продуктов, построенных на базе очередей сообщений, являются системы MQSeries компании IBM, MSMQ (Microsoft Message Queuing Server) компании Microsoft, MessageQ компании BEA, dbQ компании Sybase.

Еще одна модель обмена сообщениями – модель публикации/подписки (publlsh&subscribe) – имеет определенные перспективы для создания гибких, управляемых событиями приложений. Одно приложение публикует информацию в сети, а другое подписывается для получения данных по интересующей его теме. Взаимодействующие таким способом приложения полностью независимы друг от друга и могут ничего не знать о существовании, физическом размещении и состоянии друг друга. Это открывает путь к динамической реконфигурации всей распределенной системы, добавлению и произвольному изменению любых клиентов и серверов без прерывания их работы и полной изоляции прикладных компонентов от любых аспектов реализации других частей систе-

мы. В конечном счете, это означает возможность эффективной интеграции различных бизнес-приложений в единое корпоративное решение.Характерным примером распределенной системы на основе модели публикации/подписки является система TIB/Rendezvous компании TIBCO. Ключевой механизм, лежащий в основе системы TIB/Rendezvous, – это адресация по теме (subject-based addressing). При таком подходе процесс, который собирается посылать сообщение, не может определить точное место назначения. Вместо этого он именует сообщение названием темы (subject name), после чего посылает его в коммуникационную систему для пересылки по сети. Получатели, в свою очередь, не выясняют, от каких процессов они собираются получать сообщения. Вместо этого они сообщают коммуникационной системе, какие темы их интересуют. Коммуникационная система гарантирует, что получателю будут доставлены только те сообщения, которые несут данные по теме, интересующей получателя. Отправка сообщения методом адресации по теме также называется публикацией (publishing). Чтобы получить сообщение по определенной теме, процесс должен подписаться на эту тему. Принципиальная схема организации системы публикации/подписки, реализованная в TIB/Rendezvous, показана на рис. 1.14.

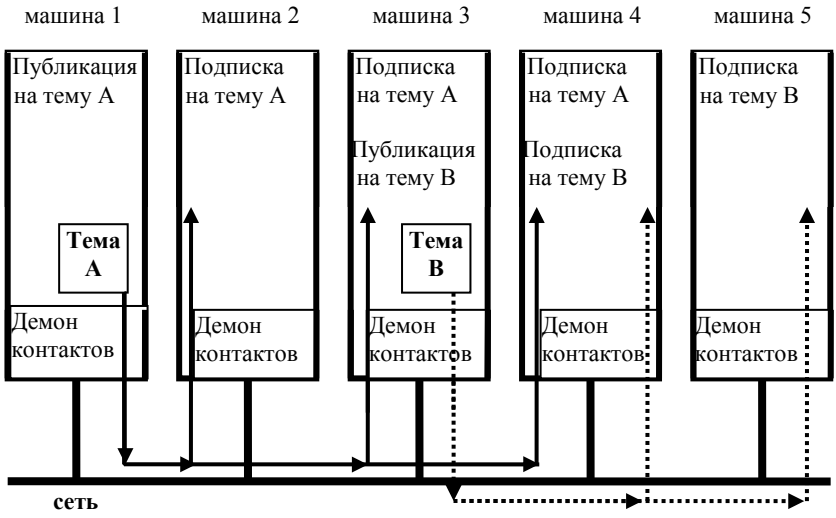


Рис. 1.14. Принципиальная схема организации системы публикации/подписки

Основой архитектуры системы TIB/Rendezvous является сеть с поддержкой групповой рассылки, хотя по возможности допускается использование более эффективных средств связи (так, например, если известно точное местонахождение подписчика, обычно выполняется сквозная передача сообщений). На каждом узле этой сети работает демон контактов (rendezvous daemon), который отвечает за то, чтобы сообщения отсылались и получались в соответствии с темой. Когда сообщение публикуется, демон контактов осуществляет его групповую рассылку всем узлам сети. Обычно групповая рассылка реализуется средствами базовой сети, такими как групповая рассылка по IP-адресам или аппаратная широковещательная рассылка.

Процессы, подписываясь на определенную тему, передают свою подписку локальному демону. Демон создает таблицу пар (процесс, тема) и при доставке сообщения с определенной темой просто просматривает эту таблицу в поисках локальных подписчиков, пересылая его каждому из процессов. Если на эту тему на данном узле никто не подписался, сообщение немедленно уничтожается.

Чтобы система могла вырасти до размера больших сетей, таких как глобальные сети, используются также маршрутизирующие демоны контактов (rendezvous router daemons). Обычно каждая локальная сеть имеет одного маршрутизирующего демона контактов. Этот демон связывается с маршрутизирующим демоном другой удаленной сети. Маршрутизирующие демоны образуют сквозную оверлейную сеть (overlay network), в которой маршрутизаторы соединены между собой попарно соединениями TCP. Вторичная сеть – это сеть маршрутизаторов прикладного уровня. Каждый маршрутизатор знает топологию вторичной сети и вычисляет дерево групповой рассылки для публикации сообщений в других сетях. Маршрутизаторы рассылают только те сообщения, которые публикуются в их локальной сети. Сообщения из других сетей пересылаются по дереву групповой рассылки той сети, из которой они первоначально исходили. В целях повышения производительности всякий раз при публикации сообщения оно доставляется только в те удаленные сети, которые были сконфигурированы на прием подобных сообщений и имеют текущих подписчиков этих сообщений.

Технологической основой для всех сред обмена сообщениями нового поколения стала спецификация JMS (Java Message Service – служба сообщений Java), в деталях определяющая, как взаимодействуют клиенты и серверы в среде асинхронных сообщений. К числу достоинств JMS относится то, что она соответствует современным представлениям о взаимодействии приложений и не требует специальных знаний и доступна для любого программиста, работающего на языке Java. Этими качествами она заметно отличается от инструментария MQSeries, где необходима специальная подготовка. Еще один стимул для рождения нового поколения MOM – появление расширяемого языка разметки данных XML (eXtensible Markup Language – «расширяемый язык разметки») для Internet-приложений, позволяющего одним приложениям «понимать» другие.

Спецификация JMS построена на основе топологии «ступицы и колеса» (hub-and-spoke), в которой все приложения подключаются к центральному процессу, называемому сервером сообщений (message server). Он отвечает за корректность маршрутизации сообщений, аутентификацию и авторизацию пользователей. Сами приложения рассматриваются как клиенты – они могут быть передатчиками и/или приемниками. При этом обеспечивается такой API-интерфейс на базе Java, который позволяет разработчикам писать клиентские приложения, не заботясь о том, какое конкретно программное обеспечение MOM будет использоваться. Спецификация только определяет доступ к корпоративной системе обмена сообщениями, а каждый производитель ПО, опирающийся на JMS, самостоятельно разрабатывает инструменты для администрирования среды обмена сообщениями. JMS стала основой целого направления программных продуктов категории MOM, таких как MQ Express компании Talarian, SonicMQ компании Progress Software, Bus компании Softwired, FioranoMQ компании Fiorano Software и других.

Основным подходом, который используется в распределенных системах на основе моделей согласования, является отделение собственно вычислительных процессов от механизмов их согласования. Если рассматривать распределенную систему как набор процессов (возможно, многопоточных), то вычислительная часть

распределенной системы образована группой процессов, каждый из которых осуществляет конкретные вычислительные операции, причем эти операции в принципе могут выполняться независимо от других процессов. В этой модели согласующая часть распределенной системы поддерживает все взаимодействие между процессами и организует их взаимную кооперацию. Она образует тот «клей», который связывает воедино деятельность, выполняемую разными процессами. В распределенных системах согласования основное внимание уделяется согласованию процессов. В том случае, если процессы обладают связностью ссылок и времени, согласование осуществляется напрямую и имеет название прямого согласования (direct coordination). Связность ссылок обычно имеет вид явной идентификации собеседника в процессе взаимодействия. Так, например, процесс может взаимодействовать с другим процессом только в том случае, если он знает идентификатор процесса, с которым хочет обменяться информацией. Временная связность означает, что оба взаимодействующих друг с другом процесса активны одновременно. Такая связность имеет место при нерезидентной связи на основе сообщений.

Другой тип согласования наблюдается в том случае, если процессы не связаны по времени, но связаны по ссылкам. Такой тип согласования называют согласованием через почтовый ящик (mailbox coordination). В этом случае для взаимодействия не нужно, чтобы два взаимодействующих друг с другом процесса выполнялись одновременно. Вместо этого взаимодействие происходит путем посылки сообщений в почтовый ящик, может быть, используемый совместно. При этом необходимо явно указать адрес почтового ящика, в котором должны храниться сообщения. Это и есть ссылочная связность.

Комбинация связности по времени и несвязности по ссылкам образует группу моделей согласования на встрече (meeting-oriented coordination). В несвязной по ссылкам системе процессы не имеют полной информации друг о друге. Другими словами, когда процесс хочет согласовать свою деятельность с другими процессами, он не может обратиться к ним напрямую. Взамен используется метафора встречи, на которой собираются процессы, чтобы скоординировать свою деятельность. Модель предполагает, что процессы, участвующие во встрече, выполняются одновременно.

Наиболее распространенный вариант согласования – это сочетание несвязных по времени и по ссылкам процессов. Этот вариант представлен генеративной связью (generative communication), которая впервые была реализована в программной системе Linda. Основная идея генеративной связи состоит в том, что набор независимых процессов может использовать разделяемое сохранное пространство данных, организуемое с помощью кортежей. Кортежи – это именованные записи, содержащие несколько (но, возможно, и ни одного) типизованных полей. Процесс может помещать в разделяемое пространство данных записи любого типа (то есть генерировать связующие записи). Для разделения кортежей в соответствии с информацией, которая в них содержится, достаточно их имен. Разделяемые пространства имен реализуют механизмы ассоциативного поиска кортежей. Другими словами, когда процесс хочет извлечь кортеж из пространства данных, ему достаточно определить значения полей, которые его интересуют. Любой кортеж, удовлетворяющий описанию, будет извлечен из пространства данных и передан процессу. Если ничего найдено не будет, процесс может заблокироваться до прихода очередного кортежа.

Примером системы согласования является система Jini («джини») компании Sun Microsystems. Отнесение Jini к системам согласования основано в первую очередь на том, что эта система способна поддерживать генеративную связь при помощи Linda-подобной службы под названием JavaSpace. Однако существует множество служб и средств, которые делают Jini больше, чем просто системой согласования. Jini – это распределенная система, состоящая из разных, но взаимосвязанных элементов. Она жестко привязана к языку программирования Java, хотя многие из ее принципов равно могут быть реализованы и при помощи других языков. Важной частью системы является модель согласования генеративной связи. Jini обеспечивает как временную, так и ссылочную несвязность процессов при помощи системы согласования JavaSpace. JavaSpace – это разделяемое пространство данных, в котором хранятся кортежи. Кортежи представляют собой типизованные наборы ссылок на объекты Java. В одной системе Jini могут сосуществовать несколько пространств JavaSpace.

Архитектура системы Jini может быть представлена в виде трех уровней. Самый нижний уровень образует инфраструктура.

На этом уровне располагаются базовые механизмы Jini, в том числе и те, которые поддерживают взаимодействие посредством обращений RMI языка Java. Службы предоставляются как обычными процессами, так и устройствами, на которых программное обеспечение Jini (в том числе и виртуальная машина Java) выполняться не может. Поэтому регистрирующие и поисковые службы также относятся к инфраструктуре Jini. Второй уровень образуют средства общего назначения, которые дополняют базовую инфраструктуру и могут быть использованы для более эффективной реализации служб. В число этих средств входят подсистемы событий и уведомлений, средства аренды ресурсов и описания стандартных интерфейсов транзакций. Самый верхний уровень состоит из клиентов и служб. В противоположность остальным двум уровням Jini не определяет состав этого уровня однозначным образом. Актуальная реализация системы поддерживает несколько служб верхнего уровня, среди которых сервер JavaSpace и менеджер транзакций, реализующий интерфейсы транзакций Jini. Программам верхнего уровня, кроме того, нередко разрешается напрямую использовать механизмы инфраструктуры Jini.

Кроме генеративной связи, присущей модели JavaSpace, в число механизмов взаимодействия Jini входит простая подсистема событий и уведомлений. Модель событий Jini относительно проста. Если в рамках объекта происходит событие, которое может быть интересно клиенту, клиенту разрешается зарегистрировать себя на этом объекте. Когда факт наступления события будет зафиксирован, то есть когда событие произойдет, объект уведомит об этом зарегистрированного клиента. С другой стороны, клиент может потребовать от объекта, чтобы тот послал уведомление о наступлении события в другой процесс. В этом случае объекту пересылается удаленная ссылка на объект-слушатель (listener object), обратный вызов которого можно выполнить при наступлении события (путем обращения RMI языка Java). Регистрация клиента на объекте всегда арендуется. Когда срок аренды истекает, зарегистрированный клиент (или процесс, которому уведомления отправлялись по поручению клиента) перестает получать уведомления. Благодаря аренде регистрация не может сохраниться вечно, например, в результате отказа зарегистрированного клиента. Уведомление о событии реализуется объектом путем удаленного вы-

зова объекта-слушателя, зарегистрированного для этого события. При следующем наступлении события объект-слушатель вызывается снова. Поскольку система Jini сама по себе не предоставляет никаких гарантий того, что уведомление о событии будет доставлено объекту-слушателю, уведомления обычно имеют порядковые номера, чтобы объект-слушатель имел представление об очередности событий.

Таким образом, системы распределенной обработки информации в виде многомашинных вычислительных комплексов и компьютерных сетей представляют собой одну из наиболее прогрессивных форм организации средств вычислительной техники. Возможность взаимодействия вычислительных систем при реализации распределенной обработки информации определяют как их способность к совместному использованию данных или к совместной работе с использованием стандартных интерфейсов. Целью распределенной обработки информации является оптимизация использования ресурсов и упрощение работы пользователя.

Распределенная система позволяет скрыть от пользователя аспекты своей внутренней организации, физические места размещения ресурсов, вопросы реализации и взаимодействия процессов, обслуживающих запросы пользователя. Распределенная система способна увеличиваться в масштабах путем подключения к системе дополнительных компонентов без принципиального влияния на работу существующих приложений и пользователей.

Прикладное программное обеспечение в общем случае может быть представлено в виде композиции трех логических слоев: слоя логики представления, слоя бизнес-логики и слоя логики доступа к данным. Послойное разделение прикладного программного обеспечения минимизирует взаимодействие между составными элементами и служит основой для выделения компонентов, которые могут быть распределены для работы на нескольких вычислительных машинах.

Децентрализованная обработка информации основывается на архитектурной модели клиент/сервер, где клиентами считаются вычислительные машины, нуждающиеся в получении тех или иных услуг, а серверами – вычислительные машины, которые эти услуги предоставляют. Под общим концептуальным названием

модели клиент/сервер скрывается несколько вариантов архитектурного построения вычислительных систем, а именно архитектуры однозвенные, двухзвенные, трехзвенные и многозвенные.

Промежуточное программное обеспечение позволяет осуществить связь и взаимодействие между разнородными компонентами распределенных систем, предоставляет стандартные интерфейсы программирования, реализует переносимость программ и прозрачность функционирования систем распределенной обработки информации. Наибольшее практическое распространение получили следующие механизмы реализации распределенной обработки информации: удаленный вызов процедур, объектно-ориентированный подход на основе удаленного обращения к методам, транзакционное взаимодействие на базе мониторов обработки транзакций, использование моделей обмена сообщениями и моделей согласования. К новой категории прикладных систем для распределенных вычислений относятся серверы приложений, разработка которых нацелена на создание объектно-ориентированных распределенных систем и построение прикладных программ из готовых компонентов. Одним из наиболее эффективных примеров такого подхода является сервер приложений на платформе Java.

Развитие глобальной сети Интернет привело к появлению новых стандартов и организации распределенной обработки информации на основе сетевых служб. Сетевые службы играют ту же роль, что и традиционные промежуточные слои программного обеспечения, но имеют гораздо более широкий масштаб. Координация и композиция работы сетевых служб позволяет нескольким службам осуществлять одновременный обмен информацией между разными службами.В последнее время достаточно успешно продвигается разработка концепции Grid – географически распределенной инфраструктуры, объединяющей множество ресурсов разных типов (процессоры, долговременная и оперативная память, хранилища и базы данных, сети), доступ к которым пользователь может получить из любой точки, независимо от места их расположения. Объединение различных вычислительных систем в рамках единой сети позволяет сформировать специальную вычислительную среду, которая с точки зрения пользователя представляет собой единый виртуальный высокопроизводительный метакомпьютер.

Grid-технология предполагает коллективный разделяемый режим доступа к ресурсам и услугам в рамках глобально распределенных виртуальных организаций, состоящих из совместно взаимодействующих предприятий и отдельных специалистов. В результате деятельности ряда международных компаний сформулированы базовые принципы Grid-архитектуры, имеющие важное практическое значение для построения эффективных и масштабных систем распределенной обработки информации.

1.6. Единая сеть электросвязи (ЕСЭ) Российской Федерации

В историческом плане все виды электросвязи длительный период развивались независимо друг от друга, в результате чего сформировались несколько независимых сетей. Вместе с тем сети общего пользования (Минсвязи) не справлялись с объемами передачи сообщений, требуемых для нормального экономического развития страны, и поэтому ряд министерств и ведомств стали создавать свои сети для удовлетворения собственных нужд. Такая техническая политика привела к еще большему разобщению технических средств, а эффективность совокупности сетей в масштабах страны оставалась низкой. Уже в начале 60-х гг. XX в. стало ясно, что перспективным направлением развития связи должно стать объединение сетей. Можно выделить следующие предпосылки для объединения сетей: унификация методов преобразования, необходимость передачи сигналов в совпадающих направлениях, сходство функций систем передачи и коммутации.

В 70-х гг. XX в. было принято решение о создании Единой автоматизированной сети связи (ЕАСС) Союза ССР. Работа по созданию сети ЕАСС не была завершена и прекратилась в связи с развалом СССР. В настоящее время этот проект, отражая изменение геополитической ситуации и новые революционные достижения в области связи, называется Взаимоувязанной сетью связи России. (ВСС) [4].

ВСС – это совокупность технически сопряженных сетей электросвязи общего пользования, ведомственных и других сетей электросвязи на территории России независимо от ведомственной принадлежности и форм собственности, обеспеченная общим централизованным управлением. Основными требованиями к ВСС

являются надежность и экономичность. Определенные технические средства ВСС участвуют в процессе передачи независимо от вида передаваемых сообщений. Совокупность этих элементов образует первичную сеть (ПС) ВСС (рис. 1.15). В состав ПС входят сетевые узлы, сетевые станции и линии передачи. Структура ПС учитывает административное деление страны.

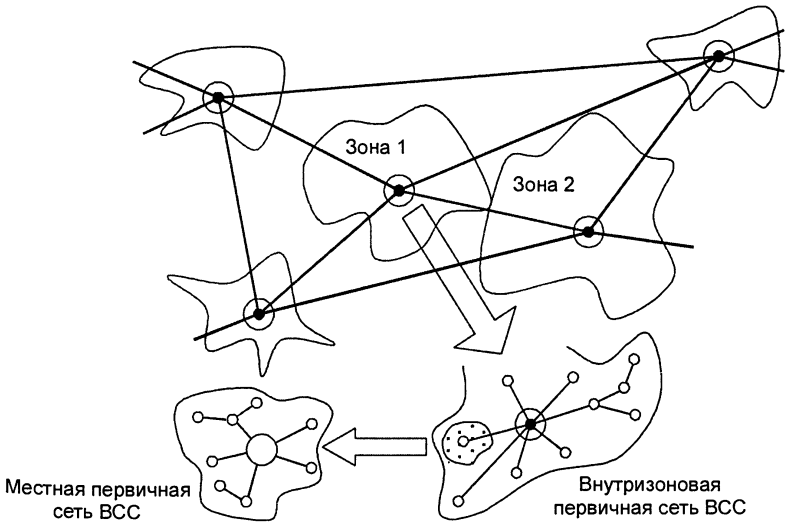


Рис. 1.15. Структура первичной сети ВСС по [1]

Территория страны поделена на зоны. Признак зоны – единая семизначная нумерация. Как правило, зоны совпадают с территориями областей. В соответствии с этим делением ПС состоит из отдельных частей:

• местные ПС (МСП) ограничены территорией города или сельского района;

• внутризоновые ПС (ВЗПС) охватывают территорию зоны и обеспечивают соединение местных сетей внутри зоны;

• магистральная ПС (СМП) соединяет зоновые сети.

Каждая сеть связи, входящая в ВСС, помимо технических средств первичной сети использует устройства, присущие этой сети. Вторичная сеть (ВС) ВСС – совокупность технических средств, обеспечивающих передачу сообщений определенного вида. В состав ВС входят: оконечные абонентские устройства, або-

нентские линии (АЛ), коммутационные устройства и каналы, выделенные из ПС для организации данной ВС.

До недавнего времени Минсвязи РФ являлось практически единственным оператором связи, предоставлявшим услуги организациям и населению. Ведомственные сети обеспечивали потребности самих организаций. Однако изменение экономической ситуации в стране и общемировая тенденция отхода от монопольного государственного или частного владения сетями и средствами связи привели к принятию Закона о связи, фактически определяющего основные принципы демонополизации отрасли связи. Закон о связи был принят Государственной Думой в 1995 г. Этот закон определяет:

• правовую основу деятельности в области связи в России;

• полномочия органов государственной власти по регулированию функционирования и развития отрасли связи (эти функции возложены на Министерство связи и информатизации Российской Федерации;

• права и обязанности физических и юридических лиц, участвующих в указанной деятельности и пользующихся ее результатами.

Кроме того, в том же году Правительство РФ утвердило программу демонополизации отрасли связи. В настоящее время тысячи предприятий имеют лицензии Минсвязи РФ на предоставление услуг электросвязи. Потребность абонентов в современных высококачественных услугах связи и, соответственно, готовность абонентов платить за услуги формируют значительный сектор рынка. Однако традиционным монопольным операторам связи во всем мире, в том числе и отечественным, отягощенным громадным количеством коммутационного и каналообразующего оборудования со значительными (до 20 лет и более) сроками окупаемости, тяжело проводить полномасштабную модернизацию своих сетей для соответствия современным потребностям в услугах связи.

Демонополизация в отрасли связи приводит к появлению новых агрессивных операторов связи, которые стучат в двери буквально каждого потенциального клиента, завлекают его более низкими ценами, повышенным качеством и разнообразием услуг. Операторы ведомственных сетей наряду с ростом услуг связи для собственных пользователей планируют предоставлять услуги сво-

их сетей прочим пользователям. Уже сейчас наметился рост конкуренции между традиционными операторами и альтернативными поставщиками услуг связи на базе сетей энергосистем, газопроводов, железных дорог и метрополитенов. Демонополизация отрасли связи и, как ее результат, конкуренция операторов будет выигрышна для абонентов, что на базе развития современных телекоммуникационных технологий выразится в расширении количества и повышении качества услуг связи при снижении их стоимости.

Литература

1. *Гаранин М.В., Журавлев В.И., Кунегин С.В.* Системы и сети передачи информации. – М.: Радио и связь, 2001.
2. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. 2-е изд. – М.: изд. дом «Вильямс», 2003.
3. *Олифер В.Г., Олифер Н.А.* Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2001.
4. Концепция развития связи Российской Федерации / В.Б. Булгак, Л.Е. Варакин, Ю.К. Ивашкевич и др. / Под ред. В.Б. Булгака, Л.Е. Варакина. – М.: Радио и связь, 1995. – 224 с.
5. *Иванов С.В.* Распределенная обработка информации. Курс лекций. [Электронный ресурс]. – Режим доступа: http://moxnatka.net.ru/load/1-1-0-81
6. Распределенная обработка данных: курс лекций / Сост. Л.В. Найханова. – Улан-Удэ: Изд-во ВСГТУ, 2001.
7. Распределенная обработка информации. Учебное пособие / С. Ф. Храпский. – Омск: Омск. гос. ин-т сервиса, 2006.
8. *Тайшин А.* Вычислительные сети и распределенная обработка данных [Электронный ресурс]. – Режим доступа: http://taishin.narod.ru/VS.html

2. ПРИНЦИПЫ ПОСТРОЕНИЯ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

2.1. Основные термины и определения

Телекоммуникационная сеть – это совокупность физических линий связи, аппаратных и программных средств, обеспечивающих информационное взаимодействие абонентских систем (АС). В общем случае телекоммуникационную сеть образуют каналы связи и узлы коммутации (УК). Обобщенная схема телекоммуникационной сети представлена на рис. 2.1. *Узлы коммутации* представляют собой специализированные ЭВМ, мосты, коммутаторы, маршрутизаторы или модульные концентраторы, управляющие выбором маршрутов передачи данных в сети.

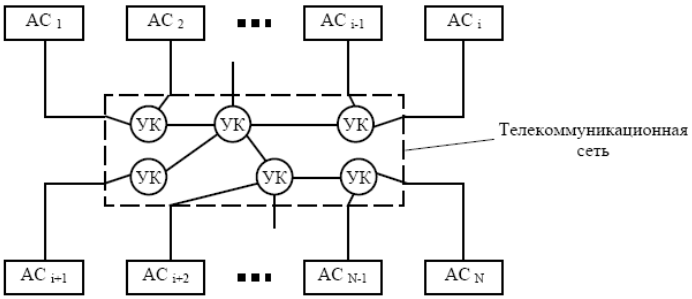


Рис. 2.1. Обобщенная схема телекоммуникационной сети

Узлы коммутации и абонентские системы обобщенно называются *оконечным оборудованием данных* (ООД).

Сеть доступа – часть телекоммуникационной сети между пунктом окончания телекоммуникационной сети и ближайшим коммутатором.

Транспортная сеть связи – это совокупность всех ресурсов, выполняющих функции транспортирования информации в телекоммуникационных сетях. Она включает не только системы передачи, но и относящиеся к ним средства контроля, оперативного переключения, резервирования, управления.

Каналом связи называют физическую среду и аппаратуру передачи данных (АПД), осуществляющих передачу информации от одного узла коммутации к другому либо между узлом коммутации и абонентской системой.

Физическая среда передачи данных – это пространство или материал, обеспечивающие распространение информационных сигналов. В качестве физической среды передачи данных в телекоммуникационных сетях могут использоваться:

– проводные (воздушные) линии связи – не изолированные провода, натянутые между телеграфными столбами и висящие в воздухе;

– кабельные линии связи – кабели на основе витых пар медных проводов, коаксиальные кабели, волоконно-оптические кабели и т.п.;

– радиоканалы наземной и спутниковой связи.

Аппаратура передачи данных – совокупность технических средств, предназначенных для преобразования дискретных сигналов, формируемых передающим ООД, в сигналы, передаваемые по физическим линиям связи, и обратного преобразования сигналов, поступающих по линиям связи в принимающее ООД. В качестве АПД используются модемы, сетевые адаптеры (сетевые карты), оптические модемы, устройства подключения к цифровым каналам и т.п. Состав канала связи телекоммуникационной сети представлен на рис. 2.2.

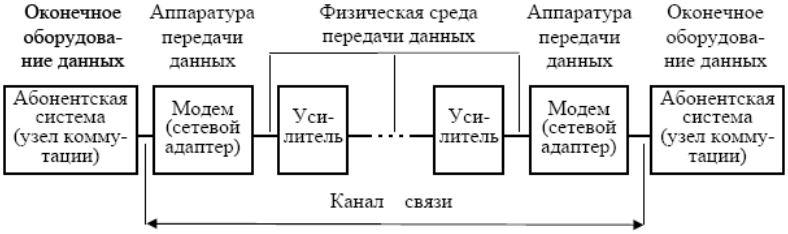


Рис. 2.2. Состав канала связи телекоммуникационной сети

При большой протяженности линий связи АПД может включать промежуточное оборудование в виде различных усилителей – формирователей передаваемых сигналов.

2.2. Архитектура и классификация телекоммуникационных сетей

Сети телекоммуникаций можно классифицировать по нескольким параметрам:

1) по размеру сети:

– *локальные сети (Local Area Network, LAN)* – сети здания или организации;

– *региональные сети (Metropolitan Area Network, MAN)* – сети уровня города или региона;

– *глобальные сети (Wide Area Network, WAN)* – сети, охватывающие большие территории и включающие в себя десятки и сотни тысяч компьютеров;

2) по типу коммутации:

– сети с коммутацией пакетов (например, TCP/IP, IPX/SPX, ATM, сети сотовой связи 3G);

– сети с коммутацией каналов (например, ТфОП, сети сотовой связи 1G и 2G);

– смешанные (например, сети сотовой связи 2,5G);

3) по установлению виртуального канала:

– с установлением виртуального канала (например, сети X.25, Frame Relay, ATM, ТфОП);

– без установления виртуального канала (например, TCP/IP, IPX/SPX);

4) по используемому стеку протоколов;

5) по количеству используемых стеков протоколов:

– монопротокольные сети;

– мультипротокольные сети (например, IP over ATM, IP over SDH/SONET);

6) по спектру оказываемых услуг:

– моносервисные сети (передача данных, передача голоса);

– мультисервисные сети;

7) по типу передаваемой информации:

– сети передачи данных;

– сети передачи голоса;

– сети передачи видео;

8) по наличию сигнализации:

– сети с выделенной сигнализацией (SS7);

– сети без выделенной сигнализации (TCP/IP);

9) по топологии сети:

– сети с топологией шина;

– сети с топологией кольцо;

– сети с топологией звезда;

– сети со смешанной топологией;

10) по среде передачи:

– проводные сети:

– связь осуществляется по медному кабелю;

– связь осуществляется по оптоволокну;

– беспроводные сети.

Архитектура телекоммуникационной сети включает три уровня (рис. 2.2.1).

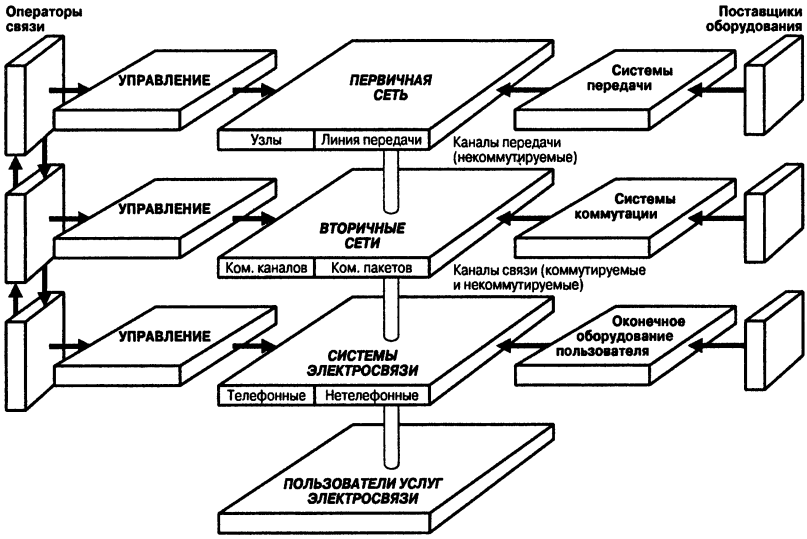


Рис. 2.2.1. Архитектура телекоммуникационной сети [1]

1. Системы (службы) электросвязи, т.е. комплекс средств, обеспечивающий предоставление пользователям услуг электросвязи.

2. Вторичные сети связи, обеспечивающие транспортировку, коммутацию, распределение сигналов в службах электросвязи.

3. Первичные сети, снабжающие вторичные сети каналами передачи и физическими цепями.

В качестве составной части соответствующей службы в архитектуру входит оконечное оборудование, расположенное у пользователя. Строится телекоммуникационная сеть на оборудовании связи: коммутационном, систем передачи и терминальном оборудовании пользователя.

Первичная сеть электросвязи. Первичной сетью телекоммуникационной сети называется совокупность линий передачи, сетевых узлов и сетевых станций, образующих сеть типовых каналов передачи и сетевых трактов. На рис. 2.2.2 поясняется принцип организации первичной сети. Сетевые узлы организуются на пересечении нескольких линий передачи, в них устанавливается каналообразующая аппаратура систем передачи и осуществляется переключение каналов или их групп, принадлежащих разным системам. На рис. 2.2.2 окончания каналов показаны кружочками. Сетевые станции являются оконечными устройствами первичной сети и предназначены для подключения потребителей к этой сети.

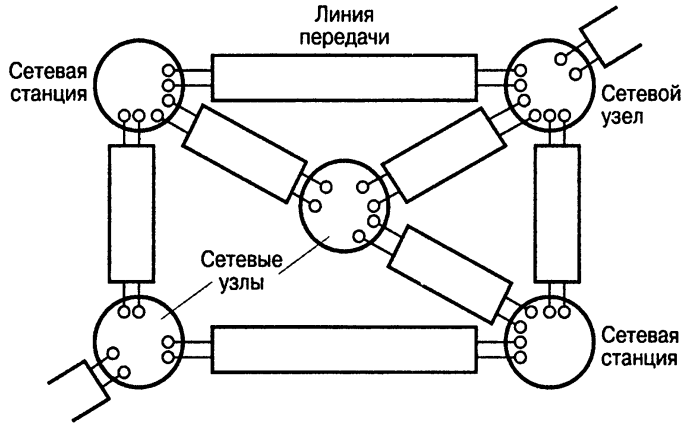


Рис. 2.2.2. Структура первичной сети [1]

Первичная сеть по территориальному принципу подразделяется на магистральные, внутризоновые и местные первичные сети. Магистральная первичная сеть соединяет каналами различных типов все областные и республиканские центры. Внутризоновая первичная сеть, в основном, соединяет различными каналами районные сети данной области друг с другом и с областным центром. Местные первичные сети ограничены территорией города или

сельского района. Они обеспечивают возможность организации каналов (или физических пар проводов) между станциями и узлами этих сетей, а также между абонентами.

Часто внутризоновую сеть и местные первичные сети объединяют одним названием – зоновая первичная сеть.

Рассмотренное территориальное деление предполагает трехъярусную структуру первичной сети. Самый низкий ярус включает в себя местные сети, распределенные по всей территории страны. Средний ярус – внутризоновые сети. Самый высокий ярус – магистральная сеть связи, объединяющая в единую сеть связи все внутризоновые сети.

Все магистральные сетевые узлы относятся к узлам первого класса, внутризоновые – к узлам второго класса и местные – к узлам третьего класса.

Среди сетевых узлов первых двух классов самыми крупными являются территориальные сетевые узлы, которые располагаются на пересечении нескольких достаточно мощных кабельных, радиорелейных и других линий. На этих узлах все линии заканчиваются каналообразующей аппаратурой. С помощью этих узлов можно соединить каналы и их группы, принадлежащие разным системам передачи, а также передавать каналы потребителям. На местных первичных сетях такие узлы не организуются. Сетевые узлы переключения являются менее крупными, располагаются на всех ярусах первичной сети и организуются на пересечении различных линий передачи малой мощности. На этих узлах осуществляется переключение каналов и усиление сигналов.

Сетевые узлы выделения устанавливаются на магистральной и внутризоновой первичных сетях и предназначены для организации выделения каналов потребителям. Сетевые станции (магистральные, внутризоновые, местные) являются оконечными точками сети и размещаются либо в удалении от соответствующих сетевых устройств и тогда соединяются с последними соединительными линиями либо располагаются совместно с сетевыми узлами.

Основным связующим звеном первичной сети являются системы передачи. На первичной сети широко используются системы ЧРК, ВРК и цифровые системы передачи на основе технологий PDH и SDH.

Основным типовым каналом передачи первичной телекоммуникационной сети является канал тональной частоты (ТЧ), обеспечивающий передачу между двумя сетевыми узлами (станциями) или между сетевым узлом и сетевой станцией электрических сигналов с полосой частот 0,3...3,4 кГц. Для передачи сигналов с широким спектром частот в первичной сети создаются широкополосные каналы передачи: первичные (объединяются 12 каналов ТЧ) и вторичные (объединяются 60 каналов ТЧ). Они используются для высокоскоростной передачи данных или факсимильной передачи газет. Могут быть организованы каналы и с более широкой полосой пропускания.

Вторичные сети электросвязи. Каналы первичной сети служат основой для построения вторичных сетей, которые различаются по виду передаваемых сообщений. В состав вторичной сети входят: оконечные абонентские установки, абонентские линии, узлы коммутации, каналы, выделенные из первичной сети для образования данной вторичной сети. В зависимости от вида передаваемых сообщений различают следующие вторичные сети: телефонную, телеграфную, передачи данных, факсимильную, передачи газет, звукового вещания, интегрального обслуживания (ISDN).

Из определения первичной сети следует, что она обеспечивает связь только между определенными узлами. Поэтому для образования путей передачи сообщений к любому узлу сети нужно осуществить соединение между каналами (группами каналов) различных магистралей, оканчивающихся на одном и том же узле. Если на узлах первичной сети установить кроссовые соединения, то на базе первичной сети будет создана вторичная некоммутируемая сеть. В узлы некоммутируемой сети могут включаться абонентские линии, которые соединяются с каналами сети также с помощью кроссовых соединений. В большинстве случаев каналы вторичных сетей являются коллективными для всех или группы абонентских пунктов, включенных в данный узел. На узле в этом случае устанавливается аппаратура коммутации, обеспечивающая подключение абонентских линий к каналу лишь на время передачи информации. Таким образом, на базе вторичной некоммутируемой сети образуются вторичные сети другого типа - вторичная коммутируемая сеть.

Основную долю оборудования УК как совокупности технических или программных средств для приема, обработки, распределения и передачи сообщений или вызовов представляют кросс и коммутационное оборудование. Кросс – это устройство ввода/вывода входящих и исходящих каналов, где осуществляются долговременные (кроссовые) соединения. Подключаемые каналы и линии передачи можно разделить на четыре типа: каналы и линии некоммутируемой сети связи, которые в УК проходят только через кросс; каналы и линии коммутируемой сети связи, которые через кросс подключаются к оборудованию коммутации каналов; каналы и линии коммутируемой сети связи, которые через кросс подключаются к оборудованию коммутации сообщений (пакетов); абонентские линии, которые кроссируются на коммутационное оборудование.

Коммутационное оборудование обеспечивает какой-либо способ коммутации: коммутацию каналов, реализующую установление соединения по вызову; коммутацию сообщений, предполагающую прием, обработку, хранение и транзит сообщения; коммутацию пакетов, осуществляющую прием, обработку, хранение и транзит пакета; гибридную или адаптивную коммутацию. Такие вторичные сети, как телефонные и факсимильные, чаще всего используют способ коммутации каналов, а телеграфные и передачи данных могут использовать различные способы коммутации: каналов, сообщений, пакетов.

В зависимости от числа абонентов и размеров территории вторичные сети могут иметь различную структуру. При радиальном построении вторичной сети все оконечные пункты (ОП) соединяются в один узел, который является узлом коммутации и осуществляет соединения между ОП. Радиальный способ обычно используется на небольшой территории (топология «звезда»). На значительной территории реализация этого способа не оправдана, так как требует большого расхода кабеля. Кроме того, при повреждении узла вся сеть перестает функционировать. Для устранения этих недостатков используется радиально-узловой способ построения сети, при котором кроме центрального (главного) узла, называемого узлом 1-го класса, создаются узлы более низких классов. Радиально-узловой принцип допускает только один путь установ-

ления соединения. Часто возникает необходимость в организации обходных путей для повышения надежности и живучести сети, уменьшения числа отказов в соединении и т.д.

С этой точки зрения, более предпочтительно соединение узлов по принципу «каждый с каждым». Такая сеть имеет другой недостаток – большое число соединительных линий между узлами и, следовательно, высокая стоимость.

На реальных сетях связи обычно применяются комбинированные принципы – радиально-узловой и «каждый с каждым». При этом узлы 1-го класса соединяются между собой по принципу «каждый с каждым» и одновременно являются центрами радиально-узлового построения сети.

2.3. Локальные сети

Построение локальных сетей, объединяющих большое количество ЭВМ, приводит к необходимости решения задачи обеспечения требуемой эффективности их функционирования. Одним из перспективных направлений в этой области является логическая структуризация сетей. Под логической структуризацией локальной сети понимается разбиение общей разделяемой среды передачи данных на логические сегменты, которые представляют самостоятельные разделяемые среды с меньшим количеством узлов. Сеть, разделенная на логические сегменты, обладает более высокой производительностью и надежностью. Взаимодействие между отдельными логическими сегментами сети организуется в этом случае с помощью специального коммуникационного оборудования: мостов, коммутаторов, маршрутизаторов и т.п.

На рис. 2.3.1 показан фрагмент локальной сети со структурообразующим оборудованием. Для построения локальных связей между компьютерами используются различные виды кабельных систем, сетевые адаптеры, концентраторы-повторители, мосты, коммутаторы и маршрутизаторы. Для подключения локальных сетей к глобальным связям используются специальные выходы (WAN-порты) мостов и маршрутизаторов, а также аппаратура передачи данных по длинным линиям – модемы (при работе по аналоговым линиям) или же устройства подключения к цифровым каналам (ТА – терминальные адаптеры сетей ISDN, устройства

обслуживания цифровых выделенных каналов типа CSU/DSU (channel service unit – блок обслуживания канала/ digital service unit – цифровой блок) и. т.п.

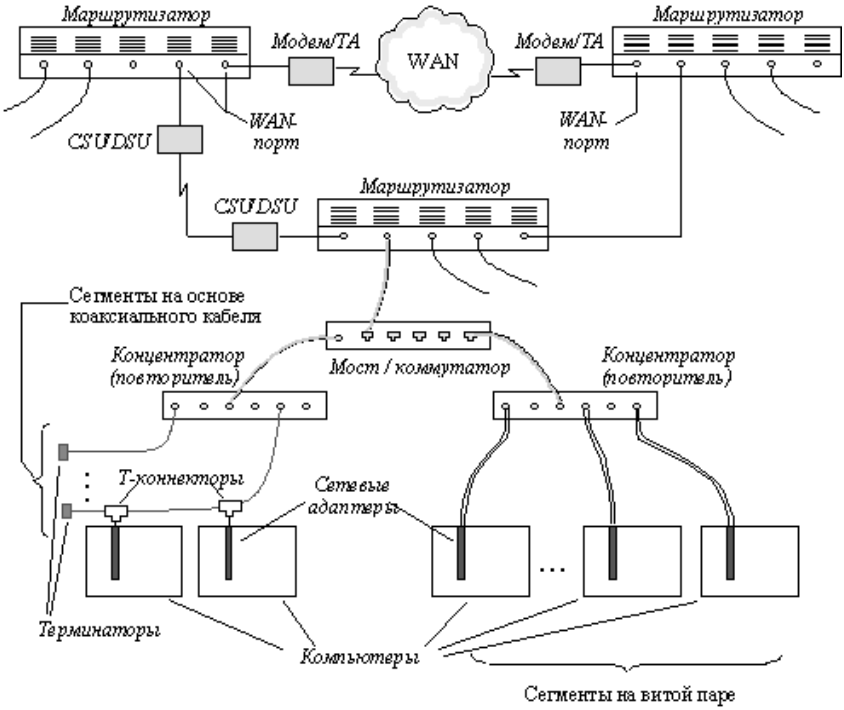


Рис. 2.3.1. Фрагмент локальной сети со структурообразующим оборудованием

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

В первых локальных сетях сетевой адаптер с сегментом коаксиального кабеля представлял собой весь спектр коммуникационного оборудования, с помощью которого организовывалось взаимодействие компьютеров. Сетевой адаптер компьютера-отправителя непосредственно по кабелю взаимодействовал с сетевым адаптером компьютера-получателя. В большинстве современных стандартов для локальных сетей предполагается, что между сетевыми адаптерами взаимодействующих компьютеров устанавливается специальное коммуникационное устройство (концентратор, мост, коммутатор или маршрутизатор), которое берет на себя некоторые функции по управлению потоком данных.

Сетевой адаптер обычно выполняет следующие функции:

- Оформление передаваемой информации в виде кадра определенного формата. Кадр включает в себя несколько служебных полей, среди которых имеется адрес компьютера назначения и контрольная сумма кадра, по которой сетевой адаптер станции назначения делает вывод о корректности доставленной по сети информации.
- Получение доступа к среде передачи данных. В локальных сетях в основном применяются разделяемые между группой компьютеров каналы связи (общая шина, кольцо), доступ к которым предоставляется по специальному алгоритму (наиболее часто применяются метод случайного доступа или метод с передачей маркера доступа по кольцу). В последних стандартах и технологиях локальных сетей наметился переход от использования разделяемой среды передачи данных к использованию индивидуальных каналов связей компьютера с коммуникационными устройствами сети, как это всегда делалось в телефонных сетях, где телефонный аппарат связан с коммутатором АТС индивидуальной линией связи. Технологиями, использующими индивидуальные линии связи, являются 100VG-AnyLAN, ATM и коммутирующие модификации традиционных технологий - switching Ethernet, switching Token Ring и switching FDDI. При использовании индивидуальных линий связи в функции сетевого адаптера часто входит установление соединения с коммутатором сети.
- Кодирование последовательности бит кадра последовательностью электрических сигналов при передаче данных и деко-

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

- Преобразование информации из параллельной формы в последовательную и обратно. Эта операция связана с тем, что для упрощения проблемы синхронизации сигналов и удешевления линий связи в вычислительных сетях информация передается в последовательной форме, бит за битом, а не побайтно, как внутри компьютера.
- Синхронизация битов, байтов и кадров. Для устойчивого приема передаваемой информации необходимо поддержание постоянного синхронизма приемника и передатчика информации. Сетевой адаптер использует для решения этой задачи специальные методы кодирования, не использующие дополнительной шины с тактовыми синхросигналами. Эти методы обеспечивают периодическое изменение состояния передаваемого сигнала, которое используется тактовым генератором приемника для подстройки синхронизма. Кроме синхронизации на уровне битов, сетевой адаптер решает задачу синхронизации и на уровне байтов, и на уровне кадров.

Сетевые адаптеры различаются по типу и разрядности используемой в компьютере внутренней шины данных – ISA, EISA, PCI, MCA. Сетевые адаптеры различаются также по типу принятой в сети сетевой технологии – Ethernet, Token Ring, FDDI и т.п. Как правило, конкретная модель сетевого адаптера работает по определенной сетевой технологии (например, Ethernet). В связи с тем, что для каждой технологии сейчас имеется возможность использования различных сред передачи данных (тот же Ethernet поддерживает коаксиальный кабель, неэкранированную витую пару и

оптоволоконный кабель), сетевой адаптер может поддерживать как одну, так и одновременно несколько сред. В случае когда сетевой адаптер поддерживает только одну среду передачи данных, а необходимо использовать другую, применяются трансиверы и конверторы.

Для определения точки назначения пакетов данных (frames) в сети используется MAC-адрес. Это уникальный серийный номер присваиваемый каждому сетевому устройству для идентификации его в сети. MAC-адрес присваивается адаптеру его производителем, но может быть изменен с помощью программы. Делать это не рекомендуется (только в случае обнаружения двух устройств в сети с одним MAC-адресом). При работе сетевые адаптеры просматривают весь проходящий сетевой трафик и ищут в каждом пакете свой MAC-адрес. Если таковой находится, то устройство (адаптер) декодирует этот пакет. Существуют также специальные способы по рассылке пакетов всем устройствам сети одновременно (broadcasting). MAC-адрес имеет длину 6 байт (48 бит) и обычно записывается в шестнадцатеричном виде, например 12:34:56:78:90:AB.

Двоеточия могут и отсутствовать, но их наличие делает число более читаемым. Каждый производитель присваивает адреса из принадлежащего ему диапазона адресов. Первые три байта адреса определяют производителя.

Трансивер (приемопередатчик, **trans**mitter+re**ceiver**) – это часть сетевого адаптера, его оконечное устройство, выходящее на кабель. В первом стандарте Ethernet, работающем на толстом коаксиале, трансивер располагался непосредственно на кабеле и связывался с остальной частью адаптера, располагавшейся внутри компьютера, с помощью интерфейса AUI (attachment unit interface).Включение повторителя и концентратора показано на рис. 2.3.2 и рис. 2.3.3 соответственно. В других вариантах Ethernet'а оказалось удобным выпускать сетевые адаптеры (да и другие коммуникационные устройства) с портом AUI, к которому можно присоединить трансивер для требуемой среды.

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

Повторитель (repeater) используется для физического соединения различных сегментов кабеля локальной сети с целью увеличения общей длины сети. На рис. 3.3.2 показано, как повторитель увеличивает общую длину сети, построенной по технологии Ethernet на тонком коаксиальном кабеле, которая позволяет использовать кабельные сегменты длиной не более 185 м.

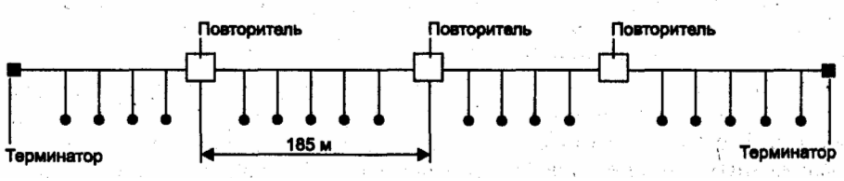


Рис. 2.3.2. Повторитель позволяет увеличить длину сети Ethernet

Повторитель, который имеет несколько портов и соединяет несколько физических сегментов называется концентратором или hub-ом. Проще говоря, хаб – это многопортовый репитер. На рис. 2.3.3 изображена задняя панель хаба с портом Uplink. Несмотря на звездообразность физической топологии сети на витой паре, построенной с помощью хаба, логически она не имеет отличий от сети на базе коаксиального кабеля – та же самая общая шина со случайным доступом и обнаружением коллизий.

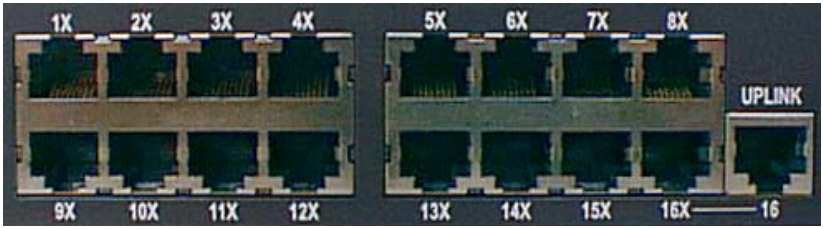


Рис. 2.3.3. Концентратор с портом Uplink

Соответственно, при возрастании числа активных узлов в сегменте растет число коллизий, в результате чего реальная пропускная способность сети падает. Еще одним недостатком концентраторов является то, что универсальные 10/100 мбит концентраторы работают на скорости 100 мбит только в том случае, если к нему не подключено ни одного 10-мбит устройства. Если такое устройство найдется, все порты концентратора будут переключены на 10 мбит. Последнего недостатка лишены устройства, называемые

Switch Hub (не путать со Switching Hub, или просто Switch - о них речь пойдет далее). Switch Hub снабжен буфером, который позволяет работать с портами разной скорости.

Вспомогательные функции, реализуемые производителями в HUBах:

– объединение сегментов с различными физическими средами (например, коаксиал, витая пара и оптоволокно) в единый логический сегмент;

– автосегментация портов, автоматическое отключение порта при его некорректном поведении (повреждение кабеля, интенсивная генерация пакетов ошибочной длины и т.п.);

– поддержка между концентраторами резервных связей, которые используются при отказе основных;

– защита передаваемых по сети данных от несанкционированного доступа (например, путем искажения поля данных в кадрах, повторяемых на портах, не содержащих компьютера с адресом назначения);

– поддержка средств управления сетями протокола SNMP, баз управляющей информации MIB;

– возможность каскадирования;

– AUTO MDIX.

Когда появились первые устройства, позволяющие разъединять сеть на несколько доменов коллизий (по сути, фрагменты ЛВС, построенные на hub-ах), они были 2-портовыми и получили название мостов (bridge-ей). По мере развития данного типа оборудования, они стали многопортовыми и получили название коммутаторов (switch-ей). Некоторое время оба понятия существовали одновременно, а поздее вместо термина "мост" стали применять "коммутатор".

Switching Hub, или просто **Switch** (коммутатор) – это более интеллектуальное по сравнению с концентратором устройство. Коммутаторы способны делить сети на сегменты и передавать пакеты между портами на основе адреса получателя, включенного в каждый пакет. Достигается это созданием внутренней таблицы, связывающей порты с адресами подключенных к ним устройств. Эту таблицу администратор сети может создать самостоятельно или задать ее автоматическое создание средствами коммутатора.

Используя таблицу адресов и содержащийся в пакете адрес получателя, коммутатор организует виртуальное соединение порта отправителя с портом получателя и передает пакет через это соединение, при этом задержка при передаче сигналов минимальна. Виртуальное соединение между портами коммутатора сохраняется в течение передачи одного пакета, т.е. для каждого пакета оно создается заново. Поскольку пакет передается только в тот порт, к которому подключен адресат, остальные пользователи не получат этот пакет, и таким образом коммутаторы снижают количество коллизий в сети и обеспечивают средства безопасности, не доступные для концентраторов. Как было замечено ранее, данные передаются напрямую из порта в порт, однако при передаче пакетов между портами, работающими на разных скоростях, коммутацию на лету использовать невозможно, поэтому при организации виртуального соединения между портами с разной скоростью производится буферизация пакетов, что приводит к возрастанию задержки передачи пакетов до 30…40 мкс. К сожалению, типичные коммутаторы работают по алгоритму "устаревания адресов". Это означает, что, если по истечении определенного промежутка времени не было обращений по какому-либо адресу, этот адрес удаляется из адресной таблицы. При поступлении нового пакета в этот адрес будет невозможным установить прямое соединение, что вызовет такую же задержку в передаче данных, что и при соединении разноскоростных портов – 30…40 мкс. Такая проблема решена в сериях коммутаторов, поддерживающих технологию SNS, которая ранее называлась SFS. Одна из ее особенностей заключается в том, что коммутаторы, составляющие сеть, хранят таблицу адресов "вечно" и обмениваются этими таблицами друг с другом, а также могут выгружать их на специальный сервер. Это позволяет не только сократить время прохождения пакета по сети, но и решить ряд специфических проблем, особенно связанных с безопасностью. У многих коммутаторов имеется возможность организации одновременных соединений между любыми парами портов устройства – это значительно расширяет суммарную пропускную способность сети.

Виртуальные локальные сети ЭВМ (VLAN) обеспечивают возможность создания логических групп пользователей в масшта-

бе большой локальной или корпоративной сети. За счет использования технологии виртуальной локальной сети администратор сети может организовать пользователей в логические группы независимо от физического расположения ЭВМ этих пользователей. Это одно из основных достижений в сетевых технологиях - возможность создавать рабочие группы на основе служебных функций пользователей, не привязываясь к сетевой топологии. Виртуальные сети позволяют организовать работу в сети более эффективно, так как обладают следующими достоинствами:

• простота внесения изменений в сеть, добавления или удаления устройств;

• более эффективное использование ограниченных сетевых ресурсов;

• высокий уровень обеспечения безопасности.

Возможность организации виртуальных ЛВС обусловлена переходом от разделяемых сред к коммутируемым. Пример построения виртуальной локальной сети на основе одного коммутатора с использованием технологии группирования портов приведен на рис. 2.3.4. При этом каждый порт приписывается к той или иной виртуальной сети. Информационный кадр, пришедший от порта виртуальной сети 1, никогда не будет передан порту, который не принадлежит этой сети. Порт может быть приписан одновременно к нескольким виртуальным сетям, но на практике такое бывает редко, так как теряется эффект полной изоляции сетей.

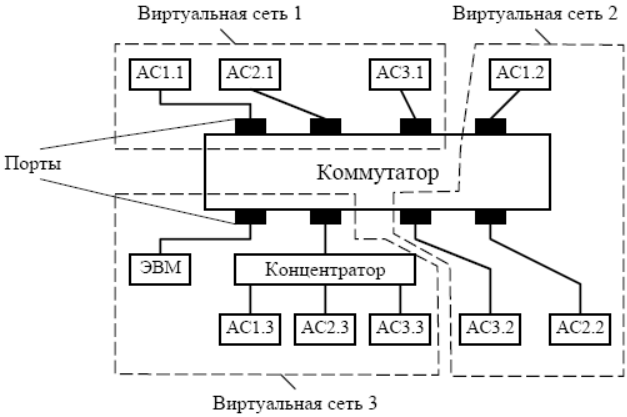


Рис. 2.3.4. Виртуальная локальная сеть на одном коммутаторе

Соединение между собой концентраторов (Hub) и коммутаторов (Switch) производится обычными кабелями, подключаемыми с использованием портов Uplink. Также важным обстоятельством является то, что для концентраторов имеется лимит на число последовательно соединенных устройств – не более 4-х между двумя рабочими станциями. Большинство концентраторов и коммутаторов имеет такую функцию, как Auto MDIX, которая позволяет не заботиться о типе используемого кабеля – прямой или кросс. Вышеописанные соединения устройств между собой имеют один существенный недостаток – скорость обмена данных между коммутаторами и/или концентраторами не может превышать скорости портов (10 или 100 мбит/с), а реально она меньше из-за коллизий. Если Вам необходимо организовать многопортовый концентратор или коммутатор, Вы получите узкое место в системе – ограниченная скорость передачи данных между устройствами. Можно, конечно использовать Gigabit порты, но их обычно мало: один-два на устройство. Такая проблема решается объединением устройств в стек, где между устройствами передача данных ведется на скоростях порядка 1 гбит/с и выше. Конечно, речь идет об устройствах, позволяющих организацию таких стеков - в их наименованиях обычно присутствует термин "Stackable". Средства объединения устройств в стек могут быть либо изначально встроены в коммутатор (концентратор) либо выпускаться в виде отдельных плат, вставляемых в слоты расширения объединяемых устройств. При этом возможны различные типы соединений в стеке – последовательное и кольцевое, когда последнее устройство в цепочке соединяется с первым. Кольцевое соединение является предпочтительным по причине более высокой надежности: при выходе из строя одного устройства в стеке стек продолжит функционирование. Встроенными средствами "Stackable" коммутаторов обычно обеспечивается последовательное соединение, а кольцевое соединение достигается чаще всего при использовании плат в слотах расширения. В некоторых вариантах возможно прямое соединение лишь двух устройств, а для соединения большего количества коммутаторов (до 4-х и более) применяются матричные модули, представляющие собой отдельные устройства типа коммутатора, но выполняющие функции управления стеком и высокоскоростного

соединения коммутаторов между собой. При использовании матричных модулей соединение коммутаторов также производится по кольцевому типу.

Еще один способ соединения – это использование функции port trunking, когда несколько портов на каждом устройстве объединяются в один виртуальный порт, суммируя их пропускную способность. Физически при таком способе подключения мы соединяем 2 или более портов на одном устройстве с аналогичным количеством портов на другом.

Hub-ы, организующие рабочую группу, bridge-и, соединяющие два сегмента сети и локализующие трафик в пределах каждого из них, а также switch-и, позволяющие соединять несколько сегментов локальной вычислительной сети – это все устройства, предназначенные для работы в сетях IEEE 802.3 или Ethernet. Однако существует особый тип оборудования, называемый ***маршрутизаторами (routers),*** который применяется в сетях со сложной конфигурацией для связи ее участков с различными сетевыми протоколами (в том числе и для доступа к глобальным (WAN) сетям), а также для более эффективного разделения трафика и использования альтернативных путей между узлами сети. Основная цель применения роутеров – объединение разнородных сетей и обслуживание альтернативных путей. Различные типы роутеров отличаются количеством и типами своих портов, что, собственно, и определяет места их использования. Маршрутизаторы, например, могут быть использованы в локальной сети Ethernet для эффективного управления трафиком при наличии большого числа сегментов сети, для соединения сети типа Ethernet с сетями другого типа, например Token Ring, FDDI, а также для обеспечения выходов локальных сетей на глобальную сеть.

Маршрутизаторы не просто осуществляют связь разных типов сетей и обеспечивают доступ к глобальной сети, но и могут управлять трафиком на основе протокола сетевого уровня (третьего в модели OSI), то есть на более высоком уровне по сравнению с коммутаторами. Необходимость в таком управлении возникает при усложнении топологии сети и росте числа ее узлов, если в сети появляются избыточные пути, когда нужно решать задачу максимально эффективной и быстрой доставки отправленного пакета по назначению.

Таким образом, маршрутизаторы:

– образуют логические сегменты посредством явной адресации, поскольку используют не аппаратные, а составные числовые адреса, в которых есть поле номера сети. Все компьютеры, у которых значение этого поля одинаково, принадлежат к одному логическому сегменту, называемому подсетью (subnet);

– выполняют функции локализации траффика и выбора рационального маршрута.

Шлюз (Gateway) – устройство, объединяющее сети с разными типами системного и прикладного программного обеспечения. Обеспечивает также локализацию трафика.

Шлюз – это:

– устройство, выполняющее трансляцию протоколов. Шлюз размещается между взаимодействующими сетями и служит посредником, переводящим сообщения, поступающие из одной сети, в формат другой сети;

– может быть реализован как чисто программными средствами, установленными на обычном компьютере, так и на базе специализированного компьютера;

– рансляция одного стека протоколов в другой представляет собой сложную интеллектуальную задачу, требующую максимально полной информации о сети, поэтому шлюз использует заголовки всех транслируемых протоколов;

– пример использования шлюза – предоставление интернет доступа пользователям некоторых сотовых систем связи.

2.4. Глобальные сети

Основные типы потенциальных потребителей услуг глобальной сети изображены на рис. 2.4.1.

Типовая структура глобальной сети приведена на рис. 2.4.2.

Сеть строится на основе некоммутируемых (выделенных) каналов связи, которые соединяют коммутаторы глобальной сети между собой. Такие каналы образуют магистраль сети. Коммутаторы устанавливаются в тех географических пунктах, в которых требуется ответвление или слияние потоков данных конечных абонентов или магистральных каналов, переносящих данные многих абонентов. Естественно, выбор мест расположения коммута-

торов определяется многими соображениями, в которые включается также возможность обслуживания коммутаторов квалифицированным персоналом, наличие выделенных каналов связи в данном пункте, надежность сети, определяемая избыточными связями между коммутаторами. Абоненты сети подключаются к коммутаторам в общем случае также с помощью выделенных каналов связи. Эти каналы связи имеют более низкую пропускную способность, чем магистральные каналы, объединяющие коммутаторы, иначе сеть бы не справилась с потоками данных своих многочисленных пользователей. Для подключения конечных пользователей допускается использование коммутируемых каналов, т.е. каналов телефонных сетей, хотя в таком случае качество транспортных услуг обычно ухудшается.

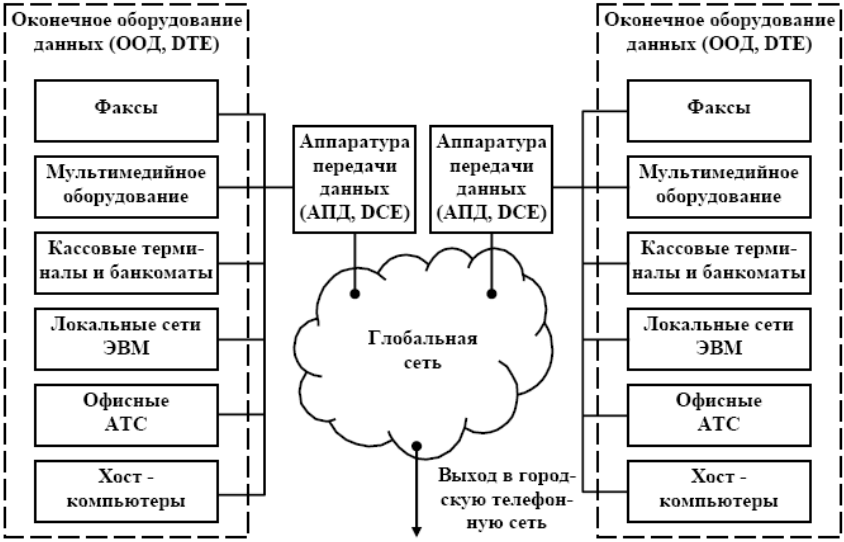


Рис. 2.4.1. Основные типы потенциальных потребителей услуг глобальной сети [2]

Принципиально замена выделенного канала на коммутируемый ничего не меняет, но вносятся дополнительные задержки, отказы и разрывы канала по вине сети с коммутацией каналов, которая в таком случае становится промежуточным звеном между пользователем и сетью с коммутацией пакетов. Кроме того, в аналоговых телефонных сетях канал обычно имеет низкое качество

из-за высокого уровня шумов. Применение коммутируемых каналов на магистральных связях коммутатор–коммутатор также возможно, но по тем же причинам весьма нежелательно.

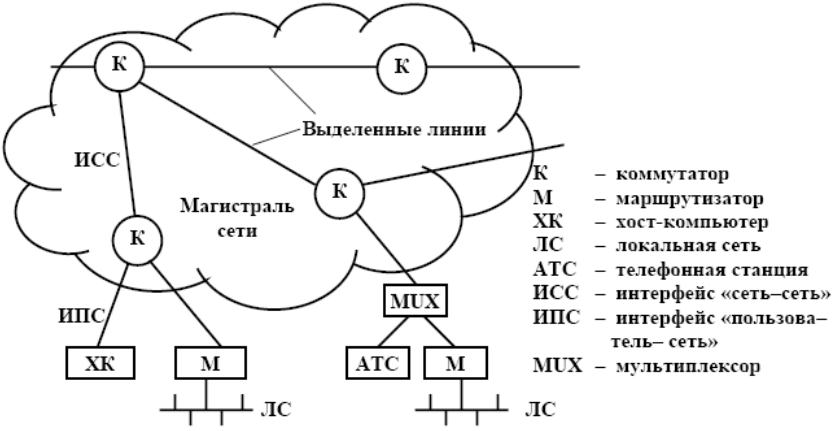


Рис. 2.4.2. Типовая структура глобальной сети

Оконечное оборудование (DTE) принимает и передает в глобальную сеть данные по каналам связи определенного стандарта. Поэтому в состав каждого устройства типа ООД (DTE) должна входить аппаратура передачи данных (DCE), реализующая протокол физического уровня данного канала. Кроме этого, должны быть четко определены все параметры интерфейса «пользователь-сеть» (ИПС).

Для связи ООД с каналами глобальной сети используется АПД трех основных типов:

• модемы для работы по выделенным и коммутируемым аналоговым каналам;

• устройства сопряжения для работы по выделенным цифровым каналам с мультиплексированием на основе разделения времени (технология TDM);

• терминальные адаптеры для работы по каналам цифровых сетей с интеграцией услуг (сети ISDN).

Протоколы взаимодействия коммутаторов внутри глобальной сети образуют интерфейс «сеть–сеть» (ИСС). Они стандартизуются не всегда. Стандартизация указанных протоколов обычно при-

меняется для организации взаимодействия двух и более глобальных сетей различных операторов. Тем не менее, если стандарт ИСС принимается, то в соответствии с ним обычно организуется взаимодействие всех коммутаторов объединенной сети, а не только пограничных.

2.5. Цифровые сети с интеграцией услуг (ISDN – ЦСИС)

Цифровая сеть с интеграцией услуг ЦСИС – ISDN (Integrated Services Digital Network) – это глобальная телекоммуникационная сеть, в которой передача данных между абонентскими системами реализуется на основе метода коммутации каналов, а данные передаются и обрабатываются в цифровой форме. Внедрение сетей ISDN в эксплуатацию началось в конце 80-х гг. XX в. Наибольшее распространение они получили в странах Европы, в США и Японии.

Архитектура сети ISDN предусматривает предоставление пользователям следующих служб и услуг:

• передача данных по выделенным некоммутируемым цифровым каналам;

• коммутируемая телефонная сеть общего пользования;

• сеть передачи данных с коммутацией каналов;

• сеть передачи данных с коммутацией пакетов;

• сеть передачи данных с трансляцией кадров (режим frame relay);

• средства контроля и управления работой сети.

Информационное взаимодействие между компонентами сети осуществляется на трех уровнях: физическом, канальном и сетевом. На рис. 2.5.1 показаны основные компоненты сетей ISDN:

– терминалы (Т);

– терминальные адаптеры (ТА);

– сетевые терминалы (СТ);

– линейные терминалы (ЛТ);

– магистральные устройства (МУ).

Специализированные ISDN терминалы Т1 (цифровые телефоны, факсы, оборудование видеоконференцсвязи, мосты/маршрутизаторы, терминальные адаптеры) обеспечивают представление данных пользователя в требуемом формате и непосредственное подключение пользователя к сети ISDN.

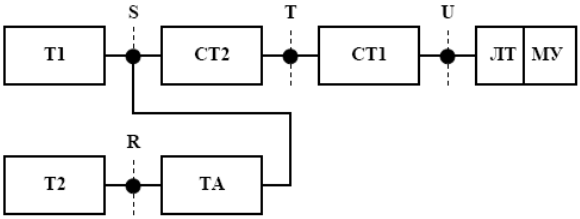


Рис. 2.5.1. Основные компоненты сети ISDN [2]

Обычные (не ISDN) терминалы T2 представляют собой такое оборудование, как аналоговые телефоны, факсы, компьютеры с аналоговыми модемами, и не обеспечивают непосредственного подключения пользователя к сети ISDN.

Терминальный адаптер TA обеспечивает подключение неспециализированных терминалов T2 к сети ISDN. Точка сопряжения R используется для подключения неспециализированных терминалов T2 к терминальным адаптерам. Сетевые терминалы CT1 и CT2 обеспечивают подключение терминалов пользователя к различным точкам сопряжения сети ISDN. Сетевой терминал CT2 обеспечивает взаимодействие с сетью терминалов пользователя, которые подключены к магистрали S. Точка сопряжения S используется для подключения терминалов пользователя к сетевому терминалу. Точка сопряжения T используется для подключения сетевых терминалов CT1 и CT2. Точка сопряжения U используется для подключения сетевого терминала CT1 к коммутатору ISDN. Обычно указанные выше компоненты сети ISDN не изготавливаются в виде отдельных блоков. Как правило, сетевые терминалы изготавливаются в виде единого устройства, которое обозначается CT (NT). Точка сопряжения с терминалами пользователя в данном случае обозначается S/T.

Существует две разновидности цифровых сетей с интеграцией услуг: сеть N-ISDN и сеть B-ISDN. Сеть N-ISDN (narrowband) обеспечивает передачу данных со скоростью до 2048 кбит/с. Сеть B-ISDN (broadband) предназначена для передачи данных со скоростью до 155 000 кбит/с. Далее рассмотрим только сети N-ISDN. Интеграция разнородных трафиков в сети ISDN выполняется по принципу временного разделения (time division multiplexing – TDM). Основные типы сервиса сетей ISDN представлены в табл. 2.5.1.

Таблица 2.5.1

Основные типы сервисов сетей ISDN

Тип канала	Скорость	Назначение
A	-	Аналоговый телефонный канал 4 кГц
B	64 Кбит/сек	Данные или оцифрованный аудиосигнал
C	8 или 16 Кбит/сек	Цифровой канал передачи данных
D	16 Кбит/сек	Цифровой канал передачи внеканальной сигнализации
E	64К бит/сек	Цифровой канал для внутренней сигнализации ISDN
H0	384 Кбит/сек	Цифровой канал передачи данных
H10	1472 Кбит/сек	Цифровой канал передачи данных
H11	1536К бит/сек	Цифровой канал передачи данных
H12	1920 Кбит/сек	Цифровой канал передачи данных

Цифровые сети с интеграцией услуг ISDN поддерживают два типа пользовательских интерфейсов (рис. 2.5.2).

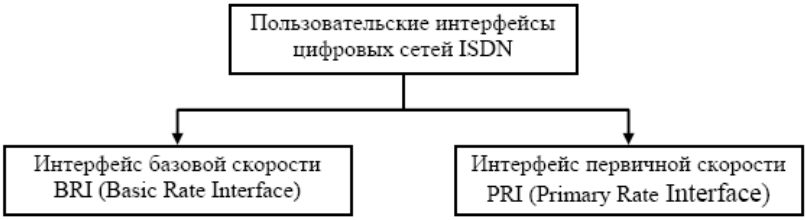


Рис. 2.5.2. Пользовательские интерфейсы сетей ISDN [2]

Интерфейс базовой скорости ISDN (Basic Rate Interface- BRI) предоставляет пользователю услуги сети ISDN в виде двух каналов с пропускной способностью 64 кбит/с (два канала типа B . Для передачи канальной сигнализации используется отдельный канал, который имеет пропускную способность 16 кбит/с (канал типа D). Таким образом, интерфейс базовой скорости обозначается 2B+D и обеспечивает общую пропускную способность 192 кбит/с.

Интерфейс первичной скорости ISDN (Primary Rate Interface-PRI) имеет различную структуру в различных регионах. В Европе PRI предоставляет пользователю сеть ISDN в виде 30 каналов B-типа и одного канала D-типа (30B+D). В США и Японии PRI предоставляет пользователю сеть ISDN в виде 23 каналов B-типа и одного канала D-типа (23B+D). Суммарная пропускная способность составляет в Европе 2048 кбит/с и 1544 кбит/с – в США и Японии.

Сети ISDN можно использовать для передачи данных, для объединения удаленных локальных сетей, для доступа к сети Internet, для интеграции передачи разного вида трафика, в том числе видео и голосового. Терминальными устройствами сети могут быть цифровые телефонные аппараты, компьютеры с ISDN-адаптерами, видео- и аудиооборудование.

Основные достоинства сетей ISDN:

• предоставление пользователям широкого круга качественных услуг;

• использование обычных линий связи с мультиплексированием одного канала между несколькими абонентами;

• высокая скорость (до 128 Кбит/с) передачи информации по телефонным каналам связи;

• высокая эффективность использования в глобальных сетях.

Недостатки сетей ISDN:

• большие затраты при создании и модернизации сети;

• синхронное использование каналов связи, не позволяющее динамически подключать к работающему каналу новых абонентов.

2.6. Особенности защищенных телекоммуникационных сетей

В соответствии с рекомендациями МСЭ-Т конфиденциальность, целостность и доступность являются характеристиками безопасности передаваемых данных. Следует заметить. что обеспечить защиту информации всех мыслимых и немыслимых воздействий со стороны злоумышленников (лиц, способных несанкционированно воздействовать на передаваемую информацию) нельзя Поэтому, создавая службу безопасности, следует проанализировать возможные угрозы безопасности и ущерб, который может

быть нанесен собственнику информации из-за потери, хищения, искажения или задержки информации вследствие воздействий на процесс передачи информации. Перечислим наиболее характерные угрозы безопасности информации при ее передаче по телекоммуникационным сетям:

– перехват данных – обзор данных несанкционированным пользователем; эта угроза проявляется в возможностях злоумышленника непосредственно подключаться к линии связи для съема передаваемой информации либо получать информацию на дистанции», вследствие побочного электромагнитного излучения средств передачи ин формации по каналам связи;

– анализ трафика – обзор информации, касающейся связи между пользователями (например, наличие/отсутствие, частота, направление, последовательность, тип, объем и т.д.); даже если подслушивающий не может определить фактического содержания сообщения. он может получить некоторый объем информации, исходя из характера потока трафика (например, непрерывный, пакетный, периодический или отсутствие информации);

– изменение потока сообщения (или одного сообщения) – внесение в него необнаруживаемых искажений, удаление сообщения или нарушение общего порядка следования сообщений;

– повтор процесса установления соединения и передачи сообщения – записывание несанкционированным пользователем с последующим повтором им процесса установления соединения с передачей ранее уже переданного и принятого пользователем сообщения;

– отказ пользователя от сообщения – отрицание передающим пользователем своего авторства в предъявленном ему принимающим пользователем сообщении или отрицание принимающим пользователем факта получения им от передающего пользователя сообщения;

– маскарад – стремление пользователя выдать себя за некоторого другого пользователя с целью получения доступа к дополнительной информации, получения дополнительных привилегий или навязывание другому пользователю системы ложной информации исходящей якобы от пользователя, имеющего санкции на передачу такого рода информации;

– нарушение связи, недопущение связи или задержка срочных сообщений.

В телематических службах, содержащих элементы обработки сообщений и хранения, например, в службе обработки сообщений, возможны специфические угрозы [3]:

– угрозы несанкционированного доступа в службу обработки сообщений;

– угрозы хранилищу данных.

Система, обеспечивающая защиту от этих угроз, может включать следующие службы:

1) служба секретности данных – может быть использована для защиты передаваемых данных от вскрытия содержащейся в них ин формации и от возможности проведения анализа интенсивности по тока данных между пользователями;

2) служба аутентификации – предназначается для обеспечения подтверждения того, что в данный момент связи пользователь является действительно тем пользователем, за которого он себя выдает;

3) служба целостности данных – обеспечивает доказательство целостности данных в процессе их передачи, т.е. обеспечивает защиту передаваемых сообщений от случайных и преднамеренных воздействий, направленных на изменение передаваемых сообщений, задержку и уничтожение; а также переупорядочивание их;

4) служба управления доступом – обеспечивает защиту от несанкционированного доступа к информации, содержащейся в удаленных банках данных, или от несанкционированного использования ресурсов сети;

5) служба сохранности информации – обеспечивает доказательство целостности сообщения, принятого от соответствующего источника и находящегося на хранении, например в терминале-приемнике, и которое может быть проверено в любой момент времени арбитром (третьей стороной);

6) служба доставки – обеспечивает защиту от попыток злоумышленника нарушить связи или задержать передачу сообщения на время, превышающее время ценности передаваемой в сообщении информации; эта служба непосредственно связана с процессами передачи информации в сетях связи.

Каждая из служб может самостоятельно решать стоящую перед ней задачу защиты с помощью тех или иных механизмов и средств защиты. При этом один и тот же механизм защиты может быть использован в интересах разных служб защиты информации.

Рекомендациями МОС и МСЭ-Т предусматриваются следующие основные механизмы защиты [3]:

– шифрование данных;

– обеспечение аутентификации;

– обеспечение целостности данных;

– цифровая подпись;

– контроль доступа.

Механизм шифрования может обеспечивать конфиденциальность либо передаваемых данных, либо информации о параметрах трафика и может быть использован в некоторых других механизмах безопасности или дополнять их. Существование механизма шифрования подразумевает использование, как правило, механизма управления ключами.

При рассмотрении механизмов аутентификации основное внимание уделяется методам передачи в сети информации специального характера (паролей, аутентификаторов, контрольных сумм и т.п.). В случае односторонней или взаимной аутентификации обеспечивается процесс проверки подлинности пользователей (передатчика и приемника сообщений), что гарантирует предотвращение соединения с логическим объектом, образованным злоумышленником.

Механизм обеспечения целостности данных предполагает введение в каждое сообщение некоторой дополнительной информации, являющейся функцией от содержания сообщения. В рекомендациях МОС рассматриваются методы обеспечения целостности двух типов: первые обеспечивают целостность единственного блока данных, вторые – потока блоков данных или отдельных их полей. Эти методы применяются как при передаче данных по виртуальному соединению. так и при использовании дейтаграммной передачи. В первом случае гарантируется устранение неупорядоченности, потерь, повторов, вставок или модификации данных при помощи специальной нумерации блоков, либо введением меток времени. В дейтаграммном режиме метки времени могут обеспе-

чить только ограниченную защиту целостности последовательности блоков данных и предотвратить переадресацию отдельных блоков.

Механизм цифровой подписи, реализующий один из процессов аутентификации пользователей и сообщения, применяется для подтверждения подлинности содержания сообщения и удостоверения того факта, что оно отправлено абонентом, указанным в заголовке в качестве источника данных. Цифровая подпись (ЦП) также необходима для предотвращения возможности отказа передатчика от факта выдачи какого-либо сообщения, а приемника – от его приема.

Механизмом цифровой подписи определяются две процедуры:

– формирование блока данных, добавляемого к передаваемому сообщению;

– подписание блока данных.

Процесс формирования блока данных содержит общедоступные процедуры и в отдельных случаях специальные (секретные) ключи преобразования, известные на приеме. Процесс подписания блока данных использует информацию, которая является информацией частного использования (т. е. уникальной и конфиденциальной). Этот процесс подразумевает либо шифрование блока данных либо получение криптографического контрольного значения блока данных с использованием частной информации под писавшёго пользователя в качестве ключа шифрования частного пользования. Таким образом, после проверки подписи в последующем третьему лицу (например, арбитру) в любое время может быть доказано, что подпись может выполнить только единственный держатель секретной («частной» информации).

Механизмы контроля доступа могут использовать аутентифицированную идентификацию объекта или информацию объекта (например, принадлежность к известному множеству объектов) либо возможности этого объекта для установления и применения прав доступа к нему. Если объект делает попытку использовать несанкционированный или санкционированный с неправильным типом доступа ресурсы, то функция контроля доступа будет отвергать эту попытку и может сообщить о ней для инициирования аварийного сигнала и (или) регистрации его как части данных про-

верки безопасности. Механизмы контроля доступа могут использоваться на любом конце соединения и (или) в любом промежуточном узле.

Механизм заверения обеспечивает гарантию свойств, относящихся к данным, которые передаются между двумя или более пользователями, например, их целостность, источник, время и место назначения. Эта гарантия дается третьим лицом (нотариусом), которому доверяют вступающие во взаимодействие пользователи и который располагает необходимой информацией для предоставления требуемой гарантии способом, допускающим возможность ее проверки. Каждый процесс установления соединения может использовать цифровую подпись, шифрование и механизмы целостности в зависимости от требований услуги. получающей заверение. Когда задействуется механизм заверения, сообщения передаются через защищенные соединения и нотариуса.

2.7. Стандартизация телекоммуникационных сетей

Универсальный тезис о пользе стандартизации, справедливый для всех отраслей, в компьютерных сетях приобретает особое значение. Суть сети – это соединение разного оборудования, а значит, проблема совместимости является одной из наиболее острых. Без принятия всеми производителями общепринятых правил построения оборудования прогресс в деле строительства сетей был бы невозможен. Поэтому все развитие компьютерной отрасли, в конечном счете, отражено в стандартах – любая новая технология только тогда приобретает законный статус, когда ее содержание закрепляется в соответствующем стандарте.

В компьютерных сетях идеологической основой стандартизации является многоуровневый подход к разработке средств сетевого взаимодействия. Именно на основе этого подхода была разработана стандартная семиуровневая модель взаимодействия открытых систем, ставшая своего рода универсальным языком сетевых специалистов. Организация взаимодействия между устройствами в сети является сложной задачей. Как известно, для решения сложных задач используется универсальный прием – декомпозиция, т. е. разбиение одной сложной задачи на несколько более простых задач-модулей. Процедура декомпозиции включает в себя

четкое определение функций каждого модуля, решающего отдельную задачу, и интерфейсов между ними. В результате достигается логическое упрощение задачи, кроме того, появляется возможность модификации отдельных модулей без изменения остальной части системы.

При декомпозиции часто используют многоуровневый подход. Он заключается в следующем. Все множество модулей разбивают на уровни. Уровни образуют иерархию, то есть имеются вышележащие и нижележащие уровни. Множество модулей, составляющих каждый уровень, сформировано таким образом, что для выполнения своих задач они обращаются с запросами только к модулям непосредственно примыкающего нижележащего уровня. С другой стороны, результаты работы всех модулей, принадлежащих некоторому уровню, могут быть переданы только модулям соседнего вышележащего уровня. Такая иерархическая декомпозиция задачи предполагает четкое определение функций каждого уровня и интерфейсов между уровнями. Интерфейс определяет набор функций, которые нижележащий уровень предоставляет вышележащему. В результате иерархической декомпозиции достигается относительная независимость уровней, а значит, и возможность их легкой замены.

Формализованные правила, определяющие последовательность и формат сообщений, которыми обмениваются сетевые компоненты, лежащие на одном уровне, но в разных узлах, называются протоколом. Модули, реализующие протоколы соседних уровней и находящиеся в одном узле, также взаимодействуют друг с другом в соответствии с четко определенными правилами и с помощью стандартизованных форматов сообщений. Эти правила принято называть интерфейсом. ***Интерфейс определяет набор сервисов предоставляемый данным уровнем соседнему уровню.*** В сущности, протокол и интерфейс выражают одно и то же понятие, но традиционно в сетях за ними закрепили разные области действия: протоколы определяют правила взаимодействия модулей одного уровня в разных узлах, а интерфейсы – модулей соседних уровней в одном узле. Средства каждого уровня должны отрабатывать, во-первых, свой собственный протокол, а во-вторых, интерфейсы с соседними уровнями.

Иерархически организованный набор протоколов, достаточный для организации взаимодействия узлов в сети, называется стеком коммуникационных протоколов. Коммуникационные протоколы могут быть реализованы как программно, так и аппаратно. Протоколы нижних уровней часто реализуются комбинацией программных и аппаратных средств, а протоколы верхних уровней, как правило, чисто программными средствами. Программный модуль, реализующий некоторый протокол, часто для краткости также называют протоколом. При этом соотношение между протоколом – формально определенной процедурой и протоколом – программным модулем, реализующим эту процедуру, аналогично соотношению между алгоритмом решения некоторой задачи и программой, решающей эту задачу.

Понятно, что одни и тот же алгоритм может быть запрограммирован с разной степенью эффективности. Точно так же протокол может иметь несколько программных реализаций. Именно поэтому при сравнения протоколов следует учитывать не только логику их работы, но и качество программных решений Более того, на эффективность взаимодействия устройств в сети влияет качество всей совокупности протоколов, составляющих стек, в частности, насколько рационально распределены функции между протоколами разных уровней и насколько хорошо определены интерфейсы между ними. Протоколы реализуются не только компьютерами, но и другими сетевыми устройствами: концентраторами, мостами, коммутаторами, маршрутизаторами.

Из того что протокол является соглашением, принятым двумя взаимодействующими объектами, совсем не следует, что он обязательно является стандартным. Но на практике при реализации сетей стремятся использовать стандартные протоколы. Это могут быть фирменные, национальные или международные стандарты. В широком смысле открытой системой может быть названа любая система, которая построена в соответствии с открытыми спецификациями. Под термином «спецификация» понимают формализованное описание аппаратных или программных компонентов, способов их функционирования, взаимодействия с другими компонентами, условий эксплуатации, ограничений и особых характеристик. Использование при разработке систем открытых специфика-

ций позволяет третьим сторонам разрабатывать для этих систем различные аппаратные или программные средства расширения и модификации, а также создавать программно-аппаратные комплексы из продуктов разных производителей.

Модульность – одно из неотъемлемых свойств сетей. Разнообразные требования, предъявляемые потребителями к компьютерным сетям, привели к такому же разнообразию выпускаемых для построения сети устройств и программ. В результате не существует компании, которая смогла бы обеспечить производство полного набора всех типов оборудования и программного обеспечения, требуемого для построения сети. Но так как все компоненты сети должны работать согласованно, необходимым оказалось принятие стандартов, которые гарантировали бы совместимость оборудования и программ различных фирм-изготовителей. Модульный подход только тогда дает преимущества, когда сопровождается следованием стандартам. Совместимость достигается после того, как все производители реализуют этот стандарт в своих изделиях, причем одинаковым образом.

В начале 80-х гг. ряд международных организаций по стандартизации – ISO, ITU-T и некоторые другие – разработали модель, которая сыграла значительную роль в развитии сетей. Эта модель называется моделью взаимодействия открытых систем. (Open System Interconnection) или моделью OSI. Эталонная модель OSI, иногда называемая стеком OSI представляет собой 7-уровневую сетевую иерархию (рис. 2.7.1) разработанную Международной организацией по стандартам (International Standardization Organization – ISO). Эта модель содержит в себе по сути две различные модели:

- горизонтальную модель на базе протоколов, обеспечивающую механизм взаимодействия программ и процессов на различных машинах;
- вертикальную модель на основе услуг, обеспечиваемых соседними уровнями друг другу на одной машине.

В горизонтальной модели двум программам требуется общий протокол для обмена данными. В вертикальной – соседние уровни обмениваются данными с использованием интерфейсов API (Application Program Interface – программный интерфейс приложения).

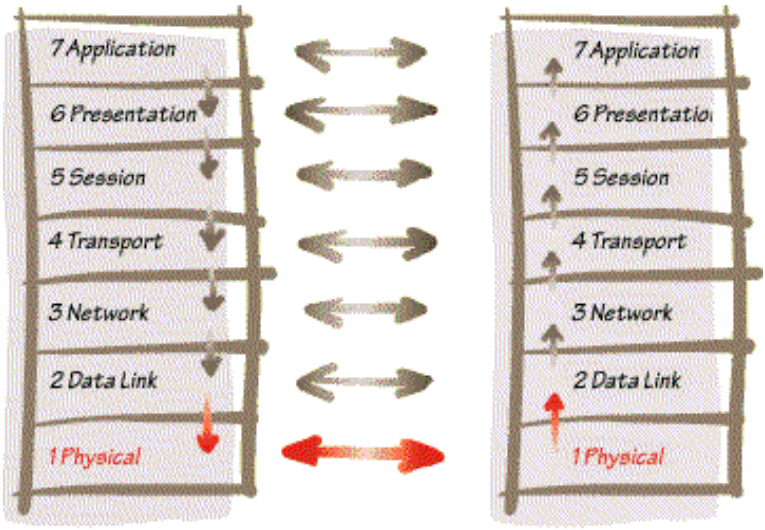


Рис. 2.7.1. Модель OSI

Протоколы нижних четырех уровней обобщенно называют сетевым транспортом или транспортной подсистемой, так как они полностью решают задачу транспортировки сообщений с заданным уровнем качества в составных сетях с произвольной топологией и различными технологиями. Остальные три верхних уровня решают задачи предоставления прикладных сервисов на основании имеющейся транспортной подсистемы.

Функции всех уровней модели OSI могут быть отнесены к одной из двух групп:

- зависящие от конкретной технической реализации сети и используемого коммуникационного оборудования (три нижних уровня). Например, переход на оборудование FDDI означает полную смену протоколов физического и канального уровней;
- ориентированные на работу с приложениями (прикладной представительный, сеансовый) – мало зависят от технических особенностей построения сети;

Транспортный уровень является промежуточным, он скрывает все детали функционирования нижних уровней от верхних. Это позволяет разрабатывать приложения, не зависящие от технических средств непосредственной транспортировки сообщений.

Уровень 1, физический. Физический уровень получает пакеты данных от вышележащего канального уровня и преобразует их в оптические или электрические сигналы, соответствующие 0 и 1 бинарного потока. Эти сигналы посылаются через среду передачи на приемный узел. Механические и электрические/оптические свойства среды передачи определяются на физическом уровне и включают:

- Тип кабелей и разъемов.
- Разводку контактов в разъемах.
- Схему кодирования сигналов для значений 0 и 1.
- Длины физических сегментов.

К числу наиболее распространенных спецификаций физического уровня относятся:

- EIA-RS-232-C, CCITT V.24/V.28 – механические/электрические характеристики несбалансированного последовательного интерфейса.
- EIA-RS-422/449, CCITT V.10 – механические, электрические и оптические характеристики сбалансированного последовательного интерфейса.
- IEEE 802.3 – Ethernet.
- IEEE 802.5 – Token ring.

Уровень 2, канальный. Канальный уровень обеспечивает создание, передачу и прием кадров данных. Этот уровень обслуживает запросы сетевого уровня и использует сервис физического уровня для приема и передачи пакетов. Задачей канального уровня является:

- проверка доступности среды передачи;
- Реализация механизмов защиты от ошибок.

Спецификации IEEE 802.x делят канальный уровень на два подуровня: управление логическим каналом (LLC) и управление доступом к среде (MAC). LLC обеспечивает обслуживание сетевого уровня, а подуровень MAC регулирует доступ к разделяемой физической среде.

Наиболее часто используемые на уровне 2 протоколы включают:

- HDLC для последовательных соединений (High – Level Data Link Control – высокоуровневый протокол управления каналом).

- IEEE 802.2 LLC (тип I и тип II) обеспечивают MAC для сред 802.x.
- Ethernet –протокол управления доступом к сети в шинных и звездообразных топологиях.
- Token ring – протокол управления доступом к среде в кольцевых LAN.
- FDDI(Fiber Distributed Data Interface – распределенный интерфейс передачи данных по волоконно-оптическим сетям) – протокол с передачей маркера в высокоскоростных сетях.
- X.25 – протокол для взаимодействия конечной системы с сетями пакетной коммутации (в сетях ISDN).
- Frame relay – ретрансляция кадров (упрощение технологии коммутации пакетов)

На канальном уровне стандартизуются; формат кадра, тип защиты от ошибок.

В протоколах канального уровня, используемых в локальных сетях, заложена определенная структура связей между компьютерами и способы их адресации. Канальный уровень обеспечивает доставку кадра между двумя узлами локальной сети с той топологией, для которой он был разработан. В локальных сетях протоколы канального уровня используются компьютерами, мостами, коммутаторами и маршрутизаторами. В компьютерах функции канального уровня реализуются совместными усилиями сетевых адаптеров и их драйверов.

В глобальных сетях, которые редко обладают регулярной топологией, канальный уровень часто обеспечивает обмен сообщениями только между двумя соседними компьютерами, соединенными индивидуальной линией связи, а доставка сообщений через всю сеть осуществляется средствами сетевого уровня. В ATM и Frame Relay функции канального уровня объединены с функциями сетевого уровня.

Уровень 3, сетевой. Чтобы, с одной стороны, сохранить простоту процедур передачи данных для типовых топологий, а с другой, допустить использование произвольных топологий, вводится дополнительный сетевой уровень. Под сетью понимается в данном случае совокупность компьютеров, соединенных между собой в соответствии с одной из сетевых топологий и использующих для

передачи данных один из протоколов канального уровня, определенных для этой топологии. Внутри сети доставка данных обеспечивается протоколом канального уровня, а доставкой данных между сетями занимается сетевой уровень, на котором стандартизируются: вид маршрутизации и процесс отображения локальных адресов в глобальный адрес сети

Сетевой уровень отвечает за деление пользователей на группы и создания надежных и гибких барьеров на пути нежелательного трафика между группами. Сетевой уровень обеспечивает также прозрачную передачу пакетов на транспортный уровень.

Наиболее часто на сетевом уровне используются протоколы:

- IP – протокол Internet.
- IPX – протокол межсетевого обмена.
- X.25 (частично этот протокол реализован на уровне 2.
- CLNP – сетевой протокол без организации соединений.

На сетевом уровне определяются:

- сетевые протоколы – реализуют продвижение пакетов через сеть;
- протоколы маршрутизации – с их помощью маршрутизаторы собирают информацию о топологии межсетевых соединений;
- протоколы разрешения адресов (Adress Resolution Protocol – ARP) – отвечают за отображение адреса узла, используемого на сетевом уровне, в локальный адрес сети.

Уровень 4, транспортный. Транспортный уровень делит потоки информации на достаточно малые фрагменты (пакеты) для передачи их на сетевой уровень.

На этом уровне стандартизуются:

– приоритеты;

– восстановление прерванной связи;

– порядок мультиплексирования нескольких соединений между различными прикладными протоколами через общий транспортный протокол;

– порядок исправления ошибок передачи (искажение, потеря, дублирование пакетов).

Как правило, все протоколы, начиная с транспортного и выше, реализуются программными средствами конечных узлов сети – компонентами их сетевых операционных систем.

Наиболее распространенные протоколы транспортного уровня включают:

- TCP – протокол управления передачей.
- NCP – Netware Core Protocol .
- SPX – упорядоченный обмен пакетами.
- TP4 – протокол передачи класса 4.

В то время как задачей сетевого уровня является передача данных между произвольными узлами сети, задача транспортного уровня заключается в передаче данных между любыми прикладными процессами, выполняющимися на любых узлах сети. Действительно, после того, как пакет средствами протокола IP доставлен в компьютер-получатель, данные необходимо направить конкретному процессу-получателю. Каждый компьютер может выполнять несколько процессов, более того, прикладной процесс тоже может иметь несколько точек входа, выступающих в качестве адреса назначения для пакетов данных.Пакеты, поступающие на транспортный уровень, организуются операционной системой в виде множества очередей к точкам входа различных прикладных процессов. В терминологии TCP/IP такие системные очереди называются *портами*. Таким образом, адресом назначения, который используется на транспортном уровне, является идентификатор (номер) порта прикладного сервиса. ***Номер порта, задаваемый транспортным уровнем, в совокупности с номером сети и номером компьютера, задаваемыми сетевым уровнем, однозначно определяют прикладной процесс в сети.***

Назначение номеров портов прикладным процессам осуществляется либо централизованно, если эти процессы представляют собой популярные общедоступные сервисы, типа сервиса удаленного доступа к файлам TFTP (Trivial FTP) или сервиса удаленного управления telnet либо локально для тех сервисов, которые еще не стали столь распространенными, чтобы за ними закреплять стандартные (зарезервированные) номера. Централизованное присвоение сервисам номеров портов выполняется организацией Internet Assigned Numbers Authority. Эти номера затем закрепляются и опубликовываются в стандартах Internet. Например, упомянутому выше сервису удаленного доступа к файлам TFTP присвоен стандартный номер порта 69. ***Локальное присвоение***

номера порта заключается в том, что разработчик некоторого приложения просто связывает с ним любой доступный, произвольно выбранный числовой идентификатор, обращая внимание на то, чтобы он не входил в число зарезервированных номеров портов. В дальнейшем все удаленные запросы к данному приложению от других приложений должны адресоваться с указанием назначенного ему номера порта.

Для обеспечения сетевых коммуникаций используются сокеты. *Сокет – это конечная точка сетевых коммуникаций. Каждый использующийся сокет имеет тип и ассоциированный с ним процесс. Сокеты существуют внутри коммуникационных доменов. Домены – это абстракции, которые подразумевают конкретную структуру адреса и множество протоколов, которое определяет различные типы сокетов внутри домена. Примерами коммуникационных доменов могут быть UNIX домен, Internet домен и т.д.*

В Internet домене сокет – это комбинация IP адреса и номера порта, которая однозначно определяет отдельный сетевой процесс во всей глобальной сети Internet. Два сокета, один – для хоста-получателя, другой – для хоста-отправителя, определяют соединение для протоколов, ориентированных на установление связи, таких, как TCP.

Уровень 5, сеансовый. Сеансовый уровень обеспечивает управление диалогом: фиксирует, какая из сторон является активной в данный момент, предоставляет средства синхронизации. На этом уровне стандартизуются:

- Порядок определения активной стороны.
- Включение контрольных точек в длинные передачи.

Протоколы сеансового уровня обычно являются составной частью функций трех верхних уровней модели и реализуются в одном протоколе с прикладным уровнем.

Уровень 6, уровень представления. Уровень представления отвечает за возможность преодоления синтаксических различий в представлении данных или же различия в кодах символов, например, кодов ASCII и EBCDIC. Стандартизуется шифрование и дешифрование данных. Пример протокола уровня представления Secure Socket Layer (SSL) который обеспечивает секретный обмен сообщениями для протоколов прикладного уровня стека TCP/IP.

Уровень 7, прикладной. Прикладной уровень отвечает за доступ приложений в сеть. Это набор протоколов, с помощью которых пользователи сети получают доступ к разделяемым ресурсам, таким как файлы, принтеры, гипертекстовые WEB-страницы, а также организуют свою совместную работу, например, с помощью протокола электронной почты. Задачами этого уровня является перенос файлов, обмен почтовыми сообщениями и управление сетью.

К числу наиболее распространенных протоколов верхних уровней относятся:

- FTP – протокол переноса файлов.
- TFTP – упрощенный протокол переноса файлов.
- X.400 – электронная почта.
- Telnet.
- SMTP – простой протокол почтового обмена.
- CMIP – общий протокол управления информацией.
- SNMP – простой протокол управления сетью.
- NFS – сетевая файловая система.
- FTAM – метод доступа для переноса файлов.

На рис. 2.7.2 показано соответствие коммуникационного оборудования модели OSI.

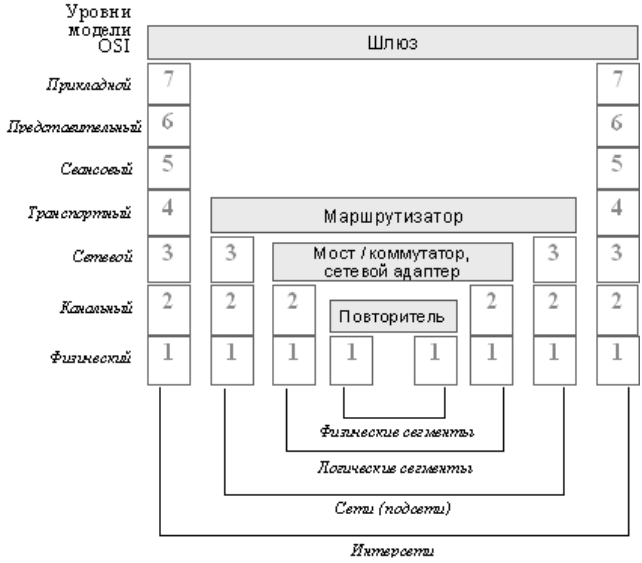


Рис. 2.7.2. Соответствие коммуникационного оборудования модели OSI

Преимущества многоуровневой модели:

1. Поскольку функции каждого уровня четко определены, стандарты могут разрабатываться одновременно и независимо для каждого уровня, что ускоряет процесс стандартизации.

2. Из-за четкого определения границ каждого уровня изменение стандартов одного уровня не затрагивает программное обеспечение на других уровнях, что облегчает ввод новых стандартов.

Недостатки многоуровневой модели:

1. Многоуровневая модель скорее предписывающая, чем описывающая, поэтому существует возможность определения на данном уровне нескольких протоколов, разных по функциональным возможностям, но общих по совместному использованию протоколов поддержки нижестоящего уровня.

2. Благодаря четким интерфейсам между уровнями можно заменять одни протоколы уровня другими без воздействия на другие уровни. Это не всегда желательно и возможно. На канальном уровне локальную сеть можно приспособить к групповой или широковещательной адресации. Если канальный уровень по стандарту IEEE 802 помещен ниже объекта сетевого протокола, не поддерживающего групповую или широковещательную передачу, то высшие уровни этой службой воспользоваться не смогут, т. е. не надо пренебрегать структурой протоколов.

2.8. Маршрутизация и управление в телекоммуникационных сетях

Маршрутизация – это комплексный, важный аспект сетей с пакетной коммутацией. К функции маршрутизации предъявляются следующие требования:

1. Правильность.
2. Простота.
3. Живучесть.
4. Стабильность.
5. Равнодоступность.
6. Оптимальность.
7. Эффективность.

Критерии эффективности используются для выбора маршрутов и могут представлять собой стремление:

- К минимуму хопов (количество переходов между узлами);
- наименьшей стоимости передачи.

На рис. 2.8.1 показана сеть, в которой пара линий со стрелками между каждыми двумя узлами изображает канал между этими узлами, а числа около них означают стоимость передачи по этому каналу в данном направлении.

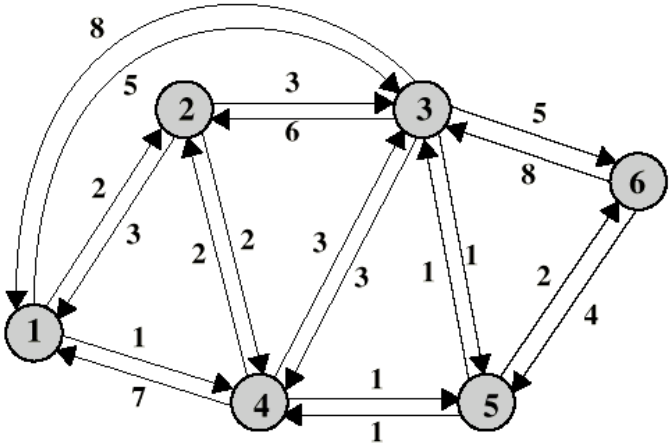


Рис. 2.8.1. Пример сети с пакетной коммутацией [4]

Кратчайший маршрут (с наименьшим числом переходов) от узла 1 к узлу 6 пролегает через узлы 1–3–б (стоимость 5 + 5= 10), однако наименьшую стоимость будет иметь маршрут 1 – 4 – 5 – б (стоимость 1 + 1 + 2= 4). Стоимость канала определяется исходя из какой-то одной или нескольких задач разработки сети. Например:

- чем больше пропускная способность участка сети, тем меньше его стоимость;
- чем больше время ожидания на участке сети, тем выше его стоимость.

Характеристиками решения о маршрутизации являются время и место его принятия.

Время принятия решения о маршруте:

- во время установки виртуального канала;
- индивидуально для каждого пакета (дейтаграммы).

Место принятия решения о маршруте продвижения сообщения по сети указывает, какой узел отвечает за принятие решения о

маршрутизации. В зависимости от места принятия решения, маршрутизация бывает:

- распределенная (решения принимаются на каждом узле сети) – более сложный, но более устойчивый метод маршрутизации;
- централизованная (решение о маршрутизации принимается на узле управления);
- маршрутизация от источника – позволяет пользователю самому задавать маршрут в сети.

Таким образом, решения о выборе маршрута в сети принимаются на основе топологии сети, нагрузки и стоимости канала. Некоторые методики маршрутизации не используют эту информацию, но позволяют передавать пакеты (например, лавинная, случайная маршрутизация).

Рассмотрим источники и интервал обновления сетевой информации.

В распределенной маршрутизации:

- узлы используют локальную информацию;
- могут получать информацию от соседних узлов сети;
- могут получать информацию от всех узлов сети;
- непрерывное обновление сетевой информации.

В централизованной (заданной) маршрутизации:

- информация собирается от всех узлов в сети;
- обновление информации не производится;
- если маршрутизация адаптивная, то обновление сетевой информации производится регулярно.

Рассмотрим стратегии маршрутизации.

При фиксированной маршрутизации:

– существует один постоянный маршрут для каждой пары источник-получатель;

– маршрут определяется по алгоритму минимальной стоимости;

– маршрут является фиксированным до изменений в топологии сети;

– алгоритм может учитывать отказы каналов и узлов назначением резервного маршрута.

При лавинной маршрутизации:

– не требует сетевой информации;

– пакет посылается узлом к каждому соседу;

– пакеты передаются по всем связям, кроме входящей, поэтому некоторое число копий достигают адресата;

– каждый пакет нумеруется, поэтому дубликаты отклоняются адресатом;

– узлы могут запоминать уже переданные пакеты, чтобы не превышать нагрузку трафика;

– алгоритм может предусматривать счетчик хопов в пакетах.

Свойства лавинной маршрутизации:

- устойчивость, так как испытываются все возможные маршруты;
- по крайней мере, один пакет будет иметь минимум хопов, это свойство можно использовать для установления виртуального канала;
- посещаются все узлы, это можно использовать для распространения информации в сети.

При случайной маршрутизации:

– сочетает простоту и живучесть лавинной маршрутизации с низким объемом трафика;

– узел выбирает исходящий путь случайно из всех связей, кроме той, по которой к нему прибывает пакет или делает это на основе вероятности $P_i = \frac{R_i}{\sum_j R_j}$, где P_i – скорость выбора *i*-го канала; R_i – скорость передачи в *i*-м канале.

– не нужно сетевой информации;

– маршрут, как правило, не является минимальным по цене и количеству хопов.

При адаптивной маршрутизации:

– используется почти всеми сетями с коммутацией пакетов;

– требует информации о сети, так как на решения о маршруте влияют отказы узлов, перегрузка трафика;

– решение о маршрутизации получается сложным, поэтому возрастает объем информации, обрабатываемой на узлах сети. Должен быть реализован компромисс между величиной заголовка и качеством сетевой информации;

– слишком быстрая реакция при адаптивной стратегии может вызвать перегрузку в сети, при слишком медленной реакции адаптация теряет смысл.

Преимуществами адаптивной маршрутизации являются:

- повышение быстродействия в сети;
- облегчение управления перегрузкой.

Однако сложность системы может уравновесить теоретические выгоды.

Адаптивная маршрутизация по источнику информации классифицируется на:

- локальную (изолированную);
- маршрутизацию по связи с самой короткой очередью;
- маршрутизацию по вводу предпочитаемого направления (так как короткая очередь может вести не в нужном направлении). Это выравнивает трафик в сети, но используется редко из-за отсутствия легко доступной сетевой информации.

Стратегии адаптивной маршрутизации удобно классифицировать по источнику информации, которым может быть локальный узел, соседние узлы или все узлы. Примером адаптивной маршрутизации, в которой используется только локальная информация, является стратегия, когда узел направляет каждый пакет в выходной канал с самой короткой очередью Q. В результате происходит выравнивание нагрузки в выходных каналах. Однако некоторые выходные каналы могут не вести в правильном общем направлении. Можно усовершенствовать эту стратегию, введя предпочитаемое направление, как при случайной маршрутизации. В этом случае каждый канал, выходящий из узла, будет иметь приоритет B_i для каждого узла назначения i. Для каждого входящего пакета, направляемого на узел i, узел выбирает выходной канал с наименьшей суммой $Q + B_i$. Таким образом, узел будет, как правило, пересылать пакеты в оптимальном направлении с учетом текущих задержек, вызванных нагрузкой.

На рис. 2.8.2 показано состояние узла 4 с рис. 2.8.1 в некоторый момент времени. Узел 4 имеет каналы к четырем другим узлам. На этот узел прибыло значительное число пакетов, и на каждом выходном канале накопились очереди пакетов, ожидающих отправки. Рассмотрим пакет, прибывший с узла 1 и предназначен-

ный для узла 6. На какой из выходных каналов он должен быть направлен? На основании текущих размеров очередей и значений приоритетов (B_6) каждого выходного канала определяем, что наименьшее значение $Q + B_6$ будет 4 – на канале к узлу 3. Таким образом, узел 4 направляет пакет через узел 3.

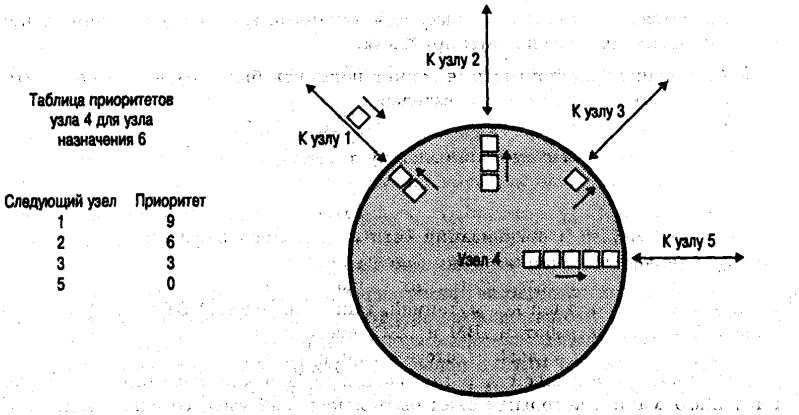


Рис. 2.8.2. Пример изолированной адаптивной маршрутизации [4]

Адаптивные схемы, использующие только локальную информацию, используются редко, так как они не прибегают к легко доступной информации. Распространены в основном стратегии, основанные на информации от соседних узлов или всех узлов. Обе они пользуются информацией о задержках и отказах на каждом узле, доступной на нем. Такие адаптивные стратегии могут быть распре деленными или централизованными. В случае распределенной стратегии каждый узел обменивается информацией с другими узлами. На основе поступающей информации узел пытается оценить ситуацию с задержками во всей сети и применяет алгоритм наименьшей стоимости. В случае централизованной маршрутизации каждый узел сообщает о задержках в своих каналах центральному узлу, который проектирует маршруты на базе этой информации и рассылает сведения о маршрутах обратно на узлы.

По отношению к автономным системам составной сети протоколы маршрутизации делятся на внешние и внутренние. Внешние протоколы переносят маршрутную информацию между автономными системами, а внутренние применяются только в преде-

лах конкретной автономной системы. Внутренние протоколы, по сравнению с внешними, оказывают более существенное влияние на общую эффективность маршрутизации пакетов в составных сетях.

В настоящее время наиболее распространенными внутренними протоколами маршрутизации являются:

• протокол RIP (Routing Information Protocol);

• протокол OSPF (Open Shortest Path First).

Для оптимизации маршрута передачи информационных пакетов в протоколе RIP используется простой *дистанционно-векторный алгоритм (алгоритм Беллмана-Форда),* не требующий существенных вычислительных ресурсов. Протокол RIP наиболее успешно работает в небольших сетях с количеством промежуточных маршрутизаторов не более 15.

RIP-маршрутизаторы при выборе маршрута обычно используют самую простую метрику – количество промежуточных маршрутизаторов между сетями, измеряемое в хопах .В сетях, использующих RIP и имеющих петлевидные маршруты, могут наблюдаться достаточно длительные периоды нестабильной работы, когда пакеты зацикливаются в маршрутных петлях и не доходят до адресатов. Для борьбы с этими явлениями в RIP-маршрутизаторах предусмотрено несколько приемов (Split Horizon, Hold Down, Triggered Updates), которые сокращают в некоторых случаях периоды нестабильности. В настоящее время из-за указанных недостатков RIP-маршрутизаторы усиленно вытесняются OSPF–маршрутизаторами.

Протокол OSPF был разработан для эффективной маршрутизации информационных пакетов в больших составных сетях со сложной топологией, включающей петли. Он основан на алгоритме *поиска наикратчайшего пути, (алгоритм «кратчайшего пути» Дейкстры),* который обладает высокой устойчивостью к изменениям топологии сети. При выборе маршрута OSPF маршрутизаторы используют метрику, учитывающую пропускную способность составных сетей. Протокол OSPF является первым протоколом маршрутизации для составных сетей, который учитывает параметры качества обслуживания (пропускная способность, задержка и надежность), указываемые в заголовках информационных пакетов. Для каждого типа качества обслуживания строится отдельная таб-

лица маршрутизации. Протокол OSPF обладает высокой вычислительной сложностью, поэтому чаще всего реализуется на мощных аппаратных маршрутизаторах.

2.9. Стратегии межсетевого взаимодействия

Средства взаимодействия компьютеров в сети организованы в виде многоуровневой структуры – стека протоколов. В однородной сети все компьютеры используют один и тот же стек. В контексте межсетевого взаимодействия понятие "сеть" можно определить как совокупность компьютеров, общающихся друг с другом с помощью единого стека протоколов. Проблема возникает тогда, когда требуется организовать взаимодействие компьютеров, принадлежащих разным сетям, то есть организовать взаимодействие компьютеров, на которых установлены разные стеки коммуникационных протоколов.

Задачи устранения неоднородности имеют некоторую специфику в зависимости от того, к какому уровню модели OSI они относятся, и даже имеют разные названия. Задача объединения транспортных подсистем, отвечающих только за передачу сообщений, обычно называется *internetworking*.

Несколько другая проблема, называемая *interoperability*, возникает при объединении сетей, использующих разные протоколы более высоких уровней. Как сделать, например, возможным для клиентов сети Novell NetWare доступ к файловому сервису Windows NT или работу с сервисом telnet ОС Unix? Очевидно, что подобные проблемы весьма характерны для корпоративных сетей, где в разных подразделениях часто работают разные сетевые операционные системы.

Проблема межсетевого взаимодействия может иметь разные внешние проявления, но суть ее одна – несовпадение используемых коммуникационных протоколов. Например, эта проблема возникает в сети, в которой используется только одна сетевая ОС, но в которой транспортная подсистема неоднородна из-за того, что сеть включает в себя фрагменты Ethernet, объединенные кольцом FDDI. Здесь в качестве взаимодействующих сетей выступают группы компьютеров, использующие различные протоколы канального и физического уровня, например, сеть Ethernet, сеть FDDI.

Равным образом проблема межсетевого взаимодействия может возникнуть в однородной сети Ethernet, в которой установлено несколько сетевых ОС. В этом случае все компьютеры и все приложения используют для транспортировки сообщений один и тот же набор протоколов, но взаимодействие клиентских и серверных частей сетевых сервисов осуществляется по разным протоколам. Здесь компьютеры могут быть отнесены к разным сетям, если у них различаются протоколы верхних уровней, например, сеть Windows NT, сеть NetWare. Конечно, эти сети могут спокойно сосуществовать, не мешая друг другу и мирно пользуясь общим транспортом. Однако, если потребуется обеспечить доступ к данным файл-сервера NetWare для клиентов Windows NT, администратор сети столкнется в необходимостью согласования сетевых сервисов. Существует три основных подхода к согласованию разных стеков протоколов:

- трансляция;
- мультиплексирование;
- инкапсуляция.

2.9.1. Трансляция протоколов

Трансляция обеспечивает согласование двух протоколов путем преобразования (трансляции) сообщений, поступающих от одной сети, в формат другой сети. Транслирующий элемент, в качестве которого могут выступать, например, программный или аппаратный шлюз, мост, коммутатор или маршрутизатор, размещается между взаимодействующими сетями и служит посредником в их "диалоге" (рис. 2.9.1). В зависимости от типа транслируемых протоколов процедура трансляции может иметь разную степень сложности. Так, преобразование протокола Ethernet в протокол Token Ring сводится к нескольким несложным действиям, главным образом благодаря тому, что в обоих протоколах используется единая адресация узлов. А вот трансляция протоколов сетевого уровня IP и IPX представляет собой гораздо более сложный, интеллектуальный процесс, включающий не только преобразование форматов сообщений, но и отображение адресов сетей и узлов, различным образом трактуемых в этих протоколах.

Сложность трансляции зависит не от того, насколько высокому уровню соответствуют транслируемые протоколы, а от того,

насколько сильно они различаются. Так, например, весьма сложной представляется трансляция протоколов канального уровня ATM-Ethernet, именно поэтому для их согласования используется не трансляция, а другие подходы. К частному случаю трансляции протоколов может быть отнесен широко применяемый подход с использованием общего протокола сетевого уровня (IP или IPX). Заголовок сетевого уровня несет информацию, которая, дополняя информацию заголовка канального уровня, позволяет выполнять преобразование протоколов канального уровня. Процедура трансляции в данном случае выполняется маршрутизаторами, причем помимо информации, содержащейся в заголовках транслируемых кадров, то есть в заголовках канального уровня, дополнительно используется информация более высокого уровня, извлекаемая из заголовков сетевого уровня.

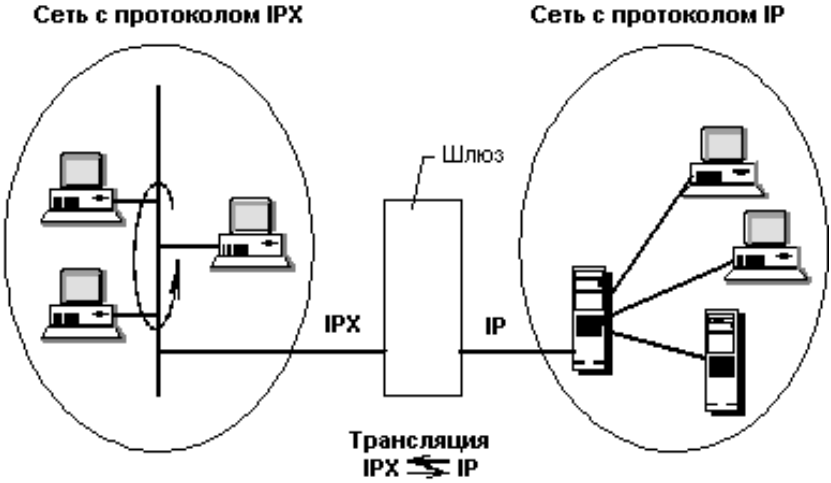


Рис. 2.9.1. Пример трансляции протоколов

Трансляцию протоколов могут выполнять различные устройства – мосты, коммутаторы, маршрутизаторы, программные и аппаратные шлюзы. Часто транслятор протоколов называют шлюзом в широком смысле, независимо от того, какие протоколы он транслирует. В этом случае подчеркивается тот факт, что трансляция осуществляется выделенным устройством, соединяющим две разнородные сети.

2.9.2. Мультиплексирование протоколов

Другим подходом к согласованию коммуникационных протоколов является технология мультиплексирования. Этот подход состоит в установке нескольких дополнительных стеков протоколов на одной из конечных машин, участвующих во взаимодействии (рис. 2.9.2). Компьютер с несколькими стеками протоколов использует для взаимодействия с другим компьютером тот стек, который понимает этот компьютер.

Для тогочтобы запрос от прикладного процесса был правильно обработан и направлен через соответствующий стек, необходимо наличие специального программного элемента - *мультиплексора протоколов*. Мультиплексор должен уметь определять, к какой сети направляется запрос клиента.

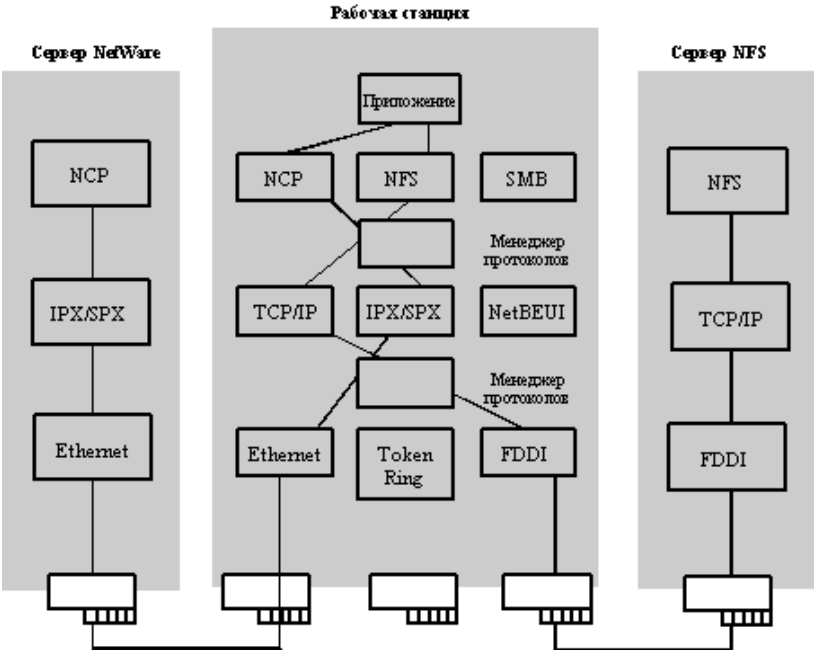


Рис. 2.9.2. Мультиплексирование протоколов

При использовании технологии мультиплексирования структура коммуникационных средств операционной системы может быть и более сложной: мультиплексирование осуществляется не

на уровне стеков, а на уровне отдельных протоколов. В общем случае на каждом уровне может быть установлено несколько протоколов, и для каждого уровня может существовать собственный мультиплексор, выполняющий коммутацию между протоколами соседних уровней. Например, рабочая станция может получить доступ к сетям с протоколами NetBIOS, IP, IPX через один сетевой адаптер. Аналогично сервер, поддерживающий прикладные протоколы NCP, SMB и NFS может без проблем выполнять запросы рабочих станций сетей NetWare, Windows NT и Sun одновременно.

2.9.3. Сравнение трансляции и мультиплексирования

Использование техники трансляции связано со следующими достоинствами:

- Не требуется устанавливать дополнительное программное обеспечение на рабочих станциях.
- Сохраняется привычная среда пользователей и приложений, транслятор полностью прозрачен для них.
- Все проблемы межсетевого взаимодействия локализованы, следовательно, упрощается администрирование, поиск неисправностей, обеспечение безопасности.

Недостатки согласования протоколов путем трансляции состоят в том, что:

- Транслятор замедляет работу из-за относительно больших временных затрат на сложную процедуру трансляции, а также из-за ожидания запросов в очередях к единственному элементу, через который проходит весь межсетевой трафик.
- Централизация обслуживания запросов к "чужой" сети снижает надежность. Однако можно предусмотреть резервирование - использовать несколько трансляторов.
- При увеличении числа пользователей и интенсивности обращений к ресурсам другой сети резко снижается производительность – плохая масштабируемость.

Достоинства мультиплексирования по сравнению с трансляцией протоколов заключаются в следующем:

- Запросы выполняются быстрее, за счет отсутствия очередей к единственному межсетевому устройству и использования

более простой, чем трансляция, процедуры переключения на нужный протокол.

- Более надежный способ – при отказе стека на одном из компьютеров доступ к ресурсам другой сети возможен посредством протоколов, установленных на других компьютерах.

Недостатки данного подхода:

- Сложнее осуществляется администрирование и контроль доступа.
- Высокая избыточность требует дополнительных ресурсов от рабочих станций, особенно если требуется установить несколько стеков для доступа к нескольким сетям.
- Менее удобен для пользователей по сравнению с транслятором, так как требует навыков работы с транспортными протоколами "чужих" сетей.

2.9.4. Инкапсуляция (туннелирование) протоколов

Инкапсуляция (encapsulation) или *туннелирование* (tunneling) – это еще один метод решения задачи согласования сетей, который однако применим только для согласования транспортных протоколов и только при определенных ограничениях. Инкапсуляция может быть использована, когда две сети с одной транспортной технологией необходимо соединить через сеть, использующую другую транспортную технологию. В приведенном на рис.2.9.3 примере две сети с протоколом NetBIOS нужно соединить через сеть TCP/IP. Необходимо обеспечить только взаимодействие узлов двух сетей NetBIOS, а взаимодействие между узлами NetBIOS и узлами сети TCP/IP не предусматривается. То есть, при инкапсуляции промежуточная сеть используется только как транзитная транспортная система.

Метод инкапсуляции заключается в том, что пограничные маршрутизаторы, которые подключают объединяемые сети к транзитной, упаковывают пакеты транспортного протокола объединяемых сетей в пакеты транспортного протокола транзитной сети. В данном случае пакеты NetBIOS упаковываются в пакеты TCP, как если бы пакеты NetBIOS представляли собой сообщения протокола прикладного уровня. Затем пакеты NetBIOS переносятся по сети TCP/IP до другого пограничного маршрутизатора. Второй

пограничный маршрутизатор выполняет обратную операцию - он извлекает пакеты NetBIOS из пакетов TCP и отправляет их по сети назначения адресату.

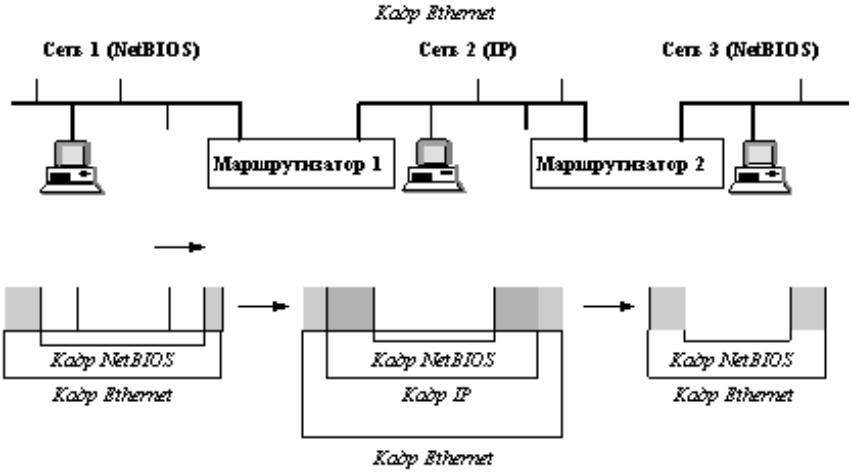


Рис. 2.9.3. Инкапсуляция протоколов сетевого уровня (вложение друг в друга)

Для реализации метода инкапсуляции пограничные маршрутизаторы должны быть соответствующим образом сконфигурированы. Они должны знать, во-первых, IP-адреса друг друга, во-вторых - NetBIOS-имена узлов объединяемых сетей. Имея такую информацию, они могут принять решение о том, какие NetBIOS-пакеты нужно переправить через транзитную сеть, какой IP-адрес указать в пакете, передаваемом через транзитную сеть и каким образом доставить NetBIOS-пакет узлу назначения в конечной сети.

Инкапсуляция может быть использована для транспортных протоколов любого уровня. Например, протокол сетевого уровня X.25 может быть инкапсулирован в протокол транспортного уровня TCP или же протокол сетевого уровня IP может быть инкапсулирован в протокол сетевого уровня X.25. Для согласования сетей на сетевом уровне могут быть использованы многопротокольные и инкапсулирующие маршрутизаторы, а также программные и аппаратные шлюзы. Обычно инкапсуляция приводит к более простым и быстрым решениям по сравнению с трансляцией, так как решает более частную задачу, не обеспечивая взаимодействия с узлами транзитной сети.

Литература

1. Основы построения телекоммуникационных систем и сетей: Учебник для вузов / В.В. Крухмалев, В.Н. Гордиенко, А.Д. Моченов и др. / Под ред. В.Н. Гордиенко и В.В. Крухмалева. – М.: Горячая линия-Телеком, 2004. – 510 с.
2. *Актерский Ю.Е.* Сети ЭВМ и телекоммуникации. Учебное пособие. – СПб.: ПВИРЭ КВ, 2005. – 223 с.
3. Телекоммуникационные системы и сети / Под ред. В.П. Шувалова. В 3-х т. – М.: Горячая линия-Телеком, 2003.
4. *Столингс В.* Компьютерные сети передачи данных. – М.: Вильямс, 2002.

3. ТРАНСПОРТНЫЕ СЕТИ

Транспортные сети предоставляют пользователям возможность передавать большие объёмы разрозненного трафика с различным, оговоренным заранее, качеством обслуживания. Первичные сети, являющиеся базовыми транспортными или магистральными сетями, служат основой для построения всего многообразия современных мультисервисных сетей связи. Таким образом, первичной сетью (ПС) называется совокупность типовых физических цепей, типовых каналов передачи и сетевых трактов системы электросвязи, образованная на базе сетевых узлов, сетевых станций, оконечных устройств первичной сети и соединяющих их линий передачи системы электросвязи [1].

Вторичная сеть связи (ВС) – совокупность линий и каналов, образованных на базе первичной сети, станций и узлов коммутации или станций и узлов переключений, предназначенная для организации связи между двумя или более, определёнными точками. Границами вторичной сети являются стыки этой сети с абонентскими оконечными устройствами. В состав ВС входят: оконечные абонентские устройства, абонентские линии (АЛ), коммутационные устройства и каналы, выделенные из ПС для организации данной ВС.

Главным требованием, предъявляемым к транспортным сетям, является выполнение сетью основной функции – обеспечения пользователям возможности доступа ко всем разделяемым ресурсам сети.

3.1. Системы передачи для транспортных сетей

Транспортные сети строятся на основе:

волоконно-оптических систем связи с применением технологий:

– DWDM (технология плотного спектрального мультиплексирования).

– CWDM – использование технологии спектрального уплотнения для передачи до 16 потоков со скоростями до 2,5 гбит/с каждый между магистральными узлами сети с возможностью ввода/вывода потоков в промежуточных узлах.

– SDH (синхронная цифровая иерархия) – создание транспортных сетей различной топологии между большим числом узлов со скоростями от 155 мбит/с до 10 гбит/с.

– PDH (плезиохронная цифровая иерархия) – соединение двух узлов со скоростью от 2 мбит/с до 34 мбит/с.

– ATM (Asynchronous Transfer Mode) – это транспортный механизм, ориентированный на установление соединения при передаче разнообразной информации в сети. Для этого в ATM разработана концепция виртуальных соединений (virtual connection) вместо выделенных физических связей между конечными точками в сети.

– IP – построение оптических сетей передачи данных с использованием технологий Gigabit Ethernet и 10 Gigabit Ethernet;

беспроводных систем связи с применением технологий:

– SDH (синхронная цифровая иерархия) – создание транспортных сетей различной топологии между большим числом узлов со скоростями от 155 мбит/с до 10 гбит/с.

– PDH (плезиохронная цифровая иерархия) – соединение двух узлов со скоростью от 2 мбит/с до 34 мбит/с.

– IP – построение сетей передачи данных с использованием технологий Ethernet.

– FSO – беспроводные оптические каналы связи. В качестве среды передачи используется луч лазера распространяющийся в свободном пространстве. Скорости передачи в таких системах могут превышать 1 гбит/с. Преимущество перед другими беспроводными системами у FSO в том, что она работает в диапазоне более 400 гГц и для её применения не требуется получать разрешения на использование частот. Возможна организация пролётов длиной до 2 км.

Проводных систем связи с применением технологий:

– SDH (синхронная цифровая иерархия) – создание транспортных сетей различной топологии между большим числом узлов со скоростями от 155 мбит/с до 10 гбит/с.

– PDH (плезиохронная цифровая иерархия) – соединение двух узлов со скоростью от 2 мбит/с до 34 мбит/с.

– ATM (Asynchronous Transfer Mode) – это транспортный механизм, ориентированный на установление соединения при пере-

даче разнообразной информации в сети. Для этого в ATM разработана концепция виртуальных соединений (virtual connection) вместо выделенных физических связей между конечными точками в сети.

– IP – построение оптических сетей передачи данных с использованием технологий Gigabit Ethernet.

– xDSL – организация транспортных потоков E1 по медному кабелю с помощью систем передачи Megatrans. Длина регенерационного участка – до 26 км, общая длина линии – до 300 км, совместная работа с АСП по двухкабельной схеме.

При выборе решения по построению транспортных сетей важно учитывать следующие критерии:

– пропускная способность – максимально возможная скорость обработки трафика, определенная стандартом технологии, на которой построена сеть. Пропускная способность отражает максимально возможный объем данных, передаваемый сетью или ее частью в единицу времени;

– отказоустойчивость – способность системы скрыть от пользователя отказ отдельных ее элементов. В отказоустойчивой системе выход из строя одного из ее элементов приводит к некоторому снижению качества ее работы (деградации), а не к полному останову;

– скорость восстановления подразумевает быстрое переключение на резервный канал передачи данных без потери информации в случае обрыва кабеля или неисправности оборудования;

– масштабируемость – означает, что сеть позволяет наращивать количество узлов и протяженность связей в очень широких пределах, при этом производительность сети не ухудшается. Для обеспечения масштабируемости сети приходится применять дополнительное коммуникационное оборудование и специальным образом структурировать сеть;

– прозрачность сети достигается в том случае, когда сеть представляется пользователям не как множество отдельных компьютеров, связанных между собой сложной системой кабелей, а как единая традиционная вычислительная машина с системой разделения времени. На уровне пользователя прозрачность означает, что для работы с удаленными ресурсами он использует те же команды и привычные процедуры, что и для работы с локальными

ресурсами. На программном уровне прозрачность заключается в том, что приложению для доступа к удаленным ресурсам требуются те же вызовы, что и для доступа к локальным ресурсам;

– гибкость подразумевает возможность быстрой структуризации, изменения конфигурации и размеров сети;

– управляемость сети подразумевает возможность централизованно контролировать состояние основных элементов сети, выявлять и решать проблемы, возникающие при работе сети, выполнять анализ производительности и планировать развитие сети.

Технической основой построения транспортных сетей являются телекоммуникационные системы передачи синхронной цифровой иерархии (Synchronous Digital Hierarchy – SDH). Их внедрение на сетях связи началось в 80-е гг. XX в. Принципиальным отличием систем SDH от ранее существовавших цифровых систем передачи считается то, что они не являются “производителями” информации, а предназначены только для высокоэффективной передачи и распределения цифровых потоков, формируемых как в традиционных структурах стандартной плезиохронной цифровой иерархии (Plesio-chronous Digital Hierarchy – PDH), так и в новых телекоммуникационных технологиях ATM, B-ISDN и т.д. Все указанные выше цифровые потоки “транспортируются” в системах SDH в виде информационных структур, названных виртуальными контейнерами (Virtual Container – VC). В структурах VC по транспортной сети переносится исходная цифровая информация, дополненная определенным количеством служебных информационных каналов, названных трактовыми заголовками (Path Overheard – POH). В общем случае дополнительные каналы предназначены для эффективного управления транспортной сетью и выполнения функции передачи оперативной, административной и обслуживающей информации (Operation, Administration, Maintenance, OAM). Это обеспечивает высокие функциональные возможности и высокую надежность сети связи.

Группы однотипных или разнотипных виртуальных контейнеров VC передаются между элементами транспортной сети (от отправителя информации к получателю) по линиям передачи в виде информационных структур, называемых синхронными транспортными модулями (Synchronous Transport Module – STM).

“Транспортирование” STM осуществляется с разными скоростями передачи соответствующим различным порядком STM-1,4, 16, 64. STM-N оснащаются соответствующими заголовками, обеспечивающими передачу STM с полной функцией OAM в пределах регенерационной секции (Regeneration Section OH – RSOH) и мультиплексорной секции (Multiplex Section OH – MSOH). Упрощенная функциональная схема системы передачи SDH, которая является основным структурным звеном транспортной сети, приведена на рис. 3.1.1. На рисунке приведены два вида секций, которые называются “Регенерационная секция” и “Мультиплексорная секция”.

“Регенерационная секция” представляет собой сегмент системы передачи между оконечным оборудованием сетевого элемента, в котором сигнал STM-N передается или принимается и регенератором, или между двумя смежными регенераторами.

“Мультиплексорная секция” – это средство передачи информации между двумя сетевыми элементами, в одном из которых формируется (собирается) сигнал STM-N, а в другом “разбирается” до компонентных потоков. В общем случае транспортная сеть SDH состоит из мультиплексорных секций, для которых уровень SDH-сигнала может быть разным в зависимости от требуемой емкости канала передачи для каждой секции.

“Тракт” – означает логическое соединение между точкой системы передач SDH, в которой производится “сборка” виртуального контейнера VC (например, из компонентных потоков PDH) и точкой, в которой VC “разбирается”. Тракт можно представить себе как трубку, проложенную через мультиплексорные секции, непосредственно соединяющую две точки, между которыми осуществляется передача информации. Для “транспортировки” различных объемов цифровой информации разработаны виртуальные контейнеры различного типа. Для европейских потоков PDH таковыми являются:

VC низшего порядка (Low order VC, LOVC).

VC-12 для “транспортировки” E1 = 2048 Кбит/с (2 М).

VC-22 для “транспортировки” E2 = 8448 Кбит/с (8 М).

VC высшего порядка (High order VC, HOVC).

VC-3 для “транспортировки” E3 = 34368 Кбит/с (34 М).

VC-4 для “транспортировки” E4 = 139264 Кбит/с (140 М).

В зависимости от “емкости” виртуального контейнера различают тракты VC-12, VC-22 (низшего порядка) и тракты виртуальных контейнеров VC-3, VC-4 (высшего порядка).

Виртуальный контейнер является элементарной единицей обрабатываемой информации в транспортной системе SDH при мультиплексировании, перекрестных соединениях (кросс-коннекция) и т.д. При этом нет необходимости доступа к “транспортируемой” информации, так как различная информация представлена в одном и том же виде, который именуется виртуальными контейнерами (в то же время к VC добавляется информация, необходимая для его обработки в пути следования).

Как указывалось выше, виртуальные контейнеры передаются между элементами транспортной сети в виде STM различного порядка. Основной (первичной) структурой для получения потоков STM является STM-1 с нормализованной скоростью передачи 155,52 Мбит/с. При этом, в зависимости от потребности сети, в цифровом потоке STM-1 возможна передача виртуальных контейнеров различного типа и в различных сочетаниях.

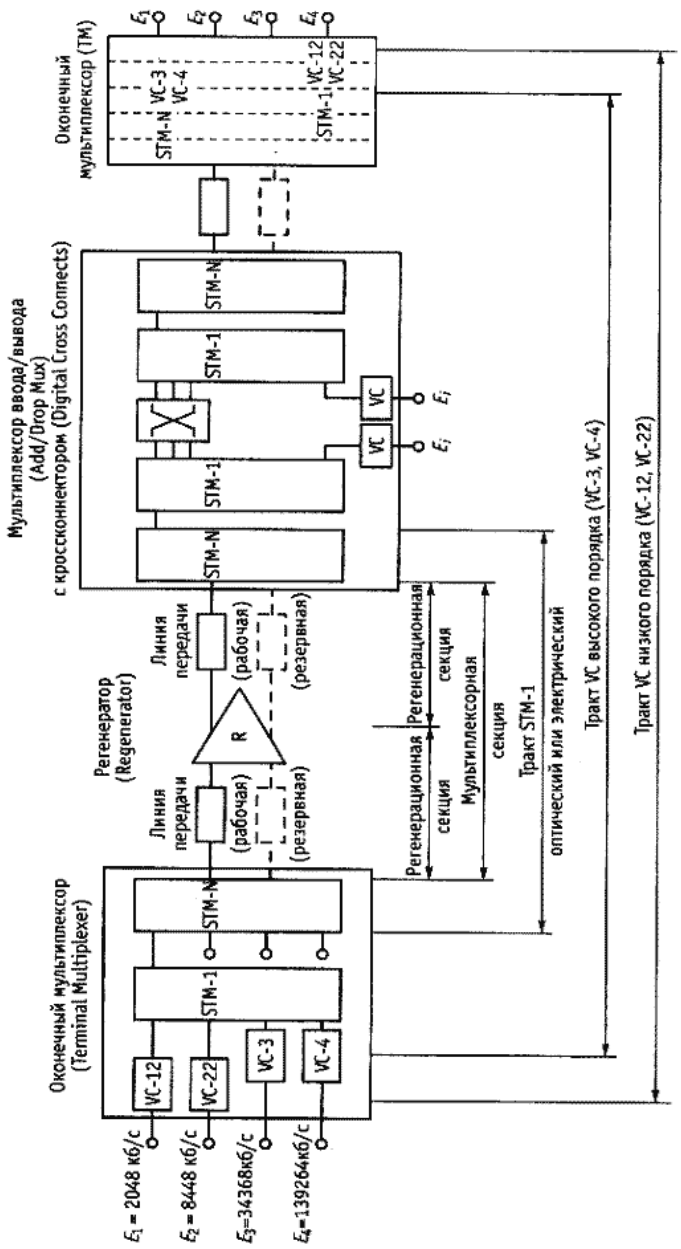
STM более высокого порядка могут быть получены из цифрового потока STM-1 простым синхронным мультиплексированием согласно рекомендации G.707 сектора телекоммуникаций Международного Союза электросвязи (МСЭ-Т). Сравнение скоростей цифровых потоков STM приведено в табл. 3.1.1.

Таблица 3.1.1

Скорости передачи цифровых потоков STM

STM - 1	155,52 Мбит/с
v	x 4
STM - 4	622,08 Мбит/с
v	x 4
STM - 16	2488,32 Мбит/с
v	x 4
STM - 64	9953,28 Мбит/с

Причем мультиплексирование, начиная с STM-4, осуществляется в оптическом диапазоне. Информационные структуры STM-N передаются между элементами транспортной сети по линиям передачи, организованным по волоконно-оптическим кабелям связи, спутниковым линиям или по цифровым радиорелейным линиям (учитывая особенности мультиплексирования, по ЦРРЛ можно передавать в электрическом виде только цифровой поток STM-1).


Оконечный мультиплексор (Terminal Multiplexer)
Мультиплексор ввода/вывода (Add/Drop Mux) с кроссконнектором (Digital Cross Connects)
Оконечный мультиплексор (ТМ)
Регенератор (Regenerator)
Линия передачи
(рабочая)
(резервная)
R
VC-12
VC-22
VC-3
VC-4
STM-1
STM-N
VC
E_1 = 2048 кб/с
E_2 = 8448 кб/с
E_3=34368кб/с
E_4=139264кб/с
Регенерационная секция
Мультиплексорная секция
Тракт STM-1
оптический или электрический
Тракт VC высокого порядка (VC-3, VC-4)
Тракт VC низкого порядка (VC-12, VC-22)

Характерной особенностью транспортных систем передачи SDH, показанных на рис. 3.1.1, является высокая степень резервирования, как линейных трактов, так и основных узлов мультиплексорного оборудования. Так, линии передачи между элементами сети обычно полностью резервируются, что позволяет избежать потерь огромных потоков информации при авариях (например, даже в первичном потоке STM-1 может передаваться трафик 1920 каналов ТЧ в режиме “транспортирования” потока 140 М).

Пример построения фрагмента транспортной сети с использованием систем передачи SDH приведен на рис. 3.1.2. Как видно из рисунка, транспортная сеть предназначена для передачи любых информационных сообщений в цифровом виде. По своей сути транспортная сеть - это совокупность узлов коммутации, пунктов ввода отдельных цифровых потоков, линий передачи с регенераторами и мультиплексорами. Во всех узлах транспортной сети возможно переключение трактов для вывода и ввода информационных потоков. Кроме того, в узлах сети тракты могут переключаться в случае повреждений на линии передачи или в оборудовании (рис. 3.1.2).

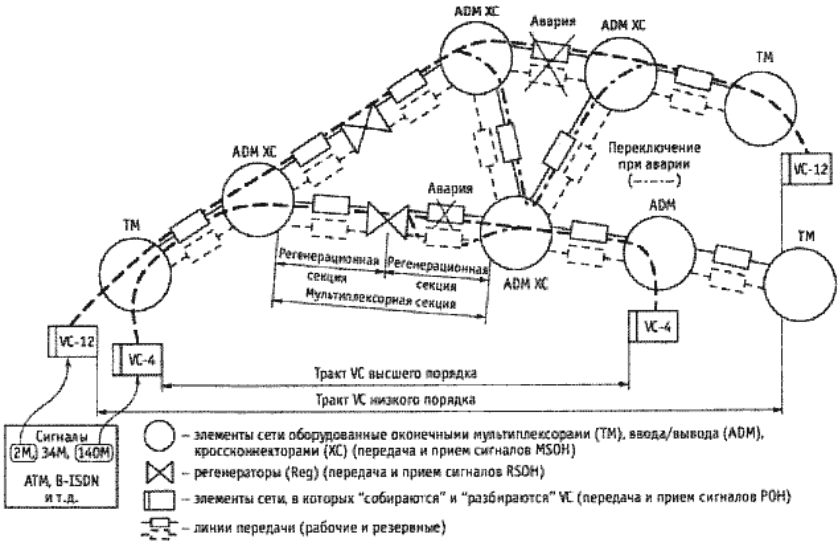


Рис. 3.1.2. Пример сети SDH с резервированием [1]

3.2. Модели транспортных сетей

Принципы построения транспортных сетей определены сектором телекоммуникаций Международного Союза Электросвязи (МСЭ-Т) в серии рекомендаций:

– G.803 – транспортная сеть SDH;

– G.805 – общая функциональная архитектура транспортных сетей;

– I.326 – функциональная архитектура транспортной сети на основе ATM;

– G.872 – оптическая транспортная сеть.

В этих рекомендациях предложено рассматривать транспортные сети в виде многоуровневых моделей (рис. 3.2.1). Каждый уровень обычно представлен отдельной службой электросвязи, предоставляющей услуги другой службе, расположенной выше.

В структурах моделей определены функциональные уровни: физический, трактов и каналов.

Рис. 3.2.1. Моногоуровневая модель транспортной сети

Физический уровень. Данный уровень образован средой передачи сигналов (волоконно-оптической линией, медной линией, радиолинией) и секциями – участками, где происходит регенерация (ретрансляция) сигналов и мультиплексирование (объединение и разделение) различных сигналов. Благодаря наличию секции

регенерации (ретрансляции) удается “очистить” сигнал от искажений и помех. Организация секций мультиплексирования позволяет эффективно использовать физическую среду за счет временного разделения передачи каналов. При этом можно реализовать резервирование любой секции мультиплексирования, если предусмотреть дополнительную физическую цепь, оборудование для передачи сигналов по ней и оборудование автоматического переключения.

Физический уровень оптической транспортной сети имеет свою особенность, которая состоит в том, что все преобразования сигналов (усиление, ретрансляция, объединение и разделение, вывод и ввод) производятся исключительно оптическими средствами. Таким способом достигаются наивысшие скорости передачи информационных данных – от десятков гигабит до десятков терабит в секунду (Тбит/с). В физической среде, представляемой одномодовым стекловолокном, объединяются (мультиплексируются) множество оптических несущих частот (от 2-х до 132 и более), каждая из которых модулирована информационным сигналом.

Уровень трактов. Тракты каждой транспортной сети создаются, чтобы обеспечить сквозное прохождение информационных сигналов. Их можно сравнить с маршрутами движения поездов на железной дороге (железнодорожные пути – это физическая среда, а крупные узловые станции подобно мультиплексорам объединяют и разделяют транспортные потоки). По маршрутам железных дорог могут следовать различные поезда и перевозить различные грузы. Аналогично в транспортной телекоммуникационной сети через физические цепи могут передаваться строго циклически цифровые потоки в виде двоичных импульсных последовательностей, сформированных из различных сигналов. Каждому сигналу отведены в циклах временные позиции. Эти позиции могут быть закреплены за соединениями - маршрутами в сети. В сети SDH маршруты прописываются в заголовках циклически передаваемых данных под названием виртуальные контейнеры (VC-12, VC-3, VC-4). При этом виртуальные контейнеры VC-12 могут быть объединены в блоки данных и помещены в виртуальные контейнеры VC-3, VC-4, имеющие большую емкость, но отправляемые также циклически, как VC-12. Это совмещение данных VC-12 и VC-3, VC-4 можно сравнить с размещением железнодорожных контей-

неров на специальных платформах, которые перемещаются по железной дороге от станции формирования состава до станции его расформирования.

Тракты в сети ATM отличаются от трактов сети SDH тем, что они образуются только при наличии информационного сообщения, а в его отсутствии физические ресурсы транспортной сети отдаются для передачи других сигналов. Сравните, на место ожидавшего пассажира в пассажирском вагоне поезда может быть посажен на любой станции пассажир, следующий своим маршрутом. По этой причине путь следования данных в сети ATM называют виртуальным. Он прописывается в специальных таблицах коммутатором ATM и ячейках, переносящих информационные сообщения. По данным таблиц считываются заголовки ячеек ATM для каждого участка сети, и происходит маршрутизация групповых информационных потоков. Маршруты в оптической транспортной сети определяются номиналами несущих частот оптического диапазона. При этом частота может быть одной и той же или изменяться на разных участках сети, однако маршрут следования информационных данных сохраняется.

Уровень каналов. Для любой из рассмотренных моделей транспортных сетей этот уровень выполняет функции интерфейса с вторичными сетями (коммутаторами телефонных, широкополосных, компьютерных сетей и т.д.). Как правило, на уровне каналов создаются типовые электрические и оптические интерфейсы. Примеры этих каналов: E1 для скорости передачи 2,048 мбит/с; E2 для скорости передачи 8,448 мбит/с; E3 для скорости передачи 34,368 мбит/с; E4 для скорости передачи 139,264 мбит/с; STM-1 для скорости передачи 155,520 мбит/с.

Транспортные сети, построенные в соответствии с различными моделями, совместимы между собой на уровнях каналов или трактов.

3.3. Элементы транспортных сетей

В качестве элементов в транспортных сетях принято рассматривать следующие устройства: терминальные мультиплексоры; мультиплексоры вывода/ввода; кроссовые коммутаторы; регенераторы. На рис. 3.3.1 – 3.3.3 показаны фрагменты транспортной сети,

приведенной на рис. 3.1.2, с пояснением функций указанных элементов на примере передачи цифровых компонентных сигналов 2М в транспортном потоке STM-1.

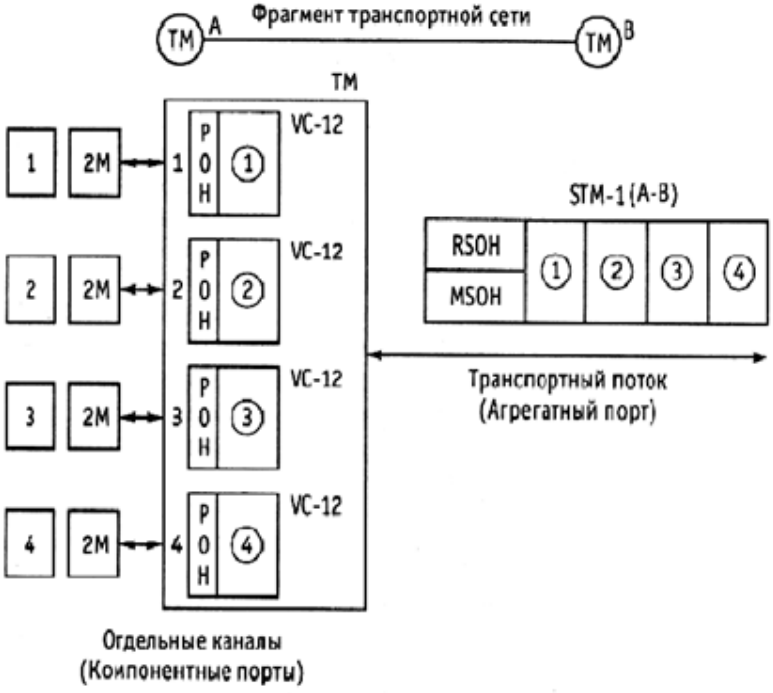


Рис. 3.3.1. Фрагмент транспортной сети SDH [1]

Терминальный мультиплексор (Terminal Multiplexer – TM). Представляет собой оконечное устройство сети с определенным числом каналов доступа (электрических и оптических) и одним или двумя оптическими входами/выходами, называемыми агрегатными портами или интерфейсами. При использовании двух агрегатных портов возможна реализация защиты линейных сигналов от повреждений линии или аппаратуры. В случае аварии происходит автоматическое переключение на резервную линию. Обычно эта линия образует секцию мультиплексирования. Защита будет наиболее эффективной, если используется два отдельных кабеля, проложенных с пространственным разнесением.

Мультиплексор ввода/вывода (Add/Drop Multiplexer – ADM). Предназначен для добавления и извлечения отдельных цифровых компонентных сигналов 2, 34, 140 мбит/с или 155 мбит/с. Мультиплексор имеет два или четыре агрегатных порта, к которым подключаются волоконно-оптические линии связи, и ограниченное число портов компонентных сигналов. В состав ADM входит коммутационный узел, создающий возможность вывода/ввода, транзита и автоматического резервирования поврежденных трактов и секций.

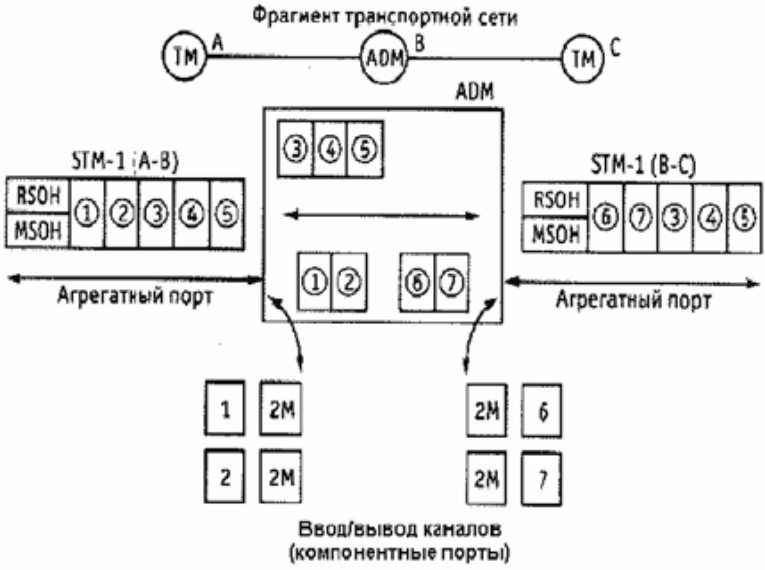


Рис. 3.3.2. Фрагмент транспортной сети SDH [1]

Кросс-коннектор (xCross Connects – XC). Это устройство предназначено для соединения каналов, закрепленных за пользователями, путем организации постоянных или полупостоянных (длительных) перекрестных соединений между ними. Кроссовый коммутатор XC обычно оснащается агрегатными и компонентными портами и обеспечивает коммутацию каналов различной пропускной способности (от 2 до 155 мбит/с).

Регенератор (Regenerator) транспортной сети обеспечивает восстановление формы и длительности импульсных посылок.

Необходимо отметить, что рассмотренные элементы обеспечивают функционирование любой из моделей транспортных сетей. Подчеркнем здесь лишь особенности элементов оптической сети. Для ретрансляции сигналов в линии оптической сети используются оптические усилители. Выделение, ввод и кроссовую коммутацию сигналов выполняют оптические мультиплексоры без использования электронных преобразований сигналов, с волновым мультиплексированием (Wavelength Division Multiplexing – WDM).

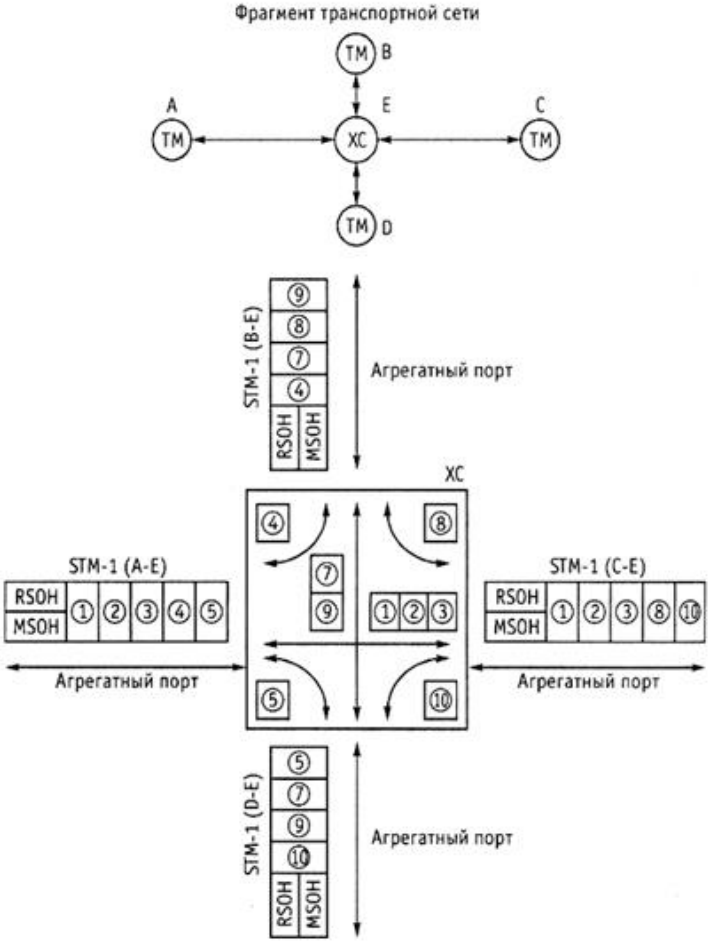


Рис. 3.3.3. Фрагмент транспортной сети SDH [1]

Мультиплексоры WDM в настоящее время разделяют по числу каналов и шагу частотного плана на три типа:

- обычные WDM;
- плотные WDM (DWDM);
- высокоплотные WDM – HDWDM (High Dense Wavelength Division Multiplexing).

При этом в соответствии с канальным или частотным планом принята классификация систем WDM, приведенная в табл. 3.3.1.

Таблица 3.3.1

Классификация систем WDM

Система	Частотный интервал, ГГц, не более	Число каналов
WDM	200	<16
DWDM	100	<64
HDWDM	50	>64

В этой классификации число каналов для каждого класса систем WDM достаточно условно, но частотный интервал между каналами имеет существенное значение. Для высокоплотных систем WDM (HDWDM) он может достигать в некоторых случаях и 25 гГц. С практической точки зрения очень важно знать взаимосвязь допустимого частотного интервала $\Delta\upsilon_{доп}$, числа каналов N, допустимого интервала по длине волны $\Delta\lambda_{доп}$ для разных уровней каналов SDH с учетом допустимого частотного интервала между оптическими несущими $\upsilon_н$.

Сравнение систем WDM различных производителей показывает, что практически все они имеют примерно сходные качественные характеристики и одинаковую конфигурацию, строятся по однотипной структурной схеме. Наблюдается общая тенденция наращивания числа каналов при одновременном повышении скорости передачи в каждом из них. Следует заметить, что возможности технологий WDM таковы, что весь сегодняшний мировой телефонный трафик можно передать по одной паре волокон.

Классификация узлов транспортной сети может быть проведена на основе определенных признаков, характерных для большинства узлов сети. Наиболее существенными являются: вид применяемого оборудования цифровых систем передачи (ATM, SDH, PDH и т.п.), объем трафика (загрузки) узла, наличие дополнительного сетевого оборудования (системы управления, коммутации,

синхронизации, доступа и др.), тип сопряжения узла с другими сегментами сети или вторичными сетями и/или сетями доступа. Классификация узлов транспортной сети, хотя и носит несколько условный характер, может быть весьма полезной при практическом планировании транспортных сетей, и в первую очередь при планировании корпоративных или ведомственных сетей. Обычно в планируемой сети предусматривают, как правило, один или два узла высшей категории и сетевые узлы первой, второй, третьей и четвертой категорий. Узел высшей категории – центральный узел цифровой первичной сети (ЦПС) обеспечивает передачу транспортных модулей синхронной цифровой иерархии (СЦИ/SDH) высшего уровня STM-N (N = 1, 4, 16, ...), управление сетью или ее сегментами (подсетями) и коммутацию скоростных цифровых потоков различных технологий. Такой узел может включать оборудование ЦСП как АТМ, так и SDH и PDH с единой системой или системами управления сетью или сегментами (подсетями) транспортной сети. Таких узлов в сети может быть несколько, например, центральный и резервный узел управления ЦПС. Сетевой узел ЦПС первой категории обеспечивает передачу транспортных модулей СЦИ/SDH высшего уровня STM-N (*N* = l, 4, 16, ...) и коммутацию скоростных цифровых потоков в пределах сегмента или между отдельными сегментами транспортной сети. Такой узел может включать оборудование ЦСП как АТМ, так и SDH и PDH.

Сетевой узел ЦПС второй категории обеспечивает передачу транспортных модулей СЦИ/SDH высшего уровня STM-N, маршрутизацию транспортных модулей STM-N более низкого уровня и коммутацию скоростных цифровых потоков как в пределах ЦПС, так и между ЦПС и сетями доступа. Такой узел может включать оборудование ЦСП как SDH, так и PDH и другое оборудование доступа к ЦПС. Сетевой узел ЦПС третьей категории обеспечивает передачу транспортных модулей STM-N более низкого уровня, чем узел первого ранга и коммутацию цифровых потоков уровня Е1 (2,048 мбит/с) между ЦПС и сетями доступа или цифровыми вторичными сетями. Такой узел может включать оборудование ЦСП как ЗОН, так и PDH и другое оборудование доступа к ЦПС.

Сетевой узел ЦПС четвертой категории обеспечивает передачу цифровых потоков уровня Е1 и основного цифрового канала ЕО

(64 кбит/с) между ЦПС и сетями доступа или цифровыми вторичными сетями. Такой узел может включать в оборудование ЦСП PDH и другое оборудование доступа к ЦПС.

3.4. Архитектура построения транспортных сетей SDH

Выбор архитектуры должен производиться на основе соображений, изложенных выше, и на основе детального технико-экономического обоснования по согласованию с фирмами-поставщиками оборудования и кабеля. «Архитектурные» решения при проектировании сети SDH могут быть сформированы на базе использования элементарных топологий сети в качестве ее отдельных сегментов. Учитывая возможность самостоятельного использования отдельных элементарных топологий, мы рассмотрим здесь только сети, комбинирующие рассмотренные элементарные топологии. Наиболее часто используется сочетание кольцевой и радиальной (типа "точка–точка") топологий или топологии последовательной линейной цепи.

Выбор архитектуры построения транспортной сети основывается на применении типовых архитектурно-топологических решений и их комбинаций для отдельных сегментов сети и сети в целом. Однако определение архитектурных решений при проектировании конкретной сети не сводится только к выбору определенных комбинаций типовых топологических структур (сетевых шаблонов). Понятие архитектуры сети шире и включает в себя три логические составляющие: принципы построения, сетевые шаблоны и технические позиции. Применительно к архитектуре ЦПС основные принципы построения определены выше. Так, постоянно открывающиеся новые возможности оборудования СЦИ/SDH расширяют возможности выбора типовых сетевых шаблонов для ЦПС и позволяют по-новому осуществлять интеграцию различных технологий на базе транспортной сети. Техническая позиция определяет и уточняет параметры выбранной технологии, сетевых элементов, протоколов взаимодействия, предоставляемого сервиса и т.д. Применительно к корпоративной сети ее архитектура может быть описана, например, следующими техническими позициями:

- Сетевые транспортные протоколы.
- Маршрутизация в сети.
- Качество обслуживания.

- Адресация в сетях передачи данных.
- Коммутация в локальных сетях.
- Объединение коммутации и маршрутизации.
- Организация городской сети.
- Организация глобальной (магистральной) сети
- Службы удаленного доступа (сети доступа).

Разработка технических позиций для конкретной цифровой первичной сети требует глубокого знания базовых сетевых технологий и тщательной проработки схем организации и топологии всех сегментов сети и сети в целом.

При планировании транспортной сети наиболее часто находят применение типовые сетевые шаблоны - радиально-кольцевая топология и топология "кольцо-кольцо" с одинаковым или различными уровнями транспортных модулей как в "кольцах", так и в линейных трактах между отдельными "кольцами". В заключение сформулируем основные правила планирования цифровых первичных сетей связи:

- Долгосрочное планирование.
- Выбор среды передачи.
- Анализ существующего и определение планируемого трафика.
- Классификация узлов сети и выбор базовых топологий сети.
- Анализ и определение требований по надежности.
- Обеспечение заданного уровня надежности в сети.
- Определение энергетического потенциала линий связи и оборудования ЦСП.
- Определение стоимости линий связи и оборудования ЦСП.
- Учет специальных условий и требований заказчика (пользователя) сети.
- Полная оптимизация сети (с помощью соответствующих программных средств).
- Деление сети на управляемые части или сегменты.
- Предусматривается необходимый уровень эксплуатации будущей сети.

Рассмотренные общие вопросы планирования цифровых первичных сетей являются основой при планировании реальных современных сетей связи и, естественно, не исчерпывают всего мно-

гообразия проблем, возникающих при разработке и планировании транспортных сетей различного масштаба. Наиболее существенным в планировании современных сетей связи становится интеграция первичной и вторичных сетей в единую мультисервисную сеть на основе интеграции современных сетевых технологий.

Радиально-кольцевая архитектура. Пример радиально-кольцевой архитектуры SDH сети приведен на рис. 3.4.1. Эта сеть фактически построена на базе использования двух базовых топологий: "кольцо" и "последовательная линейная цепь". Вместо последней может быть использована более простая топология "точка-точка". Число радиальных ветвей ограничивается из соображений допустимой нагрузки (общего числа каналов доступа) на кольцо.

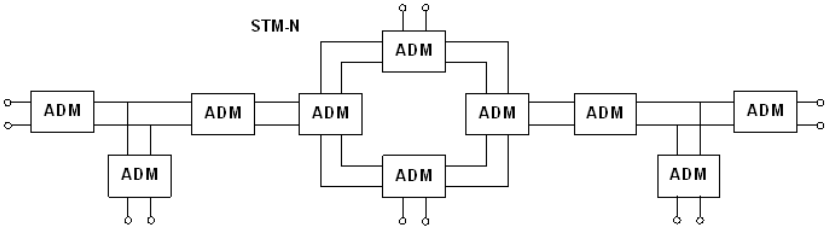


Рис. 3.4.1. Радиально-кольцевая архитектура SDH [1]

Архитектура типа "кольцо–кольцо". Другое часто используемое в архитектуре сетей SDH решение – соединение типа "кольцо-кольцо". Кольца в этом соединении могут быть либо одинакового, либо разного уровней иерархии SDH. На рис. 3.4.2 показана схема соединения двух колец одного уровня – STM-4 с помощью интерфейсных карт STM-1, а на рис. 3.4.3 – каскадная схема соединения трех колец различного (по нарастающей) уровня – STM-1, -4, -16. При таком соединении можно использовать необходимые оптические трибы предыдущего иерархического уровня при переходе от кольца одного уровня к другому (например, триб STM-1 при переходе на кольцо STM-4 и триб STM-4 при переходе на кольцо STM-16).

Линейные сети обычно содержат два приёмопередающих оконечных устройства, например мультиплексоры SDH, мультиплексоры ввода/вывода ADM и регенераторы. Пример конфигурации линейной сети приведён на рис. 3.4.4.

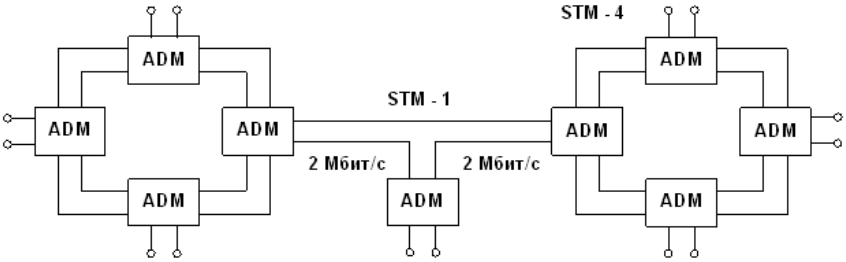


Рис. 3.4.2. Схема соединения двух колец одного уровня [1]

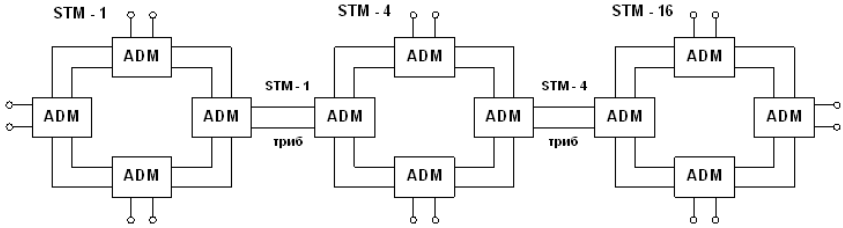


Рис. 3.4.3. Каскадная схема соединения трех колец различного уровня [1]

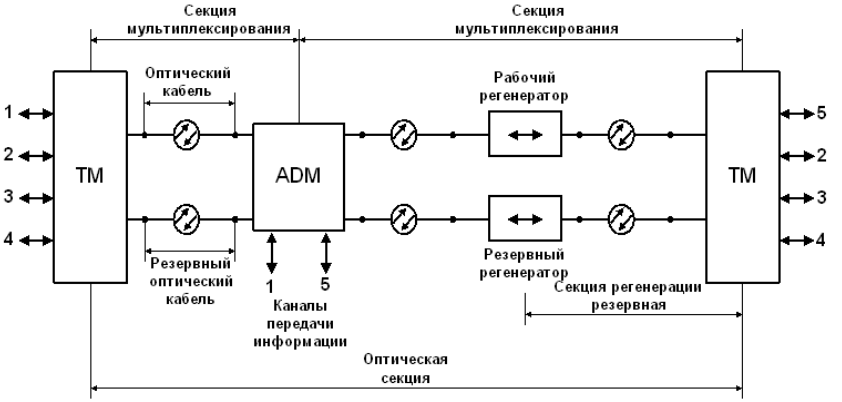


Рис. 3.4.4. Пример линейной архитектуры для сети большой протяженности по [1]

Линейная архитектура для сети большой протяженности

В приведённом примере реализован принцип защиты линейной сети в режиме 1+1, т.е. для одной рабочей секции мультиплексирования создаётся одна резервная, что обозначает полное гарантированное резервирование всего трафика между терминалами.

Для линейных сетей большой протяженности расстояние между терминальными мультиплексорами ТМ больше или много больше того расстояния, которое может быть рекомендовано с точки зрения максимально допустимого затухания волоконно-оптического кабеля. В этом случае на маршруте (в линейном тракте) между ТМ (рис. 3.4.4) должны быть установлены кроме общего проходного коммутатора еще и регенераторы для восстановления (регенерации) затухающего оптического сигнала. Эту линейную архитектуру можно представить в виде последовательного соединения ряда секций.

Принято различать три типа стандартизованных участков – секций: оптическая секция (участок от точки электронно-оптического до точки оптоэлектронного преобразований сигнала), которая, по сути, являются участком волоконно-оптического кабеля между элементами сети SDH, регенераторная секция и мультиплексная секция (рис. 3.4.4).

Оптические секции нормируются по длине, при этом выделяют три категории: I - внутристанционная секция, длиной до 2 км, *S* – короткая межстанционная секция, порядка 15 км, и *L* -длинная межстанционная секция, порядка 40 км (при длине волны 1310 нм) и 80 км (при длине волны 1550 нм). Указанные длины секций используются только для классификации (см. ниже) и не могут рассматриваться как рекомендуемые значения используемых технических параметров. Общая длина маршрута может составлять при этом сотни или же тысячи километров. Маршрут рассматривается как участок тракта между терминальными мультиплексорами, допускающий автоматическое поддержание функционирования сети с номинальной производительностью.

Мультиплексная секция рассматривается как участок тракта между транспортными узлами (мультиплексорами и коммутаторами), допускающий аналогичное автоматическое поддержание функционирования.

Регенераторная секция рассматривается как участок тракта между двумя регенераторами или между регенератором и другим элементом сети SDH. Для аналогичных определений используются опорные точки вход/выход волокна и вход/выход начала/окончания регенераторной секции RST в схеме представления регене-

раторной секции. Регенераторная секция обрабатывает RSOH, который содержит синхросигнал, а также управляющую и контрольную информацию, позволяющую локализовать поврежденную секцию. Этот заголовок, будучи сформированным и введенным во фрейм на входе RST, считывается каждым регенератором и выводится из фрейма на выходе RST.

Классификация секций приведена в табл. 3.4.1. Она дает стандартное обозначение секций в зависимости от уровня STM (1, 4, 16) и приведена для указанных трех типов применения: внутри станции (код использования I), между станциями – короткая секция (код использования *S)*, между станциями – длинная секция (код использования L). В общем случае кодировка типов использования линейных регенераторных секций как оборудования SDH включает три элемента и имеет формат: <код использований> <уровень STM> <индекс источника>

Здесь код использования и уровни STM приведены выше, а индекс источника имеет следующие значения и смысл:

- 1 или без индекса – указывает на источник с длиной волны 1310 нм;
- 2 – указывает на источник с длиной волны 1550 нм для волокна, (секции *L*);
- 3 – указывает на источник с длиной волны 1550 нм для волокна.

Например, обозначение L-4.3 расшифровывается как длинная межстанционная регенераторная секция линейного оборудования STM-4, использующая источник света с длиной волны 1550 нм.

Архитектура разветвленной сети общего вида. В процессе развития сети SDH разработчики могут использовать ряд решений, характерных для глобальных сетей, таких как формирование своего "остова" (backbone) или магистральной сети в виде ячеистой (mash) структуры, позволяющей организовать альтернативные (резервные) маршруты, используемые в случае возникновения проблем при маршрутизации виртуальных контейнеров по основному пути. Это, наряду с присущим сетям SDH внутренним резервированием, позволяет повысить надежность всей сети в целом. Причем при таком резервировании на альтернативных маршрутах могут быть использованы альтернативные среды распространения

сигнала. Например, если на основном маршруте используется волоконно-оптический кабель (ВОК), то на резервном – радиорелейная линия (РРЛ), или наоборот.

На рис. 3.4.5 представлена архитектура такой разветвленной (глобальной) сети, остов (или опорная/магистральная сеть) которой сформирован для простоты в виде одной сетевой ячейки, узлами которой являются коммутаторы типа SDXC, связанные по типу "каждый с каждым". К этому остову присоединены периферийные сети SDH различной топологии, которые могут быть "образами" либо корпоративных сетей (с выходом на LAN), либо общегородских сетей SDH или MAN (ОГС), либо сегментов других глобальных сетей WAN (ГСС). Эта структура может рассматриваться как некий образ глобальной сети SDH. Классификация стандартных оптических интерфейсов приведена в табл. 3.4.1.

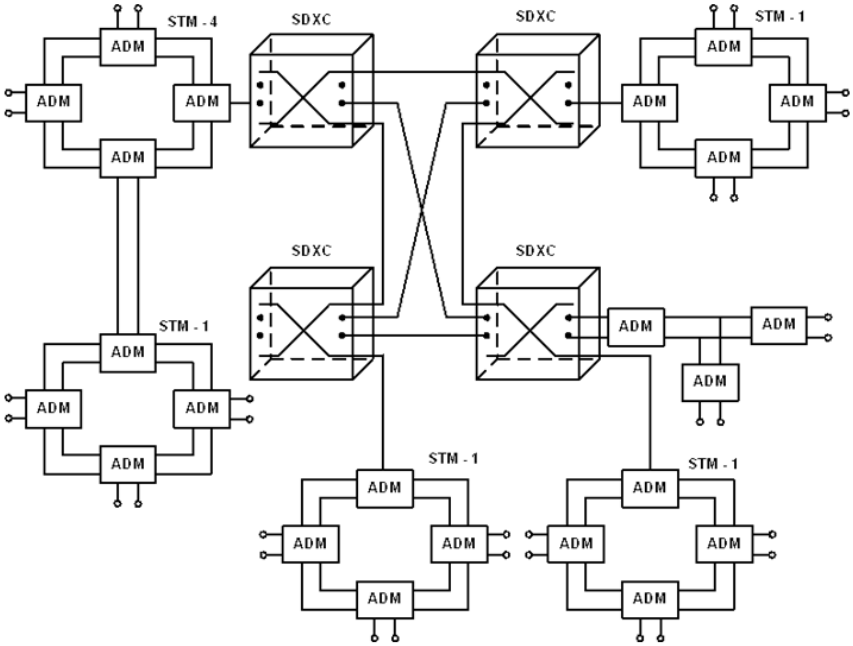


Рис. 3.4.5. Пример сети SDH с архитектура разветвленной сети общего вида [1]

Таблица 3.4.1

Классификация стандартных оптических интерфейсов

Использование		Внутри станции	Между станциями				
			Короткая секция		Длинная секция		
Номинальная длина волны источника, нм		1310	1310	1550	1310	1550	
Тип волокна		Rec. G.652	Rec. G.652	Rec. G.652	Rec. G.652	Rec. G.652 Rec. G.654	Rec. G.653
Расстояние, км		≤ 2	– 15	– 40	– 80		
Уровни STM	STM – 1	L – 1	S – 1.1	S – 1.2	L – 1.1	L – 1.2	L – 1.3
	STM – 4	L – 4	S – 4.1	S – 4.2	L – 4.1	L – 4.2	L – 4.3
	STM – 16	L – 16	S – 16.1	S – 16.2	L – 16.1	L – 16.2	L – 16.3

3.5. Синхронизация в сетях SDH

Все операции по обработке сигналов в цифровых системах передачи (будь то передающая или приемная аппаратура) и системах коммутации должны выполняться в строгой последовательности во времени и синхронно. Во всех системах передачи с временным разделением каналов (и в том числе работающих по принципу ИКМ) приемное оборудование всегда должно работать синхронно с передающим. Только в этом случае переданные сигналы попадут на приемной стороне на отведенные им временные позиции и в свои каналы. На каждой цифровой коммутационной станции скорость обработки сигналов задается одним станционным генератором. Все эти функции выполняются с помощью устройств внутри аппаратной синхронизации, входящих в состав устройств передачи и коммутации.

Проблема тактовой сетевой синхронизации возникает, когда цифровые системы передачи интегрируются с электронными цифровыми системами коммутации в единую цифровую сеть, обеспечивающую передачу и коммутацию сигналов в цифровой форме.

Современный опыт, а также ряд исследований указывают, что нарушения в сети синхронизации могут приводить к значительному ухудшению услуг связи в цифровой сети. В зависимости от типа услуг это влияние разное: одни услуги более устойчивы к нарушениям синхронизации в сети, другие – менее. В любом случае нарушения синхронизации приводят к деградации качества

услуг и значительным сбоям в работе сети.

Для выравнивания скоростей передачи на стыках включаются устройства буферной памяти так, что запись входной информации в буфер памяти происходит на скорости приходящего сигнала, а списывание – на скорости местного генератора (рис. 3.5.1).

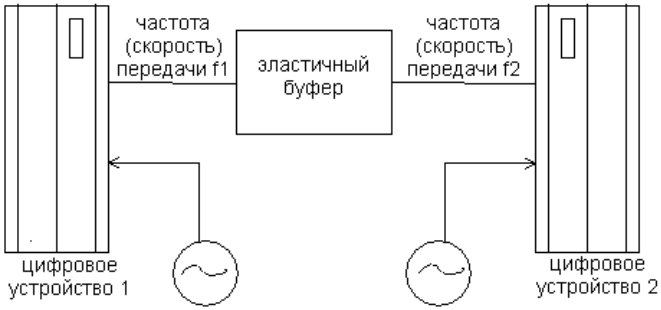


Рис. 3.5.1. Механизм возникновения проскальзываний [1]

Цифровое устройство 1 генерирует цифровой сигнал с частотой *f1*, этот сигнал с частотой *f1* записывается в оперативную память эластичного буфера, из которого считывается приемным цифровым устройством 2 с частотой *f2*. Частоты передачи и считывания определяются частотой задающих тактовых генераторов (ТГ1 и ТГ2 соответственно). При работе данной схемы случаются проскальзывания. Проскальзыванием называется повторение или исключение группы символов в двоичной последовательности в результате различая между скоростями считывания и записи в буферной памяти. В случае если $f1 > f2$ буфер постепенно переполняется, что приводит к потере информации в размере емкости буфера, возникает положительное проскальзывание. Если же $f1 < f2$, то цифровое устройство 2 рано или поздно начнет считывать информацию с дублированием битов (повторное считывание), что приведет к ошибке – отрицательному проскальзыванию.

В отсутствие эластичного буфера проскальзывания возникают по мере накопления фазового сдвига сигналов передачи и приема, будут возникать битовые проскальзывания, то есть ошибки. Битовые проскальзывания будут нарушать цикловую синхронизацию в то время как с точки зрения алгоритмов взаимодействия цифровых устройств наиболее желательным являются цикловые проскальзы-

вания, которые приводят к потере цикла информации, но не приводят к нарушению цикловой синхронизации.

Для минимизации нежелательных явлений, связанных с проскальзываниями, используют эластичные буферы размером в один или несколько циклов;

- Для услуги телефонии одно проскальзывание приводит к появлению щелчка в трубке. Этот щелчок не всегда слышен, таким образом, единичные проскальзывания незначительно влияют на параметры качества телефонной связи. Обычно несколько щелчков в минуту дает вполне приемлемое качество телефонной связи.
- Изучение вопроса о влиянии проскальзываний на передачу факсимильных сообщений показало, что единичное проскальзываний приводит к нарушению качества или потерям строк сообщения факса. Проскальзывание может приводить к нарушениям в передаче до 8 строк сообщения, что соответствует 2 мм по вертикали. В случае нескольких проскальзываний, передаваемую страницу необходимо повторно переслать.
- Воздействие проскальзываний не передачу данных в разговорном канале приводит к появлению последовательностей ошибок, длительностью от 10 мс до 1,5 с в зависимости от модемного протокола и скорости передачи.
- В случае соединения по видеотелефону проскальзывание обычно приводит к потере видеоканала и необходимости восстановления соединения.
- Воздействие проскальзываний на каналы передачи данных зависит от используемого для передачи данных протокола. Обычно проскальзывания приводят к потере части информации и необходимости ее передачи заново, что в современных протоколах передачи данных делается автоматически. Таким образом, проскальзывания приводят к увеличению времени передачи данных за счет дополнительного времени на повторную передачу.
- При передаче цифровой видеоинформации (например: видеоконференцсвязь) проскальзывания вызывают деградацию качества видеоизображения в виде пропадания кадра или его замирания на период до шести секунд. Длительность деградации видеосигнала зависит от типов кодирования и технологии компрессии.

- Наиболее существенное ухудшение проскальзывания вносят в кодированные данные. В результате проскальзывания теряется ключ кодирования. В этом случае принимаемые данные не могут быть расшифрованы до тех пор, пока ключ не будет передан заново. Таким образом, все данные будут потеряны. В ряде систем с защитой информации повторная передача ключа не опускается, поскольку в этом случае нарушается уровень защиты данных. По этой причине для таких специальных сетей норма "одно проскальзывание в сутки" считается неприемлемой.

Требования к частоте проскальзываний при соединении от абонента до абонента по каналу 64 кбит/с нормируются согласно рекомендации МСЭ-Т G.822 с помощью стандартного цифрового условного эталонного соединения длиной 27500 км (рис. 3.5.2).

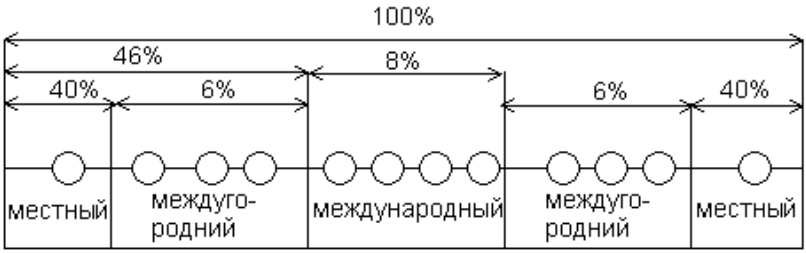


Рис. 3.5.2. Правило распределение проскальзываний по участкам международных соединений, соответствующие рекомендации G.822 [1]

Для оценки качества синхронизации сети используются следующие три категории качества: "*a", "b", "c*". Категория качества "*a*" – высшая категория – соответствует нормальному режиму работы сети синхронизации в условиях, когда в цепях синхронизации отсутствуют неисправности. Работа по категории качества "*a*" за длительный промежуток времени (например, год) должна составлять не менее 98,9 % от времени эксплуатации, несмотря не то, что в этом случае сохраняется синхронизация, категория *"a*" допускает появление проскальзываний из-за наличия псевдосинхронных участков и сбоев в работе в результате воздействия шумов и помех. Категория качества "*b*" – категория ухудшенного качества – соответствует появлению неисправности в цепях синхронизации. За время работы с этой категорией качества проводится диагностика и устранение повреждений. В расчетах предлагается

учитывать одиночную неисправность. Работа по категории "*b*" за длительный промежуток времени не должна превышать 1 процента от времени эксплуатации. Категория качества "*c*" – категория, зарезервированная для работ по монтажу и перестройке цепей синхронизации. Работа по категории качества "*c*" за длительный промежуток времени не должна превышать 0,1 процента от времени эксплуатации.

В идеально работающей синхронной цифровой сети возможность возникновения проскальзываний исключена. Нормирование проскальзываний в рекомендации G.822 означает, что МСЭ-Т в принципе допускает в известных пределах нарушение в работе синхронизации и использование на синхронных цифровых сетях несинхронных режимов работы.

3.5.1. Режим работы сети тактовой сетевой синхронизации

Рекомендацией МСЭ-Т G.803 определены четыре режима работы сети синхронизации:

- синхронный;
- псевдосинхронный;
- плезиохронный;
- асинхронный.

Классификация режимов классификации приведена на рис. 3.5.3.

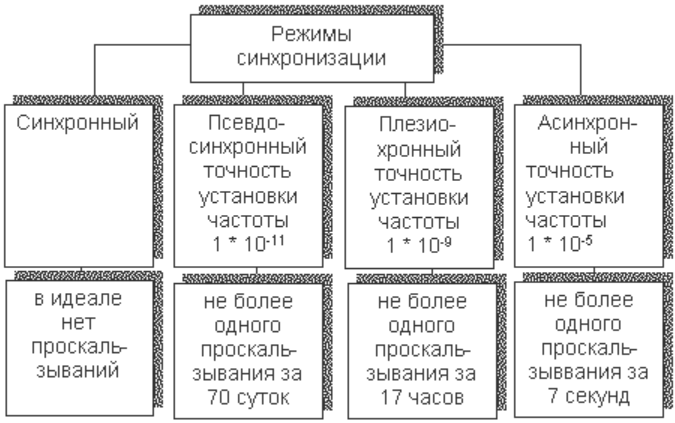


Рис. 3.5.3. Режимы синхронизации [1]

Синхронный режим является нормальным режимом работы цифровой сети, при котором проскальзывания носят только случайный характер. Этот режим обычно используется в пределах достаточно обширных географических регионов, границы которых во многих случаях совпадают с границами национальных цифровых сетей государств средних размеров. Псевдосинхронный режим имеет место, когда на цифровой сети независимо друг от друга работают два (или несколько) генераторов, точность установки частоты которых не хуже 1×10^{-11} в соответствии с рекомендацией G.811. Такой режим работы возникает, например, при соединении 2 независимых синхронных национальных сетей или регионов синхронизации одной национальной сети.

Согласно рекомендации G.802, когда национальные сети с независимой синхронизацией соединяются через международный тракт, который не синхронизирован ни с одной из двух национальных сетей (например, проходит через третью цифровую национальную сеть), то этот тракт должен быть синхронизирован от источника, удовлетворяющего рекомендации G.811, а в случае, когда национальные сети с независимой синхронизацией соединяются через международный цифровой тракт, который синхронизирован со страной передачи, то стык псевдосинхронных серей должен осуществляться в стране приема.

По рекомендации G.810 национальные цифровые сети могут состоять не из одного тракта образующих в странах с обширных территорией национальную псевдосинхронную сеть. Если два синхронных региона работают от двух независимых первичных эталонных генераторов и соединяются через цикловые или октетные выравниватели, то в цифровых каналах 64 кбит/с управляемые проскальзывания будут происходить не чаще одного раза в течение интервала времени *T*:

$$T = \frac{n}{2*10^{-11}*2048*10^3} = \frac{n1}{2*10^{-11}*2048*10^3} = 70 сутток$$

где $2 * 10^{-11}$ – максимально допустимое относительное расхождение частот первичного эталонного генератора; $n = 256$ и $n = 8$ – число выравнивающих бит соответственно при цикловом или октетном выравнивании.

Из проведенной выше оценки возникновения проскальзываний следует, что на псевдосинхронной сети, которая оборудована высокостабильными генераторами, обеспечивающими точность частот до одиннадцатого знака, ухудшение качества для всех видов связи за счет расхождения частот будет практически неощутимо малым по сравнению со всеми другими нарушениями в передаче сигналов, которые могут произойти в течение промежутка времени между проскальзываниями вследствие других, часто трудно предсказуемых причин.

Рассмотренный псевдосинхронный режим работы, хотя принципиально и относится к асинхронным, является полноценным режимом. Преимущество псевдосинхронного режима перед синхронным состоит в том, что при его использовании, вследствие переприема входного сигнала в выравнивающих устройствах буфера памяти, происходит практически полное подавление накопленных перед этим фазовых дрожаний и блужданий входного сигнала.

Плезиохронный режим работы возникает на цифровой сети, когда генератор ведомого узла полностью теряет возможность внешней принудительной синхронизации вследствие отказов как основного, так и всех резервных путем синхронизации. В этом случае генератор ведомого узла полностью теряет возможность внешней принудительной синхронизации вследствие отказов как основного, так и всех резервных путей синхронизации. В этом случае генератор переходит в так называемый режим удержания (holdover mode), при котором запоминается частота сети принудительной синхронизации. Далее по мере ухода с течением времени частоты вследствие дрейфа от величины, зафиксированной в начальный момент в памяти, генератор переходит в так называемый свободный режим (free-run mode).

На ведомых узлах и станциях, начиная со второго иерархического уровня, используются кварцевые генераторы, стабильность частоты которых на два – три порядка ниже, чем у цезиевых стандартов, относящихся к первому иерархическому уровню. При переходе какого-либо ведомого генератора в режим удержания та часть цифровой сети, которая синхронизируется от этого генератора, начинает работать на частоте, все более отличающейся с течением времени от частоты остальной сети. Поэтому для соблю-

дения рекомендации G.822 по частности проскальзываний длительность работы в режиме удержания, в отличие от псевдосинхронного режима, должна быть жестко ограничена во времени. Асинхронный режим характеризуется значительно большим расхождением частот генераторов, при котором, однако, еще не нарушается траффик. Необходимые для этого пределы МЧЭ-Т еще не установлены. Вместе с тем известно, что для передачи общего сигнала индикации аварийного состояния расхождение частот не должно превышать $2 * 10^{-5}$.

Так, например, потребность в стандартизации соединений компьютеров с периферийными устройствами привела Ассоциацию Электронной Промышленности (EIA) в 1969 г. к созданию спецификации RS-232-C. Этот стандарт допускает скорость обмена информацией до 38 400 бит/с по 4 или 12 проводам на расстояние до 15 м. Стандарт RS-232-C по сей день широко применяется и известен как последовательный порт. Примером организации асинхронного соединения является соединение компьютера и принтера. При этом передаваемые данные принимаются и передаются позначно. Два знака должны быть разделены минимальным временным интервалом. Знак представляет собой группу из 7 или 8 бит, в зависимости от используемого кода. Такой тип передачи называется асинхронным, поскольку последовательная передача знаков может происходить в произвольные моменты времени при соблюдении требований минимального временного разделения. Принимающая сторона начинает вырабатывать тактовые сигналы, как только обнаруживает начало знака. Используя эти тактовые сигналы, принимающая сторона считывает биты. Для осуществления этой процедуры число битов в знаке должно быть достаточно малым: если бы число битов было велико, то даже малое различие в частотах тактовых символов принимающей и передающей сторон привело бы к ошибкам, поскольку принимающее устройство могло бы пропустить биты или считать один бит дважды.

Потребность в быстрых соединениях с автоматическим контролем ошибок привела к созданию набора процедур, называемых протоколами канального уровня, известных под аббревиатурами SDLC, LAP, LAPB, HDLC. Эти соединения синхронны: они переносят информацию в форме пакетов. Пакет – это группа битов

обычно от нескольких сотен до тысяч, которые передаются в точно определенный промежуток времени. Передающая сторона кодирует биты пакета в сигнал, который содержит информацию для синхронизации. Принимающая сторона выделяет эту информацию для точного восстановления последовательности битов. Такая синхронизация принимающей стороны с использованием специальной информации позволяет осуществлять передачу длинных пакетов, которые невозможно передавать по асинхронным линиям.

Метод синхронизации в этих протоколах основан на генерации частотного компонента со скоростью передачи символов, при пропускании поступающего узкополосного сигнала через последовательность фильтра и нелинейного устройства (рис. 3.5.4).

Рис. 3.5.4. Разомкнутый символьный синхронизатор [2]

Работа данного устройства аналогична восстановлению несущей в контуре сопровождения с подавленной несущей. Поступающий сигнал фильтруется с использованием согласованного фильтра. Выход этого фильтра – автокорреляционная функция исходного сигнала. Затем полученная последовательность спрямляется с помощью нелинейности четного порядка. Полученный сигнал будет содержать пики положительной амплитуды, которые с точностью до временной задержки, соответствуют переходам входных символов через нуль. Последовательность описанных процессов изображена на рис. 3.5.5.

Рис. 3.5.5. Иллюстрация процессов,
происходящих в разомкнутом битовом синхронизаторе [2]

Таким образом, сигнал с выхода четного устройства будет содержать Фурье-компонент на собственной частоте тактового гене-

ратора. Эта частотная составляющая изолируется от остальных гармоник с помощью полосового фильтра и ей придается форма посредством насыщающего усилителя с передаточной функцией вида.

Обычно пакет состоит из заголовка, информации пользователя, хвостовой части. Заголовок и хвостовая часть содержат управляющую информацию, которая используется сетью при передаче для проверки правильности доставки. Заголовок обычно содержит адреса получателя и отправителя пакета. Заголовок также может содержать порядковый номер, который используется узлом назначения для проверки порядка следования пакетов и факта доставки всех пакетов. Хвостовая часть содержит биты контроля ошибок, используемые узлами сети для контроля правильности передачи. Как и в случае асинхронной передачи, когда обязательным является разделение между знаками, при синхронной передаче также не обходим определенный промежуток между передаваемыми пакетами. Однако синхронный способ передачи является более быстрым, чем асинхронный, так как время простоя линии, приходящееся на переданный бит, в случае синхронной передачи меньше, чем в случае асинхронной. Синхронная передача может быть применена и по телефонной линии, при наличии на обоих концах модемов.

Важно обратить внимание на то, что значение термина «синхронность» при сравнении синхронных и асинхронных линий не то же, что в сети SDH. В SDH синхронность обусловлена тем фактом, что все передающие устройства синхронизированы общим тактовым сигналом, что позволяет мультиплексировать потоки чередованием байтов. При синхронной передаче принимающая сторона синхронизируется по содержащейся в сигнале информации. В канале SDLC тактовый сигнал не передается, приемник синхронизируется только по принимаемому сигналу. В разных передатчиках отдельных каналов SDLC используются разные, не синхронизированные между собой, тактовые генераторы. В противоположность этому все передатчики SDH привязаны к общей частоте.

3.5.2. Сигналы синхронизации. Факторы, влияющие на них

Одним из главных требований при организации системы синхронизации является наличие альтернативных хронирующих ис-

точников для каждого сетевого элемента. В качестве них обычно используются сигналы:

- сетевого таймера (внешний эталонный генератор синхросигнала 2048 кГц);
- внутреннего таймера (внутренний генератор синхросигнала 2048 кГц);
- канального интерфейсного блока или сигнал 2048 кГц, выделяемый из канала 2 мбит/с. Этот источник синхронизации не рекомендуется использовать, так как мультиплексирование канальных блоков TU-12 по умолчанию происходит в плавающем режиме. Фиксированное синхронное отображение структурированной информации канальных блоков на поле полезной нагрузки контейнеров верхних уровней не используется, что подразумевает определенную асинхронность в транспортировке контейнеров VC-12 и не позволяет применять канал два мега бит в секунду в качестве хронирующего источника;
- линейного таймера или сигнал 2048 кГц, выделяемый из линейного сигнала 155 520 мбит/с или сигнала более высокого уровня иерархии.

Для достижения синхронизации в сети необходимо передать информацию о тактовой частоте всем устройствам в сети. Для этой цели используются синхросигналы или сигналы синхронизации. Такие сигналы могут передаваться в линейных сигналах или отдельно в виде специальных сигналов. В результате качество сигнала ухудшается, что приводит к нарушениям параметров синхронизации в сети.

Нестабильности сигналов синхронизации возникают как по физическим параметрам линии передачи в сигнале на приеме, так и по алгоритмическим причинам (например, джиттер стаффинга и смещения указателей). Джиттер – фазовое дрожание с частотой выше 10 Гц, вандер – с частотой ниже 10 Гц. Вандер представляется для систем синхронизации одним из наиболее важных параметров. Он легко проходит без изменений через цепи фазовой синхронизации, может значительно накапливаться в сети и воздействует на систему синхронизации.

Основными физическими причинами нестабильности частоты являются: электромагнитная интерференция; шум и помехи, воз-

действующие на цепь синхронизации в приемнике; изменения длины тракта; изменение скорости распространения; доплеровские сдвиги от подвижных оконечных устройств; нерегулярное поступление хронирующей информации.

Шумы и помехи, возникающие на входе приемных устройств, имеют, как правило, широкий спектр и перекрывают спектр принимаемого сигнала. При этом они складываются аддитивно и могут воздействовать на тактовый генератор приема. Чаще всего генератор приема содержит цепь фазовой автородстройки частоты (рис. 3.5.6).

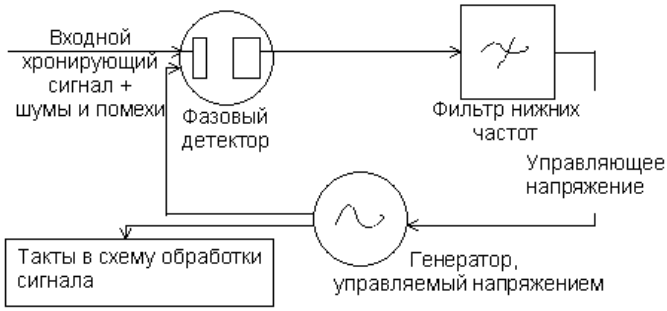


Рис. 3.5.5. Схема восстановления тактовой частоты
в приемнике цифрового сигнала

Фазовый детектор непрерывно измеряет разность фаз между колебаниями тактовых генераторов передатчика и приемника. Сигнал с выхода фазового детектора подается на фильтр нижних частот, что уменьшает неточность измерения фаз в некоторых известных пределах, Однако шум остается и после фильтра и вызывает неточную подстройку частоты генератора приемника под частоту генератора передатчика. Эта схема надежно отрабатывает изменение фазы сигнала с некоторой погрешностью. Таким способом в приемнике поддерживается средняя частота тактов и сохраняется неточность настройки, относительная величина которой может составить плюс минус пять на десять в минус пятой степени за год.

Изменение длины тракта происходят в результате температурного расширения или сжатия среды передачи или в результате изгиба радиотракта в атмосфере. При удлинении тракта эффективная скорость передачи на входе приемника уменьшается, поскольку все больше и больше битов “накапливается” в среде передачи.

Аналогично, при укорочении тракта скорость передачи на входе приемника увеличивается, поскольку число битов, “накапливаемых” в линии передачи, уменьшается. После того как длина тракта стабилизируется, восстанавливается номинальная скорость передачи цифрового сигнала. Наиболее значительны изменения длины тракта при связи через спутники. Для современных спутников на геостационарной орбите изменения длины тракта составляют примерно 300 rv, что соответствует изменениям времени прохождения примерно на 1 мс. Из сказанного выше следует, что изменение длины тракта влияет на систему частотной синхронизации, поскольку изменение скорости передачи эквивалентно вандеру – основному параметру нестабильности систем частотной синхронизации.

Изменение скорости распространения сигнала jбычно связано с изменением характеристик среды передачи и наиболее характерно для радиочастотных систем. Механизм воздействия этого параметра приблизительно такой же как изменения длины тракта. Точно так же изменение скорости распространения сигналов приводит к вандеру.

Наиболее значительным источником потенциальной нестабильности тактовой частоты на приеме являются доплеровские сдвиги, возникающие при движении самолетов, спутников и других подвижных объектов. Например, доплеровский сдвиг при движении самолета со скоростью 500 км/ч эквивалентен нестабильности тактовой частоты, равной 0,000005. По существу оказывается, что доплеровские сдвиги являются результатом изменения длины тракта.

Основное требование к коду в цифровой системе передачи состоит в том, чтобы он обеспечивал получение достаточной хронирующей информации для установления и поддержания колебаний тактовой частоты в приемнике на конце линии. Если уровень хронирующей информации зависит от цифрового сигнала, то фазовые дрожания в восстановленных колебаниях тактовой частоты увеличиваются в течение периодов времени с относительно низкими плотностями импульсов, от которых зависит хронирование. Амплитуда фазовых дрожаний зависит не только от плотности импульсов, но также и от структуры цифрового сигнала (в смысле содержания хронирующей информации).

Литература

1. *Крук Б.И., Попантонопуло В.Н., Шувалов В.П.* Телекоммуникационные системы и сети: Уч. пос. В 3-х т. – М.: Горячая линия-Телеком, 2004.
2. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение. 2-е изд. / Пер. с англ. – М.: Изд. дом «Вильямс», 2003. – 1104 с.
3. Телекоммуникационные системы СЦИ и ПЦИ. Конспект лекций – [Электронный ресурс]. – Режим доступа: http://siblec.ru/
4. *Гордиенко В.Н., Ксенофонтов С.Н., Кунегин С.В., Цыбулин М.К.* Современные высокоскоростные цифровые телекоммуникационные системы. Ч. 3. Группообразование в синхронной цифровой иерархии: Уч. пос. – М.: МТУСИ, 1999. – 76 с.
5. *Соколов Н.А.* Телекоммуникационные сети. Монография в 4-х ч. – М.: Альварес Паблишинг, 2003.

4. ТЕЛЕФОННАЯ СЕТЬ ОБЩЕГО ПОЛЬЗОВАНИЯ

Положение телефонной сети общего пользования (ТФОП) в современном телекоммуникационном пространстве [1] определяется двумя параметрами: телефонной плотностью (ТП) и количеством основных телефонных аппаратов (СТА). Телефонная плотность в РФ составляет 22 СТА на 100 жителей (22 %), а количество СТА – 32 млн. Под СТА понимается количество основных абонентских линий, соединенных с АТС. По количеству СТА Россия занимает шестое место в мире (после США – 143 млн, Японии – 59 млн, Германии –35 млн, Франции – 33 млн и Англии – 32 млн). По ТП Россия замыкает четвертый десяток стран мира. Самую низкую ТП в первой десятке имеет Испания (36 %). Телефонная плотность является интегральным показателем развития любой страны. Она отражает состояние сети связи и косвенно характеризует качественный уровень сети. С ростом ТП практически во всех странах наблюдаются следующие изменения: переход от аналогов систем передачи и коммутации к цифровым, расширяется количество служб и предоставляемых услуг, усложняются терминалы пользователей (они становятся многофункциональными), сеть эволюционирует от аналоговой к аналого-цифровой, затем к цифровой и интеллектуальной.

Общегосударственная система автоматизированной телефонной связи (ОГСТфС) предназначена для удовлетворения населения и предприятий в передаче сообщений пользователей как в пределах страны, так и при выходе на международную телефонную сеть, ОГСТфС предоставляет два вида услуг: услуги доставки (передачи) информации и специальные. К услугам доставки информации относятся: передача сообщений – речевых, факсимильных, электронной почты, данных. Эти услуги предоставляются техническими службами, использующими физические ресурсы сети. К специальным услугам относят информационно-справочные, заказные и дополнительные. Их предоставляют службы сервиса автоматически или с помощью оператора. К службам сервиса Госкомитета РФ по связи и информатизации относятся, например, такие:

– справочная местной телефонной сети (предоставляет справки о номерах телефонов абонентов местной сети);

– справочная точного времени;

– заказная междугородной телефонной сети МТС (принимает и оформляет заказы на междугородные и международные телефонные переговоры);

– справочная междугородной и международной сети;

– заказная телеграфа (принимает по телефону тексты телеграмм);

– заказная ремонта местной телефонной сети;

– заказная ремонта таксофонов.

Дополнительные услуги (их также называют дополнительными видами обслуживания – ДВО) могут предоставляться общесетевыми службами или службой той станции, куда подключена линия абонента, программно-аппаратными средствами станции или сети. К ДВО относятся, например, такие:

– сокращенный набор номера вызываемого абонента;

– передача входящего вызова на другой аппарат (переадресация);

– предоставление возможности пол справку во время разговора с одним из пользователей (с возможностью возврата к прежнему собеседнику без повторного набора его номера),

– конференц-связь трех и более пользователей;

– прямой вызов (соединение без набора номера).

4.1. Структура телефонной сети общего пользования

Телефонные сети РФ еще в недостаточной степени цифровизированы. Межстанционная связь в большей степени цифровизована с помощью цифровых СП. Подавляющее количество местных телефонных сетей РФ относится к типу аналого-цифровых. Цифровизация местной телефонной сети — актуальная задача ближайших лет.

Цифровые сети телефонной связи обладают рядом положительных свойств, отличающих их от телефонных сетей аналогового типа. Этими свойствами являются:

1. Простота группообразования (организация многоканальных систем передачи данных).

2. Простота сигнализации.

Возможность использования современной интегральной технологии:

1. Интеграция систем передачи и коммутации.
2. Возможность работы при малых значениях сигнал-шум.
3. Регенерация сигналов.
4. Приспосабливаемость к другим видам обслуживания.
5. Возможность контроля рабочих характеристик.
6. Легкость засекречивания информации.

При построении многоканальных систем передачи данных эффективность таких сетей по существу обусловлена обменом стоимости оконечных электронных узлов тракта передачи данных на стоимость многих пар проводов в тракте. Этот обмен с каждым годом становится все более выгодным. Используемый в цифровых многоканальных системах метод временного разделения каналов ВРК значительно дешевле метода частотного разделения каналов в аналоговых многоканальных системах. В аналоговых многоканальных системах также может использоваться и достаточно просто метод ВРК. Однако в этом случае узкие аналоговые импульсы сильно подвержены действию помех и искажений и их нельзя, как в цифровых системах, устранить с помощью регенерации.

Все управляющие сигналы в телефонной сети (вызов, отбой, цифры адреса и др.) по своей природе являются цифровыми и, следовательно, достаточно просто реализуются в цифровых системах, в то время как для аналоговых систем это является сложной и дорогой процедурой.

В настоящее время с развитием ЭВМ появились мощные технологии производства цифровых схем в виде БИС и СБИС, что позволило значительно снизить стоимость таких схем, при наличии у них высоких показателей качества работы. Все это можно использовать при реализации цифровых АТС.

Интегрирование систем передачи информации и коммутации за счет использования единого цифрового способа представления и обработки сигналов позволяет исключить каналообразующие блоки аналоговых систем, исключить многократные аналого-цифровые и цифро-аналоговые преобразования, и, тем самым, существенно увеличить качество передачи речи.При передаче цифровых сигналов их амплитуда поддерживается постоянной, что

обеспечивает требуемое качество речи при относительно небольших отношениях сигнал/шум. Для цифровых сигналов достаточно просто реализуется процедура регенерации, т.е. восстановление исходной формы импульсов. Наличие таких регенераторов в линии связи позволяет практически исключить ошибки при передаче данных и тем самым увеличить качество передачи речи.

Любое цифровое сообщение, независимо от того, было ли оно первоначально представлено в цифровой форме или получилось после преобразования аналоговых сигналов в цифровую форму, может быть представлено в едином формате. Поэтому по линиям цифровой телефонной связи могут дополнительно передаваться любые другие виды данных в цифровой форме.

Возможность использования помехоустойчивых кодов позволяет контролировать и исправлять ошибки в передаваемых данных. Простота кодирования цифровой информации методами криптографии. Основной проблемой при построении цифровых систем телефонной связи является преобразование первичных аналоговых сигналов в цифровую форму. Однако эти методы достаточно хорошо изучены и были уже представлены выше. При таком преобразовании используется импульсно-кодовая модуляция непрерывных сигналов. В многоканальных системах цифровой телефонной связи основным является метод временного разделения каналов. Об этом уже было сказано выше.

Для построения цифровых телефонных систем в 1960 г. МККТТ и МОС был принят международный стандарт РСМ 64 кбит/с. Этот стандарт предусматривает преобразование аналоговых речевых сигналов в 64 кбит/с цифровой сигнал на основе импульсно-кодовой модуляции. Человеческий голос можно воспроизводить с приемлемым качеством в полосе частот от 200 до 3400 Гц. Согласно теореме отсчетов для преобразования речевых сигналов требуется частота выборок 8 кГц или 8000 выборок в секунду. Каждая выборка представляется цифровым 8-разрядным кодом. Поэтому общая скорость ИКМ сигнала составит 8000×8 бит = =64 кбит/с. На основе этого стандарта строятся современные цифровые телефонные системы, которые в последнее время реализуются в виде интегрированных систем, позволяющих передавать не только речевую информацию, но и видеоданные, и цифровые данные ЭВМ.

Недостатки цифровых сетей передачи речи:

- расширение полосы частот по сравнению с аналоговой передачей речи;
- необходимость аналого-цифрового и цифро-аналогового преобразования;
- необходимость высокоточной временной синхронизации;
- технологические ограничения группообразования;
- несовместимость с существующим аналоговым оборудованием.

Структура телефонной сети существенно зависит от количества абонентов и размеров территории. При проектировании сети выбирается один из четырех принципов построения: радиальный, радиально-узловой, каждый с каждым, смешанный (сочетание радиально-узлового и «каждый с каждым»). Эти принципы приведены на рис. 4.1.1, *а–г*. Структура городской телефонной сети зависит от ее емкости, формы территории и других факторов. Структура старых нецифровизованных телефонных сетей существенно зависела от их емкости. На территории России до сих пор существуют сети больших городов с очень сложной структурой. Территорию города делят на телефонные районы, совпадающие или не совпадающие с административным делением. Если количество абонентов не превышало 10 000, то обычно строили одну станцию. При емкости сети в 40–50 тыс. номеров строили районированную сеть с одной автоматической телефонной станцией (АТС) в каждом телефонном районе. Станции соединялись пучками физических линий или каналами СП по способу «каждый с каждым» На сетях большой емкости необходимо было вводить узлы входящего сообщения (УВС). В каждом узловом районе УВС соединялся со всеми АТС сети радиально, объединяя информационные потоки от АТС всех других узловых районов с АТС своего района. В пределах каждого узлового района АТС соединялись каналами по способу «каждый с каждым». При емкости сети более 400–500 тыс. номеров приходилось еще более усложнять структуру, вводя новый тип узлов исходящего сообщения (УИС). Такой узел собирал информационные потоки от всех АТС своего узлового района и распределял их к УВС всех других районов. Такая структура смешанного типа характерна, например, для городской телефонной

сети Москвы, Санкт-Петербурга и других крупных промышленных центров и столиц республик РФ. Сельские телефонные сети (СТС) строят по радиальному или по радиально-узловому способу с одним узлом первого класса УСІ (центральная АТС сельского района области) и несколькими узлами второго УСІІ и, возможно, третьего УСІІІ класса.

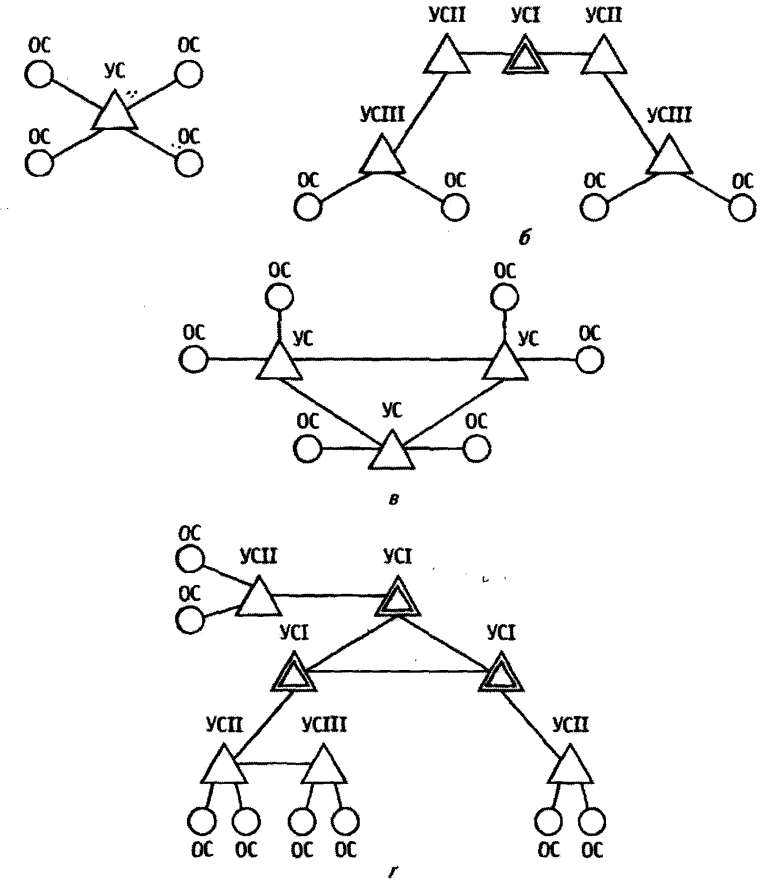


Рис. 4.1.1. Структура аналоговой вторичной телефонной сети [1]

В телефонной сети общего пользования РФ различают две разновидности систем нумерации – закрытую и открытую. Если на сети используется закрытая система нумерации, то из любого пункта требуемый абонент вызывается набором одного и того же

количества знаков, для открытой системы нумерации это условие не выполняется. На междугородной сети России используется открытая система нумерации, а на городских телефонных сетях ОП – закрытая. Вся территория РФ разделена на зоны семизначной нумерации. Семизначный номер абонента внутри зоны состоит из двух составляющих: двузначного внутризонового кода (*ab*) и пятизначного номера абонента местной сети (xxxxx). Полный внутризоновый номер имеет вид – *abxxxxx*. Начинаться внутризоновый номер может с любой цифры, кроме 0 и 8. С нуля начинаются номера служб специального на значения внутри зоны, а цифра 8 является индексом междугородной связи. Ограничений в применении десятичных знаков для и и xxxxx не устанавливается. Такие ограничения в использовании цифр для первого знака внутризонового номера позволяют иметь в зоне нумерации не более 8 млн. абонентов Количество зон на территории РФ может в ближайшем будущем превысить 100.

Поэтому каждой зоне присваивается трехзначный междугородный код АВС. Абонент местной сети, желающий вызвать абонента другой зоны, набирает 11 знаков: 8АВСаЬxxxxx, Если необходимо установить соединение между местными сетями одной зоны, то нужно набрать 9 знаков 82abxxxxx. Для международной связи выделен индекс 810.

На местных телефонных сетях зоны применяют закрытую систему нумерации. Значность нумерации определяется структурой сети (без узлов, с УВС, с УВС и УИС) и количеством абонентов. На городской сети без узлов используется пятизначная нумерация, на сети с УВС – шестизначная, на сети с УВС и УИС – семизначная. На сельской телефонной сети обычно используется закрытая пятизначная система нумерации.

Преобразование аналоговых вторичных сетей в цифровые – актуальная задача для ТФОП России. Возможны разные пути перехода от аналоговых сетей к цифровым. Для крупных сетей этот переход можно реализовать в несколько этапов: замена всех аналоговых межстанционных линий цифровыми, замена электромеханических узлов и станций цифровыми системами коммутации (ЦСК), построение цифровой сети интегрального обслуживания ЦСИО или сети нового поколения NGN.

Может быть предложена и другая стратегия перехода – создание так называемой наложенной цифровой сети (рис. 4.1.2). Такой путь позволяет минимизировать единовременные затраты так как в момент ввода первых ЦСК возможно создание полностью цифрового участка сети, в пределах которого информация от абонента до абонента может передаваться в цифровой форме. Пользователи наложенной сети сразу получают современные услуги цифровых сетей.

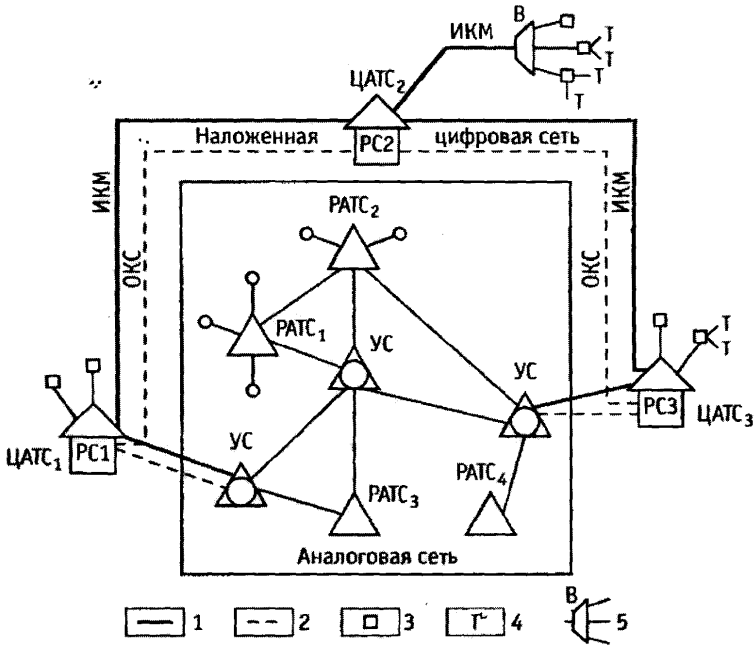


Рис. 4.1.2. Структура аналоговой вторичной сети переходного периода, развиваемой с помощью «наложенной цифровой сети» [1]. 1 – линия ИКМ; 2 – ОКС; 3 – абонентский пункт; 4 – терминал абонента; 5 – концентратор

Кроме этого, часть услуг цифровой сети смогут получать и абоненты аналоговой сети, благодаря специально организованному доступу к ресурсам наложенной сети.

Имеется еще одно преимущество такой стратегии, состоящее в том, что рационально выбранный участок для построения наложенной сети позволяет проложить определенное число маршрутов межстанционной связи через сеть. Это сразу должно сказаться на

повышении качества предоставляемых услуг благодаря использованию протяженных маршрутов только с цифровыми каналами. Естественной для цифровой сети является централизованная межстанционная сигнализация по общеканальной сигнализации (ОКС).

Применение централизованной сигнализации позволяет существенно повысить верность передачи сигнальной информации (адресной, линейных и информационных сигналов). Удаленные группы пользователей могут быть экономично включены в цифровые системы коммутации (ЦСК) с помощью выносов (В), являющихся частью программно-аппаратных средств этих ЦСК, приближенных к местам группирования пользователей. Функционально выносы цифровой сети отличаются от подстанций аналоговой сети способностью замыкать внутренние потоки информации без занятия каналов, связывающих вынос с ЦСК. Эти каналы используются только для внешней связи (входящей и исходящей) пользователей выноса.

Структура вторичных цифровых сетей общего пользования. Структура цифровой сети может быть существенно упрощена по сравнению со структурой аналоговой вторичной телефонной сети. Это связано, прежде всего, с тем, что нет таких жестких ограничений максимальной емкости ЦСК (количества портов – абонентских и соединительных линий), какие существуют для аналоговых оконечных станций и узлов. Поэтому для построения цифровой сети заданной емкости требуется меньшее количество станций, чем для по строения аналоговой сети. Еще одно важное отличие цифровой сети от аналоговой – практическое отсутствие ограничений на расстояние между станциями и узлами благодаря использованию систем передачи с ИКМ. Эти особенности позволяют строить цифровую городскую или ведомственную вторичную сеть как одноуровневую (т.е. без узлов). Станции такой сети могут быть связаны друг с другом по способу «каждая с каждой» линиями с ИКМ (рис. 4.1.3).

Эти станции могут использоваться как оконечные или как совмещенные (оконечные и транзитные) для целей обмена сигнальными сообщениями при межстанционной связи в цифровой сети выделяют сигнальную подсеть с КП. Эта подсеть образована

пунктами сигнализации (ПС) и связывающими их ОКС. Сигнальные сообщения в этой подсети передаются в форме пакетов переменной длины с высокой скоростью и верностью. В сигнальной подсети, являющейся эффективным транспортным средством, передаются не только сигнальные сообщения традиционных пользователей, но и команды управления сетью, а также данные для администрирования Сеть с описанными свойствами может поддерживать множество служб, таких, как телефонную, передачи данных, изображений – и ее принято называть цифровой сетью интегрального обслуживания. Станции цифровой сети, реализуя функции оконечных и транзитных, могут иметь емкость до 60 тыс. портов и более. В цифровой сети исключительно широко используются выносы (концентраторы) части оборудования оконечных станций, так как это позволяет снизить затраты на абонентскую сеть, называемую сетью доступа (сетью доступа пользователей к ресурсам цифровой сети).

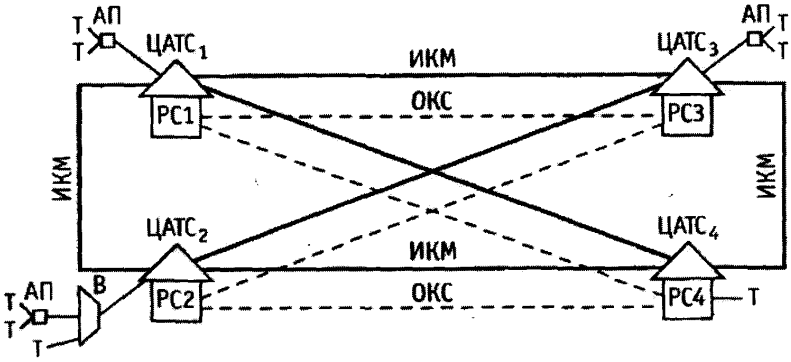


Рис. 4.1.3. структура вторичной одноуровневой сети [1]

Задачи развития телефонной сети общего пользования России таковы:

– переход от аналоговой телефонной сети к аналого-цифровой;

– создание цифровой сети связи ОП (ЦСС ОП) (для обслуживания в основном коммерческих пользователей);

– полная замена декадно-шаговых АТС.

4.2. Особенности передачи сигналов по телефонным сетям общего пользования

В состав телефонных аппаратов, предназначаемых для работы в телефонных сетях, входят следующие обязательные элементы: микрофон и телефон, объединенные в микротелефонную трубку, вызывное устройство, трансформатор, разделительный конденсатор, номеронабиратель, рычажный переключатель. На принципиальных электрических схемах телефонный аппарат обозначают буквой Е.

Микрофон служит для преобразования звуковых колебаний речи и электрический сигнал звуковой частоты. Микрофоны могут быть угольными, конденсаторными, электродинамическими, электромагнитными, пьезоэлектрическими. Их можно классифицировать на активные и пассивные. Активные микрофоны непосредственно преобразуют звуковую энергию в электрическую. В пассивных же микрофонах звуковая энергия преобразуется в изменение какого-либо параметра (чаще всего – емкости и сопротивления). Для работы такого микрофона обязательно требуется вспомогательный источник питания. В массовых телефонных аппаратах применяют, как правило, угольные микрофоны, в которых под действием звуковых волн изменяется электрическое сопротивление угольного порошка, находящегося под мембраной. На принципиальных схемах микрофон обозначают латинскими буквами BM.

Телефоном называют прибор, предназначенный для преобразования электрических сигналов в звуковые и рассчитанный для работы в условиях нагрузки на ухо человека. В зависимости от конструктивных особенностей телефоны подразделяют на электромагнитные, электродинамические, с дифференциальной магнитной системой и пьезоэлектрические. В телефонных аппаратах наибольшее распространение получили телефоны электромагнитного типа. В таких телефонах катушки закреплены неподвижно. Под действием протекающего в катушках тока возникает переменное магнитное поле, приводящее в движение подвижную мембрану, которая и излучает звуковые колебания. Полоса рабочих частот для микрофонов и телефонов, используемых в телефонных аппаратах, составляет примерно 300...3500 Гц. На принципиальных схемах телефон обозначают латинскими буквами *BF*.

Для удобства пользования микрофон и телефон объединены в *микротелефонной трубке.*

Вызывное устройство служит для преобразования вызывного сигнала переменного тока в звуковой сигнал. Применяют электромагнитные или электронные вызывные устройства. Первое из них представляет собой одно- или двухкатушечный звонок. Вызовой сигнал образуется в результате удара бойка о звонковые чашки. Протекающий в катушках ток частотой 16...50 Гц создаст переменное магнитное поле, которое приводит в движение якорь с бойком. Как правило, в телефонных звонках используют постоянные магниты, создающие определенную полярность магнитопровода, поэтому такие звонки называют поляризованными. На принципиальных схемах звонок обозначают латинскими буквами НА. Электронное вызывное устройство преобразует вызывной сигнал в звуковой тональный сигнал, который может имитировать, например, пение птицы. Электронные вызывные устройства выполняют на транзисторах.

Трансформатор телефонного аппарата предназначен для связи отдельных элементов разговорной части и для согласования их сопротивлений с входным сопротивлением абонентской линии. Он, кроме того, позволяет устранять так называемый местный эффект, о чем будет сказано ниже. Трансформаторы изготавливают с отдельными обмотками или в виде автотрансформаторов.

Разделительный конденсатор служит элементом подключения вызывного устройства к абонентской линии в режиме ожидания и приема вызова. При этом обеспечивается практически бесконечно большое сопротивление телефонного аппарата постоянному току и малое сопротивление – переменному.

Номеронабиратель обеспечивает подачу импульсов набора номера в абонентскую линию с целью установления требуемого соединения. Импульсы служат для периодических замыканий и размыканий линии. В современных телефонных аппаратах применяют механические и электронные номеронабиратели. Дисковый механический номеронабиратель имеет диск с десятью отверстиями. При вращении диска по часовой стрелке заводится пружина механизма номеронабирателя. После отпускания диска он вращается в обратную сторону под действием пружины, при этом про-

исходит периодическое размыкание контактов, коммутирующих абонентскую линию. Необходимая скорость и равномерность вращения диска достигаются наличием центробежного регулятора или фрикционного механизма. Формирование импульсов при свободном движении диска обеспечивает их стабильную частоту и необходимый интервал между импульсными посылками, соответствующими двум соседним цифрам набираемого номера. Необходимый интервал обеспечивается благодаря тому, что число размыканий импульсных контактов всегда выбирается на одно-два больше, чем требуется подать импульсов в линию. Этим обеспечивается гарантированная пауза между пачками импульсов (0,2...0,8 с). При этом указанные лишние импульсы в линию не поступают, поскольку в это время импульсные контакты шунтируются одной из групп контактов номеронабирателя. Имеются также контакты, замыкающие телефон при наборе номера, чтобы исключить неприятные щелчки. Частота импульсов, формируемых номеронабирателем, должна составлять (10±1) имп./с. Число проводов, соединяющих номеронабиратель с другими элементами телефонного аппарата, может быть 3…5. Дисковые Номеронабиратели по принципу действия не являются источником радиопомех, не чувствительны к индустриальным радиопомехам.

Электронные номеронабиратели, которыми комплектуются многие современные телефонные аппараты, выполнены на интегральных микросхемах и транзисторах. Набор номера осуществляют нажатием кнопок клавиатуры - так называемой тастатуры. Поскольку скорость нажатия кнопок может быть сколь угодно большой, в среднем на наборе одной цифры номера экономится 0,5 с. Кроме того, тастатурные номеронабиратели предоставляют пользователям различные удобства, экономящие время:

запоминание последнего набранного номера, возможность запоминания нескольких десятков номеров и др. Питание электронных номеронабирателей осуществляется как от абонентской линии, так и от сети напряжением 220 В через блок питания.

Рычажный переключатель обеспечивает подключение к абонентской линии вызывного устройства телефонного аппарата в нерабочем состоянии (микротелефонная трубка лежит) и разговорных цепей или номеронабирателя в рабочем состоянии (трубка

снята). Рычажный переключатель представляет собой группы из нескольких переключающих контактов, срабатывающих при снятии телефонной трубки.

Кроме перечисленных элементов в состав телефонного аппарата входят также резисторы, конденсаторы, диоды, транзисторы, образующие разговорную цепь аппарата. При работе телефонного аппарата в разговорном режиме возникает местный эффект, т.е. прослушивание собственной речи в телефоне аппарата. Местный эффект объясняется тем, что ток, протекающий через микрофон, поступает не только в абонентскую линию, но и в собственный телефон. Для устранения этого нежелательного явления в современных телефонных аппаратах используют противоместные устройства.

Существуют различные типы подобных устройств. Рассмотрим одно из них – противоместное устройство мостового типа, представленного на рис. 4.2.1.

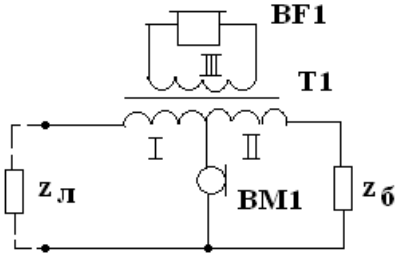


Рис. 4.2.1. Функциональная схема телефонного аппарата с противоместным эффектом

Микрофон BM1, телефон BF1, балансный контур Zб и линия Zл связаны между собой обмотками трансформатора T1: линейной I, балансной II и телефонной III. Во время разговора, когда сопротивление микрофона изменяется, разговорные токи звуковой частоты протекают по двум цепям: линейной и балансной. Из схемы видно, что токи, протекающие через обмотки I и II, суммируются с противоположными знаками, поэтому ток в обмотке 111 будет отсутствовать в том случае, если токи в линейной и балансной обмотках равны по величине. Это достигается соответствующим выбором элементов балансного контура Zб, параметры которого зависят от параметров линии Zл. Сопротивление линии содержит

активную и емкостную составляющие, поэтому балансный контур выполняют из резисторов и конденсаторов.

Полное устранение местного эффекта достигается только на одной определенной частоте и определенных параметрах линии, что в реальных условиях невыполнимо, поскольку речевой сигнал содержит широкий спектр частот, а параметры линии изменяются в широких пределах (зависят от удаленности абонента от АТС, переходных сопротивлений и емкостей в кабелях и др.), поэтому на практике местный эффект не уничтожается полностью, а только ослабляется.

Рассмотрим схему телефонного аппарата ТА-72М-5 (рис. 4.2.2), предназначенного для работы в городских сетях. Его коммутационно-вызывную часть образуют рычажный переключатель SA1, звонок HA1, разделительный конденсатор C1 и номеронабиратель SA2. Разговорная часть телефонного аппарата состоит из телефона BF1, микрофона BM 1, трансформатора T 1, балансного контура (конденсаторы C1 и C2, резисторы R1-R3) и ограничительных диодов VD1, VD2. Разговорная часть выполнена по противоместной схеме мостового типа.

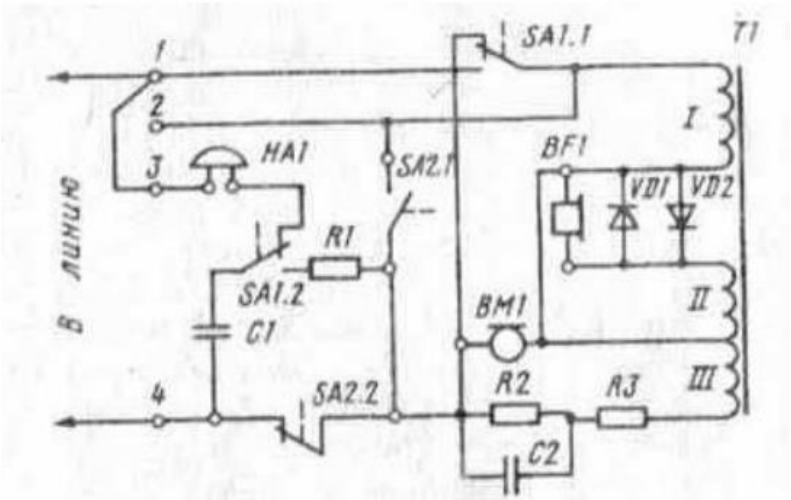


Рис. 4.2.2. Схема телефонного аппарата ТА-72М-5

В исходном состоянии контактов рычажного переключателя SA1 и номеронабирателя SA2, показанном на схеме, к линии под-

ключены последовательно соединенные между собой звонок HA1 и конденсатор C1, а разговорная часть отключена. При появлении вызывного напряжения на зажимах 1 и 4 телефонного аппарата ток протекает по цепи: зажим 1 – перемычка – зажим 3 – обмотка звонка – нормально замкнутые контакты SA1.2 рычажного переключателя – конденсатор C1 – зажим 4. (Направление тока выбрано условно – с таким же успехом его можно было бы считать протекающим от зажима 4 к зажиму 1.)

Услышав звонок, абонент снимает трубку. При этом контакты SA1.1 и SA1.2 переключаются в другое положение, отключая вызывную цепь и подключая к линии разговорную цепь. Сопротивление постоянному току между зажимами 1 и 4 изменяется от очень большого (сотни килоом – мегаомы) до относительно малого (сотни ом), это фиксируется приборами телефонной станции, и они переключаются в разговорный режим.

При наборе номера контакты SA2.1 номеронабирателя находятся в замкнутом состоянии во время прямого и возвратного вращения диска, что обеспечивает шунтирование разговорной цепи и исключает прослушивание щелчков в телефоне. При возвратном вращении диска номеронабирателя контакты SA2.2 разрывают линейную цепь, и приборы станции по числу таких размыканий фиксируют номер вызываемого абонента. Диоды VD1 и VD2 ограничивают выбросы напряжения на обмотках телефона и исключают резкие звуки, неприятные для уха.

Передача данных в сетях может быть симплексной и дуплексной. При симплексной передаче сигналы передаются только в одном направлении, одна станция является приемником, а другая – передатчиком. В принципе, передавать могут обе станции, но только по очереди. При дуплексном режиме работы обе станции могут передавать одновременно. Дуплексная работа требует наличия двух различных трактов передачи (например, двух витых пар), тогда как полудуплексная (симплексная) работа требует всего одного. Впрочем, можно одновременно передавать в обоих направлениях и по одной линии передачи, используя для этого методику эхоподавления (echo cancellation).

Рассмотрим принцип эхоподавления на примере телефонной сети.

На рис. 4.2.3 изображена телефонная сеть, использующая двухпроводные линии для соединения абонентских телефонов с АТС. Каждая из 2-проводных линий между телефоном и АТС несет голосовые сигналы в двух направлениях, от одного телефона к другому и обратно. Очевидно, что двухпроводные линии дешевле, чем 4-проводные, поэтому стандартные телефонные аппараты и АТС ориентированы на связь друг с другом посредством двухпроводных линий.

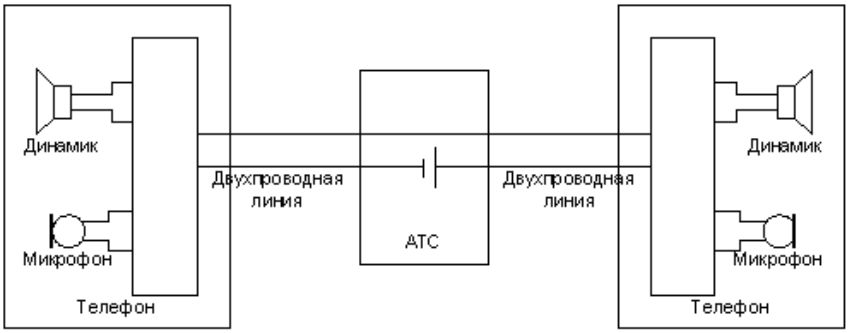


Рис. 4.2.3. Упрощенная двухпроводная телефонная сеть с двумя абонентами

Описанная выше телефонная сеть весьма проста и может хорошо работать на коротких расстояниях между абонентами. Однако, если мы хотим нормально общаться с очень удаленными абонентами, мы должны усилить сигналы, затухающими в длинных аналоговых линиях. Однако сначала надо отделить посылаемые и получаемые сигналы. Это разделение осуществляется с помощью специального прибора, называемого гибридом, который конвертирует сигналы между двухпроводной и 4-проводной линиями (АТС соединяются между собой 4-проводными линиями).

Телефонная сеть, к которой подключены удаленные абоненты с помощью гибридов, приведена на рис. 4.2.4.

Часть сигнала, посланная гибриду с четырехпроводной стороны, возвращается обратно, как эхо, наложенное на принимаемый сигнал. Если, например, левый гибрид на рис. 5.2.4 подвержен подобному искажению, то воображаемый абонент в правой части рисунка будет слышать в телефонной трубке эхо своего собственного голоса.

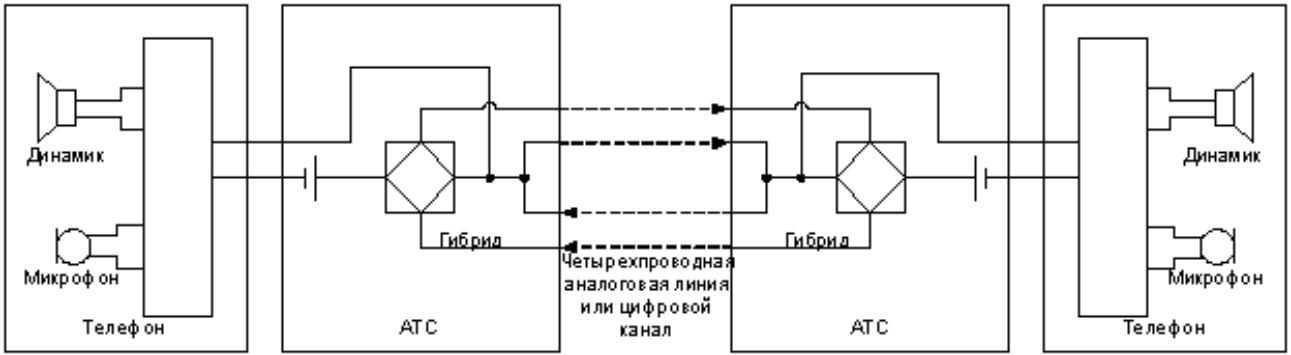


Рис. 4.2.4. Междугородная телефонная сеть
с переходом с двухпроводной линии
на четырехпроводную

На рис. 4.2.5 показана АТС с системой эхоподавления, встроенной с четырехпроводной стороны между точками *A, B, C* и *D*. Имеются следующие сигналы (показанные как функции от *i*-го сэмпла): *x*(*i*) – сигнал от абонента, подключенного через двухпроводную линию к АТС (сигнал от локального абонента), *y*(*i*) и *u*(*i*) – сигналы от и к другому абоненту (дальнему абоненту), который проходит через четырехпроводную линию. Основной принцип подавления эхо достаточно прост. Сигнал от дальнего абонента *y*(*i*), проходя через эхопуть гибрида (между точками *B* и *A*) подвергается воздействию импульсного отклика этого эхопути и трансформируется в сигнал *r*(*i*), представляющий из себя нежелательное эхо. Сигнал от дальнего абонента, *x*(*i*), складывается с сигналом *r*(*i*) в точке *A*.

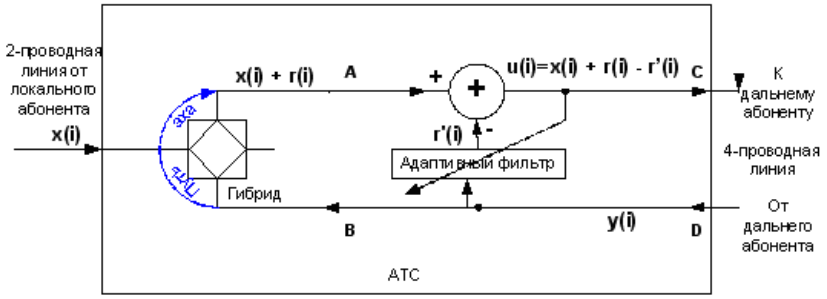


Рис. 4.2.5. АТС с подавлением гибридного эха (линии питания не показаны)

Адаптивный фильтр (обычно КИХ-фильтр), используемый в системе, воспроизводит импульсный отклик и создает копию, *r*'(*i*), эхо сигнала *r*(*i*). Если *r*(*i*) и *r*'(*i*) совпадают, то они будут подавлять друг друга в сумматоре, подсоединенном между точками *A* и *C* и выходом фильтра. Если *r*(*i*) и *r*'(*i*) не совпадают, то удаленный абонент будет слышать не только сигнал локального абонента, но также и разницу между *r*(*i*) и *r*'(*i*). Именно эта разница и называется сигналом остаточного эха.

Сигнал остаточного эха, $e(i) = r(i) - r'(i)$, используется для адаптивной настройки коэффициентов фильтра. То есть эхоподавитель – это система слежения с сигналом остаточного эха в обратной связи. Этот сигнал является сигналом ошибки для системы, и основная задача системы – минимизация этого сигнала.

Очевидно, что ввиду того, что импульсный отклик эхопути неизвестен, требуется некоторое время, чтобы эхоподавитель минимизировал сигнал остаточного эха до необходимого уровня. Это время называется "временем сходимости".

Хорошая производительность эхоподавителя может быть достигнута при использовании алгоритма NLMS (Normalized Least Mean Squares, нормированный метод наименьших квадратов). Вышеупомянутый алгоритм является наиболее широко используемым алгоритмом, т.к. он позволяет определять оптимальные коэффициенты фильтра с наименьшими затратами.

Ниже приводится общая формула вычисления адаптивных коэффициентов в NLMS алгоритме (без вывода, так как вы можете найти его сами в литературе по адаптивной обработке сигналов):

$$a_k(i+1) = a_k(i) + 2 \cdot \beta \cdot \frac{e(i) \cdot y(i-k)}{N \cdot \sigma^2}, \qquad (4.2.1)$$

где i – номер отсчета; a_k – k-й коэффициент фильтра; N – номер коэффициента фильтра; B – шаг адаптации, управляющий временем сходимости и качеством адаптации; e – сигнал остаточного эха; y – сигнал дальнего абонента; σ^2 – энергия опорного сигнала.

4.3. Особенности передачи данных по телефонным сетям общего пользования

Для передачи по линиям ТФОП данных, телеграфных и факсимильных сообщений для преобразования сигналов к форме, совместимой с сигналами ТФОП, необходимо использовать дополнительное сетевое оборудование – модемы и шлюзы. Модемы обеспечивают операции кодирования источника сообщения для передачи по сетям ТФОП и модуляции для передачи сигнала с определенной скоростью. Известно, например, что факсимильное сообщение обладает большой избыточностью. Для сокращения этой избыточности применяется кодирование источника, например, с использованием кода Хаффмена (рекомендация Т.4 МСЭ-Т). Устранение избыточности с помощью МКХ обеспечивает реализацию коэффициента сжатия по битам более 4,7.

Решетчатое кодирование (Trellis code modulation – TCM) применяется для улучшения качества связи при передаче данных по телефонным каналам**.** Пространство сигналов расширяется путем

добавления к информационным битам вспомогательных, которые образуются благодаря сверточному кодированию части информационных бит. Если, к примеру, информационные биты разбиты на группы по 4 бита (всего возможно 16 различных комбинаций), то добавление пятого треллис-бита приведет к расширению числа возможных комбинаций информационных бит, равному 32. Но при этом часть комбинаций, имеющих наихудшие пространственные характеристики в смысле вероятности ошибки объявляются запрещенными. Расширенная таким образом группа подвергается многопозиционной амплитудно-фазовой модуляции. На принимающей стороне осуществляется декодирование принятого сигнала по алгоритму Витерби. Если принимаемые последовательности являются разрешенными, то считается, что передача происходит без ошибок и треллис бит просто удаляется. Если среди принимаемых последовательностей встречаются запрещенные, то при помощи алгоритма декодирования декодер Витерби находит наиболее подходящую разрешенную последовательность, исправляя таким образом ошибки передачи.

Как известно, данные в компьютере, представленные в цифровой форме, закодированы в виде нулей и единиц, которым физически соответствует низкий или высокий уровень напряжения. Как известно, для передачи данных по аналоговому каналу необходимо управлять одним из параметров сигнала несущей частоты, например, амплитудой, частой или фазой. Типичным аналоговым каналом является телефонный канал. В нем при передаче речи воспринимаемые микрофоном звуки преобразуются в электрические сигналы, которые модулируют сигнал тональной частоты, являющийся несущим колебанием. При передаче цифровой информации управление параметрами несущего колебания производят информационные биты – потенциальный импульсный код.

Таким образом, если для передачи цифровой информации по телефонному каналу связи необходимо поток битов преобразовать в аналоговые сигналы, то при приеме информации из канала связи в ЭВМ нужно выполнить обратное действие - преобразовать аналоговые сигналы в поток битов, которые может обрабатывать ЭВМ. Такие преобразования выполняет специальное устройство, включаемое между компьютером и телефонной линией, называе-

мое модемом (сокращение от МОдулятор-ДЕМодулятор). Типовая схема организации связи при помощи модемов представлена на рис. 4.3.1.

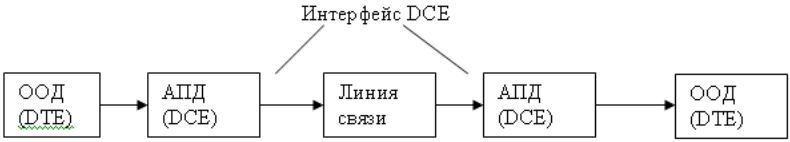


Рис. 4.3.1. Типовая схема организации связи при помощи модемов

Оконечное оборудование данных (ООД) – в терминологии систем связи обозначает оконечные цифровые устройства, генерирующие или получающие данные. Соответствующий ООД международный термин имеет аббревиатуру DTE (Data Terminal Equipment). В качестве DTE может выступать персональный компьютер, большая ЭВМ, терминал, устройство сбора данных, кассовый аппарат, приемник сигналов глобальной навигационной системы или любое оборудование, способное передавать или принимать данные.

Оконечное оборудование передает и(или) принимает данные посредством аппаратуры передачи данных (АПД) и канала связи. Соответствующий АПД международный термин – DCE (Data Communication Equipment – оборудование передачи данных). Этим термином обозначаются модемы. Оборудование DCE может являться аналоговым модемом, если используется аналоговый канал, или, устройством обслуживания канала/данных (CSU/DSU – Channel Service Unit/Data Service Unit), если используется цифровой канал. В настоящее время модемы наиболее широко используются для передачи данных между компьютерами через коммутируемую телефонную сеть общего пользования (ТфОП, GTSN – General Switched Telephone Network). Линия связи между DCE – аналоговая, между DCE и DTE – цифровая.

Важную роль во взаимодействии DTE и DCE играет интерфейс, который состоит из входящих/исходящих цепей, разъемов и соединительных кабелей. Интерфейс определяет логику работы DTE и DCE.

По функциональным возможностям можно выделить модемы:

- без системы управления;
- поддерживающие набор АТ-команд;

• с поддержкой команд V.25bis;
• с фирменной системой команд;
• поддерживающие протоколы сетевого управления.

Большинство современных модемов наделено широким спектром интеллектуальных возможностей. Стандартом де-факто стало множество АТ команд, разработанных в свое время, фирмой Hayes которые позволяют пользователю или прикладному процессу полностью управлять характеристиками модема и параметрами связи. По этой причине модемы, поддерживающие АТ-команды, носят название Hayes-совместимых модемов. Следует заметить, что АТ-команды поддерживаются не только модемами для ТфОП, но и пакетными радиомодемами, внешними адаптерами ISDN, и рядом других модемов для более узких сфер применения. Наиболее распространенным набором команд, позволяющих управлять режимами установления соединения и автовызова, являются команды, определенные рекомендацией ITU-TV.25bis.

Специализированные модемы для промышленного применения часто имеют фирменную систему команд, отличную от набора АТ-команд. Причиной тому является большое различие в режимах работы и выполняемых функциях между модемами широкого применения и промышленными (сетевыми) модемами. Промышленные модемы часто поддерживают протокол сетевого управления SNMP (Simple Network Management Protocol), позволяющий администратору управлять элементами сети (включая модемы) с удаленного терминала.

По конструкции различают модемы:
• внешние;
• внутренние;
• портативные;
• групповые.

Внешние модемы представляют собой автономные устройства, подключаемые к компьютеру или другому DTE посредством одного из стандартных интерфейсов DTE-DCE. Внутренний модем – это плата расширения, вставляемая в соответствующий слот компьютера. Каждый из вариантов конструктивного исполнения имеет свои преимущества и недостатки. Портативные модемы предназначены для использования мобильными пользователями

совместно с компьютерами класса Notebook. Они отличаются малыми габаритами и высокой ценой. Их функциональные возможности, как правило, не уступают возможностям полнофункциональных модемов. Часто портативные модемы оснащены интерфейсом PCMCIA. Групповыми модемами называют совокупность отдельных модемов, объединенных в общий блок и имеющих общие блок питания, устройства управления и отображения. Отдельный модем группового модема представляет собой плату с разъемом, устанавливаемую в блок, и рассчитан на один или небольшое число каналов.

Модемы также можно классифицировать в соответствии с реализованными в них протоколами. Все протоколы, регламентирующие те или иные аспекты функционирования модемов, могут быть отнесены к двум большим группам: международным и фирменным.

Протоколы международного уровня разрабатываются под эгидой ITU-T и принимаются им в качестве рекомендаций (ранее ITU-T назывался Международным Консультативным Комитетом по Телефонии и Телеграфии – МККТТ, международная аббревиатура – CCITT). Все рекомендации ITU-T относительно ТфОП модемов относятся к серии V.

Фирменные протоколы разрабатываются отдельными компаниями – производителями модемов, с целью преуспеть в конкурентной борьбе. Часто фирменные протоколы становятся стандартными протоколами де-факто и принимаются частично, либо полностью в качестве рекомендаций ITU-T, как это случилось с рядом протоколов фирмы Microcom. Наиболее активно разработкой новых протоколов и стандартов занимаются такие известные фирмы, как AT&T, Motorolla, U.S. Robotics, ZyXEL и другие.

С функциональной точки зрения модемные протоколы могут быть разделены на следующие группы:

• определяющие нормы взаимодействия модема с каналом связи (V.2,V.25);

• регламентирующие соединение и алгоритмы взаимодействия модема и DTE (V.10, V. 11 ,V.24,V.25,V.25 bis);

• определяющие основные характеристики модемов, предназначенных для коммутируемых и выделенных телефонных кана-

лов. К ним относятся такие протоколы, как V. 17, V.22, V.32, V.34, HST, ZyX и другие;

• коррекции ошибок (V.41, V.42, MNP1 -MNP4);

• сжатия передаваемых данных, такие как MNP5, MNP7, V.42bis;

• определяющие процедуры диагностики модемов, испытания и измерения параметров каналов связи (V.51, V.52, V.53, V.54, V.5б);

• согласования параметров связи на этапе ее установления (Handshaking), например V.8.

Приставки «bis» и «ter» в названиях протоколов обозначают, соответственно, вторую и третью модификацию существующих протоколов или протокол, связанный с исходным протоколом. При этом исходный протокол, как правило, остается поддерживаемым.

В модемах факсимильных аппаратов наиболее часто используются следующие протоколы:

– V.27ter – полудуплексный протокол, в котором применяется трехкратная ОФМ с частотой несущего колебания 1,8 кГц. Существуют два режима с разными информационными скоростями: 2,4 и 4,8 кбит/с. Линейная скорость 2,4 кбит/с достигается при использовании двухкратной ОФМ со скоростью модуляции 1200 Бод, 4,8 кбит/с – трехкратной ОФМ со скоростью модуляции 1600 Бод.

Существует еще два модемных протокола данного семейства – V.27 и V.27bis, которые отличаются от V.27ter в основном, типом канала, для которого они предназначены (выделенный четырехпроводной). В настоящее время V.27 и V.27bis практически не применяются.

– V29 – первый стандарт, в котором было предложено использовать метод модуляции QAM. В конце 70-х годов XX в. он нашел широкое применение в нашей стране и за рубежом для передачи данных по выделенным каналам с четырехпроводным окончанием со скоростью 9,6 кбит/с. Позднее этот протокол был стандартизован для факсимильной связи в полудуплексном режиме и работал по обычным коммутируемым каналам. Частота несущего сигнала 1,7 кГц, модуляционная скорость 2400 Бод. Стандарт имеет режимы двухпозиционной однократной ОФМ, четырехпозиционной двукратной ОФМ, восьмипозиционной трехкратной ОФМ, шест-

надцатипозиционной QAM модуляции. Соответственно информационная скорость может быть 2,4; 4,8; 7,2; 9,6 кбит/с (в некоторых модемах нижний предел 4,8 кбит/с).

– V17 – по своим параметрам точный аналог V32bis, но предназначен только для полудуплексного режима работы. В нем используется модуляция с решетчатым кодированием без алгоритмов эхокомпенсации. Частота несущего сигнала 1,8 кГц, модуляционная скорость 2400 Бод. Имеет режимы 160TCM, 32-TCM, 64-TCM и 128-TCM. Информационная скорость – 7,2; 9,6; 12,0;14,4 кбит/с соответственно.

Шлюзы при необходимости обеспечивают преобразование и согласование интерфейсов, форматов, способов адресации при подключении сетей ТФОП к сетям передачи данных.

Необходимо отметить, что ТФОП на в полной мера отвечает требованиям передачи данных, несмотря на ее широкую разветвленность, по следующим причинам:

– аналоговый способ передачи сообщений;

– невысокая скорость передачи;

– значительное время установления соединения; частые отказы в установлении соединения.

4.4. Сетевые технологии в телефонных сетях общего пользования

Совокупность линейных и станционных средств, предназначенных для соединения оконечных абонентских устройств в сети ТФОП, называется соединительным трактом. Число коммутационных узлов между соединяемыми абонентскими устройствами зависит от структуры сети и направления соединения. Для осуществления требуемого соединения коммутационный узел и абонентское устройство обмениваются управляющими сигналами. На коммутационном узле соединение может устанавливаться на время, необходимое для передачи одного сообщения (например, одного телефонного разговора), или на длительное время, превышающее время передачи одного сообщения. Коммутация первого вида называется оперативной, а второго – кроссовой (долговременной).

Коммутационный узел представляет собой устройство, предназначенное для приема, обработки и распределения поступающей

информации. Для выполнения своих функций коммутационный узел должен иметь (рис. 4.4.1):

• коммутационное поле (КП), предназначенное для соединения входящих и исходящих линий (каналов) на время передачи информации;

• управляющее устройство (УУ), обеспечивающее установление соединения между входящими и исходящими линиями через коммутационное поле, а также прием и передачу управляющей информации.

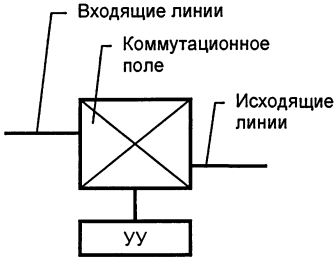


Рис. 4.4.1. Основные составляющие коммутационного узла [2]

К аппаратуре приема и передачи управляющей информации относятся (рис. 4.4.2):

• регистры (Рег), или комплекты приема номера (КПН), кодовые приемопередатчики и пересчетные устройства;

• линейные комплекты (ЛК) входящих и исходящих линий (каналов), предназначенные для приема и передачи линейных сигналов (сигналов взаимодействия) по входящим и исходящим линиям или каналам для выделения каналов в системах передачи, а также для приема и передачи сигналов взаимодействия с управляющими устройствами узла;

• шнуровые комплекты (ШК), предназначенные для питания микрофонов телефонных аппаратов, приема и посылки служебных сигналов в процессе установления соединения;

• устройства ввода и вывода линий (Кросс).

Кроме того, на узле имеются источники электропитания, устройства сигнализации и учета параметров нагрузки (количество сообщений, потерь, длительности занятия и др.).

В некоторых случаях коммутационный узел может иметь устройства приема и хранения информации, если таковая переда-

ется не непосредственно потребителю информации, а предварительно накапливается на узле. Такие узлы применяются в системах коммутации сообщений.

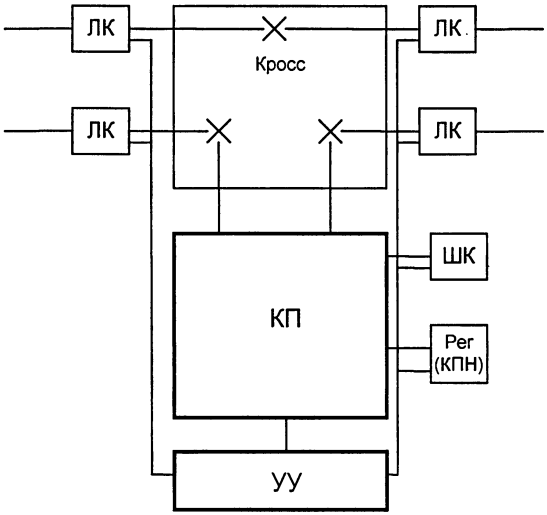


Рис. 4.4.2. Структура коммутационного узла в сети ТФОП [2]

Для осуществления коммутации (соединения) линий (или каналов) и управления процессами установления соединения применяются коммутационные приборы. Коммутационным прибором называется устройство, обеспечивающее замыкание, размыкание или переключение электрических цепей, подключенных к его входам и выходам, при поступлении в прибор управляющего сигнала. Замыкание, размыкание и переключение электрических цепей в коммутационном приборе осуществляется коммутационным элементом (КЭ), который в простейшем случае представляет собой один контакт на замыкание. К коммутационному прибору могут подключаться линии с различной проводностью (двух-, трехпроводные и т.д.), поэтому их коммутация осуществляется несколькими КЭ, объединенными в коммутационную группу, коммутационные элементы которой переключаются одновременно под влиянием поступающего управляющего сигнала.

В коммутационном приборе в зависимости от его конструкции может быть установлено различное число коммутационных

групп. Совокупность коммутационных групп называется коммутационным полем прибора. Местоположение коммутационной группы в коммутационном поле прибора (или в коммутационном блоке, построенном из нескольких приборов) называется точкой коммутации. Коммутационные приборы различаются между собой структурными и электрическими параметрами, обусловленными их конструкцией. К структурным параметрам относятся: число входов n, число выходов m, доступность D входов по отношению к выходам, проводность коммутируемых линий l, свойство памяти. Производными от этих параметров являются общее число точек коммутации T, число коммутационных групп и число коммутационных элементов, а также максимальное число одновременных соединений.

К электрическим параметрам коммутационных приборов относятся: сопротивление коммутационного элемента в разомкнутом (закрытом) состоянии $R_З$ и замкнутом (открытом) состоянии $R_о$, отношение которых называется коммутационным коэффициентом $K = R_0/R_З$, время переключения КЭ из одного состояния в другое; вносимое затухание в разговорный тракт; уровень шумов; напряжение питания; сила тока, необходимого для переключения КЭ; потребляемая мощность.

Коммутационные приборы характеризуются также сроком службы или долговечностью, под которыми понимается допустимое число переключений или допустимое время работы, и интенсивностью отказов (повреждений), т.е. вероятностью отказов в единицу времени.

Некоторые коммутационные приборы обладают свойством памяти, т.е. способностью сохранять рабочее состояние после прекращения управляющего воздействия. Это позволяет сократить расход электроэнергии для поддержания рабочего состояния прибора. Для возвращения прибора в исходное состояние требуется новое управляющее воздействие.

Используемые в настоящее время коммутационные приборы по структурным параметрам можно разделить на четыре типа:

1. Коммутационные приборы типа (1×1), имеющие один вход и один выход. Число входов и выходов прибора указывается в круглых скобках, где первая цифра – число входов n, а вторая –

число выходов m. Прибор имеет два состояния, в одном из которых соединение между входом и выходом отсутствует, а в другом – установлено. Переход коммутационного элемента (или коммутационной группы) из одного состояния в другое осуществляется под воздействием сигнала, поступающего на управляющий вход из устройства управления.

2. Коммутационные приборы типа (1 × *m*), имеющие один вход *n* = 1 и *m* выходов. В приборе можно установить соединение входа с любым из m выходов, следовательно, доступность прибора *D* = *m*. Одновременно в приборе может быть установлено только одно соединение.

3. Коммутационные приборы типа *n*(1×*m*), имеющие n входов и *nm* выходов. Каждому входу из n доступно только m определенных выходов, следовательно, *D* = *m* из общего числа выходов nm. В приборе одновременно может быть установлено n соединений.

4. Коммутационные приборы типа (nxm), имеющие n входов и m выходов. Каждому из n входов доступен любой из m выходов, следовательно, *D* = *m*. В приборе одновременно может быть установлено n соединений, если $n \le m$, или т соединений, если $n > m$.

Коммутационное поле строится из отдельных коммутационных блоков, которые, в свою очередь, могут объединяться в более крупные блоки, а последние – в ступени искания. Совокупность ступеней искания образуют коммутационное поле. По функциональному назначению ступени искания подразделяются на ступени линейного, предварительного и группового искания.

Режим искания, при котором производится поиск конкретной абонентской линии по командам управляющего устройства АТС, называется линейным, а соответствующая ступень – ступенью линейного искания (ЛИ). На рис .4.4.3 показано условное обозначение ступени ЛИ.

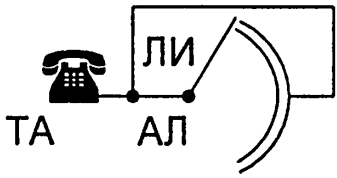


Рис. 4.4.3. Условное обозначение ступени линейного искания. ТА – телефонный аппарат; АЛ – абонентская линия; ЛИ – ступень линейного искания

В зависимости от числа вызовов от абонентов и продолжительности разговоров могут потребоваться одновременные соединения, число которых составит 10...15 % общего числа абонентов АТС. Поэтому для обслуживания, например, 100 абонентов достаточно иметь 10…15 100-линейных искателей. При этом следует предусмотреть возможность использования абонентом любого из свободных искателей, т.е. необходимо сделать искатели приборами коллективного пользования. Для этого применяются так называемые искатели вызова (ИВ), которые совместно с ЛИ образуют шнуровую пару ИВ-ЛИ. Число таких пар составляет 10...15 % емкости АТС. Упрощенная схема АТС на основе шнуровых пар ИВ-ЛИ показана на рис. 4.4.4.

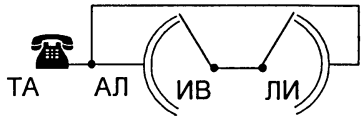


Рис. 4.4.4. Упрощенная схема АТС на основе шнуровых пар ИВ-ЛИ

Процесс установления соединения протекает следующим образом. При снятии абонентом микротелефонной трубки ИВ свободной шнуровой пары отыскивает в своем поле линию этого (вызывающего) абонента. Данный поиск (искание) называют свободным. Кроме того, поскольку искание осуществляется до набора вызываемого абонента, оно называется предварительным или предысканием. В данном случае применено так называемое обратное предыскание, поскольку процесс установления соединения протекает от свободного ИВ к АЛ вызывающего абонента. После приема номера происходит процесс линейного искания АЛ вызываемого абонента также, как в АТС с одной ступенью ЛИ.

Наряду с обратным используется прямое предыскание, протекающее от АЛ вызывающего абонента к ступени ЛИ. В этом случае за каждой АЛ закрепляется искатель малой емкости (на 10…15 линий), вместе образующие так называемый предварительный искатель (ПИ) или просто предыскатель. В контактное поле предыскателя включаются входы ЛИ. Упрощенная схема АТС с прямым предысканием показана на рис. 4.4.5.

При одинаковом количестве абонентов АТС с обратным предысканием выгодно применять при малой удельной нагрузке

в часы наибольшей нагрузки (ЧНН) на одну абонентскую линию, АТС с прямым предысканием – при средних значениях удельной нагрузки – и вариант без ступени предыскания – при высоких значениях.

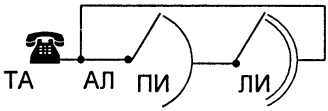


Рис. 4.4.5. Упрощенная схема АТС с прямым предысканием

Способ группового искания позволяет построить АТС, имеющие неограниченную емкость, на основе коммутационных приборов с относительно небольшой емкостью контактного поля. На АТС, емкость которой превышает емкость контактного поля искателей, т.е. $N>m$, где N – емкость АТС, а m – емкость контактного поля искателя, все АЛ разбиваются на группы по m линий в каждой. Для выбора группы, в которой находится нужная линия, устанавливается специальный прибор - групповой искатель (ГИ); совокупность этих приборов называется ступенью группового искания (рис. 4.4.6).

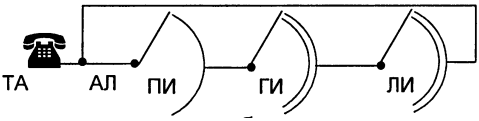


Рис. 4.4.6. Упрощенная схема АТС со ступенью группового искания

Типовая емкость АТС городских телефонных сетей составляет 10 000 номеров (нумерация АЛ в пределах АТС – 4-значная). Для обеспечения этой емкости в АТС вводится вторая ступень группового искания (рис. 4.4.7).

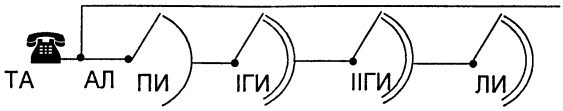


Рис. 5.4.7.Условное обозначение АТС с двумя ступенями ГИ

Первая цифра определяет выбор первой ступенью ГИ (1ГИ) тысячной группы, вторая – ступенью IIГИ сотенной группы и последние две цифры поступают на ЛИ для отыскания АЛ вызывае-

мого абонента в данной сотенной группе. Функции 1ГИ и IIГИ по отысканию линий полностью совпадают.

При требуемой емкости телефонной сети более 10 тыс. номеров дальнейшее увеличение емкости АТС обычно не производят. В этом случае сеть строят районированно, т.е. не одну АТС, а несколько.

Одним из наиболее распространенных способов построения временных коммутационных полей является использование разделяемой высокоскоростной шины (магистрали) (рис. 4.4.8). Входные устройства осуществляют необходимые преобразования входящих сигналов: аналого-цифровое для аналоговых сигналов или согласование скоростей для цифровых входных сигналах. На основе некоторого правила арбитража шины (например, на основе ярлыков, как показано на рис. 4.4.8) происходит ее совместное использование. Выходные устройства (фильтры ярлыков, выходные буферы) выполняют обратное преобразование сигналов.

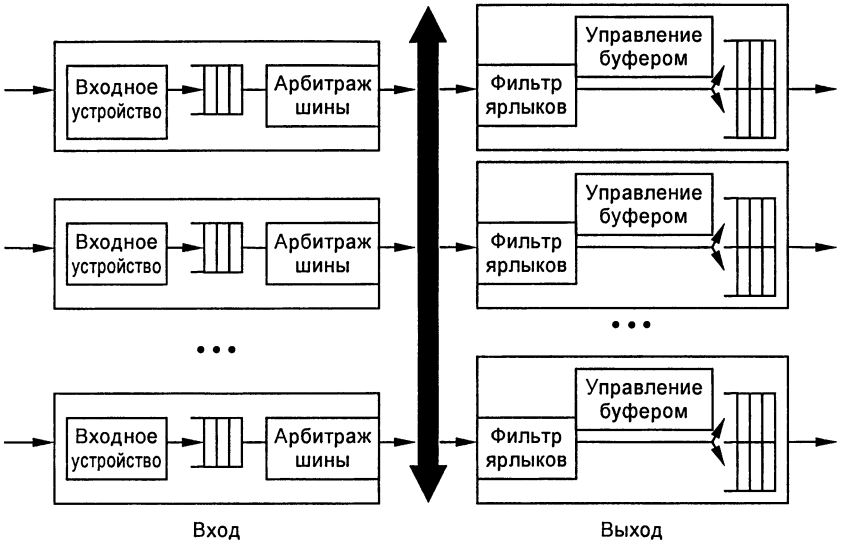


Рис. 4.4.8. Схема временного коммутационного поля на основе разделяемой магистрали [2]

Другим популярным способом построения временных коммутационных полей является использование разделяемой памяти

(рис. 4.4.9). Назначение входных и выходных устройств аналогично рассмотренному на рис. 4.4.8. В качестве разделяемого ресурса выступает высокоскоростная память с возможностью одновременной записи и чтения.

В общем случае процесс коммутации требует изменения как временной, так и пространственной позиции, поэтому на практике ступени временной и пространственной коммутации комбинируют, например, в виде структуры коммутационного поля «время–пространство–время».

Процесс коммутации состоит из нескольких этапов, выполняемых в определенной последовательности на различных ступенях искания. На каждой ступени происходит соединение входящих и исходящих линий коммутационных приборов. Для выполнения этой операции предварительно необходимо определить (найти) входящую линию, по которой поступил вызов, нужную исходящую линию, а также убедиться, свободна ли последняя. Все эти операции осуществляются управляющими устройствами АТС.

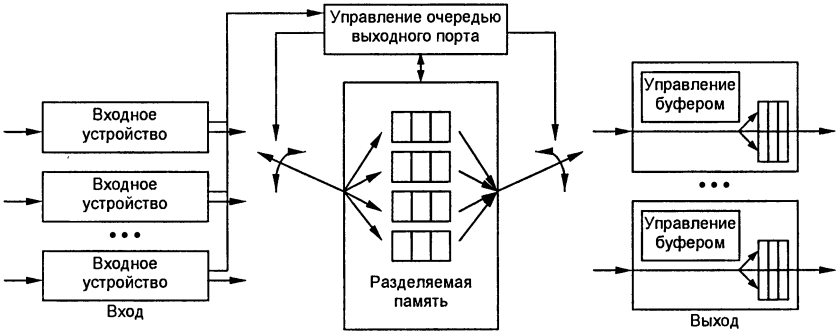


Рис. 4.4.9. Схема временного коммутационного поля на основе разделяемой памяти [2]

Управляющее устройство (УУ) управляет процессом установления соединения на коммутационном узле путем взаимодействия с приборами коммутационного поля, линейными и станционными комплектами. Основными функциями УУ являются:

• прием сигналов управления от линейных и станционных комплектов и приборов коммутационного поля;

• распределение принятых сигналов по функциональным блокам УУ;

• определение состояния коммутационных приборов и линий;

• выбор соединительного пути между входом и выходом коммутационного поля;

• включение коммутационных приборов, соответствующих выбранному пути;

• выдача команд на посылку абонентам акустических сигналов.

Управляющие устройства могут быть индивидуальными и общими (групповыми). В первом случае каждое УУ обслуживает один коммутационный прибор и занимается на время установления соединения и ведения переговоров между абонентами. Во втором случае каждое УУ обслуживает в заданной последовательности группу коммутационных приборов. Такие УУ занимаются только на время установления соединения. В зависимости от способа использования сигналов, несущих адресную информацию, различают УУ с непосредственным и регистровым (косвенным) управлением. Непосредственное управление применяется на АТС с индивидуальными УУ. В таких устройствах импульсы набора номера, посылаемые абонентами, непосредственно используются для работы коммутационных приборов.

Процесс коммутации осуществляется одновременно с набором номера вызываемого абонента. Если АТС имеет несколько ступеней искания, то УУ разных ступеней работают последовательно по мере набора цифр номера. При косвенном управлении импульсы набора номера запоминаются регистром. Проанализировав полученные импульсы, регистр формирует и передает сигналы на УУ всех ступеней искания, которые обеспечивают срабатывание коммутационных приборов. В результате будет установлено соединение. После этого регистр освобождается и может быть использован для обслуживания других вызовов. Косвенное управление может применяться как в индивидуальных, так и групповых УУ.

При регистровом управлении процесс приема импульсов набора номера вызываемого абонента и процесс установления соединений на ступенях искания разделены во времени. Регистр и управляющие устройства обслуживают вызовы с момента их появления до установления соединения. Чем меньше это время, т.е. чем выше быстродействие элементов управляющих устройств, тем большее число коммутационных приборов может быть обслужено.

Наибольшим быстродействием обладают УУ, реализованные на электронных элементах. Электронные УУ способны обслуживать сразу группу коммутационных приборов или даже всю коммутационную систему АТС. В последнем случае УУ станции состоит из периферийных управляющих устройств (ПУУ) и электронной управляющей машины (ЭУМ). ПУУ предназначены для приема импульсов набора номера, определения состояний абонентских и соединительных линий и т.п. Вся эта информация из ПУУ передается в ЭУМ для анализа и выработки команд. Команды возвращаются на ПУУ и используются для управления работой коммутационных приборов. Применение электронных УУ и ЭУМ не только многократно ускоряет процесс коммутации, но и значительно расширяет возможности станции, повышает эффективность использования станционных и линейных сооружений, делает сеть более гибкой и обеспечивает предоставление абонентам новых высококачественных услуг. Кроме того, ЭУМ позволяют автоматизировать учет переговоров, контроль состояния элементов станции, выявление неисправностей, сбор и обработку различных статистических данных и др. Электронные УУ используются в квазиэлектронных и электронных АТС.

Сигнализацию на телефонной сети обычно рассматривают как средство обмена информацией, связанной с управлением сетью, между различными оконечными устройствами, коммутационными узлами и абонентами сети. Можно указать на две основные задачи системы сигнализации: формирование специально закодированных электрических колебаний (сигналов) и их интерпретация. Функции сигнализации в широком смысле можно классифицировать по принадлежности к одному из двух типов: контроля или переноса информации. Сигналы контроля сообщают о состоянии элементов сети или об управлении ими. Наиболее очевидными примерами являются требование на обслуживание (вызов), готовность принять адрес (сигнал ответа станции), оповещение о вызове (посылка вызова), завершение разговора (отбой), требование на обслуживание оператором (кратковременные нажатия на рычаг телефонного аппарата), сигнал оповещения вызывающего абонента о посылке вызова вызываемому (контроль посылки вызова) и зуммерные сигналы занятости, относящиеся к сети или к вызыва-

емому абоненту. Сигналы переноса информации включают: адрес вызываемого абонента, адрес вызывающего абонента, стоимость междугородных переговоров. Кроме выполнения функции сигнализации, относящихся к обслуживанию вызова, коммутационные узлы обмениваются информацией между собой и с центрами управления сетью для обеспечения некоторых функций, относящихся к эксплуатации сети. Сигналы, относящиеся к сети, могут переносить информацию такого вида, как эксплуатационные тестовые сигналы, сигналы о занятости всех соединительных линий, сигналы о повреждениях оборудования; кроме того, они могут содержать информацию, относящуюся к маршрутизации или управлению потоками.

Внутриканальная сигнализация. При передаче сигналов применяется один из двух основных методов: внутриканальная сигнализация и сигнализация по общему каналу. При внутриканальной сигнализации (иногда называемой «сигнализацией по речевому каналу») для передачи сигналов управления используются те же устройства или тот же канал, что и для передачи речи. При сигнализации по общему каналу, как будет подробно обсуждено в следующем пункте, для реализации функций сигнализации из группы речевых каналов специально выделяется один канал. В прошлом большая часть систем сигнализации телефонной сети относилась к системам внутриканальной сигнализации. Однако за последнее время проявляется стремление к переходу на сигнализацию по общему каналу.

Системы внутриканальной сигнализации можно разделить на системы, использующие методы внутриполосной или внеполосной передачи сигналов. В первом случае сигнальная информация передается в той же самой полосе частот, в которой размещается речевой сигнал. Основное преимущество этих систем состоит в том, что может быть использована любая среда передачи. Основной недостаток связан с необходимостью исключения взаимного влияния речевых сигналов и сигналов, относящихся к сигнализации. Наиболее широко распространенным примером системы внутриполосной сигнализации является система одночастотной сигнализации (SF), где в качестве сигнала отбоя на межстанционных соединительных линиях используется сигнал частотой 2600 Гц. Хотя

в основном речевом сигнале частота 2600 Гц встречается редко, тем не менее, возможно возникновение непредвиденных разъединений, как результат «ложных» сигналов, создаваемых самими абонентами.

Другим распространенным примером системы внутриполосной сигнализации является передача адреса частотным способом кодом «два из многих», посылаемым с телефонных аппаратов с тастатурой, или многочастотная сигнализация между коммутационными станциями. Рассмотренные способы сигнализации предполагают обмен сигналами управления в период, когда речь не передается, поэтому вероятность неправильного истолкования сигналов управления (сигнализации) и сигналов речи чрезвычайно мала.

Способ внутриканальной сигнализации с внеполосной передачей сигналов управления предполагает применение таких устройств, которые для передачи сигналов управления используют речевой канал, но в этом случае передача осуществляется по другой части полосы частот. По сути дела, внеполосная сигнализация представляет собой разновидность частотного разделения отдельного речевого канала. Наиболее общим примером внеполосной сигнализации является сигнализация постоянным током, которая используется на большинстве абонентских линий. При данном способе сигнализации станция распознает поступление требования на обслуживание по наличию постоянного тока в линии. Другими примерами способов, также широко используемых на телефонных сетях, являются формирование импульсов набора номера с помощью дискового номеронабирателя со скоростью 10 импульсов в секунду, посылка вызова сигналами переменного тока частотой 20 Гц, передаваемыми в аппарат абонента с центральной станции. Частоты этих сигналов ниже частот спектра речевого сигнала. Таким образом, исключается возможность их взаимного отрицательного влияния. Основной недостаток внеполосной сигнализации – ее зависимость от системы передачи. Например, системы передачи с ОБП отфильтровывают самые низкие частоты речевого канала. Таким образом, сигнал вызова (отбоя) нужно предварительно преобразовать в форму, аналогичную многочастотному сигналу, передачу которого можно организовать в системе с ЧРК. Внеполосная сигнализация реализуется также с помощью сигналов, частота

которых лежит выше частоты среза фильтра разделения речевых каналов, но ниже граничной частоты полосы канала, равной 4 кГц. МККТТ рекомендует использовать для этих целей частоту 3825 Гц.

Межстанционная сигнализация по общему каналу. Сигнализация по общему каналу предполагает использование отдельного канала управления для выполнения всех функций сигнализации, связанных с обслуживанием некоторой группы каналов. Впервые сигнализация по общему каналу была введена фирмой Bell System в 1976 г. Совокупность устройств для реализации сигнализации по общему каналу передачи получила название системы межстанционной сигнализации по общему каналу (ОКС). Согласно рабочим планам фирмы Bell System в дальнейшем предполагается во все большей степени оснащать телефонные сети оборудованием ОКС в сочетании с внедрением коммутационных станций с управлением по записанной программе. Со временем 15 000 станций в Соединенных Штатах будут связаны между собой сетью сигнализации по общему каналу; МККТТ также принял рекомендации относительно сигнализации по общему каналу, которые определяют основные положения системы сигнализации № 6.

Ниже перечисляются преимущества сигнализации по общему каналу.

1. Для каждого конкретного пучка линий требуется лишь одна группа устройств сигнализации вместо отдельных устройств сигнализации для каждого отдельного канала.

2. Наличие специально выделенного канала управления дает возможность организовать непосредственный обмен информацией (такой, например, как набор номера) между управляющими устройствами (ЭВМ) коммутационных станций. В то же время при использовании внутриканальных систем сигнализации необходимо обеспечить коммутацию управляющей информации из группового оборудования исходящей станции в исходящий канал связи, а уже затем на входящей станции обеспечить коммутацию поступающей по речевому каналу управляющей информации в групповое оборудование данной станции.

3. Так как каналы передачи речи и каналы управления разделены, нет опасности взаимных влияний. При использовании ОКС каналы управления будут первоначально организованы на базе выделенных каналов ТЧ, оборудованных модемами.

4. Поскольку канал управления при использовании системы ОКС недоступен абонентам, то исключается возможность мошеннического использования сети.

5. Значительно ускоряется процесс установления соединений, проходящих через несколько коммутационных станций, поскольку продвижение управляющей информации от одной станции к другой опережает установление соединения на узле. При использовании внутриканальной сигнализации передать управляющую информацию можно только после установления соответствующего соединения.

6. Общий канал сигнализации не должен быть связан с определенным пучком соединительных линий. По существу, управляющая информация может направляться на некоторый центральный объект управления, где требования будут обработаны и откуда коммутационные станции получат управляющую информацию относительно требуемых соединений.

На рис. 4.4.10 показана сеть с ОКС, структура которой не соответствует основной сети передачи сообщений. Одно из преимуществ централизованного управления состоит в возможности обрабатывать требования с учетом состояния трафика на сети.

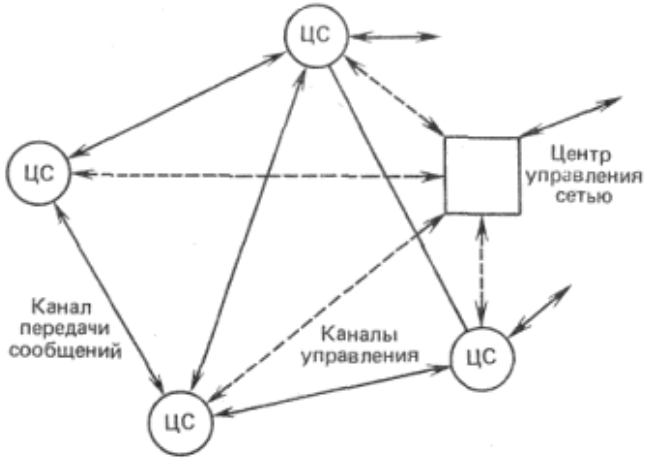


Рис. 4.4.10. Сеть с сигнализацией по общему каналу

Централизованное управление привлекательно также для организации обслуживания многих коммутационных станций, кото-

рые имеют слишком малую емкость, чтобы оправдать установку индивидуальных устройств обработки данных при обслуживании вызова. Переход от системы внутриканальной сигнализации к системе с ОКС на уровне сети аналогичен переходу на более низком уровне от систем коммутации с непосредственным управлением и прямым способом установления соединения (шагового типа) к системам коммутации с общим управлением.

Основные недостатки системы с ОКС сводятся к следующему.

Управляющая информация, относящаяся к уже установленному соединению, такая, например, как сигнал разъединения, должна передаваться от одного узла к другому в режиме передачи с промежуточным накоплением. С другой стороны, сигнал разъединения при внутриканальной сигнализации автоматически распространяется по сети и позволяет всем участвующим в соединении коммутационным узлам приступить к обработке сигнала разъединения и освобождения соответствующих устройств практически одновременно.

При использовании системы с ОКС выход из строя одного узла может привести к тому, что информация о разъединении не поступит на следующие за ним узлы и в результате этого не произойдет освобождение занятого оборудования. Таким образом, при использовании сигнализации по ОКС требуется обеспечить высокую степень надежности как аппаратуры (путем дублирования оборудования), так и контроля ошибок при передаче данных, относящихся к управляющей информации.

Поскольку управляющая информация проходит по пути, отличному от пути передачи речи, то не происходит автоматическая проверка речевого канала, как в том случае, когда речевой канал используется для передачи управляющей информации. Система сигнализации по ОКС обычно содержит специальные средства обеспечения проверки речевого канала после того, как он установлен.

И наконец, следует отметить, что некоторые функции сигнализации, особенно те, которые связаны с взаимодействием станций с оконечным оборудованием абонентов, принципиально требуют применения метода внутриканальной сигнализации. Например, сигнал ответа станции, сигнал контроля посылки вызова и зуммерный сигнал «занято», которые получает пользователь,

должны быть внутриканальными. Кроме того, пользователю иногда нужно иметь возможность доступа к некоторым элементам управления на сети, которые связаны с установленным соединением. Наиболее практичным средством выполнения этого является использование внутриканальных сигналов. Например, требование помощи оператора по уже установленному соединению обычно осуществляется путем кратковременных нажатий на рычаг телефонного аппарата для оповещения оператора. Кроме того, терминалы передачи данных, желающие отключить эхо-заградители при автоматически коммутируемых соединениях, должны послать специальные сигнальные частоты, которые будут распознаны эхозаградителями, включенными в данный канал.

Устройства сопряжения. Проектирование, реализация и обслуживание любой большой и сложной сети требуют ее разделения на управляемые подсистемы или модули. С каждым модулем связан стык, который определяет требования к различным входам и выходам со стороны внешнего окружения модуля.

Полная спецификация стыка включает перечень механических, электрических и эксплуатационных характеристик входов и выходов модуля. В идеале четко определенный стык позволяет осуществлять подключение к прибору, не интересуясь внутренними процессами, протекающими при его работе. Правильно установленный стык – это главнейшее условие для того, чтобы обеспечить совместимость старого и нового оборудования на сети. Необычайная сложность телефонной сети означает существование большого числа стыков. Из-за разнообразия областей применения и различного окружения иногда возникают ситуации, когда требуется специальное рассмотрение обоих концов в остальном стандартного стыка. Например, слишком длинные абонентские линии не могут быть заведены на стандартные устройства сопряжения (комплекты), потому что они требуют установки специальных усилителей на центральной станции.

Одним из главных источников, обусловливающих сложность и наличие большого числа различных видов устройств сопряжения на сети, можно считать различные процедуры сигнализации, которые используются на сети. Чаще всего именно несовместимость систем сигнализации вызывает необходимость введения промежу-

точных устройств сопряжения. Одно из наиболее часто используемых устройств сопряжения осуществляет преобразование тастатурного набора номера в декадные импульсы постоянного тока, воспринимаемые устройствами декадно-шаговых станций. Преобразование тастатурного набора в декадный является достаточно общим требованием, которому должны удовлетворять стандартные модули с тем, чтобы обеспечить согласование стыков.

Устройство сопряжения абонентского шлейфа (абонентский комплект). Самым распространенным видом устройства сопряжения на сети, иным, чем в случае соединений оконечных устройств, является абонентский комплект на центральной станции. Вследствие особенностей обычных оконечных устройств абонентов, с одной стороны, и свойств электромеханических коммутационных приборов, с другой стороны, это устройство сопряжения обладает рядом характеристик, которые оказываются особенно обременительными для электронных приборов коммутации. Основные функциональные требования, предъявляемые к этому устройству сопряжения на существующей аналоговой сети, сводятся к следующему.

Питание.

Подключение источника постоянного тока к шлейфу (обычно напряжением 48 В) для обеспечения возможности сигнализации постоянным током и создания тока подмагничивания угольных микрофонов.

Защита от опасных напряжений.

Защита оборудования и обслуживающего персонала от поражения молнией, мощных наводок на линиях или коротких замыканий.

Посылка вызывных сигналов.

Подача сигнала частотой 20 Гц и амплитудой 86 В для запуска звонка в телефонном аппарате. Этот сигнал обычно подается периодически в течение 2 с с интервалом в 4 с.

Контроль и наблюдение.

Обнаружение сигнала вызова (снятия микротелефонной трубки с рычага) по протеканию тока в линии.

Проверка.

Возможность внешней проверки абонентского шлейфа или внутренней проверки коммутационной схемы.

Новые системы коммутации, которые работают в окружении оборудования различных типов с различными процедурами обслуживания, должны обеспечить выполнение всех перечисленных выше функций обычным образом. В результате этого стоимость станционных окончаний абонентских шлейфов может достигать 50 % общей стоимости цифровой системы коммутации. Разработчики электронной техники усиленно работают над тем, чтобы создать экономически оправданную реализацию этого устройства сопряжения. Проблема исключительно трудна для решения средствами полупроводниковой электроники (как аналоговой, так и цифровой) из-за необходимости обеспечения высоких напряжений и больших токов.

Литература

1. Телекоммуникационные системы и сети / Под ред. В.П. Шувалова. В 3-х т. – М.: Горячая линия-Телеком, 2003.
2. *Гаранин М.В., Журавлев В.И., Кунегин С.В.* Системы и сети передачи информации. – М.: Радио и связь, 2001.
3. *Беллами Дж.* Цифровая телефония. – М.: Радио и связь, 1986.
4. *Гольдштейн Б.С.* АТС, МГТС и как это работает. – СПб.: БХВ-Санкт-Петербург, 2006.

5. СЕТИ ПОДВИЖНОЙ СВЯЗИ

В последние два десятилетия мы являемся свидетелями бурного развития систем и сетей связи с подвижными объектами. В первую очередь здесь следует назвать системы и сети персональной связи, сотовые наземные системы общего пользования, спутниковые системы связи. В течение первого десятилетия с начала 80-х гг. были разработаны, практически построены и введены в коммерческую эксплуатацию аналоговые системы первого поколения. Принято считать, что первая сотовая сеть связи общего пользования начала работать в Японии в 1979 г. Коммерческая эксплуатация аналогичной сети в скандинавских странах начата в 1981 г., в США – в 1983 г.

В течение 90-х гг. было создано и введено в эксплуатацию второе поколение цифровых систем и сетей связи с подвижными объектами. По имеющимся данным число мобильных телефонов в мире в 2004 г. превысило число стационарных. В настоящее время ведутся активные исследования и разработки технологии аналогичных систем третьего и четвертого поколений, которые войдут в нашу жизнь в этом тысячелетии.

Характерной особенностью систем второго и третьего поколений является стремление разработчиков обеспечить потребителю максимально широкий набор услуг, начиная от передачи очень коротких цифро-буквенных сообщений и даже просто звуковых сигналов вызова до передачи движущихся изображений и предоставления возможности мобильного доступа к обширным базам данных в глобальном масштабе. Эта цель может быть успешно достигнута при одном обязательном условии: системы и сети должны обладать большой пропускной способностью, обеспечивать передачу цифровых данных с высокой скоростью вплоть до нескольких мегабит в секунду. Это означает, что разработчики подобных систем должны обеспечить практическую реализацию потенциальных возможностей используемых в технике связи физических явлений и принципов.

5.1. Эволюция сетей подвижной связи

В общем случае, согласно классификации по рекомендациям МСЭ, подвижные службы и службы радиоопределения разделяют:

– на сухопутную подвижную службу, за исключением подвижных систем электросвязи общего пользования IMT-2000;

– систему IMT-2000;

– морскую и авиационную подвижные службы;

– службу радиоопределения;

– подвижные спутниковые службы и спутниковые службы радиоопределения.

Сухопутная подвижная служба охватывает:

– беспроводные телефоны и беспроводные системы связи;

– сотовые сухопутные подвижные системы электросвязи (ССПСЭ);

– системы транкинговой радиосвязи.

В марте 1994 г. на Первой всемирной конференции по развитию электросвязи, проводимой МСЭ, была заявлена идея создания глобальной информационной инфраструктуры (ГИИ) для формирования глобального информационного сообщества (ГИС). «Улучшить жизнь каждого человека, дав ему новые услуги. Создать необходимую инфраструктуру для экономического роста» – так определены основные цели создания ГИИ. Для ГИИ сформулированы общие принципы концепции, выделены главные направления развития и сделаны определённые шаги по реализации. Созданы региональные и глобальные сообщества и инфраструктуры. В развитых странах образуются национальные информационные структуры с четкой ориентацией на развитие ГИС. В июле 2000 г. Россия присоединилась к Хартии глобального информационного сообщества.

Спутниковая связь играет важную роль в создании ГИИ. Для построения глобальной сети электросвязи могут быть задействованы все спутниковые системы связи, пригодные для предоставления услуг электросвязи конечным пользователям. Это фиксированные и подвижные спутниковые службы, широкополосные и узкополосные, глобальные и региональные, существующие и запланированные. Все они могут быть объединены в рамках гло-

бальной персональной подвижной спутниковой связи. Ведущую роль здесь играют спутниковые сети, предназначенные для глобального или регионального охвата абонентов, использующих портативные переносные терминалы.

Сотовые сухопутные подвижные системы электросвязи подразделяют по поколениям. Первое поколение – это системы аналоговых стандартов. Второе поколение представлено системами цифровых стандартов. Наконец, IMT-2000 рассматривается сегодня как стандарт подвижной системы электросвязи третьего поколения. Примеры стандартов приведены в табл. 5.1.1.

Таблица 5.1.1

Примеры стандартов

Стандарт	Полное наименование стандарта	Диапазон частот, мГц	Год ввода
Аналоговые стандарты			
NMT 450	Nordic Mobile Telephony	450	1981
AMPS	Advanced Mobile Phone System	800	1983
TACS	Total Access Communication System	900	1985
NMT-900	Nordic Mobile Telephony	900	1986
Цифровые стандарты			
GSM-900	Global System for Mobile Communication	900	1991
D-AMPS	Advanced Mobile Phone Service	800 и 1800	1991
DCS-1800	Digital Cellular System	1800	1992
PDC	Personal Digital Cellular	800/900 и 1500	1994
CDMA	Code Division Multiple Access	800 и 1800	1995

Для нашего времени характерно широкое распространение систем второго поколения и активное внедрение систем третьего поколения. Системы первого поколения постепенно снимаются с эксплуатации.

На рис. 5.1.1 представлена классификация сетей подвижной связи Российской Федерации. В них включены наземные и спутниковые сети подвижной связи общего пользования, с помощью которых абонентам сети предоставляются различные услуги электросвязи, включая связь с абонентами телефонной сети общего пользования (ТФОП). Абоненты получают доступ в свою сеть с помощью подвижных абонентских терминалов, которые будем называть абонентскими станциями (АС), по радиоканалу между

АС и базовой станцией (БС). Так организована сеть доступа. Между БС создается транспортная сеть с помощью радиолиний или кабельных линий связи. Сети доступа и транспортные сети вместе образуют сеть подвижной связи. Взаимодействие с ТФОП возможно на любом иерархическом уровне: местном, внутризоновом и междугородном.

Наземные сети подвижной связи рассматриваются как основа сетей подвижной связи общего пользования. В тех регионах РФ, где возможен доступ одновременно в обе сети (наземные и спутниковые), абоненту преимущественно предоставляется канал связи через наземную сеть, а при выходе из зоны обслуживания наземной сети – через спутниковую сеть.

Рис. 5.1.1. Классификация сетей подвижной связи Российской Федерации [2]

Спутниковые сети подвижной связи в первую очередь должны предоставлять услуги международной и междугородной связи. При этом спутниковые сети также могут поддерживать внутризоновую и местную связь. Спутниковые сети подвижной связи РФ классифицированы по видам используемых орбит искусственных спутников Земли (ИСЗ).

Наземные сети разделяют на федеральные и региональные. На основе аналогового стандарта NMT-450 и цифрового стандарта

GSM-900, которые были приняты в качестве федеральных, в РФ организованы две федеральные сети. Абоненты этих сетей могут связываться друг с другом через ТФОП.

Нижняя строчка рис. 5.1.1 отражает классификацию сетей по методу территориального планирования. Федеральные стандарты используют сотовый принцип деления территории.

Региональные сети рассматриваются как дополнение или временное замещение федеральных сетей, но при условии, что они не будут сдерживать развитие последних. Каждая региональная сеть обслуживает только своих абонентов.

В качестве региональных выступают сотовые сети стандартов AMPS/D-AMPS, радиальные и радиально-зоновые сети, включая транкинговые. Несколько радиальных линий связи можно объединить через центральную коммутационную станцию в радиально-зоновую структуру. Транкинговая сеть организуется на базе специальных систем радиосвязи, обеспечивающих многостанционный доступ к небольшому числу радиоканалов с ограниченным выходом в ТФОП либо без выхода в эту сеть, и используется в первую очередь для обслуживания абонентов ведомственных сетей. К региональным наземным сетям относятся также сети персонального радиовызова (СПРВ). Персональный радиовызов (пейджинг) – это услуга электросвязи, заключающаяся в односторонней передаче коротких сообщений на ограниченной территории по радиоканалу. Региональные СПРВ должны включаться в ТФОП на местном уровне. Региональные СПРВ могут быть объединены в федеральные. Существуют стандарты для общеевропейской СПРВ.

В рассматриваемую классификацию сетей подвижной радиосвязи не включены беспроводные телефоны и беспроводные системы электросвязи – сухопутные подвижные службы, обеспечивающие связь в радиусе нескольких сотен метров. В беспроводных системах используется микросотовая и пикосотовая структура. Одна из основных областей их применения – это организация сети доступа для расширения возможностей сотовой региональной и федеральной сети.

Сотовые структуры принято классифицировать по размерам сот: макросотовые с радиусом $R < 500$ м, микросотовые с радиусом $100 \text{ м} \le R \le 500$ м и пикосотовые, для которых радиус $R < 100$ м.

Согласно концепции развития в России сотовых систем подвижной связи общего пользования приоритетным направлением развития являются федеральные сети. Региональные аналого-цифровые сети стандарта AMPS/ D-AMPS существовали только до 2010 г.

Основные услуги, предоставляемые абоненту в сетях подвижной связи, подразделяются на два типа: транспортные услуги и услуги связи. Конкретно набор возможных услуг любого типа определяется стандартом. Так, транспортные услуги для систем второго поколения, как правило, включают: передачу речи; синхронную, асинхронную и пакетную передачи данных со скоростью не выше 9,6 кбит/с и др.

В системах второго поколения пользователю могут быть предоставлены основные и дополнительные услуги связи. Основные услуги связи: телефонная связь, экстренные вызовы, передача коротких сообщений, факсимильная связь. Услуга экстренного вызова позволяет устанавливать абонентской станции речевую связь с ближайшим центром экстренной службы. К дополнительным услугам связи относятся:

– услуги по распознаванию номера;

– переадресация и перенаправление вызова;

– услуги завершения связи (вызов на удержании, вызов с ожиданием и т.п.);

– конференц-связь;

– услуги по учету стоимости переговоров;

– услуги группового соединения;

– услуги по ограничению вызовов и др.

В условиях конкурентной борьбы за абонента операторы крупных сетей стараются внедрять новые услуги. В последнее время была введена такая услуга, как подключение абонента на условиях предоплаты, услуга WAP – доступ в сеть Интернет непосредственно с мобильного терминала.

Качественную передачу информационных сигналов в сетях подвижной связи обеспечивает ее собственная система управления. Информация, служащая для управления системой, называется сигнальной информацией. В качестве эталонной системы для передачи сигнальной информации используется эталонная модель OSI (Open System Interconnection – открытая система взаимных

соединений). В этом контексте открытой называется система, которая может взаимодействовать с другими в соответствии с заранее определенными протоколами. Модель задает набор стандартных процедур, устанавливающих правила обмена сигнальной информацией между терминалами, процессорами, сетями. Благодаря взаимному использованию этих процедур каждая система оказывается открытой для других систем.

Для управления сетями подвижной связи используют систему общеканальной сигнализации ОКС 7, которая разработана и развивается в соответствии с эталонной моделью OSI. Система ОКС 7 содержит подсистему сетевых услуг и подсистемы пользователя, различные для разных стандартов.

5.2. Общие принципы построения сотовых сетей подвижной связи

Главные элементы сотовой сухопутной подвижной сети электросвязи (ССПСЭ) – это центр коммутации подвижной службы (ЦКПС), а также станции (БС и АС). Все БС соединены со своим ЦКПС стационарными линиями связи (кабельными, радиорелейными и др.), а асе ЦКПС сети – стационарными линиями с транзитными коммутаторами ТФОП и обмениваются информацией по общему каналу сигнализации ОКС 7.

Сотовые сухопутные подвижные системы электросвязи строят на основе частотно-территориальных планов (ЧТП). При составлении ЧТП обслуживаемую территорию разделяют между базовыми станциями. Если на БС используется всенаправленная антенна, то граница территории, которую обслуживает одна БС, – окружность, в центре которой располагается БС (рис.5.2.1,а). Границы трех соседних окружностей пересекаются в одной точке. Соединив точки пересечения окружностей, уточним границы территории, которую обслуживает каждая БС. Получается шестиугольник – сота. Сота – это территория, обслуживаемая одной БС при всенаправленных антеннах. Каждая БС поддерживает радиосвязь с абонентскими станциями, находящимися в своей соте. Во избежание взаимных помех, соседние БС работают на разных частотах. Каждой соте присваивается частотная группа и для всей ССПСЭ составляется частотно-территориальный план.

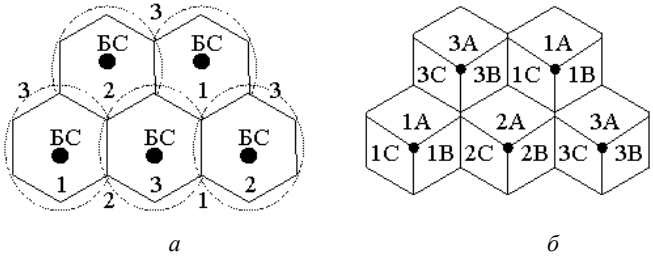
Основой ЧТП является кластер. Кластер образован совокупностью соседних сот, в которых используются разные частотные группы. Частотные группы внутри кластера не повторяются. Число таких сот в кластере называется его размерностью. Все частотные каналы системы делят между БС, входящими в один кластер. На рис. 5.2.1 показаны фрагменты сотовых структур, построенных на базе кластера размерностью 3 ($N_{кл}$ = 3). Цифрами на рис. 5.2.1, *а* обозначены частотные группы.

Сотовая структура может быть двух типов:

• регулярная, использующая всенаправленные антенны (рис. 5.2.1, *а*);

• секторная на основе направленных антенн (рис. 5.2.1, *б*).

В качестве направленных антенн на БС используются секторные антенны. Получили распространение секторные антенны с шириной главного лепестка ДНА (*а*), равной 60, 90 или 120°. На рис. 5.2.1, *б* показаны соты с секторными антеннами при а = 120°. В этом случае сота делится на три сектора *A*, *B*, *C*. В каждом секторе устанавливается своя БС, причем в центре соты. Каждая БС работает на своей частоте. Частотные группы обозначены 1А, 1В, ...



а *б*

Рис. 5.2.1. Сотовые структуры: *а* – регулярная; *б* – секторная

Как правило, в центре соты устанавливается несколько антенн. Это могут быть три передающие антенны, две–шесть приемных (для разнесенного приема) и две антенны радиорелейных линий (РРЛ). Место размещения БС получило название «сайт» (от англ. site – местоположение).

При шестиугольной соте удобно использовать кластер размерностью 7. В этом случае можно выбрать разные частотные группы в одной центральной соте и шести пограничных сотах. На рис. 5.2.2 приведен фрагмент ЧТП для сети с использованием кла-

стера размерностью 7. Точки соответствуют местам установки базовых станций. Цифрами обозначены номера частотных групп. Утолщенными линиями выделен центральный кластер. Пунктиром показаны пути прихода интерференционных помех на АС, которая находится на границе соты 1 центрального кластера, от БС, работающих на совпадающих частотах. ЧТП составляют так, чтобы уровень интерференционных помех не превышал допустимых значений, что позволяет многократно повторять кластер и реализовать достоинства сотовых систем. Например, если в подвижной системе используется 119 частотных каналов ($N_ч$ = 119) и кластер размерностью 7 ($N_{кл}$ = 7), то число частотных каналов, содержащихся в частотной группе в одной соте, определяется по формуле $N_{чк} = N_{кл} / N_{кл} = 119/7 = 17$.

Основное достоинство любых сотовых систем – эффективное использование выделенной полосы частот за счет многократного повторения кластера на территории. Такой подход позволяет обслуживать большое число абонентов при ограниченном частотном ресурсе спектра.

В зависимости от радиуса соты r_0 различают макросоты с $r_0 \geq 0{,}5$ км, микросоты с $r_0 < 0{,}5$ км и пикосоты радиусом несколько десятков метров. Макросоты предназначены для обслуживания абонентов в быстро передвигающемся транспорте, микросоты и пикосоты целесообразны при медленном перемещении абонентов. Микросоты были реализованы впервые в системах беспроводных телефонов. Пикосоты служат для обслуживания абонентов в городских районах с большой плотностью населения и в закрытых зонах (подземные гаражи, вокзалы, универмаги).

Область обслуживания ЦКПС разделяется на зоны обслуживания. Например, в стандарте NMT-450 область обслуживания одного ЦКПС содержит 16 зон, в каждой зоне находится до 128 БС, всего в области обслуживания одного ЦКПС может быть до 1024 БС. Адрес (номер) зоны обслуживания базовая станция непрерывно передает по каналу управления. Этот номер принимается абонентской станцией и записывается в ее память. АС оценивает принимаемый сигнал и при необходимости инициирует процедуру обновления информации о своем местоположении, которое определяется с точностью до зоны, а не до соты. Деление на зоны уменьшает время поиска абонентской станции.

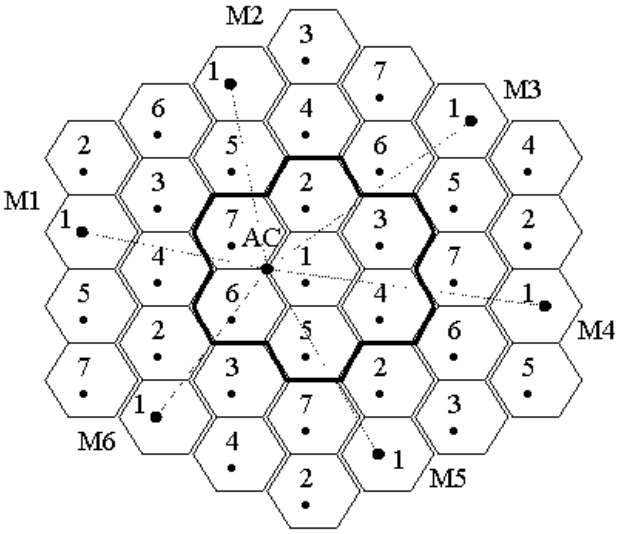


Рис. 5.2.2. Фрагмент ЧТП с $N_{кл} = 7$.
М1-М6 – мешающие базовые станции с частотной группой 1

Ведение абонента. При включении АС выполняется определение ее местоположения и выделение для нее рабочих частот. При пересечении станцией границы соты сеть передает абонента другой БС, при этом на АС производится автоматическая смена рабочих частот. Ведение абонента включает несколько функций. Одна из них – эстафетная передача АС от одной БС к другой при движении абонента с включенной АС. Другая функция – переключение частотных каналов внутри одной соты, например, при поражении сигнала рабочего канала помехой. Наконец, при перегрузке соты ЦКПС может передавать абонентскую станцию другой БС, имеющей свободные частотные каналы. Процедура «ведение абонента» часто называется процедурой эстафетной передачи (ПЭП). Ее называют также хэндовер или хэнд-офф (от англ. handover или амер. hanhd-off). Решение о выполнении ПЭП обычно принимает ЦКПС на основании результатов измерений, сделанных на АС и БС. На станциях измеряются уровни принимаемых сигналов, отношение сигнал-шум в канале и другие параметры. Эти результаты передаются на ЦКПС по каналам управления. Измеренные параметры используются также для регулирования мощности АС.

Роуминг. Если АС находится вне области обслуживания своего ЦКПС, то при ее включении выполняется процедура роуминга. Эта процедура предусматривает определение местоположения АС вне «собственной» зоны обслуживания и предоставление абонентской станции каналов связи при перемещении абонентов в пределах сети. Роуминг возможен между ЦКПС сети и между странами. Роуминг бывает автоматический и заказной.

Каналы трафика и управления. В ССПСЭ предусмотрены две основные категории каналов:

– каналы трафика (или линейные каналы), предназначенные для передачи речи и данных (англ. аббревиатура ТСН);

– каналы управления, которые используются для сигнализации и управления, включая ведение абонента (англ. аббревиатура ССН).

Наличие каналов для ведения абонента отличает ССПСЭ от неподвижных систем радиосвязи с сотовой структурой, например, от цифровых радиорелейных линий (ЦРРЛ) со структурой «точка – много точек».

Передача сигналов между БС и ЦКПС. Все БС соединены со своим ЦКПС стационарными линиями связи. На рис. 5.2.3 показан фрагмент сети, в которой БС соединены с помощью ЦРРЛ. На каждой БС установлена всенаправленная антенна для связи с АС и две направленные антенны РРЛ. Частоты ЦРРЛ обозначены f_1, …, f_4.

Функциональная схема ССПСЭ аналогового стандарта. Напомним, что ЦКПС является одним из основных элементов ССПСЭ. В ССПСЭ аналоговых стандартов в состав ЦКПС включены опорный регистр местонахождения (ОРМ) и визитный регистр местонахождения (ВРМ). Регистрами называют базы данных, которые содержат основные сведения об абонентах и оборудовании. В ОРМ хранятся основные сведения об абонентах, постоянно зарегистрированных в области обслуживания данного ЦКПС. Под основными сведениями подразумеваются те данные о статусе и местоположении абонента, которые позволяют послать вызов и предоставить соответствующие услуги. При перемещении АС в область обслуживания другого ЦКПС основные сведения об этом абоненте временно записываются в ВРМ этого ЦКПС и хранятся до тех пор, пока там находится эта АС.

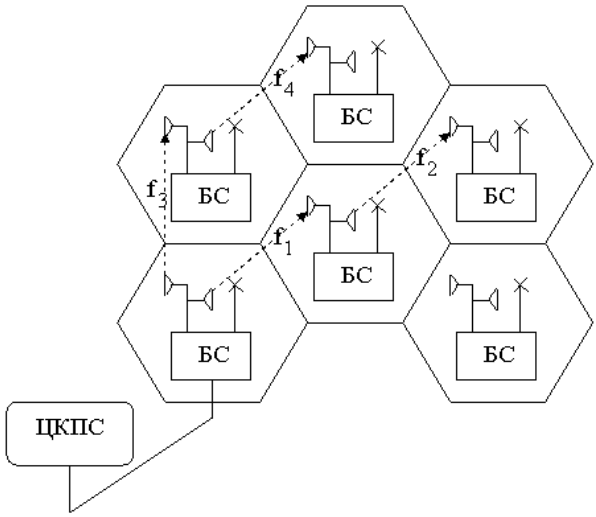


Рис. 5.2.3. Фрагмент сети, в которой БС соединены цифровыми радиорелейными линиями

На функциональной схеме ССПСЭ аналогового стандарта, рис. 5.2.4 для каждой АС можно указать опорный центр коммутации (ЦКПС-О), в ОРМ которого зарегистрирована рассматриваемая АС. Когда эта АС оказывается в зоне обслуживания любого другого ЦКПС, сведения о ней записываются в ВРМ. Все такие центры коммутации для рассматриваемого абонента являются ЦКПС визитера (ЦКПС-В).

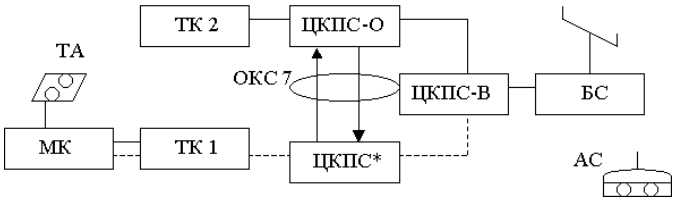


Рис. 5.2.4. Функциональная схема ССПСЭ аналогового стандарта

Центр коммутации подвижной службы обеспечивает соединение между абонентами сети, а также выход в ТФОП; отслеживает местоположение АС в своей области обслуживания; управляет процедурой эстафетной передачи АС, а также переключением частотных каналов при нарушении связи из-за помех или неисправ-

ностей; выполняет функции центра эксплуатации и технического обслуживания сети; начисляет оплату абонентам. На рис. 5.2.4 показана установленная линия связи между абонентами сети ТФОП и ССПСЭ. В ТФОП показаны местный коммутатор (МК) и транзитные коммутаторы (ТК), ТА – телефонный аппарат. В варианте 1 (сплошные линии) вызов к АС проходит по линии ТА, МК, ТК1, ТК2, ЦКПС-О, ЦКПС-В, БС, АС.

В ССПСЭ предусмотрена шлюзовая функция (Gateway). ЦКПС, обладающий такой функцией, обозначен ЦКПС*. Шлюзовая функция – специальный принцип маршрутизации вызова через ближайший ЦКПС, который теперь становится шлюзовым. Этот ЦКПС* опрашивает ЦКПС-О по каналам ОКС 7 и находит самый короткий путь для установления связи (линия связи обозначена пунктиром). Шлюзовую функцию реализуют, как правило, все ЦКПС.

5.3. Сетевая технология GSM

Рассмотрим ССПСЭ стандарта GSM, схема которой приведена на рис 5.3.1.

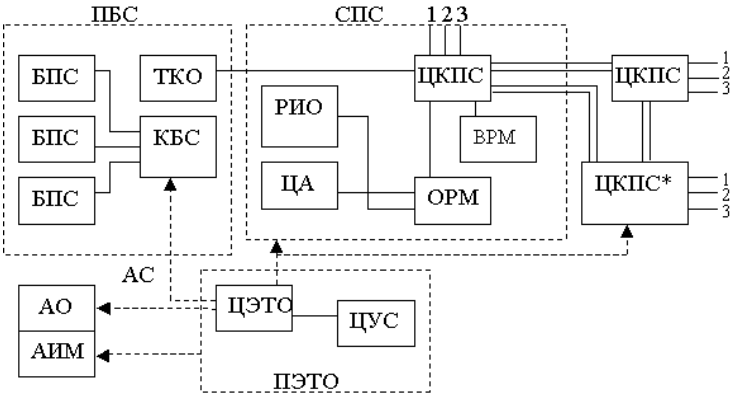


Рис. 5.3.1. Функциональная схема ССПСЭ стандарта GSM

Схема содержит подсистему базовых станций (ПБС); сетевую подсистему (СПС) и подсистему эксплуатации и технического обслуживания (ПЭТО), а также АС. В АС входит абонентское оборудование (АО) и абонентский идентификационный модуль (АИМ) (SIM-карта). Пока не установлен этот модуль, не выполня-

ются соединения АС с вызывающим и вызываемым номером. Подсистема базовых станций содержит: базовые приемопередающие станции (БПС); контроллер БС (КБС) и оборудование транскодирования (ТКО). В составе СПС показаны: ЦКПС, ОРМ, ВРМ, центр аутентификации (ЦА), регистр идентификации оборудования (РИО). ПЭТО содержит центр эксплуатации и технического обслуживания (ЦЭТО) и центр управления сетью (ЦУС). Подсистема базовых станций выполняет функции радиосвязи. Все БС в зоне ПБС соединены линиями связи с контроллером. Каждая БПС обслуживает одну соту. Содержит несколько приемопередатчиков (до 16) – по одному для каждого частотного канала. Каждой БПС стандарта GSM доступны все 124 частотных канала, что позволяет реализовать метод скачкообразной перестройки частоты в стандарте GSM. Один из способов переключения частоты состоит в переключении модулирующего сигнала на входе передатчика. В этом случае число частот, используемых для скачкообразной перестройки, определяется числом приемопередатчиков БС.

Контроллер БС управляет несколькими БПС. Основное назначение контроллера – правильное распределение радиоканалов между БС и АС и определение необходимости их переключений при передвижении. Другая его задача – управление конфигурацией БПС и загрузка программного обеспечения. Контроллер обеспечивает передачу вызова на АС, контролирует соединения, выполняет согласование скоростей передачи для речи, данных и сигналов вызова, кодирование и декодирование, сигналов. Количество приемопередатчиков, которые может обслужить один контроллер, может быть более 100. Оборудование транскодирования включается между КБС и ЦКПС и служит для согласования скоростей цифровых потоков. В ТКО образуется стандартный первичный цифровой поток (ПЦП) из цифровых сигналов базовых станций. ТКО может размещаться вместе с КБС. Как известно, ПЦП образуют 32 сигнала, каждый со стандартной скоростью 64 кбит/с. Номинальная скорость передачи ПЦП: $B_1 = (30 + 2) \cdot 64 = 2048$ кбит/с.

В стандарте GSM скорость передачи сигнала в одном речевом канале $B_{1GSM} = 13$ кбит/с. В транскодере с помощью добавочных битов эта скорость увеличивается до величины $B_{1TKO} = 16$ кбит/с. Таким образом, в полосе одного канала стандартной ИКМ переда-

ют сигналы четырех речевых каналов, всего речевых каналов в транскодере $N_{ТКО} = 30 \cdot 4 = 120$. Оставшиеся два стандартных цифровых канала занимает сигнальная информация. Например, один канал – информация ОКС 7 и один канал – информация управления по протоколу X.25.

Сетевая подсистема выполняет соединение неподвижных и подвижных пользователей с помощью коммутационных средств и баз данных. В системе стандарта GSM функционально разделены ЦКПС и регистры ОРМ и ВРМ. ЦКПС обеспечивает включение подвижного абонента в общие и выделенные сети связи (через выходы 1, 2, 3). Кроме того, центр выполняет коммутацию радиоканалов, а также обеспечивает непрерывность связи при перемещении АС. Как правило, один ВРМ присоединен к одному ЦКПС. Этот регистр – база данных, временно содержащая информацию о подвижных пользователях, находящихся на территории, которой он управляет. ВРМ позволяет правильно определить местоположение АС. Данные о местоположении АС постоянно обновляются. В СПС входят: ЦА – база данных, используемых при аутентификации абонента (ключи и алгоритмы аутентификации и др.) и РИО – база данных, содержащая сведения о подвижных устройствах, позволяющие предотвращать несанкционированное использование АО (угон, кража).

Сотовая сухопутная подвижная система электросвязи стандарта GSM территориально разделяется на зоны действия ЦКПС, которые, в свою очередь, делятся на зоны действия контроллеров БС, называемые зонами местоположения (ЗМ). ЦКПС отслеживает местоположение АС с помощью регистров. ВРМ позволяет вызывать АС, пока она находится в зоне действия, определенного контроллера. Когда АС перемещается в ЗМ другого контроллера, он ее регистрирует, и в ВРМ записывается новый адрес ЗМ.

Входящие вызовы поступают к ЦКПС* – центру коммутации, обладающему шлюзовой функцией, который по номеру вызываемого абонента находит его ОРМ. Последний обращается к ВРМ, который «находит» АС. Шлюзовой ЦКПС* имеет интерфейс с внешними сетями связи. Здесь, как и в случае аналоговых систем, шлюзовую функцию можно установить для каждого ЦКПС. Все ЦКПС в сети соединены линиями связи (ВОЛС, РРЛ, спутниковыми).

Подсистема эксплуатации и техобслуживания построена по иерархическому принципу и состоит из центра эксплуатации и технического обслуживания (ЦЭТО) и центра управления сетью (ЦУС). ЦЭТО позволяет выполнять дистанционный контроль, управление элементами сети и конфигурацией сети, техническое обслуживание, целостность и обновление сети, сбор данных по трафику, загрузку программного обеспечения.

ЦУС организуют для сетей большой площади. Он служит для надзора за сетью в целом, за анализом характеристик и т.п.

Система стандарта GSM подчиняется принципам эталонной модели OSI. Она имеет три общих внутрисистемных интерфейса:

1) радиоинтерфейс U_m между БС и АС;

2) интерфейс А между ЦКПС и ПБС;

3) интерфейс A_{bis} между БПС и КБС.

Положение внутрисистемных интерфейсов отражено на рис. 5.3.2.

В данном контексте интерфейс – это точка соединения реально существующих устройств. Благодаря данным интерфейсам оператор системы может соединять аппаратуру разных производителей. Информационные потоки, проходящие через один интерфейс, могут принадлежать различным протоколам.

Кроме этих внутрисистемных интерфейсов система GSM имеет интерфейсы между сетью и внешним оборудованием и интерфейсы для выхода во внешние сети: в сети подвижной связи общего пользования, в ТФОП, в цифровые сети с интеграцией служб (ЦСИС) и др.

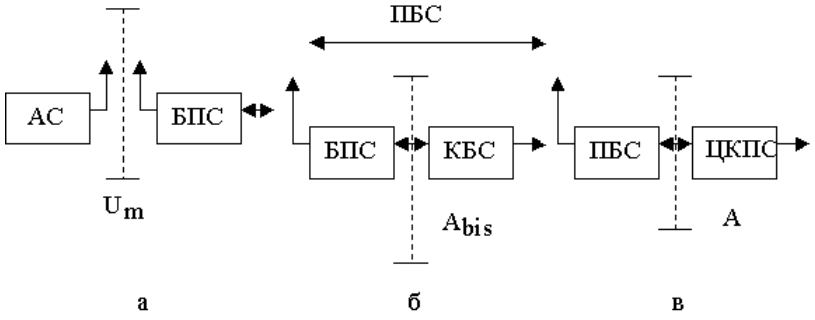


Рис. 5.3.2. Интерфейсы стандарта GSM.
а – радиоинтерфейс U_m; *б* – интерфейс A_{bis}; *в* – интерфейс А

Эфирный интерфейс в стандарте GSM. Передача информации в стандарте GSM организуется кадрами, которые имеют длительность 4,616 мс. Каждый кадр состоит из восьми слотов по 577 мс, и каждый слот соответствует своему каналу речи, т.е. в каждом кадре передается информация восьми речевых каналов.

Частотный канал – это полоса частот, отводимая для передачи информации одного канала связи. В стандарте GSM 900 для передачи информации прямого канала отводится полоса 935.960 мГц, а обратного – 890.915 мГц, т.е. дуплексный разнос по частоте составляет 45 МГц. Один частотный канал занимает полосу = 200 кГц, так что всего в полном диапазоне, с учетом защитных полос, размещается 124 частотных канала.

Физический канал в системе с множественным доступом на основе временного разделения (TDMA) – это временной слот с определенным номером в последовательности кадров эфирного интерфейса. Таким образом, в Стандарте GSM всегда передается информация восьми физических каналов, но при полускоростном кодировании один физический канал содержит два канала трафика, информация которых передается по очереди, через кадр. Иными словами, при этом реализуется временное уплотнение каналов в 3 или 8 раз соответственно при полноскоростном кодировании и в 6 или 16 раз – при полускоростном. В этом и заключается одно из основных преимуществ цифрового поколения сотовой связи по сравнению с аналоговым.

Логические каналы различаются по виду (составу) информации, передаваемой в физическом канале. В принципе в физическом канале может быть реализован один из двух видов логических каналов — канал трафика или канал управления; каждый из них, в свою очередь, может в общем случае существовать в одном из не скольких вариантов (типов).

Каналы трафика TCH (Traffic Channels), в свою очередь, делятся на полноскоростные TCH/FS (с полноскоростным кодированием; *F* – сокращение от full – полный; *S* – speech – речь) и полускоростные TCH/HS (*H* – сокращение от half – половина); в обоих случаях имеется в виду передача речи.

Каналы управления CCH (Control Channels) делятся на 4 типа: вещательные каналы управления BCCH (Broadcast Control Chan-

nels), общие каналы управления CCCH (Common Control Channels), выделенные закрепленные каналы управления SDCCH (Stanalone Dedicated Control Channels), совмещенные каналы управления ACCH (Associated Control Channels).

Вещательные каналы управления BCCH предназначены для передачи информации от базовой станции к подвижным в вещательном режиме, т.е. без адресования к какой-либо конкретной подвижной станции. В число вещательных каналов управления входят: канал коррекции частоты FCCH (Frequency Correction Channel)- для подстройки частоты подвижной станции под частоту базовой, канал синхронизации SCH (Synchronization Channel) для кадровой синхронизации подвижных станций, а также канал общей информации, не имеющий отдельного наименования.

Общие каналы управления CCCH включают: канал вызова PCH (Paging Channel), используемый для вызова подвижной станции базовой; канал разрешения доступа AGCH (Access Grant Channel) – для назначения закрепленного канала управления, которое также передается от базовой станции на подвижную; канал случайного доступа RACH (Random Access Channel) – для выхода с подвижной станции на базовую с запросом о назначении выделенного канала управления. При передаче информации по общим каналам управления прием информации не сопровождается подтверждением.

Выделенные закрепленные каналы управления SDCCH – автономные каналы управления для передачи информации с базовой станции на подвижную и в обратном направлении.

Совмещенные каналы управления ACCH, также используемые для передачи информации а обоих направлениях (от базовой станции к подвижным и от подвижных к базовой) и имеющие несколько вариантов, включают медленный совмещенный канал управления SACCH (Slow Associated Control Channel) – объединяется с каналом трафика (кадр 13 мультикадра канала трафика) или с каналом FACCH (Fast Associated Control Channel) – совмещается с каналом трафика, заменяя в соответствующем слоте информацию речи, причем эта замена помечается скрытым флажком .

В отличие от дуплексных каналов (трафика и совмещенных каналов управления, размещаемых в канале трафика эфирного ин-

терфейса) симплексные каналы управления BCCH и CCCH размещаются в нулевом слоте кадров канала управления эфирного интерфейса на так называемых несущих BCCH, имеющихся в ячейке.

Сообщение канала RACH передается подвижной станцией раз в 235 мс, т/е. только в одном из кадров мультикадра, при этом используется структура слота, соответствующая пачке доступа. Сообщения логических каналов управления в большинстве случаев кодируются со значительной избыточностью с целью защиты от ошибок при передаче информации.

Рассмотрим сначала наиболее простой случай – работу подвижной станции в пределах одной ячейки своей (домашней) системы, без передачи обслуживания. В этом случае в работе подвижной станции можно выделить четыре этапа, которым соответствуют четыре режима работы:

– включение и инициализация;

– режим ожидания;

– режим установления связи (вызова);

– режим ведения связи (телефонного разговора).

После включения подвижной станции, т.е. после замыкания цепи питания, производится инициализация – начальный запуск. В течение этого этапа происходит настройка подвижной станции на работу в составе системы – по сигналам, регулярно передаваемым базовыми станциями по соответствующим каналам управления, после чего подвижная станция переходит в режим ожидания. В стандарте GSM подвижная станция сканирует все имеющиеся частотные каналы, настраивается на канал с наиболее сильным сигналом и по наличию пачки коррекции частоты определяет, передается ли в этом частотном канале информация канала BCCH. Если нет, то станция перестраивается на следующий по уровню сигнала частотный канал, и так до тех пор, пока не будет найден канал BCCH. Затем подвижная станция находит пачку синхронизации, синхронизируется с выбранным частотным каналом, расшифровывает дополнительную информацию о базовой станции (в частности, 6-битовый код идентификации базовой станции) и принимает окончательное решение о продолжении поиска или о работе в данной ячейке.

Находясь в режиме ожидания, подвижная станция отслеживает:

– изменения информации системы – эти изменения могут быть связаны как с изменениями режима работы системы, так и с перемещениями самой подвижной станции, например с переходом ее в другую ячейку;

– команда системы – например, команду подтвердить свою работоспособность («регистрация» в конкретной ячейке);

– получение вызова со стороны системы;

– инициализацию вызова со стороны собственного абонента.

Кроме того, подвижная станция может периодически, например раз в 10...15 мин, подтверждать свою работоспособность, передавая соответствующие сигналы на базовую станцию (подтверждение «регистрации» или уточнение местоположения). В центре коммутации для каждой из включенных подвижных станций фиксируется ячейка, в которой она зарегистрирована, что облегчает организацию процедуры вызова подвижного абонента. Если подвижная станция не подтверждает свою работоспособность в течение определенного промежутка времени, например, пропускает два или три подтверждения «регистрации подряд, центр коммутации считает ее выключенной, и поступающий на ее номер вызов не передается.

В стандарте GSM подвижная станция измеряет и периодически передает на базовую станцию следующие параметры:

– уровень сигнала базовой станции рабочей («своей») ячейки и до 16 смежных ячеек, измеряемый по сигналу канала BCCH;

– код качества принимаемого сигнала в рабочей ячейке – функцию оценки частоты битовой ошибки (BER – Bit Error Rate) по принятому сигналу перед канальным декодированием.

Если со стороны системы поступает вызов номера подвижного абонента, центр коммутации направляет этот вызов на базовую станцию той ячейки, в которой «зарегистрирована подвижная станция, или на несколько базовых станций в окрестности этой ячейки с учетом возможного перемещения абонента за время, прошедшее с момента последней «регистрации», а базовые станции передают его по соответствующим каналам вызова. Подвижная станция, находящаяся в режиме ожидания, получает вызов и отвечает на него через свою базовую станцию, передавая одновременно данные, необходимые для проведения процедуры аутенти-

фикации. При положительном результате аутентификации назначается канал трафика, и подвижной станции сообщается номер соответствующего частотного канала, Подвижная станция настраивается на выделенный канал и совместно с базовой станцией выполняет необходимые шаги по подготовке сеанса связи. На этом этапе подвижная станция настраивается на заданный номер слота в кадре, уточняет задержку во времени, подстраивает уровень излучаемой мощности и т.п.

Выбор временной задержки производится с целью временного согласования слотов в кадре (на прием в базовой станции) при организации связи с подвижными станциями, находящимися на разных дальностях от базовой. При этом временная задержка передаваемой подвижной станцией пачки регулируется по командам базовой станции. В стандарте С8М при выборе задержки используются пачки доступа. Задержка регулируется в пределах от 0 до 63 бит с дискретом 1 бит (3,69 мкс). В дальнейшем базовая станция отслеживает изменение дальности до подвижной станции и корректирует величину задержки, выдавая соответствующие команды на подвижную станцию. При малых геометрических размерах ячейки, т.е. при малых величинах задержки (в пределах защитного бланка или защитного интервала), компенсация временной задержки может не производиться.

В стандарте О8М производятся также привязка подвижной станции к базовой по частоте с использованием пачки коррекции частоты и временная синхронизация подвижной станции с базовой с точностью до 1/4 бита, для чего в пачке синхронизации передаются номера четверти бита (QN – Quarter Bit Number,, в пределах от 0 до 624), бита (BN – Bit Number, в пределах от 0 до 156), слота (TN – Timeslot Number, в пределах от 0 до 7) и кадра (FN – Frame Number, в пределах от 0 до 2715648); одновременно в пачке синхронизации передаются 3-битовый код (код цвета – color code) сети сотовой связи и 3-битовый код базовой станции, составляющие е совокупности уникальный б-битоеый идентификатор базовой станции (BSIC – Base Station Identifier Code).

Затем базовая станция выдает сообщение о подаче сигнала вызова (звонка), которое подтверждается подвижной станцией, и вызывающий абонент получает возможность услышать сигнал вы-

зова. Когда вызываемый абонент отвечает на вызов («снимает трубку», т.е. нажимает соответствующую кнопку на панели управления абонентского аппарата), подвижная станция выдает запрос на завершение соединения. С завершением соединения начинается собственно сеанс связи – абоненты ведут разговор.

В процессе разговора подвижная станция производит обработку передаваемых и принимаемых сигналов речи, а также пере даваемых одновременно с речью сигналов управления. По окончании разговора происходит обмен служебными сообщениями между подвижной и базовой станцией (Запрос или команда на отключение с подтверждением), после чего передатчик подвижной станции выключается, и станция переходит в режим ожидания,

Если вызов инициируется со стороны подвижной станции, т.е. абонент набирает номер вызываемого абонента, убеждается в правильности набора по отображению на дисплее и нажимает соответствующую кнопку («вызова) на панели управления, то подвижная станция передает через свою базовую станцию сообщение с указанием вызываемого номера и данными для аутентификации подвижного абонента. После аутентификации базовая станция назначает канал трафика, и последующие шаги подготовке сеанса связи производятся таким же образом, как и при поступлении вызова со стороны системы.

Затем базовая станция сообщает на центр коммутации о готовности подвижной станции, центр коммутации передает вызов в сеть, а абонент подвижной станции получает возможность следить за ходом его выполнения (слышит сигналы «вызов» или «занято»). Соединение завершается на стороне сети.

Описанная процедура схематически иллюстрируется на рис. 5.3.3.

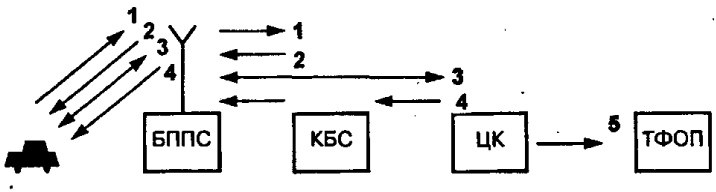


Рис. 5.3.3. Упрощенная схема установления связи (исходящий вызов, стандарт GSM) [2]. БППС – базовая приемо-передающая станция; КБС – контроллер базовой станции; ЦК – цент коммутации; ТФОП – телефонная сеть общего пользования

Цифрами на рис. 5.3.3 обозначена такая последовательность действий:

1. Подвижная станция через канал случайного доступа (RACH) запрашивает выделенный закрепленный канал управления (SDCCH) для установления связи.

2. Контроллер базовой станции через канал разрешения доступа (AGCH) назначает канал SDCCH.

3. Подвижная станция через канал SDCCH проводит аутентификацию и выдает запрос на вызов (с номером вызываемого абонента).

4. Центр коммутации выдает команду на назначение канала трафика (TCH).

5. Центр коммутации выдает вызываемый номер на стационарную телефонную сеть, и после ответа вызываемого абонента завершает соединение.

Процесс разговора и завершение сеанса связи не отличаются от предыдущего случая.

Если подвижный абонент разговаривает с другим подвижным абонентом, то процедура установления связи и проведения сеанса связи происходит практически таким же образом. Если при этом оба подвижных абонента относятся к одной и той же сотовой системе, то связь между ними устанавливается через центр коммутации системы без выхода в стационарную телефонную сеть.

Аутентификация – процедура подтверждения подлинности абонента системы подвижной связи, предотвращающая несанкционированный доступ к услугам сотовой сети. Идентификация – процедура отождествления подвижной станции, т.е. процедура установления ее принадлежности к одной из групп, обладающих определенными свойствами или признаками.

В стандарте GSM процедура аутентификации связана с использованием модуля идентификации абонента (Subscriber Identity Module – SIM), называемого также SIM-картой (или смарт-картой). Модуль SIM – это съемный модуль, напоминающий по внешнему виду пластиковую кредитную карточку. Модуль вручается абоненту одновременно с аппаратом. Модуль содержит персональный идентификационный номер абонента (Personal Identification Number – PIN) международный идентификатор абонента подвижной

связи (International Mobile Subscriber Identity - IMSI), индивидуальный ключ аутентификации абонента Ki, индивидуальный алгоритм аутентификации абонента A3, алгоритм вычисления ключа шифрования A8. Для аутентификации используется зашифрованный отклик (signed response S), являющийся результатом применения алгоритма A3 к ключу Ki и квазислучайному числу R, получаемому подвижной станцией от центра аутентификации через центр коммутации. Алгоритм A8 используется для вычисления ключа шифрования сообщений. Уникальный идентификатор IMSI для текущей работы заменяется временным идентификатором TMSI (Temporary Mobile Subscriber Identity – временный идентификатор абонента подвижной связи), присваиваемым аппарату при его первой регистрации в конкретном регионе, определяемом идентификатором LAI (Location Area Identity – идентификатор области местоположения), и сбрасываемым при выходе аппарата за пределы этого региона. Идентификатор PIN-код, известный только абоненту, который должен служить защитой от несанкционированного использования SIM-карты, например, при ее утере. После трех неудачных попыток набора PIN SIM-карта блокируется и блокировка может быть снята либо набором дополнительного кода – персонального кода разблокировки (Personal unblocking key – PUK), либо по команде с центра коммутации.

Процедура аутентификации стандарта GSM схематически показана на рис. 5.3.4. Пунктиром отмечены элементы, не относящиеся непосредственно к процедуре аутентификации, но используемые для вычисления ключа шифрования Kc. Вычисление производится каждый раз при проведении аутентификации.

Процедура идентификации заключается в сравнении идентификатора абонентского аппарата с номерами, содержащимися в соответствующих черных списках регистра аппаратуры с целью аутентификации из обращения украденных и технически неисправных аппаратов. Идентификатор аппарата делается таким, чтобы его изменение или подделка были трудными и экономически невыгодными.

Базовая станция, находящаяся примерно в центре ячейки, обслуживает все подвижные станции в пределах своей ячейки. При перемещении подвижной станции из одной ячейки в другую ее

обслуживание соответственно передается от базовой станции первой ячейки к базовой станции второй. Этот процесс называется передачей обслуживания (американский термин – handoff , англо-европейский – hanover.). Процедура передачи обслуживания имеет место только в том случае, когда подвижная станция пересекает границу ячеек во время сеанса связи и связь (телефонный разговор) при этом не прерывается. Если же подвижная станция перемещается из одной ячейки в другую, находясь в режиме ожидания, она просто отслеживает эти перемещения по информации системы, передаваемой по каналам управления, и в нужный момент перестраивается на более сильный сигнал другой базовой станции.

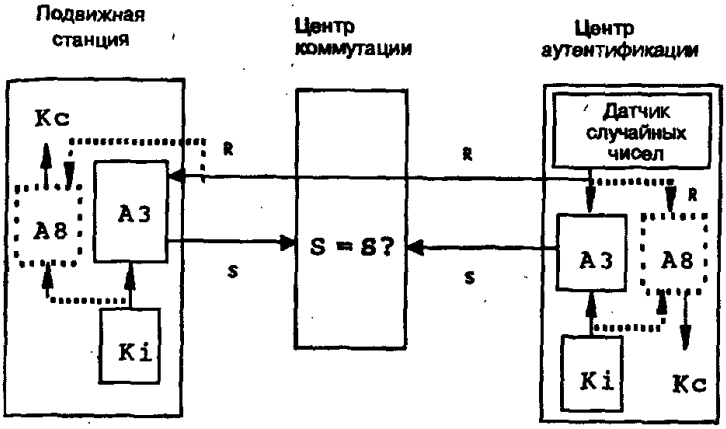


Рис. 5.3.4. Схема процедуры аутентификации (стандарт GSM).
R – случайное число; А3 – алгоритм аутентификации; А8 – алгоритм вычисления ключа шифрования; *Ki* – ключ аутентификации; *Kc* – ключ шифрования; *S* – зашифрованный отклик (Signed Response – SRES)

Роуминг – эта функция или процедура предоставления услуг сотовой связи абоненту одного оператора в системе другого оператора. В стандарт GSM функция роуминга заложена как обязательный элемент. Кроме того, в стандарте GSM имеется возможность так называемого роуминга с SIM-картами, или пластикового роуминга, с перестановкой SIM-карт между аппаратами различных вариантов стандарта GSM (GSM 900, GSM 1800 и GSM 1900), поскольку во всех трех вариантах стандарта GSM используются унифицированные SIM-карты. Процедура роуминга в стандарте

GSM становится еще более удобной с появлением двухрежимных, а в дальнейшем – и трехрежимных абонентских терминалов (GSM 900/GSM 1800/GSM 1900). Из технических и организационных трудностей, связанных с развитием роуминга, отметим следующие: аутентификация абонентов с учетом неизбежного, инициативного и даже агрессивного фрода; организация оплаты услуг роуминга, существенно усложняющаяся с ростом масштабов и расширением географии роуминга; протекционизм (например, в некоторых странах запрещается применение абонентских аппаратов иностранного производства).

Стандарт GSM дает четкую классификацию поддерживаемых им услуг (функций). Функции сотовой связи состоят из основных и дополнительных функций. Первые из них могут существовать сами по себе, они разделяются на два больших класса; функции передачи (bearer services) и телефункции (teleservices). Дополнительные функции (supplementary services) могут предоставляться только одновременно с основными.

Функции передачи включают четыре категории:

1. Асинхронный обмен данными с коммутируемыми телефонными сетями общего пользования со скоростями 300...9600 бит/с.

2. Синхронный обмен данными с коммутируемыми телефонными сетями общего пользования, коммутируемыми сетями передачи данных общего пользования и цифровыми сетями с интеграцией функций со скоростями 300...9600 бит/с.

3. Асинхронный пакетный обмен данными с сетью передачи данных общего пользования с пакетной коммутацией (доступ через ассемблер/дисассемблер) со скоростями 300…9600 бит/с.

4. Синхронный пакетный обмен данными с сетью передач, данных общего пользования с пакетной коммутацией со скоростями 2400...9600 бит/с.

Функции передачи могут быть прозрачными (transparent) и непрозрачными. В прозрачных функциях передачи защита от ошибок обеспечивается только за счет текущей коррекции ошибок (коррекции ошибок на проходе – forvard error correction) В непрозрачных функциях передачи предусматривается дополнительная защита в виде автоматического перезапроса (Automatic Repeat Request).

Телефункции включают следующие категории:

1. Передача информации речи и тональной сигнализации в полосе речи.

2. Передача коротких сообщений (буквенно-цифровые сообщения – до 180 символов в сторону подвижного абонента).

3. Доступ к системе обработки сообщений (например, передача сообщения от системы персонального радиовызова на подвижную станцию сотовой связи).

4. Передача факсимильных сообщений.

Дополнительные функции включают категории:

1. Идентификация и отображение вызывающего или подключенного номера и ограничение идентификации и отображения вызывающего или подключенного номера (вызывающей стороне предоставляется право ограничить – возможность идентификации ее номера).

2. Переадресация вызова на другой номер (безусловная переадресация и переадресация в случаях, когда абонент занят или не отвечает) и передача вызова (переключение установленной линии связи на другого абонента).

3. Ожидание вызова (при занятом терминале абонент получает извещение о поступившем вызове и может ответить на него, отказаться от приема вызова или проигнорировать его поступление) и сохранение вызова (абонент имеет возможность прервать проводимый сеанс связи, ответив на другой вызов или сделав другой вызов, а затем вернуться к продолжению прерванного разговора).

4. Конференц-связь – одновременный разговор трех или более абонентов.

5. Закрытая группа пользователей – эта функция позволяет группе пользователей общаться только между собой; при необходимости один или более членов группы могут иметь доступ по входу/выходу к абонентам, не входящим в группу.

6. Оперативная информация о стоимости оказываемых или оказанных услуг (об оплате).

7. Запрет на определенные функции, например, на входящие вызовы, на международные вызовы или на исходящие вызовы для ромеров.

8. Предоставление линии связи сеть/пользователь для реализации функций, определяемых оператором.

Функция передачи (т.е. переноса данных) ориентирована только на транспортировку информации между соответствующими стыками пользователь/сеть, и в отличие от телефункции забота о совместимости протоколов связи оконечных устройств (терминальной аппаратуры) остается за пользователями этих устройств. Телефункция ориентирована на непосредственную связь пользователь/пользователь и включает функцию связи оконечных устройств (рис.5.3.5) .

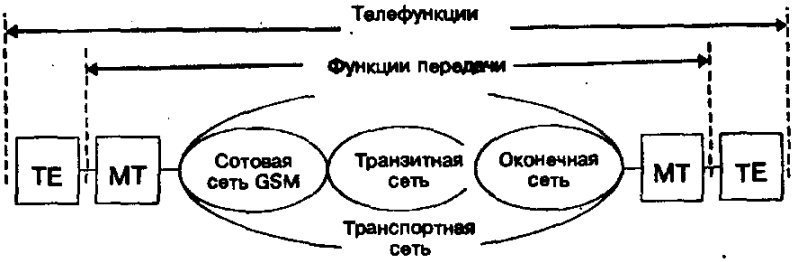


Рис. 5.3.5. Функциям передачи и телефункциям соответствуют разные точки доступа [2]. MT – терминал системы подвижной связи (Mobil Termination); TE – терминальная аппаратура (Terminal Equipment)

В соответствии с изложенным возможны различные варианты конфигурации подвижной станции системы GSM, обеспечивающие различные точки доступа приведены на рис. 5.3.6.

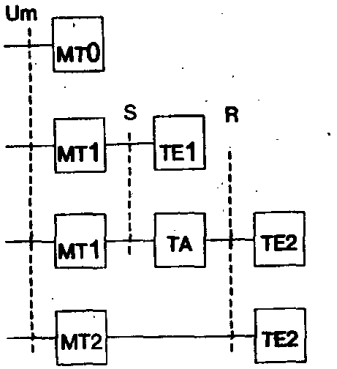


Рис. 5.3.6. Точки доступа сотовой сети стандарта GSM (четыре варианта конфигурации подвижной станции). MT – терминал системы подвижной связи (Mobil Termination); TE – терминальная аппаратура (Terminal Equipment); TA – терминальный адаптер (Terminal Adapter)

В общем случае подвижная станция состоит из терминала системы подвижной связи (МоЬИие Тегпііпа – МТ) и терминальной аппаратуры (Terminal Equipment – ТЕ). Терминалы могут быть трех типов:

МТО – функционально законченная подвижная станция, включающая как сетевой терминал, так и терминальную аппаратуру.

МТ1 – поддерживает терминальную аппаратуру типа ТЕ1 с интерфейсом ISDN.

МТ2 – поддерживает терминальную аппаратуру типа ТЕ2 с интерфейсами серий X и V МККТТ; терминальная аппаратура типа ТЕ2 может быть подключена также к терминалу МТ1 ч рез терминальный адаптер ТА.

Точки доступа *S* и *R* (обозначения ISDN) соответствуют функциям передачи, выходы терминала МТО и терминальной аппаратуры – телефункциям.

Экстенсивная фаза роста сетей GSM всех ведущих операторов в России в настоящее время заканчивается. Операторы «большой тройки» (МТС, «ВымпелКом», «МегаФон») и крупные региональные операторы (НСС, СМАРТС, «Уралсвязьинформ» и т.д.) вступили в этап насыщения рынка с совершенно новыми бизнес-приоритетами. Если до 2006 г. основными конкурентными показателями считались зона покрытия и количество абонентов, то сейчас на первый план вышли выручка с абонента (ARPU), доля в ней неголосовых услуг (VAS) и качество предоставляемых пользователям сервисов.

Важным фактором является и то, что для операторов GSM, претендующих на получение лицензий 3G, выручка в существующей сети 2G – один из самых дешевых источников финансирования развития сети третьего поколения. В результате, если оценить ситуацию с одновременным развитием GSM и 3G услуг по методике BSG (Boston Consulting Group), то для российских операторов очевидна необходимость постоянного совершенствования GSM-сетей, которые приносят значимую прибыль, с одновременным смещением фокуса на развитие неголосовых услуг.

Литература

1. Основы построения телекоммуникационных систем и сетей: Учебник для вузов / В.В. Крухмалев, В.Н. Гордиенко, А.Д. Моченов и др. / Под ред. В.Н. Гордиенко и В.В. Крухмалева. – М.: Горячая линия-Телеком, 2004. – 510 с.
2. *Ратынский М.В.* Основы сотовой связи./ Под ред. Д.Б. Зимина. – М.: Радио и связь, 2000.
3. Основы построения телекоммуникационных систем и сетей. Конспект лекций. – [Электронный ресурс]. – Режим доступа: http://siblec.ru/
4. *Крук Б.И., Попантонопуло В.Н., Шувалов В.П.* Телекоммуникационные системы и сети: Уч. пос. В 3-х т. – М.: Горячая линия-Телеком, 2004.
5. *Бабков В.Ю., Вознюк М.А., Михайлов П.А.* Сети мобильной связи. Передача информации в системах подвижной связи. – СПб.: СПбГУТ, 2000.

6. ЛОКАЛЬНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ

Архитектура локальных сетей ЭВМ базируется на принципе многоуровневого управления процессами, реализуемого иерархической совокупностью протоколов и интерфейсов, и практически полностью соответствует семиуровневой архитектуре эталонной модели взаимодействия открытых систем (модели OSI). Основное отличие архитектур заключается в реализации физического и канального уровней. Эти уровни в наибольшей степени отражают специфику локальных сетей. Физический уровень определяет тип используемого кабеля, электрических разъемов, форму и способ кодирования дискретных сигналов. Канальный уровень обеспечивает передачу информационных кадров (пакетов) между абонентскими системами, входящими в состав одной сети. В архитектуре локальных сетей канальный уровень делится на два подуровня:

• управления логическим каналом передачи данных (Logical Link Control, LLC);

• управления доступом к среде (Media Access Control, MAC).

Подуровень MAC управляет доступом к разделяемому моноканалу. Он преобразует разделяемый физический моноканал в виртуальные каналы типа «точка–точка» между парами абонентских систем.

В современных локальных сетях получили распространение несколько протоколов MAC-уровня, реализующих различные алгоритмы доступа к разделяемой среде. Эти протоколы полностью определяют специфику таких сетевых технологий как Ethernet, Token Ring, FDDI, 100VG-AnyLAN.

Подуровень LLC обеспечивает достоверную передачу информационных кадров между абонентскими системами, а также реализует функции интерфейса с прилегающим к нему сетевым уровнем. Для подуровня LLC также существует несколько вариантов протоколов, отличающихся наличием или отсутствием на этом подуровне процедур восстановления кадров в случае их потери или искажения, то есть отличающихся качеством транспортных услуг этого уровня. Протоколы подуровней MAC и LLC взаимно

независимы - каждый протокол MAC-уровня может применяться с любым типом протокола LLC-уровня и наоборот.

Проектирование и построение локальных сетей осуществляется на основе стандартов, разработанных рабочей группой 802 IEEE (Института инженеров по электротехнике и электронике США). Стандарты, получившие наибольшее распространение, приведены в табл. 6.1. Для каждого из этих стандартов определены спецификации физического уровня, определяющие среду передачи данных (коаксиальный кабель, витая пара или оптоволоконный кабель), ее параметры, а также методы кодирования информации для передачи по данной среде.

Таблица 6.1

Стандарты IEEE 802.x

Стандарт	Содержание стандарта
802.1	Основные понятия и определения, общие характеристики и требования к локальным сетям.
802.2	Определяет подуровень управления логическим каналом LLC.
802.3	Описывает коллективный доступ с опознаванием несущей и обнаружением конфликтов (Carrier sense multiple access with collision detection - CSMA/CD), прототипом которого является метод доступа стандарта Ethernet;
802.4	Определяет метод доступа к шине с передачей маркера (Token bus network), прототип - ArcNet;
802.5	Описывает метод доступа к кольцу с передачей маркера (Token ring network), прототип - Token Ring.
802.11 802.16	Определяют принципы построения и функционирования беспроводных локальных сетей.

Сетевая технология – это совокупность согласованных между собой протоколов и реализующих их технических и программных средств, необходимых и достаточных для построения и нормального функционирования локальной сети.

В настоящее время для построения локальных сетей наибольшее распространение получили сетевые технологии Ethernet, Token Ring, FDDI, использующие для передачи данных кабельные каналы связи с различной топологией, также активно развиваются и внедряются технологии беспроводных локальных сетей, передача данных в которых между абонентскими системами осуществляется по каналам радиочастотной связи.

6.1. Технология Ethernet

Ethernet – это самый распространенный на сегодняшний день стандарт локальных сетей, использующий метод доступа к среде CSMA/CD.

Главным достоинством сетей Ethernet, благодаря которому они стали такими популярными, является их экономичность. Для построения сети достаточно иметь по одному сетевому адаптеру для каждого компьютера плюс один физический сегмент коаксиального кабеля нужной длины (сегмент – часть сетевого кабеля, ограниченная мостами, маршрутизаторами, повторителями или терминаторами). Другие базовые технологии, например Token Ring, для создания даже небольшой сети требуют наличия дополнительного устройства – концентратора.

Кроме того, в сетях Ethernet реализованы достаточно простые алгоритмы доступа к среде, адресации и передачи данных. Простота логики работы сети ведет к упрощению и, соответственно, удешевлению сетевых адаптеров и их драйверов. По той же причине адаптеры сети Ethernet обладают высокой надежностью.

И, наконец, еще одним замечательным свойством сетей Ethernet является их хорошая расширяемость, то есть легкость подключения новых узлов. Основные характеристики технологии Ethernet приведены в табл. 6.1.1.

Другие базовые сетевые технологии – Token Ring, FDDI, l00VGAny-LAN, хотя и обладают многими индивидуальными чертами, в то же время имеют много общих свойств с Ethernet. В первую очередь – это применение регулярных фиксированных топологий (иерархическая звезда и кольцо), а также разделяемых сред передачи данных. Существенные отличия одной технологии от другой связаны с особенностями используемого метода доступа к разделяемой среде. Так, отличия технологии Ethernet от технологии Token Ring во многом определяются спецификой заложенных в них методов разделения среды – случайного алгоритма доступа в Ethernet и метода доступа путем передачи маркера в Token Ring.

Что в действительности обозначают сокращения 10Base2, 10BaseT и т.д.? Это – имена для различных физических типов Ethernet. "10" обозначает скорость передачи сигнала 10MHz, "Base" означает "Baseband", "Broad" – broadband. Первоначально

последняя секция предназначалась для отображения максимальной длины кабельного сегментов без репитеров в сотнях метров. Эта договоренность была изменена с введением 10BaseT, где T – обозначает "twisted pair" – витая пара и 10BaseF, где F обозначает "fiber" – волокно.

Таблица 6.1.1

Основные характеристики разновидностей технологии Ethernet

Ethernet	Fast Ethernet	Gigabit Ethernet
10Base2 – Сетевая среда с использованием тонкого коаксиального кабеля, однополосный режим, скорость передачи данных 10 Мбит/с, топология – шина	100BaseTX- Сетевая среда с использованием неэкранированной витой пары 5 кат, скорость передачи данных 100 Мбит/с, топология – звезда	1000Base-SX 850mn, лазерный источник, многомодовое оптоволокно [не более 300 м (волокно 62,5 мкм) и 550 м (волокно 50 мкм)]
10Base5 – Сетевая среда с использованием толстого коаксиального кабеля, однополосный режим, скорость передачи данных 10 Мбит/с, топология – шина		
10BaseT- Сетевая среда с использованием неэкранированной витой пары 3, 4, 5 кат, однополосный режим, скорость передачи данных 10 Мбит/с, топология – звезда	100BaseFX- Сетевая среда с использованием волоконно-оптического кабеля, скорость передачи данных 100 Мбит/с, топология – звезда	1000Base-LX 1300 mn, лазерный источник и одномодовое оптоволокно (не более 3000м)
10BaseFL – Сетевая среда с использованием волоконно-оптического кабеля однополосный режим, скорость передачи данных 10 Мбит/с, топология – звезда		1000Base-CX двухпроводной экранированный кабель (STP), экранированная витая пара не более 25 м

Рассмотрим эволюцию основных технологий Ethernet.

На рис. 6.1.1 изображена часть сети, построенной по технологии 10Base5 (Толстый Ethernet). Основными характеристиками технологии 10Base5 являются:

– Используемая топология – общая шина.

– Используемый провод – коаксиальный кабель толстый (так называемый "желтый") с волновым сопротивлением 50 Ом.

– Максимальная длина сегмента (отрезок сети без повторителя, ограниченный терминаторами) 500 м.

– Минимальное расстояние между точками подключения 2,5 м.

– Максимальное количество точек подключения к сегменту 100.

– Максимальное количество сегментов сети 5.

– Устройства подключаются к сети посредством устанавливаемого на кабель трансивера (transceiver – MAU(Media Access Unit).

– Максимальная длина трансиверного кабеля (длина кабеля между трансивером и устройством) 25 м.

– При подключении используется разъем AUI 15 pin.

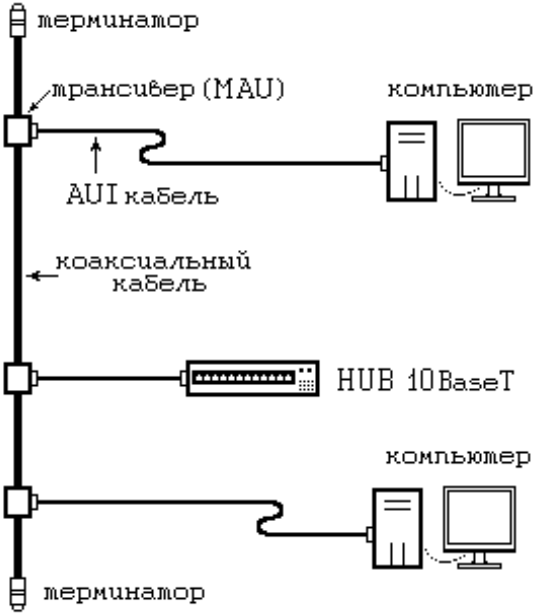


Рис. 6.1.1. Часть сети, построенной по технологии 10Base5 (Толстый Ethernet)

На рис. 6.1.2 изображена часть сети, построенной по технологии 10Base2 или тонкий Ethernet. Основными характеристиками технологии 10Base2 являются:

– Основная используемая топология – общая шина.

– Используемый провод – коаксиальный кабель 50 Ом, тонкий.

– Максимальная длина сегмента – 185 м.

– Минимальное расстояние между точками подключения – 0,5 м.

– Максимальное количество точек подключения к сегменту – 30.

– Максимальное количество сегментов в сети – 5.

На рис. 6.1.3 изображен монтаж и прокладка сети 10Base2 (Тонкий Ethernet).

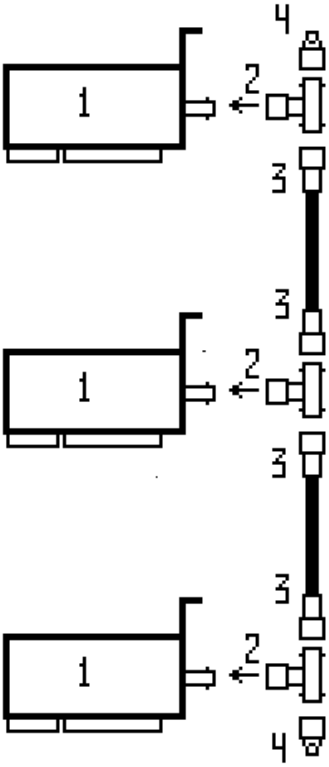


Рис. 6.1.2. Часть сети, построенной по технологии 10Base2 или тонкий Ethernet. 1 – сетевая карта, установленная на компьютере, 2 – Т-коннектор, 3 – разъемы на концах кабеля, 4 – терминатор

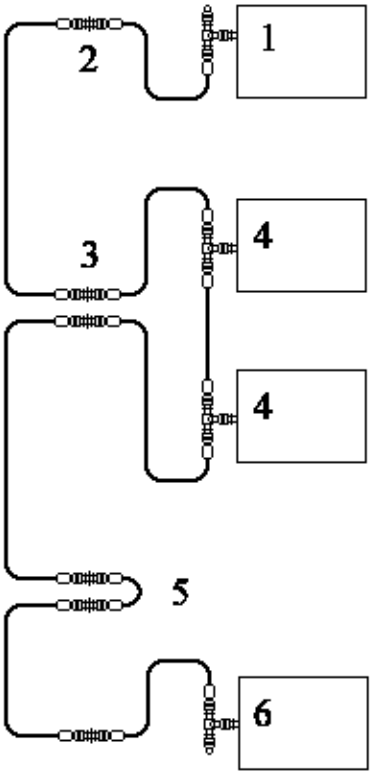


Рис. 6.1.3. Монтаж и прокладка сети 10Base2. 1. Крайний компьютер или другое сетевое устройство сегмента. 2. Прямой переход типа "Bulk-head connector". 2-3. Проброс кабеля между точками подключения. 3. Два прямых перехода. 4. Компьютер или другое сетевое устройство. 5. Перемычка из коаксиального кабеля вместо компьютера. 6. Крайний компьютер или другое устройство сегмента

На рис. 6.1.4 показан монтаж и прокладка сетей на основе витой пары. Максимальная длина кабеля между розетками или между розеткой и patch панелью – 90 м. Это правило разработано исходя из ограничения максимального расстояния в 100 м между DTE (компьютер) и хабом. Причем оставшиеся 10 м отводятся на

провод (patch cord) между розеткой и компьютером, а также розеткой (patch панелью) и хабом. Для сетей категории 5 может быть не более 3-х отрезков кабеля между двумя устройствами (как на рис. 6.1.5).

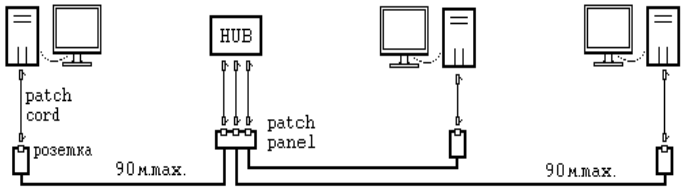


Рис. 6.1.4. Монтаж и прокладка сетей на основе витой пары

На рис. 6.1.5 показан монтаж и прокладка сетей на основе стандарта 10BaseF (волоконная оптика). В этом случае используется топология звезда, максимальная длина сегмента 2 км.

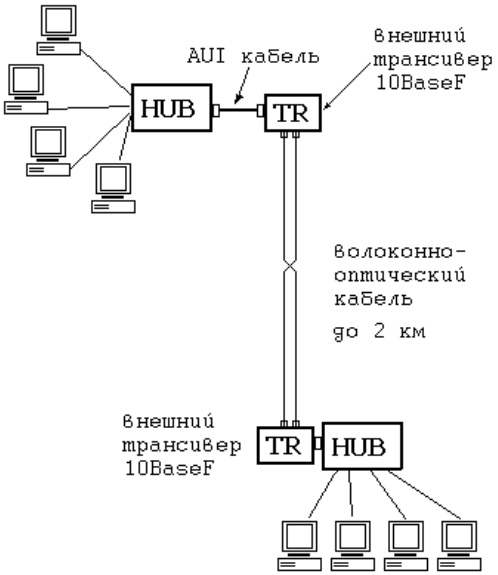


Рис. 6.1.5. Монтаж и прокладка сетей на основе стандарта 10BaseF

В процессе развития Ethernet и стандарта IEEE 802.3 было предложено 4 варианта формата кадра. В 1980 г. консорциум трёх фирм DEC, Intel, Xerox представил на рассмотрение комитета

802.3 свою версию стандарта Ethernet (тип кадра Ethernet DIX), но комитет принял стандарт, отличающийся деталями (в том числе и форматом кадра) от предложения DIX (тип кадра 802.3/LLC). Novell, являющаяся в то время лидером сетевой индустрии в области персональных компьютеров, предложила свой формат кадра (Raw 802.3). Четвёртый вариант был предложен комитетом 802.2 для ликвидации недостатков формата кадра 802.3/LLC и приведения всех форматов кадров к общему виду (тип кадра Ethernet SNAP).

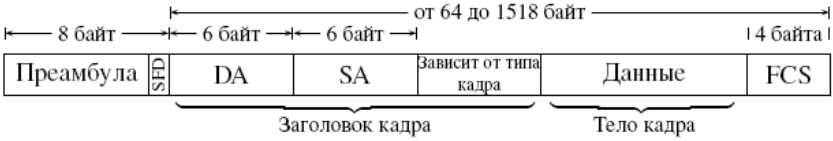


Рис. 6.1.6. Формат кадра Ethernet

Каждый кадр начинается с *преамбулы (Preamble)* (длина 7 байт), заполненной шаблоном 0b10101010 (для синхронизации источника и получателя). После преамбулы идёт байт *начального ограничителя кадра (Start of Frame Delimiter, SFD)*, содержащий последовательность 0b10101011 и указывающий на начало собственно кадра. Далее идут поля *адрес получателя (Destination Address, DA)* и *адрес отправителя (Source Address, SA)*. В Ethernet используют 48-битные адреса MAC-уровня IEEE . Следующее поле имеет разный смысл и разную длину в зависимости от типа кадра:

– Тип кадра Ethernet DIX.

Тип кадра Ethernet DIX – изначальный тип кадра стандарта Ethernet. Этот тип кадра носит также названия Ethertype, Ethernet II (в терминологии NetWare). После поля адреса источника этот тип кадра содержит 16-битное поле *типа (Ethertype)*, идентифицирующее инкапсулированный в кадре протокол верхнего уровня (рис. 6.1.7, *а*).

– Тип кадра Raw 802.3. Этот тип кадра предложен компанией Novell для своей системы NetWare. Он также носит названия Novell 802.3, Ethernet 802.3 (в терминологии Net-Ware). За адресом источника он содержит 16-битное поле *длины (Length, L)*, определяющее число байт, следующее за полем длины (без учёта поля

контрольной суммы) (рис. 6.1.7, *б*). В этот тип кадра всегда вкладывается пакет протокола IPX. Первые два байта заголовка протокола IPX содержат контрольную сумму датаграммы IPX. Однако по умолчанию это поле не используется и выставлено в 0xFFFF.

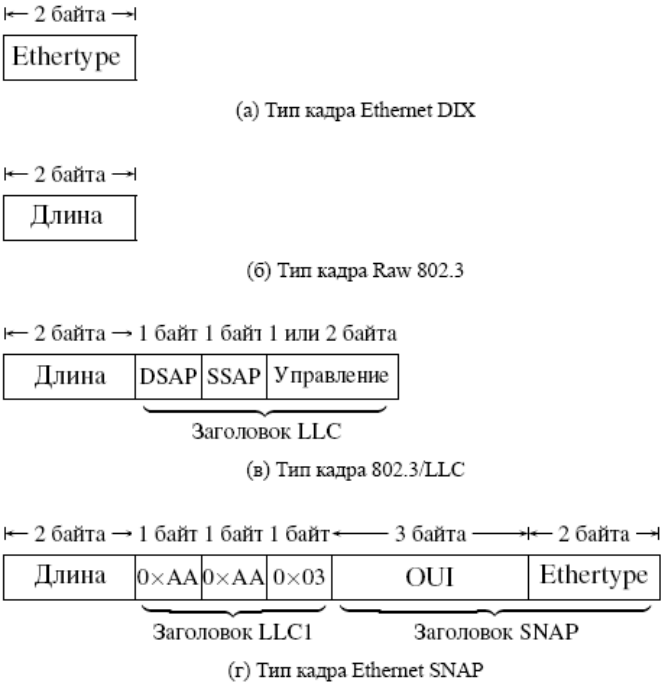


Рис. 6.1.7. Типы кадров Ethernet (только поле, зависящее от типа кадра)

– Тип кадра 802.3/LLC. Поскольку группа стандартов IEEE 802 разделяет канальный уровень на подуровни MAC и LLC, то в кадр MAC-подуровня вкладывается кадр LLC-подуровня. За полем адреса источника идёт 16-битное поле *длины (Length, L)*, определяющее число байт, следующее за полем длины (без учёта поля контрольной суммы). За ним следует заголовок LLC (рис. 6.1.7, *в*). Он состоит из 8-разрядных полей *точки доступа к услуге источника (Source Service Access Point, SSAP)* и *точки доступа к услуге получателя (Destination Service Access Point, DSAP)*, а также поля управления, имеющего длину 8 или 16 бит, в зависимости от типа протокола LLC. Поля SSAP и DSAP размером по 6 бит предназна-

чены для описания типа протокола следующего уровня. Но при такой разрядности можно указать не более 64 различных протоколов. Таким образом, недостаточный размер полей SAP создаёт трудности при применении этого типа кадра (например, нет типа SAP для протокола ARP).

– Тип кадра Ethernet SNAP. Преждевременная стандартизация протокола LLC привела к значительным трудностям в применении типа кадра 802.3/LLC. Для решения этой проблемы комитетом 802.2 был предложен тип кадра *Ethernet SNAP (SubNetwork*

Access Protocol, протокол доступа к подсети). Кадр Ethernet SNAP является расширением кадра 802.3/LLC за счёт введения дополнительного заголовка протокола SNAP (рис. 6.1.7, *г*). Заголовок SNAP состоит из 3-байтного поля *уникального идентификатора организации (Organizationally Unique Identifier, OUI)* и 2-байтного поля *типа (Type, Ethertype)*. Тип идентифицирует протокол верхнего уровня, а поле OUI определяет идентификатор организации, контролирующей назначение кодов типа протокола.

Коды протоколов для стандартов IEEE 802 контролирует IEEE, имеющая код OUI, равный 0x000000. Для этого кода OUI поле типа для Ethernet SNAP совпадает со значением типа для Ethernet DIX.

Протокол SNAP вкладывается в протокол LLC1. Код SAP для него – 0xAA. Поле управления устанавливается в 0x03, что соответствует использованию ненумерованных кадров. Далее идёт поле *данных (Data)*. Если длина поля данных недостаточна для получения минимальной длины кадра, то вводится дополнительное поле *заполнения (Padding)*, призванное обеспечить минимальную длину кадра. В конце кадра идёт 32-битное поле *контрольной суммы (Frame Check Sequence,FCS)*. Контрольная сумма вычисляется по алгоритму CRC-32.

Размер кадра Ethernet от 64 до 1518 байт (без учёта преамбулы, но с учётом поля контрольной суммы). Алгоритм автоматического распознавания разных типов кадров Ethernet достаточно прост. Поле, следующее за полем адреса источника, имеет длину 2 байта и может быть либо полем Ethertype, либо полем длины данных. Максимальная длина поля данных равна 1500 байт (0x05DC). Значение поля Ethertype всегда больше, чем 0x05DC.

Следовательно, если значение поля больше, чем 0x05DC, то мы имеем кадр Ethernet DIX. В противном случае – поле длины. Если следующие за полем длины два байта выставлены в 0xFFFF, то это кадр Raw 802.3. В противном случае мы имеем либо кадр типа 802.3/LLC, либо кадр типа Ethernet SNAP, которые можно различить по значению полей SSAP и DSAP. Если они выставлены в 0xAA, то имеем кадр Ethernet SNAP, иначе – кадр типа 802.3/LLC.

В табл. 6.1.2 приведены данные об использовании разных кадров Ethernet протоколами более высоких уровней.

В сетях Ethernet используется метод доступа к среде передачи данных, называемый *методом коллективного доступа с опознаванием несущей и обнаружением коллизий (carrier-sense-multiply-access with collision detection, CSMA/CD),* разработанный корпорацией Xerox. Этот метод используется исключительно в сетях с общей шиной (к которым относятся и радиосети, породившие этот метод). Все компьютеры такой сети имеют непосредственный доступ к общей шине, поэтому она может быть использована для передачи данных между любыми двумя узлами сети. Простота схемы подключения – это один из факторов, определивших успех стандарта Ethernet. Говорят, что кабель, к которому подключены все станции, работает в режиме *коллективного доступа (multiply-access, MA).*

Таблица 6.1.2

Использование разных типов кадров Ethernet протоколами высших уровней

Тип кадра	Протоколы
Ethernet DIX	IPX, IP, AppleTalk Phase I
Raw 802.3	IPX
802.3/LLC	IPX, NetBEUI
Ethernet SNAP	IPX, IP, AppleTalk Phase II

Данный метод основывается на предположении, что каждое локальное устройство может узнать состояние общего широковещательного канала связи перед попыткой его использования. Такой метод называется множественным доступом к среде с обнаружением конфликтов и детектированием несущей (carrier-sense multiple access with collision detection – CSMA/CD) В данном случае “несущая” означает любую электрическую активность в кабеле.

При описанном подходе возможна ситуация, когда две станции одновременно пытаются передать кадр данных по общему ка-

белю. Для уменьшения вероятности этой ситуации непосредственно перед отправкой кадра передающая станция слушает кабель (то есть принимает и анализирует возникающие на нем электрические сигналы), чтобы обнаружить, не передается ли уже по кабелю кадр данных от другой станции. Если *опознается несущая (carrier-sense, CS)*, то станция откладывает передачу своего кадра до окончания чужой передачи, и только потом пытается вновь его передать. Но даже при таком алгоритме две станции одновременно могут решить, что по шине в данный момент времени нет передачи, и начать одновременно передавать свои кадры. Говорят, что при этом происходит *коллизия*, так как содержимое обоих кадров сталкивается на общем кабеле, что приводит к искажению информации.

Чтобы корректно обработать коллизию, все станции одновременно наблюдают за возникающими на кабеле сигналами. Если передаваемые и наблюдаемые сигналы отличаются, то фиксируется *обнаружение коллизии (collision detection, CD)*. Для увеличения вероятности немедленного обнаружения коллизии всеми станциями сети, ситуация коллизии усиливается посылкой в сеть станциями, начавшими передачу своих кадров, специальной последовательности битов, называемой *jam-последовательностью*.

После обнаружения коллизии передающая станция обязана прекратить передачу и ожидать в течение короткого случайного интервала времени, а затем может снова сделать попытку передачи кадра.

Из описания метода доступа видно, что он носит вероятностный характер, и вероятность успешного получения в свое распоряжение общей среды зависит от загруженности сети, то есть от интенсивности возникновения в станциях потребности передачи кадров. При разработке этого метода предполагалось, что скорость передачи данных в 10 мбит/с очень высока по сравнению с потребностями компьютеров во взаимном обмене данными, поэтому загрузка сети будет всегда небольшой. Это предположение остается часто справедливым и по сей день, однако уже появились приложения, работающие в реальном масштабе времени с мультимедийной информацией, для которых требуются гораздо более высокие скорости передачи данных. Поэтому наряду с классическим Ethernet'ом растет потребность и в новых высокоскоростных технологиях.

В алгоритме множественного доступа Ethernet определены следующие действия или отклики пользователя.

1. Отложить. Пользователь не должен передавать данные при наличии несущей или в течение минимального времени, разделяющего пакеты.

2. Передать. Если не используется предыдущее действие, пользователь может передавать данные до окончания времени передачи пакета или до возникновения конфликта.

3. Прервать. При возникновении конфликта пользователь должен прекратить передачу данных и оповестить других пользователей, участвующих в конфликте.

4. Передать повторно. Пользователь должен предпринять попытку повторной передачи после паузы случайной протяженности.

5. Откат. Пауза перед n-й попыткой повторной передачи – это равномерно распределенное случайное число от 0 до $2^n - 1$, где ($0 < n \leq 10$). При $n > 10$ интервал остается в пределах от 0 до 1023. Единицей измерения времени для интервала задержки перед повторной передачей является 512 бит (51,2 мкс).

При использовании манчестерской схемы PCM из спецификации Ethernet каждый однобитовый элемент или позиция двоичного разряда содержит переход. Двоичная единица описывается переходом с низкого уровня на высокий, двоичный нуль – переходом с высокого уровня на низкий. Следовательно, наличие переходов служит показателем наличия несущей. Если в течение определенного промежутка времени (от 0,75 до 1,25 периода передачи бита) переход не наблюдается – несущая потеряна, что свидетельствует об окончании пакета.

Метод CSMA/CD определяет основные временные и логические соотношения, гарантирующие корректную работу всех станций в сети:

- Между двумя последовательно передаваемыми по общей шине кадрами информации должна выдерживаться пауза в 9.6 мкс; эта пауза нужна для приведения в исходное состояние сетевых адаптеров узлов, а также для предотвращения монопольного захвата среды передачи данных одной станцией.
- При обнаружении коллизии (условия ее обнаружения зависят от применяемой физической среды) станция выдает в среду

специальную 32-битную последовательность (jam-последовательность), усиливающую явление коллизии для более надежного распознавания ее всеми узлами сети.

- После обнаружения коллизии каждый узел, который передавал кадр и столкнулся с коллизией, после некоторой задержки пытается повторно передать свой кадр. Узел делает максимально 16 попыток передачи этого кадра информации, после чего отказывается от его передачи. Величина задержки выбирается как равномерно распределенное случайное число из интервала, длина которого экспоненциально увеличивается с каждой попыткой. Такой алгоритм выбора величины задержки снижает вероятность коллизий и уменьшает интенсивность выдачи кадров в сеть при ее высокой загрузке.

Все параметры протокола Ethernet подобраны таким образом, чтобы при нормальной работе узлов сети коллизии всегда четко распознавались. Именно для этого минимальная длина поля данных кадра должна быть не менее 46 байт (что вместе со служебными полями дает минимальную длину кадра в 72 байта или 576 бит). Длина кабельной системы выбирается таким образом, чтобы за время передачи кадра минимальной длины сигнал коллизии успел бы распространиться до самого дальнего узла сети. Поэтому для скорости передачи данных 10 Мб/с, используемой в стандартах Ethernet, максимальное расстояние между двумя любыми узлами сети не должно превышать 2500 м.

С увеличением скорости передачи кадров, что имеет место в новых стандартах, базирующихся на том же методе доступа CSMA/CD, например, Fast Ethernet, максимальная длина сети уменьшается пропорционально увеличению скорости передачи. В стандарте Fast Ethernet она составляет 210 м, а в гигабитном Ethernet ограничена 25 м.

Независимо от реализации физической среды, все сети Ethernet должны удовлетворять двум ограничениям, связанным с методом доступа:

- максимальное расстояние между двумя любыми узлами не должно превышать 2500 м,
- в сети не должно быть более 1024 узлов.

Количество обрабатываемых пакетов Ethernet в секунду часто используется при указании внутренней производительности мо-

стов и маршрутизаторов, вносящих дополнительные задержки при обмене между узлами. Поэтому интересно знать чистую максимальную производительность сегмента Ethernet в идеальном случае, когда на кабеле нет коллизий и нет дополнительных задержек, вносимых мостами и маршрутизаторами.

Так как размер пакета минимальной длины вместе с преамбулой составляет 64+8 = 72 байта или 576 битов, то на его передачу затрачивается 57.6 мкс. Прибавив межкадровый интервал в 9.6 мкс, получаем, что период следования минимальных пакетов равен 67.2 мкс. Это соответствует максимально возможной пропускной способности сегмента Ethernet в 14 880 п/с.

В технологии Fast Ethernet такие же формат кадра, механизм доступа к среде CSMA/CD и топология, как и в Ethernet. Эволюция коснулась нескольких элементов конфигурации средств физического уровня, включая типы применяемого кабеля, длину сегментов и количество концентраторов, что позволило увеличить пропускную способность. Технология Fast Ethernet может использовать различные типы кабеля: витую пару разной категории, оптоволокно, причём по сравнению с Ethernet меняется как количество используемых проводников (для витой пары), так и методы кодирования. При кодировании сигнала применяются методы NRZI и MLT-3, при физическом кодировании – 4B/5B и 8B/6T. В технологии Fast Ethernet реализована возможность выбора наиболее эффективного режима работы двух взаимодействующих портов: скорость передачи – 10 или 100 Мбит/с, вид передачи данных – дуплекс (full-duplex mode) или полудуплекс. Кроме того, во время выбора режима работы осуществляется проверка целостности линии. В режиме full-duplex вместо CSMA/CD используется соединение P2P (точка–точка) и отсутствует понятие коллизий – каждый узел может одновременно передавать и принимать кадры данных. Работа в данном режиме возможна только при соединении сетевого адаптера с коммутатором или же при непосредственном соединении коммутаторов.

Достоинства технологии Fast Ethernet:

– увеличение пропускной способности сегментов сети до 100 мбит/с;

– сохранение совместимости с методом случайного доступа CSMA/CD;

– сохранение формата кадра Ethernet;

– сохранение топологии звезда при построении сети;

– поддержка традиционных сред передачи данных – витой пары и оптово-волоконного кабеля.

Недостатки технологии Fast Ethernet (унаследованы от Ethernet):

– большие задержки доступа к среде при коэффициенте использования среды выше 30–40 %, что связано с применением алгоритма доступа CSMA/CD;

– небольшие расстояния между узлами даже при использования оптоволокна, что связано с работой метода обнаружения коллизий;

– отсутствие механизмов выбора резервных связей;

– отсутствие поддержки приоритетного трафика приложений реального времени.

Технология Gigabit Ethernet представляет собой эволюционное развитие технологии Fast Ethernet. В данной технологии используются такой же формат кадра (за исключением длины кадра – все кадры с длиной меньше 512 байт расширяются до 512 байт), механизм доступа к среде CSMA/CD и топологию. Изменения (как и в технологии Fast Ethernet) произошли как на физическом уровне, так и на уровне MAC, в частности, изменились аппаратная составляющая, физическое кодирование, параметры сети.

Технология Gigabit Ethernet может использовать в качестве среды передачи как витую пару, так и оптоволокно, причём по сравнению с Ethernet и Fast Ethernet меняется как количество используемых проводников (для витой пары), так и методы кодирования. При кодировании сигнала применяются методы NRZI и MLT-3, при физическом кодировании – 8B/10B. В технологии Gigabit Ethernet (как и в Fast Ethernet) возможна как дуплексная (full-duplex mode), так и полудуплексная передача данных. В режиме full-duplex вместо CSMA/CD используется соединение P2P (точка–точка) и отсутствует понятие коллизий – каждый узел одновременно передаёт и принимает кадры данных. Работа в данном режиме возможна только при соединении сетевого адаптера с коммутатором или же при непосредственном соединении коммутаторов.

Проблемы технологии Gigabit Ethernet:

– обеспечение приемлемого диаметра сети для работы на разделяемой среде – в связи с ограничениями, накладываемыми методом CSMA/CD на длину кабеля, версия Gigabit Ethernet для разделяемой среды допускала бы длину сегмента всего 25 м;

– достижение битовой скорости 1 гбит/с на оптическом кабеле – технология Fibre Channel, физический уровень которой был взят за основу для оптоволоконной версии Gigabit Ethernet, обеспечивает скорость передачи данных всего 800 мбит/с;

– использование в качестве кабеля витой пары.

Для расширения максимального диаметра сети Gigabit Ethernet в полудуплексном режиме до 200 м был увеличен минимальный размер кадра – с 64 до 512 байт (без учёта преамбулы). Это повлекло за собой увеличение времени двойного оборота до 4095 бит, что сделало допустимым диаметр сети около 200 м при использовании одного повторителя. Для увеличения длины кадра до требуемой величины сетевой адаптер должен дополнить поле данных до длины 448 байт так называемым расширением (extention), представляющим собой поле, заполненное запрещёнными символами кода 8B/10B, которые невозможно принять за коды данных.

Для сокращения накладных расходов при использовании слишком длинных кадров для передачи коротких квитанций узлам разрешено передавать несколько кадров подряд, без передачи среды другим станциям. Такой режим получил название *Burst Mode – форсированный режим передачи данных*. Станция может передать подряд несколько кадров с общей длиной не более 65 536 бит или 8192 байт. Если станции нужно передать несколько небольших кадров, то она может не дополнять их до размера в 512 байт, а передавать подряд до исчерпания предела в 8192 байт (в этот предел входят все байты кадра, в том числе преамбула, заголовок, данные и контрольная сумма).

Достоинства технологии Gigabit Ethernet:

– увеличение пропускной способности сегментов сети до 1 Гбит/с;

– сохранение совместимости с методом случайного доступа CSMA/CD;

– сохранение формата кадра Ethernet;

– сохранение звездообразной топологии сетей и поддержка традиционных сред передачи данных – витой пары u1080 и оптоволоконного кабеля.

Недостатки технологии Gigabit Ethernet (унаследованы от Ethernet):

– большие задержки доступа к среде при коэффициенте использования среды выше 30–40 %, что связано с применением алгоритма доступа CSMA/CD;

– небольшие расстояния между узлами даже при использовании оптоволокна, что связано с работой метода обнаружения коллизий;

– отсутствие механизмов выбора резервных связей;

– отсутствие поддержки приоритетного трафика приложений реального времени.

6.2. Организация и сервис виртуальных частных сетей (VPN)

VPN (англ. *Virtual Private Network* – виртуальная частная сеть) – обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим неизвестным уровнем доверия (например, по публичным сетям), уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений передаваемых по логической сети сообщений). В зависимости от применяемых протоколов и назначения, VPN может обеспечивать соединения трёх видов: *узел-узел*, *узел-сеть* и *сеть-сеть*.

Обычно VPN развёртывают на уровнях не выше сетевого, так как применение криптографии на этих уровнях позволяет использовать в неизменном виде транспортные протоколы (такие как TCP, UDP).

Пользователи Microsoft Windows обозначают термином VPN одну из реализаций виртуальной сети – PPTP, причём используемую зачастую *не* для создания частных сетей.

Чаще всего для создания виртуальной сети используется инкапсуляция протокола PPP в какой-нибудь другой протокол – IP (такой способ использует реализация PPTP – Point-to-Point Tunneling Protocol) или Ethernet (PPPoE) (хотя и они имеют различия). Технология VPN в последнее время используется не только для создания собственно частных сетей, но и некоторыми провайдерами «последней мили» на постсоветском пространстве для предоставления выхода в Интернет.

При должном уровне реализации и использовании специального программного обеспечения сеть VPN может обеспечить высокий уровень шифрования передаваемой информации. При правильной настройке всех компонентов технология VPN обеспечивает анонимность в Сети.

VPN состоит из двух частей: «внутренняя» (подконтрольная) сеть, которых может быть несколько, и «внешняя» сеть, по которой проходит инкапсулированное соединение (обычно используется Интернет). Возможно также подключение к виртуальной сети отдельного компьютера. Подключение удалённого пользователя к VPN производится посредством сервера доступа, который подключён как к внутренней, так и к внешней (общедоступной) сети. При подключении удалённого пользователя (либо при установке соединения с другой защищённой сетью) сервер доступа требует прохождения процесса идентификации, а затем процесса аутентификации. После успешного прохождения обоих процессов, удалённый пользователь (удаленная сеть) наделяется полномочиями для работы в сети, то есть происходит процесс авторизации.

Классифицировать VPN решения можно по нескольким основным параметрам:

– По степени защищенности используемой среды:

Защищённые. Наиболее распространённый вариант виртуальных частных сетей. С его помощью возможно создать надежную и защищенную сеть на основе ненадёжной сети, как правило, Интернета. Примером защищённых VPN являются: IPSec, OpenVPN и PPTP.

Доверительные. Используются в случаях, когда передающую среду можно считать надёжной и необходимо решить лишь задачу создания виртуальной подсети в рамках большей сети. Проблемы безопасности становятся неактуальными. Примерами подобных VPN решений являются: Multi-protocol label switching (MPLS) и

L2TP (Layer 2 Tunnelling Protocol) (точнее сказать, что эти протоколы перекладывают задачу обеспечения безопасности на другие, например L2TP, как правило, используется в паре с IPSec).

– По способу реализации:

В виде специального программно-аппаратного обеспечения. Реализация VPN сети осуществляется при помощи специального комплекса программно-аппаратных средств. Такая реализация обеспечивает высокую производительность и, как правило, высокую степень защищённости.

В виде программного решения. Используют персональный компьютер со специальным программным обеспечением, обеспечивающим функциональность VPN.

Интегрированное решение. Функциональность VPN обеспечивает комплекс, решающий также задачи фильтрации сетевого трафика, организации сетевого экрана и обеспечения качества обслуживания.

– По назначению:

Intranet VPN. Используют для объединения в единую защищённую сеть нескольких распределённых филиалов одной организации, обменивающихся данными по открытым каналам связи.

Remote Access VPN. Используют для создания защищённого канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который, работая дома, подключается к корпоративным ресурсам с домашнего компьютера, корпоративного ноутбука, смартфона или интернет-киоска.

Extranet VPN. Используют для сетей, к которым подключаются «внешние» пользователи (например, заказчики или клиенты). Уровень доверия к ним намного ниже, чем к сотрудникам компании, поэтому требуется обеспечение специальных «рубежей» защиты, предотвращающих или ограничивающих доступ последних к особо ценной, конфиденциальной информации. Классификация VPN приведена на рис. 6.2.1.

Internet VPN. Используется для предоставления доступа к интернету провайдерами, обычно в случае если по одному физическому каналу подключаются несколько пользователей.

Client/Server VPN. Он обеспечивает защиту передаваемых данных между двумя узлами (не сетями) корпоративной сети.

Особенность данного варианта в том, что VPN строится между узлами, находящимися, как правило, в одном сегменте сети, например, между рабочей станцией и сервером. Такая необходимость очень часто возникает в тех случаях, когда в одной физической сети необходимо создать несколько логических сетей. Например, когда надо разделить трафик между финансовым департаментом и отделом кадров, обращающихся к серверам, находящимся в одном физическом сегменте. Этот вариант похож на технологию VLAN, но вместо разделения трафика, используется его шифрование.

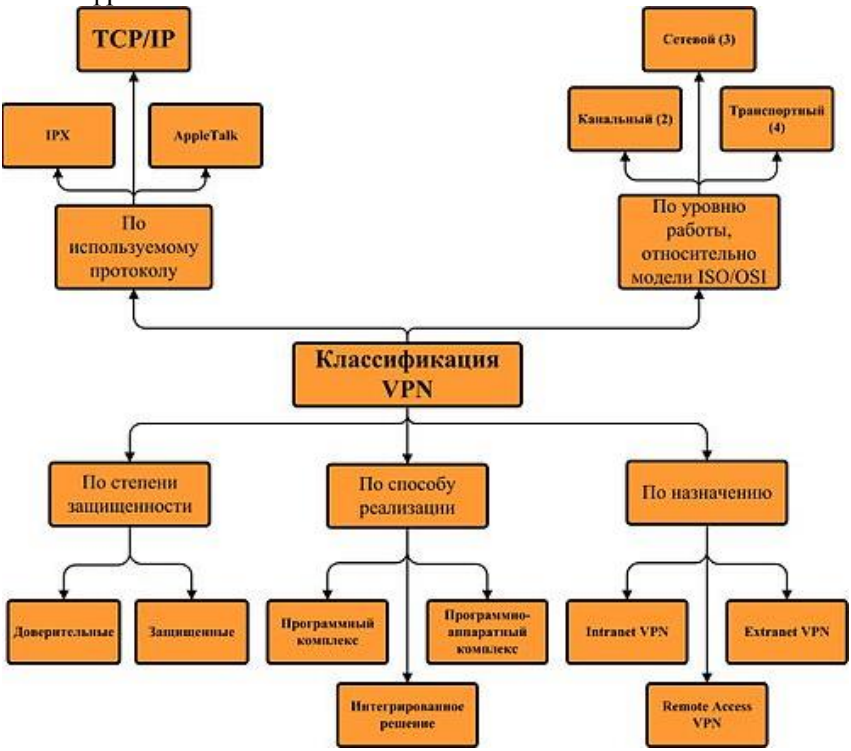


Рис. 6.2.1. Классификация VPN [7]

– По типу протокола:

Существуют реализации виртуальных частных сетей под TCP/IP, IPX и AppleTalk. Но на сегодняшний день наблюдается тенденция к всеобщему переходу на протокол TCP/IP, и абсолют-

ное большинство VPN решений поддерживает именно его. Адресация в нём чаще всего выбирается в соответствии со стандартом RFC5735, из диапазона Приватных сетей TCP/IP.

– По уровню сетевого протокола:

По уровню сетевого протокола на основе сопоставления с уровнями эталонной сетевой модели ISO/OSI.

Примеры VPN

- IPSec (IP security) – часто используется поверх IPv4.
- PPTP (point-to-point tunneling protocol) – разрабатывался совместными усилиями нескольких компаний, включая Microsoft.
- PPPoE (PPP (Point-to-Point Protocol) over Ethernet)
- L2TP (Layer 2 Tunnelling Protocol) – используется в продуктах компаний Microsoft и Cisco.
- L2TPv3 (Layer 2 Tunnelling Protocol version 3).
- OpenVPN SSL VPN с открытым исходным кодом, поддерживает режимы PPP, bridge, point-to-point, multi-client server

Пример построения безопасных локальных сетей на основе VPN.

На рис. 6.2.2 изображен вариант организации частной сети небольшой компанией с двумя филиалами.

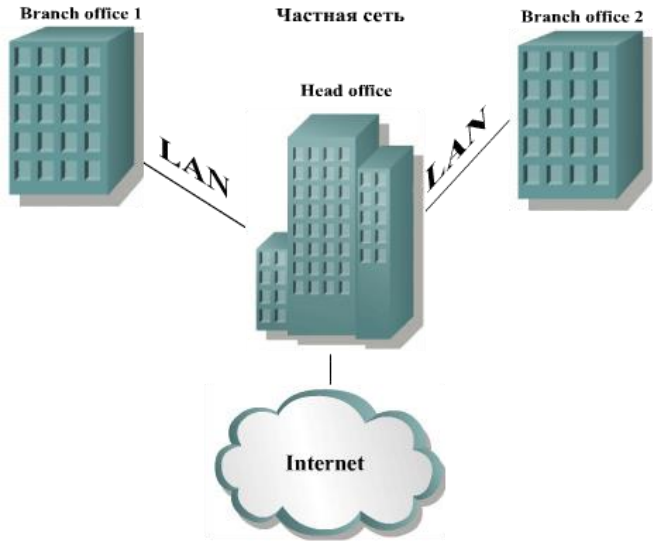


Рис. 6.2.2. Вариант организации локальной сети компании с двумя филиалами [7]

Доступ во внешнюю сеть может осуществляться как через центральный офис, так и децентрализовано. Данная организация сети обладает следующими неоспоримыми преимуществами:

- высокая скорость передачи информации, фактически скорость при таком соединении будет равна скорости локальной сети предприятия;
- безопасность, передаваемые данные не попадают в сеть общего пользования;
- за пользование организованной сетью ни кому не надо платить, действительно капитальные вложения будут только на стадии изготовления сети.

На рис. 6.2.3 изображен аналогичный вариант организации сети учреждения с филиалами, но только с использованием виртуальных частных сетей.

Рис. 6.2.3. Вариант организации локальной сети компании с двумя филиалами с использованием VPN [7]

В данном случае преимущества, приведенные для частных сетей, оборачиваются недостатками для виртуальных частных сетей, но так ли значительны эти недостатки? Давайте разберемся:

- Скорость передачи данных. Провайдеры могут обеспечить достаточно высокоскоростной доступ в Интернет, однако с локальной, проверенной временем 100 мбит сетью он все равно не сравнится. Но так ли важно каждый день перекачивать сотни ме-

габайт информации через организованную сеть? Для доступа к локальному сайту предприятия, пересылки электронного письма с документом вполне достаточно скорости, которой могут обеспечить Интернет-провайдеры.

- Безопасность передаваемых данных. При организации VPN передаваемая информация попадает во внешнюю сеть, поэтому об организации безопасности придется позаботиться заранее. Но уже сегодня существуют достаточно стойкие к атакам алгоритмы шифрования информации, которые позволяют владельцам передаваемых данных не беспокоиться за безопасность. Подробнее о способах обеспечения безопасности и алгоритмах шифрования чуть ниже.
- За организованную сеть никому не надо платить. Достаточно спорное преимущество, поскольку в противовес дешевизне пользования сетью стоят большие капитальные затраты на ее создание, которые могут оказаться неподъемными для небольшого учреждения. В то же время плата за использование Интернет в наши дни сама по себе достаточно демократичная, а гибкие тарифы позволяю выбрать каждому оптимальный пакет.

Теперь разберемся с наиболее очевидными преимуществами VPN:

- Масштабируемость системы. При открытии нового филиала или добавления сотрудника, которому позволено пользоваться удаленным доступом, не нужно никаких дополнительных затрат на коммуникации.
- Гибкость системы. Для VPN не важно, откуда вы осуществляете доступ. Отдельно взятый сотрудник может работать из дома, а может во время чтения почты из корпоративного почтового ящика фирмы пребывать в командировке в абсолютно другом государстве. Также стало возможным использовать так называемые мобильные офисы, где нет привязки к определенной местности.
- Из предыдущего вытекает, что для организации своего рабочего места человек географически неограничен, что при использовании частной сети практически невозможно.

Отдельным пунктом можно выделить создание непроводных частных сетей, а беспроводных. При таком подходе можно даже рассмотреть вариант со своим спутником. Однако в этом случае

начальные затраты достигают астрономических высот, скорость снижается фактически до скорости пользования всемирной паутиной, а для надежного обеспечения безопасности необходимо применять опять таки шифрование. И в итоге получаем туже виртуальную частную сеть, только с неимоверно высокими начальными затратами и затратами на поддержание в рабочем состоянии всего оборудования.

Способы организации.

В VPN наиболее целесообразно выделить следующие три основных способа:

1. Удаленный доступ отдельно взятых сотрудников к корпоративной сети организации через модем либо общедоступную сеть (рис. 6.2.4).

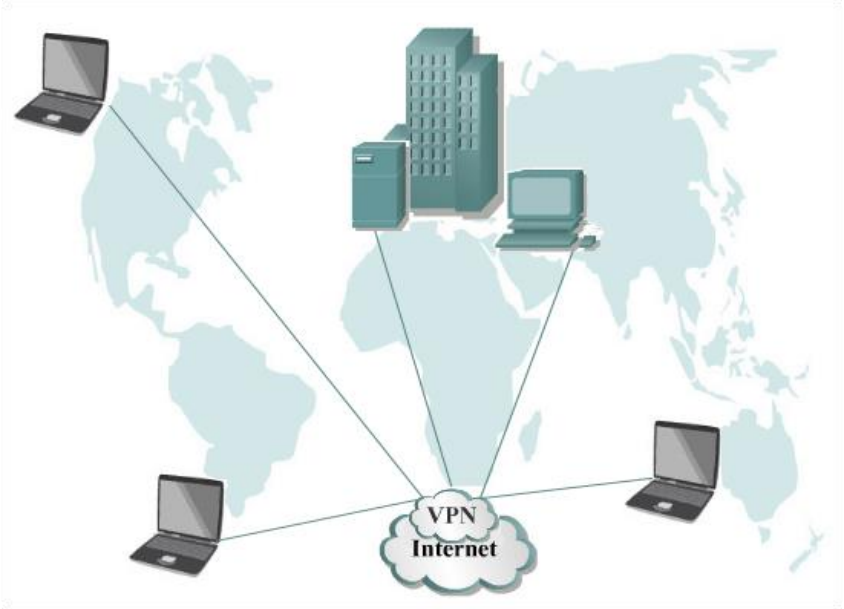


Рис. 6.2.4. Удаленный доступ отдельно взятых сотрудников к корпоративной сети организации через модем либо общедоступную сеть [7]

Организация такой модели виртуальной частной сети предполагает наличие VPN-сервера в центральном офисе, к которому подключаются удаленные клиенты. Удаленные клиенты могут работать на дому, либо, используя переносной компьютер, из любого

места планеты, где есть доступ к всемирной паутине. Данный способ организации виртуальной частной сети целесообразно применять в случаях:

- географически не привязанного доступа сотрудников к корпоративной сети организации;
- доступа к Интернету. Часто провайдеры создают для своих клиентов VPN подключения для организации доступа к ресурсам Интернет.

2. Связь в одну общую сеть территориально распределенных филиалов фирмы. Этот способ показан на рис. 6.2.5 и называется Intranet VPN.

При организации такой схемы подключения требуется наличие VPN серверов равное количеству связываемых офисов. Данный способ целесообразно использовать как для обыкновенных филиалов, так и для мобильных офисов, которые будут иметь доступ к ресурсам «материнской» компании, а также без проблем обмениваться данными между собой.

3. Так называемый Extranet VPN, когда через безопасные каналы доступа предоставляется доступ для клиентов организации. Набирает широкое распространение в связи с популярностью электронной коммерции. В этом случае для удаленных клиентов будут очень урезаны возможности по использованию корпоративной сети, фактически они будут ограничены доступом к тем ресурсам компании, которые необходимы при работе со своими клиентами, например, сайта с коммерческими предложениями, а VPN используется в этом случае для безопасной пересылки конфиденциальных данных.

Средства защиты информации – протоколы шифрования . Поскольку данные в виртуальных частных сетях передаются через общедоступную сеть, следовательно, они должны быть надежно защищены от посторонних глаз. Для реализации защиты передаваемой информации существует множество протоколов, которые защищают VPN, но все они подразделяются на два вида и работают в паре:

- протоколы, инкапсулирующие данные и формирующие VPN соединение;
- протоколы, шифрующие данные внутри созданного туннеля.

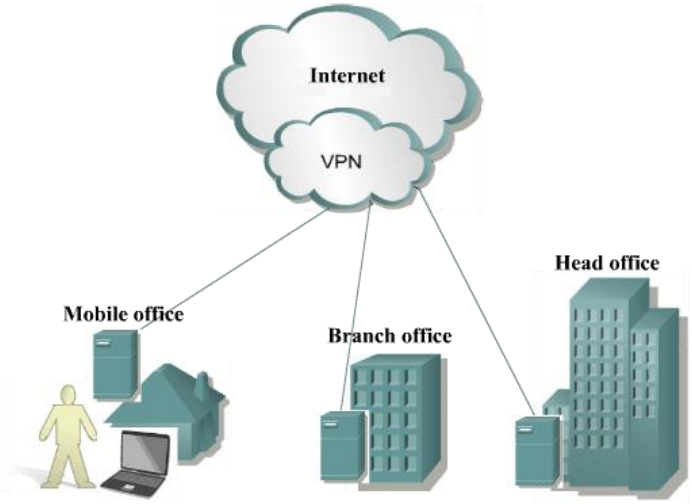


Рис. 6.2.5. Организация Intranet VPN [7]

Первый тип протоколов устанавливает туннелированное соединение, а второй тип отвечает непосредственно за шифрование данных. Рассмотрим некоторые стандартные, предлагаемые всемирно признанным мировым лидером в области разработки операционных систем, решения.

В качестве стандартного набора в данном случае предлагается сделать выбор из двух протоколов, точнее будет сказать наборов:

1. PPTP (Point-to-Point Tunneling Protocol) – туннельный протокол «точка-точка», детище Microsoft и является расширением PPP (Point-to-Point Protocol), следовательно, использует его механизмы подлинности, сжатия и шифрования. Протокол PPTP является встроенным в клиент удаленного доступа Windows XP. При стандартном выборе данного протокола компанией Microsoft предлагается использовать метод шифрования MPPE (Microsoft Point-to-Point Encryption). Можно передавать данные без шифрования в открытом виде.

Инкапсуляция данных по протоколу PPTP происходит путем добавления заголовка GRE (Generic Routing Encapsulation) и заголовка IP к данным обработанных протоколом PPP.

2. L2TP (Layer Two Tunneling Protocol) – более совершенный протокол, родившийся в результате объединения протоколов PPTP

(от Microsoft) и L2F (от Cisco), вобравший в себя все лучшее из этих двух протоколов. Предоставляет более защищенное соединение, нежели первый вариант, шифрование происходит средствами протокола IPSec (IP-security). L2TP является также встроенным в клиент удаленного доступа Windows XP, более того при автоматическом определении типа подключения клиент сначала пытается соединиться с сервером именно по этому протоколу, как являющимся более предпочтительным в плане безопасности.

Инкапсуляция данных происходит путем добавления заголовков L2TP и IPSec к данным обработанным протоколом PPP. Шифрование данных достигается путем применения алгоритма DES (Data Encryption Standard) или 3DES. Именно в последнем случае достигается наибольшая безопасность передаваемых данных, однако в этом случае придется расплачиваться скоростью соединения, а также ресурсами центрального процессора.

В вопросе применения протоколов компания Microsoft и Cisco образуют некий симбиоз, так как протокол PPTP – разработка Microsoft, но используется совместно с GRE, а это продукт Cisco, далее более совершенный в плане безопасности протокол L2TP – это не что иное, как гибрид, вобравший в себя все лучшее PPTP и L2F, разработанный Cisco. Возможно именно поэтому VPN, при правильном подходе в организации, считается надежным способом передачи конфиденциальных данных.

Литература

1. Основы построения телекоммуникационных систем и сетей: Учебник для вузов / В.В. Крухмалев, В.Н. Гордиенко, А.Д. Моченов и др. / Под ред. В.Н. Гордиенко и В.В. Крухмалева. – М.: Горячая линия-Телеком, 2004. – 510 с.
2. *Актерский Ю.Е.* Сети ЭВМ и телекоммуникации: Уч. пос. – СПб: ПВИРЭ КВ, 2005. – 223 с.
3. Телекоммуникационные системы и сети / Под ред. В.П. Шувалова. В 3-х т. – М.: Горячая линия-Телеком, 2003.
4. *Столингс В.* Компьютерные сети передачи данных. – М.: Вильямс, 2002.
5. *Скляр Б.* Цифровая связь. Теоретические основы и практическое применение, 2-е изд. / Пер. с англ. – М.: Изд. дом «Вильямс», 2003. – 1104 с.
6. *Кулябов Д. С., Королькова А. В.* Архитектура и принципы построения современных сетей и систем телекоммуникаций: Уч. пос. – М.: РУДН, 2008. – 281 с.
7. VPN [Электронный ресурс] – Режим доступа: http://ru.wikipedia.org/wiki/VPN
8. *Колдовский Н.* Построение безопасных сетей на основе VPN. [Электронный ресурс] – Режим доступа: http://www.3dnews.ru/communication/postroenie_bezopasnih_setei_na_osnove_vpn

Содержание

Contents

Научное издание

Елена Анатольевна Чернецова

СИСТЕМЫ И СЕТИ ПЕРЕДАЧИ ИНФОРМАЦИИ

Часть 1
Телекоммуникационные сети

Монография

Редактор О.С. Крайнова
Компьютерная верстка Н.И. Афанасьевой

ЛР № 020309 от 30.12.96

Подписано в печать 20.05.13. Формат 60×90 $^{1}/_{16}$. Гарнитура Times New Roman.
Печать цифровая. Усл. печ. л. 15,25. Тираж 200 экз. Заказ № 178.
РГГМУ, 195196, Санкт-Петербург, Малоохтинский пр., 98.
Отпечатано в ЦОП РГГМУ