

ЧАСТЬ I

МАГИСТРАЛЬНЫЕ СЕТИ И СЕТИ ДОСТУПА

ГЛАВА I

ДОРОЖНАЯ КАРТА СЕТЕЙ СВЯЗИ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ

Мария Ангелеш Каллежо Родригез и Жозе Энрике Габейраш

В последние годы по всему миру был запущен ряд проектов, призванных способствовать построению Интернета будущего (GENI [1] и FIND [2] в США, недавно созданный в Европе Future Internet Assembly [3] и Akari Project [4] в Японии). Во всех этих инновационных программах сообщества разработчиков предлагают новые стратегии развития существующего Интернета, которые с точки зрения поддержания статус-кво являются либо революционными, либо эволюционными. В случае революционного подхода, то есть при проектировании новых сетей, что называется, «с чистого листа», этот принцип предлагается использовать с самых первых этапов разработки (таких как обеспечение безопасности или создание новой технологии сетевой виртуализации), отбрасывая любые требования для обеспечения совместимости с существующей инфраструктурой. С другой стороны, эволюционный путь в качестве отправной точки рассматривает инфраструктуру Интернета и предполагает преобразование архитектуры сетей следующего поколения для соответствия требованиям будущих сервисов.

Цель главы – представить: 1) обзор того, как проходит эволюция сетей NGN (Next-Generation Communication Network), и 2) описание ее роли в создании Интернета будущего, а также определить основные требования к сетям будущего, кроме того, в главе обсуждается, как улучшение возможностей существующих сетей NGN позволит обеспечить эти требования.

Для этого в главе описываются критерии, которым должны соответствовать сети будущего с учетом поведения пользователей и развитием трафика Интернета, затем анализируются основные проблемы и решения, связанные с обеспечением качества обслуживания (Quality of Service, QoS). И, наконец, предлагается дорожная карта, которая должна задать направление эволюции существующих сетей в мультитранспортный Интернет будущего с множественным доступом.

1.1. Требования к сетям NGN и роль QoS в Интернете будущего

В качестве первого шага построения Интернета будущего необходимо проанализировать ожидаемую эволюцию поведения пользователей Интернета. Одна из основных черт, характеризующих планирование работы современных сетей – это высокая неопределенность эволюции требований, предъявляемых к сетям пользователями. В наши дни пользователи отличаются разнообразием. Существует множество приложений с разными требованиями (соединения P2P, потоковое вещание, IP-телефония, блоги, социальные сети, чаты, игры и пр.), доступ к которым может производиться с различных устройств (мобильные устройства, персональные компьютеры, игровые приставки и т.п.) с использованием различных способов подключения (мобильные подключения разных типов, стационарные подключения с разными способами передачи данных).

Были предприняты многочисленные попытки оценить, как ведут себя пользователи Интернета, но, вероятно, при определении потребностей Интернета будущего наилучшим подходом для предсказания пользовательских ожиданий могла бы быть классификация их поведения в зависимости от возраста. Основные группы поколений идентифицируются следующим образом:

- поколение X (1960–1970-е годы рождения) использует Интернет для веб-серфинга и доступа к электронной почте;
- поколение Y (1980-е) использует Интернет в течение всего дня, поэтому оно оценивает подключения к нему с точки зрения повсеместной распространенности и надежности;
- и, наконец, поколение Z (1990–2000-е) привыкло к технологическим переменам и гораздо лучше использует технологии связи [5]. Оно находится в сети почти постоянно, все время используя средства телекоммуникации и медиатехнологии.

Ясно, что даже на протяжении небольшого отрезка времени появляются новые модели использования сетевых технологий, и связано это с предложением все более увеличивающегося набора сервисов, а также с тем, что люди начинают пользоваться Интернетом в раннем возрасте. Следовательно, в зависимости от возможностей взаимодействия при развитии сетей следующего поколения необходимо рассматривать множество новых требований, а именно: сети будущего должны удовлетворять требованиям к трафику и требованиям надежности, которые позволят конечным пользователям полагаться на доступность подключения, повсеместность доступа к сети, безопасность при использовании услуг, гибкость в удовлетворении различных требований, прозрачность и открытость, не препятствующие развитию новых услуг, а также способность предоставлять перспективные сервисы, объединяющие в себе все эти характеристики.

Важным индикатором для оценки пропускной способности каналов, которую должны гарантировать сети будущего, являются оценки роста трафика в ближайшие годы.

По информации компании Cisco [6], как видно из рис. 1.1, можно отметить значительный рост потребностей в новых мультимедийных приложениях, таких как онлайн-игры, потоковое видео или видеоконференции, требующих более высокой производительности сетей или гарантированного QoS.

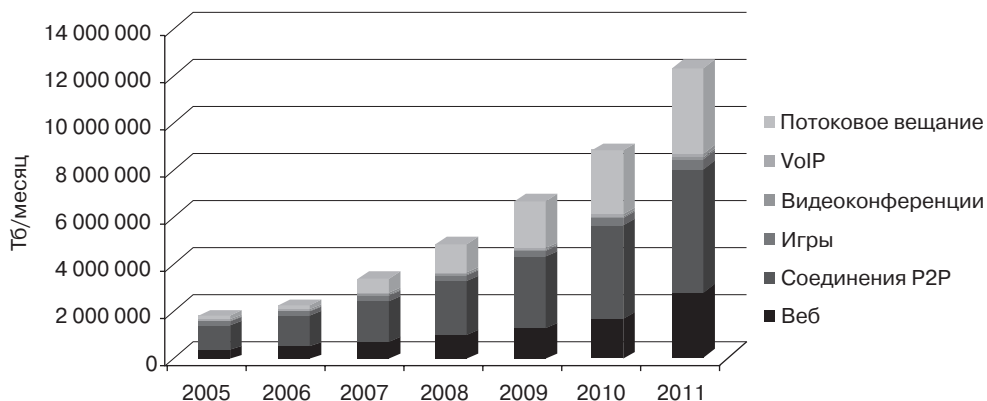


Рис. 1.1. Рост интернет-трафика по типу приложений [6]

Более того, это особенно важно для нового поколения молодых людей (упомянутого выше), которое всегда «висит» в Интернете. Для них можно организовывать собственные сервисы и обеспечивать подключение как важную услугу, за которую они готовы платить, чтобы иметь возможность доступа к широкому набору интернет-услуг. Предоставление сервисов подключения с улучшенным QoS станет ключевым элементом для бизнес-модели операторов в Интернете будущего.

Из-за той стратегической роли, которую стандарты играют в инновациях, конкуренции и регулировании в процессе создания сетей NGN важно обнаруживать изъяны в стандартизации, чтобы гарантировать честную игру участников во время создания дорожных карт новых технологий. В этом контексте ключевую роль будут играть спецификации архитектуры сетей NGN. Каковы же основные цели разработки таких сетей? Большинство специалистов согласно с тем, что они могут быть выражены следующими основными положениями:

- *предоставление услуг высокого качества.* В понятие «сети нового поколения» входит эволюция технологий доступа и организации ядра сети, способная обеспечить более высокую пропускную способность как мобильных, так и стационарных сетей. Развитие этих технологий – одна из основных тем, рассматриваемых в следующих главах;
- *эффективная среда доставки различных услуг.* Важным вопросом, связанным с сетями нового поколения, является интеграция новых сервисов в IP-сети. Все сервисы должны быть интегрированы таким образом, чтобы обеспечивать возможности операторского уровня. Это позволит операторам предоставлять услуги (как по месту работы, так и по месту жительства) с помощью одной сети.

Кроме того, должно гарантироваться предоставление таких же возможностей другим поставщикам услуг, не имеющих собственной сетевой инфраструктуры. Для эффективного выполнения такого сценария все возможности, связанные с предоставлением различных услуг в сетях NGN, должны быть реализованы таким образом, чтобы управлять ими было просто операторам и конечным пользователям;

- *интеграция мобильных и стационарных сетей и сервисов.* Поскольку конечные пользователи привыкли подключаться к Интернету посредством различных устройств и через разнотипные сети, то можно ожидать, что в будущем все сервисы станут доступны из сетей всех типов путем адаптации к характеристикам этих сетей и оконечных пользовательских устройств.

В главе планируется рассмотреть, каким образом должно развиваться управление сетями NGN, чтобы сделать возможными обеспечение QoS и конвергенцию сетевых сервисов независимо от того, используется стационарный или же мобильный доступ. Это означает, что важно избегать ненужного усложнения, которое делает принятые решения невыполнимыми на практике.

В этой главе не планируется рассматривать эволюцию сетевых технологий, которая могла бы обеспечить более развитые сетевые функции (этому посвящены остальные части книги), а основной упор будет сделан на то, как различные механизмы управления этими функциями должны быть реализованы и стандартизированы для достижения целей, поставленных перед сетями нового поколения.

Для оценки способа реализации таких механизмов необходимо рассмотреть структуру этих сетей. В документе сектора стандартизации электросвязи Международного союза электросвязи (ITU-T) [8] представлен предварительный проект архитектуры сетей NGN.

В ней можно различить следующие уровни:

- транспортный уровень, включающий:
 - транспортные функции (в сетях доступа, региональных и опорных сетях). Их развитие связано с эволюцией сетевых технологий (новые оптические решения для опорных сетей, FTTH, механизмы беспроводной связи и пр.);
 - функции управления транспортом (функции управления доступом к ресурсам, в сеть, а также присоединением к сети). В настоящее время существуют несколько организаций по стандартизации, отвечающих за направление развития этого уровня: ETSI/TISPAN [9], 3GPP [10] и ITU-T [11];
- сервисный уровень, который включает функции управления сервисами (в том числе сервисы, обслуживающие профиль пользователя) и функции обеспечения сервисов и приложений. Любой сервисный уровень может использовать возможности транспортного уровня, но наиболее четким вариантом стандартизации (а также коммерческого применения) пока является IMS (мультимедийная подсистема IP), развиваемая в проекте 3GPP, которая отвечает за обеспечение сервисов, а также использует преимущества от использования функций управления.

Таким образом, принимая во внимание предъявляемые запросы пользователей к качеству услуг и рассматривая различные технологически ориентирован-

ные решения, предлагаемые для обеспечения сетями NGN требуемого уровня QoS, одной из главнейших и сложных задач можно считать гарантированное обеспечение требований пользователей к QoS между конечными точками, вовлеченными в коммуникационный процесс, затрагивающий несколько сегментов сети. Как поясняется в документах ITU-T [7] и [8], новая архитектура должна быть разработана так, чтобы гарантировать выполнение этой цели. Ее главная особенность – объединение и синхронизация задач, выполняемых на различных уровнях сетей при передаче данных из конца в конец (end-to-end, e2e). Более того, решение также должно предусматривать взаимодействие с домашним шлюзом, поскольку этот объект отвечает за управление домашней сетью – первым и/или последним звеном в цепочке сетевых соединений, и будет играть ключевую роль в обеспечении качественной связью конечных пользователей.

В этом смысле возможности управления транспортом являются важнейшим элементом, необходимым для успешного выполнения требований QoS при сквозной передаче. Несмотря на то что многочисленные усилия по стандартизации привели к разработке и воплощению этой функции управления в документах ETSI/TISPAN [9], 3GPP [10] и ITU-T [11], общего решения до сих пор не существует, поскольку каждый из предлагаемых вариантов стандарта основывается на различных технологиях и предлагаемые решения содержат различные интерфейсы для резервирования и выделения ресурсов. Таким образом, к настоящему времени реализованы только частичные решения по обеспечению QoS в отдельных базовых технологиях, не имеющих существенного значения для передачи данных из конца в конец. Кроме того, они обычно требуют ручного конфигурирования администратором (что приводит к значительным операционным затратам). Таким образом, изменение конфигурации по интерактивным запросам пользователей при таких решениях крайне затруднено.

В следующем разделе будет приведен обзор экспериментальной системы, предназначенной для решения этой проблемы (система EuQoS). Она разработана для создания инфраструктуры обеспечения e2e QoS для конечных пользователей при работе в гетерогенных сетях. Ее разработка и внедрение позволили авторам решить проблемы, имеющиеся в настоящее время в существующих спецификациях управления транспортными функциями сетей NGN, а также предоставить ряд рекомендаций по разработке архитектуры, способной реализовать интеграцию стационарного и мобильного доступа для обеспечения IP-сервисов операторского уровня.

1.1.1. Система EuQoS как решение для обеспечения QoS при сквозной передаче данных

Главным достижением проекта EuQoS [12] стали проектирование, разработка, интеграция, тестирование и утверждение механизмов QoS в гетерогенных сетях при сохранении принципа открытости Интернета. В сущности, система EuQoS обеспечила новый подход, который позволяет оператору сети получать преимущества от того, что требования новых интернет-сервисов становятся движущей силой новых коммерческих предложений, основанных на улучшенных возможностях, затребованных конечными пользователями.

Архитектура этой системы, представленная в [13], дает возможность операторам обеспечивать качественное соединение конечных пользователей поверх гетерогенных сетей. Такой подход рассматривает нейтральность сети как требование к Интернету будущего, выдвигаемое и пользователями, и регуляторами. Следовательно, система должна давать возможность конечному пользователю затребовать от сети специфический тип услуг (реального времени, нереального времени и т.д.) независимо от конкретных услуг, предоставляемых данным провайдером. Это означает, что нельзя заранее установить связь между приложениями и уровнями сервиса. Система EuQoS способна гарантировать e2e QoS в соответствии с требованиями пользователя путем координации работы механизмов QoS, имеющихся в различных сетевых технологиях и встречающихся на пути прохождения сигнала. Это достигается определением набора хорошо известных классов обслуживания e2e, которые ставятся в соответствие с различными базовыми сетевыми механизмами в каждом коммуникационном сегменте.

Для обеспечения масштабируемости такого решения используются два подхода: долговременный период предоставления услуг (ресурсы резервируются в соответствии с интегральными показателями размеров сети и ожидаемыми потребностями пользователей) и краткосрочный период сессий, устанавливаемых конечными пользователями (в течение которых процессы, применяющиеся в технологиях доступа, должны вызываться для обеспечения соединения на долгосрочный период).

Для построения и использования маршрутов с гарантированным QoS, а также наблюдения за их состоянием в [13] была предложена многоуровневая архитектура. Она изображена на рис. 1.2, на котором показаны основные уровни и интерфейсы. Кратко опишем реализованную в ней функциональность:

- плоскость услуг обеспечивает интерфейс *QoS по требованию*, который дает возможность конечным пользователям запросить для своих приложений гарантированное QoS. Кроме того, в ней выполняются аутентификация, авторизация, управление учетными записями (Authentication, Authorization and Accounting, AAA) и начисление платы за услуги. Этот интерфейс обеспечивает QoS как службу, которая может использоваться любым приложением или другой службой без необходимости интеграции в плоскость услуг полного стека прикладной сигнализации;
- плоскость управления отвечает за работу процедур управления для обеспечения QoS как на этапе запроса данных, так и на этапе их получения. Она разделена на два уровня;
- уровень, независимый от сетевых технологий, предоставляет опорную точку, которая используется плоскостью услуг и домашним шлюзом, чтобы запрашивать резервирование ресурсов. Он управляет абстракцией топологии домена, поддерживает набор правил оператора, определяет местоположение пользователей и взаимодействует с другими доменами, вовлеченными в маршрут e2e с гарантированным QoS, используя интерфейс, предоставляемый другими независимыми от сетевых технологий уровнями;



Рис. 1.2. Архитектура EuQoS (опорные точки и протоколы)

- уровень, зависимый от сетевых технологий, предоставляет хорошо известный интерфейс для независимых уровней и соотносит классы обслуживания e2e со специфическими базовыми механизмами сети. Он также применяет специальные алгоритмы входного контроля (например, в мобильных сетях может учитывать физические параметры, а в стационарных эта возможность опциональна) и взаимодействует с сетевым оборудованием для настройки политики QoS.

Согласно замыслу и оценке системы EuQoS, следующие принципы должны обеспечиваться при создании спецификации возможностей управления сетями будущего:

- 1) должен предоставляться набор хорошо известных не зависящих от технологий классов обслуживания. Эти e2e-классы обслуживания должны допускать реализацию сервисов при использовании различных технологий без необходимости применения специфических для каждого типа сети решений. Такие классы перечислены в [14];
- 2) необходимо провести разграничение между различными уровнями и дать четкое определение опорных точек на каждом уровне или плоскости. Это позволит реализовать многочисленные сценарии поверх одной и той же инфраструктуры (с возможностями прямого доступа к плоскости управления для домашнего шлюза или провайдера услуг; домашний пользователь сможет использовать интерфейс QoS по требованию);
- 3) необходимо различать механизмы, зависящие и не зависящие от сетевых технологий. Это сделает внедрение решений более простым. Поставщики услуг или вендоры должны лишь обеспечить общий интерфейс для применения возможностей QoS в их системах управления. Кроме того, если в будущем такой интерфейс будет предоставляться сетевым оборудованием, разработка специальных систем управления окажется ненужной.

Все эти принципы применимы к проектированию систем управления с целью обеспечения гарантированного QoS, но некоторые из них можно использовать и при разработке других элементов.

1.2. Проблемы развития сетей NGN и связанные с этим рекомендации

На основании опыта авторов в разработке, внедрении и проверке систем, способных обеспечить услугу QoS в гетерогенных сетях, в этом разделе определяется ряд проблем, связанных с разработкой сетей NGN. Кроме того, рассматриваются возможности и даются рекомендации по их преодолению, способные ускорить процессы стандартизации некоторых инициатив ИТУ-Т по развитию сетей NGN в области обеспечения возможности конечных пользователей управлять услугами, такими как AMS (Advanced Multimedia System), а также любой другой процесс стандартизации.

1.2.1. Проблемы эффективного обеспечения QoS

В результате исследований различных решений и архитектур были обнаружены возможные узкие места в существующих стандартах и коммерческих решениях.

Проблема 1: интеграция прикладной сигнализации в сетях NGN. Большинство современных спецификаций сетей NGN предполагает интеграцию прикладной сигнализации. Это означает, что для предоставления QoS некоторым специфическим службам, такая сеть должна не только знать о существовании этой сигнализации, но также участвовать в процессе согласования служб между собой (при выборе кодеков, обнаружении пользователей и др.).

Широко известным примером является IMS, описывающая использование протокола SIP (Session Initiation Protocol) как единственного способа взаимодействия с функцией P-CSCF (Proxy Call Session Control Function – первая точка взаимодействия конечного пользователя с управляющими объектами IMS). Если обнаружится, что протокол SIP не подходит для работы с различными приложениями или сервисами, основа управления IMS становится бесполезной в качестве плоскости услуг (или на уровне приложений) NGN в сетях Интернета будущего для любых типов приложений. К тому же есть жалобы от разработчиков приложений в связи с недостатком спецификаций, описывающих действия в случае обнаружения сигнализации приложения.

Более того, необходимо учитывать большое разнообразие прикладных протоколов, используемых в настоящее время в Интернете (MSN, Skype, потоковые P2P-приложения и т.п.). Сохранение существующих принципов разработки может привести к появлению сложных систем, в которых для взаимодействия с наиболее популярными пользовательскими приложениями должны быть интегрированы несколько шлюзов, причем не обязательно основанных на протоколе SIP. Наконец, если принять во внимание, что в Интернете будущего пользователи будут не только потреблять услуги, но и предоставлять их и даже создавать новые, можно ожидать, что в будущем появятся разнообразные приложения, не использующие IMS.

Подводя итог, отметим, что требование интеграции в NGN прикладной сигнализации может привести к двум основным сценариям:

- сложные системы, ответственные за управление многочисленными протоколами сигнализации или с несколькими шлюзами, в которых предоставление перспективных услуг для новых (и, возможно, популярных среди пользователей) приложений будет занимать больше времени. Этот сценарий может привести к появлению решений, управление которыми затруднено из-за их сложности, а также недостаточной масштабируемости;
- «огороженные сады» (walled gardens), где только отдельные услуги будут предоставляться по принципу QoS, теряя при этом открытость как основной принцип Интернета. Вероятно, такой вариант не станет привлекательным для операторов, поскольку они не смогут предложить своим конечным пользователям передовые услуги соединения (пользователи главным критерием качества услуг сервис-провайдера считают возможность взаимодействия с другими точками сети), а также предоставить свои сетевые ресурсы приложениям третьих сторон.

Проблема 2: нечеткие спецификации интерфейсов. В текущих рекомендациях и спецификациях имеются явно выраженные слабые места в описании спецификаций интерфейсов и опорных точек. Эту проблему можно выразить следующими положениями:

- существуют три основных подхода в стандартизации, описывающие функционал управления транспортом в сетях. Каждый из подходов предлагает свой, отличный от других, интерфейс, что приводит к появлению проблем взаимодействия. Это хорошо известная проблема, и даже появляются попытки найти общее для всех решение (например, наблюдается попытка интеграции 3GPP и ETSI/TISPAN);
- некоторые интерфейсы не имеют точного определения и оставлены для дальнейшего изучения (как, например, интерфейс взаимодействия между доверенным CPE (Customer Premises Equipment) и RACF (Resource and Admission Control Functions) в Y.2111, что важно для полной интеграции домашних шлюзов с плоскостью управления оператора);
- другие интерфейсы определены только в терминах методов, параметров и требований к транзакциям. Какие протоколы выбирать для этих интерфейсов, пока неясно.

Такое отсутствие четких спецификаций опорных точек может привести к тому, что разные вендоры будут предлагать свои собственные решения для системы в целом. В свою очередь это повлечет за собой проблемы согласования между оборудованием различных производителей, что, безусловно, приведет к проблемам взаимодействия нескольких поставщиков (то есть возможности управления одного производителя будут совместимы с оборудованием двух различных поставщиков) или при взаимодействии между различными доменами сети.

В качестве примера можно упомянуть рекомендацию ITU-T Y.2111, в которой подробности взаимодействия между различными RACF (опорная точка Ri) оставлены для изучения в будущем. Это взаимодействие является обязательной, если разные домены, вовлеченные в сквозную передачу, совместно используют инфор-

мацию QoS и определяется другими органами стандартизации и реализовано некоторыми поставщиками, в частности:

- ETSI/TISPAN предоставило протокол RCIP (Resource Connection Initiation Protocol), который предложен, чтобы разрешить взаимодействие между различными RACS (Resource Admission Control Subsystem, аналогична ITU-T NGN RACF) в ходе резервирования ресурсов для гарантирования определенного уровня QoS;
- в ходе работы над книгой изготовитель телекоммуникационного оборудования¹ выпустил коммерческую реализацию RACS (модуль ETSI/TISPAN, аналогичный ITU-T NGN RACF), который предоставляет интерфейс, основанный на RCIP, для связи между различными диспетчерами ресурсов.

При таком сценарии весьма вероятно, что окончательная спецификация взаимодействия, основанная на протоколе RCIP, будет отличаться от его реализации в коммерческом оборудовании, выпускаемом сейчас, и в будущем станет источником проблем при организации взаимодействия.

Проблема 3: нечеткие спецификации функциональных модулей. Текущие спецификации некоторых модулей фактически не описывают общие конечные автоматы модулей и функций. Такой сценарий может привести к появлению решений, привязанных к производителю. Данный факт приведет к соперничеству не только из-за проблем взаимодействия оборудования различных поставщиков, но также из-за того, что будет иметь место перекрывающаяся функциональность или, наоборот, изъяны в ней.

Таким образом, возникает необходимость в руководствах и рекомендациях, облегчающих определение спецификаций интерфейсов и процесс разработки, в целом. Это означает, что определение и стандартизация алгоритмов не приведут к конкуренции между различными поставщиками и, как минимум, четко определят входные и выходные параметры, а также будут содержать описание процессов, которые будут вызываться в каждом модуле.

Проблема 4: закрытые интерфейсы конфигурирования сетевого оборудования. Одним из ключевых моментов в предоставлении QoS является координация различных механизмов предоставления этой услуги, доступных в различных сетевых технологиях. Для такой координации важен доступ к сетевому оборудованию, вовлеченному в процесс сквозной передачи данных и не менее важно иметь доступные механизмы, передающие команды конфигурирования различного оборудованию.

К примеру, во время интеграции системы EuQoS в некоторые сетевые технологии оказалось необходимым обратить внимание на ряд проблем интеграции в связи с отсутствием общих опорных точек в различных элементах сети. В частности, при интеграции технологии UMTS имелись различные опорные точки для взаимодействия с GGSN, зависящие от провайдера. Это привело к необходимости для EuQoS при настройке контекста PDP полагаться на пользовательский интерфейс UMTS, который является единственным удовлетворяющим требованиям стандартов решением по интеграции встроенных в UMTS механизмов QoS.

¹ Huawei RM9000 Resource Manager.

С похожими проблемами пришлось столкнуться при интеграции технологий Ethernet, при которой различные стратегии взаимодействия с коммутаторами привели к усилившейся зависимости от поставщика оборудования.

Если в сетевом оборудовании имеются закрытые интерфейсы, будет сложно организовать предоставление гарантированного QoS из-за сильной зависимости от специфических решений поставщиков, которые, вероятно, будут предлагать для нового оборудования свои собственные системы управления. Если к этому присовокупить отсутствие четких спецификаций интерфейса между различными уровнями управления (в частности, между RACS, реализованных в различных доменах), это может в целом привести к проблемам при организации взаимодействия (как между технологиями, так и между сетевыми доменами), делая услугу предоставления QoS при передаче данных из конца в конец почти невозможной.

Проблема 5: неопределенная среда регулирования. В настоящее время реализовано множество сценариев регулирования и наблюдается четкая тенденция к усилению некоторых способов разделения сервисов и сетевых операций. При таком сценарии все системы, основанные на вертикальной интеграции сервисов и сетей, вероятно, окажутся неработоспособными. Таким образом, чтобы гарантировать обоснованность предложений NGN в различных сценариях, необходима четкая спецификация интерфейсов между уровнем сервисов и сетевым уровнем. Это означает, что спецификации NGN должны отвечать требованиям, предъявляемым различными ролями, которые могут возникнуть в разных бизнес-моделях, их появление можно предсказать в недалеком будущем.

В этом контексте наличие четких спецификаций опорных точек будет обязательным.

1.2.2. Рекомендации и предложения по обеспечению QoS в NGN

В соответствии с проблемами, показанными в разд. 1.2.1, и на основе опыта авторов в данном разделе приведены рекомендации, которые позволяют интегрировать возможности предоставления QoS при сквозной передаче данных в концепцию NGN ITU-T.

Все рекомендации даны с учетом того, что и конечные пользователи (которые хотят улучшить свое качество восприятия (Quality of Experience, QoE) в Интернете), и регуляторы (чья позиция явно выражает неприятие «огороженных садов») будут требовать обеспечения прозрачности сети.

Рекомендация 1: четко анализировать знания пользователей и их требования. В эпоху Интернета поведение конечных пользователей стало трудно прогнозируемым. Операторы являются свидетелями эволюции от ситуации с одной услугой и хорошо предсказуемыми требованиями до состояния с множеством услуг, большинство из которых создается пользователями, и их требования являются весьма непредсказуемыми. Следовательно, следует оценить требования пользователей и тенденции развития в настоящее время. Важно провести маркетинговые исследования, чтобы узнать ожидания конечных пользователей и оценить, как они могут использовать новые возможности QoS с новыми услугами. В ходе исследований должны быть получены ответы на следующие вопросы:

- 1) каковы знания конечных пользователей о QoS? Что они действительно знают об этой концепции?
- 2) какие атрибуты соединения из конца в конец (безопасность, надежность, доступность, восстановление после сбоев и пр.) могут быть востребованы конечными пользователями?
- 3) какие устройства (iPhone, PDA, ноутбуки и пр.) конечные пользователи используют чаще всего? Как много особенностей услуги должен оговаривать пользователь?
- 4) какие сервисы Интернета более востребованы конечными пользователями? Какая величина добавленной стоимости услуг оператора для них приемлема?

Ответив на вопросы, можно описать текущее использование Интернета и сделать вывод о требованиях доступа к Интернету будущего. Для этого важно решить следующие проблемы:

- определить имеющиеся ограничения доступа в Интернет в терминах QoS с точки зрения конечного пользователя;
- определить новые требования к производительности сети, особенно принимая во внимание такие новые услуги, как телевидение высокой четкости (и ассоциированные с ним требования к QoS), 3D- или P2P-приложения. Это позволит определить классы обслуживания Интернета будущего в терминах e2e QoS (IPTD, IPDV и IPLR) и других характеристик производительности (доступность, безопасность, время восстановления после сбоев и пр.);
- первоначальный вариант спецификации (draft) интерфейсов конечного пользователя, который позволит создать услуги с расширенными сетевыми возможностями.

Такой анализ обязателен при спецификации опорных точек конечного пользователя AMS, при этом надо обеспечить поддержку запросов от различных приложений Интернета с различными требованиями к QoS.

Рекомендация 2: QoS не должно противопоставляться нейтральности сети. Эволюция транспортных технологий NGN, предложенная в виде сетевых сервисов, создает прекрасные возможности для инноваций, но не только для операторов (предоставляющих свои собственные услуги), но также для конечных пользователей и поставщиков услуг. Если эти возможности предоставляются на равных условиях, QoS становится явным стимулом для продвижения услуг любой стороне.

Фактически для гарантированного QoS не обязательно сокращение трафика приложений, не использующих QoS. Для соответствия этому требованию важно предоставить конечному пользователю и поставщику услуг понятный интерфейс (или набор интерфейсов), позволяющий ему выбирать, какой уровень QoS требуется для каждого из его потоков данных. Таким образом, услуга QoS будет предоставляться не только для услуг, оказываемых этим оператором, но также и для других услуг Интернета согласно требованиям конечного пользователя.

Если инфраструктура соответствует этим требованиям, то у оператора сети может появиться возможность продвигать свои собственные службы, а также использовать приложения третьих сторон (интернет-услуги), побудившие его пред-

лагать улучшенный сервис подключений с QoS. В сценарии, когда QoS предлагается как услуга, необходимо обеспечить наличие механизмов, гарантирующих эффективное предоставление возможностей, и, следовательно, такие возможности мониторинга должны быть учтены при разработке самой системы.

Рекомендация 3: предварительные наброски новых бизнес-моделей. В [15] утверждается, что:

«Можно учиться у прошлого. Для некоторых членов сообщества разработчиков настоящим потрясением в последние несколько лет стала неудача попытки описать как открытую услугу, предоставляемую из конца в конец. Это последовало за неудачной попыткой сделать такой же услугой широко вещание в сети. Проанализируем эти попытки.

Вот одно из предположений. Для провайдеров внедрение QoS означает, что они должны будут потратить деньги на модернизацию маршрутизаторов, произвести дополнительные управленческие и операционные расходы. И это реальные затраты. Гарантий увеличения прибыли нет. Зачем в таком случае рисковать и делать инвестиции?

Если бы пользователи могли обеспечить эффективное конкурентное давление на провайдеров, выбирая из них, то страх и жадность могли бы подтолкнуть их к инвестированию, но конкурентного давления в этом случае недостаточно. С другой стороны, если провайдеры используют закрытые механизмы QoS, не делая их открытыми для всех, они значительно увеличивают возможности получения доходов. К примеру, если они внедрят механизмы QoS, но будут применять их только для тех приложений, которые продают сами, то смогут уменьшать открытость Интернета и обеспечат возможность для вертикальной интеграции. Если интернет-телефония требует для своей работы QoS, и провайдеры включают эту услугу только для своей версии телефонии, то они могут устанавливать монопольные цены».

Это утверждение дает нам основание предполагать, что развитие текущей модели Интернета может проходить двумя способами: классический Интернет и Интернет высокого качества («премиум-класса»), в котором провайдеры будут вкладывать деньги в оборудование NGN, чтобы гарантировать высокие показатели QoS.

С общественной точки зрения это означало бы потерю Интернетом универсальности. В этом контексте описание бизнес-модели, призванной обеспечивать лучшее использование ресурсов и прибыль, является обязательным.

Также должно быть учтено развитие общества. При изучении новое поколение было охарактеризовано как «постоянно подключенное», использующее широкий набор сервисов и приложений в Интернете (социальные сети, файлообмен, потоковое видео, игры и пр.). Таким образом, эти люди должны высоко ценить прозрачность этих сервисов, их надежность и способность обеспечивать многочисленные требования к профилям трафика, что безусловно может стать отправной точкой для описания бизнес-моделей, которые могли бы гарантировать внедрение QoS для передачи из конца в конец.

С другой стороны, некоторые поставщики услуг, не объединенные с сетевыми провайдерами, могли бы сотрудничать с ними (из числа тех, которые контроли-

руют «последнюю милю») для предоставления операторских услуг. Это может представлять определенный интерес для сервисов, использующих потоковую передачу¹ или игровые приложения².

Необходимо отметить, что спецификации этих бизнес-моделей должны также принимать во внимание развитие соглашений о взаимодействии.

Рекомендация 4: продвижение стандартизации коммерческого оборудования и реализация в нем опорных точек. Как уже говорилось, одной из ключевых особенностей предоставления QoS является координация различных механизмов предоставления данной услуги, доступных в различных технологиях. Для такой координации важно иметь доступ к сетевому оборудованию, задействованному в процессе передачи данных, и возможность внести небольшие изменения в различное оборудование.

Для достижения поставленной цели необходимо подробное описание опорных точек в различном сетевом оборудовании для использования встроенных в него механизмов обеспечения сквозного QoS. Это поможет избежать схожих проблем, с которыми столкнулись в проекте EuQoS при интеграции UMTS и технологий Ethernet, описанных в предыдущем разделе.

Как первый шаг в этом направлении некоторые компании³ недавно сделали свои интерфейсы и операционные системы открытыми и предоставили третьей стороне возможность интегрировать различные приложения, такие, например, как стратегии управления пропускной способностью.

Рекомендация 5: разработка общей структуры предоставления сквозного QoS – модели взаимодействия IP. Чтобы соответствовать требованиям QoS, важно гарантировать, что услуга предоставляется на протяжении всего маршрута, из конца в конец. Таким образом, необходима координация между различными доменами и технологиями по меньшей мере при использовании различных технологий доступа. В таком случае следует определить общие принципы для взаимодействия по протоколу IP в качестве основы для синхронизации механизмов QoS, использующихся в различных доменах, и их влияние на протоколы. Как указано в [8], система EuQoS представляет свою технологию междоменной маршрутизации, основанную на протоколе EQBGP и дающую возможность различным доменам объявлять о своих возможностях обеспечения QoS.

Для гарантии предоставления e2e QoS в любой сети важно определить классы обслуживания (class of services, CoS), которые были бы хорошо известны всем доменам (отсюда следует, что каждый класс они будут реализовывать в соответствии

¹ В документе <http://www.layer3media.com/joost/joost-network.pdf> сервис Joost описывает свой вариант архитектуры обеспечения услуги VoD (Video-on-Demand), основанный на сервисе P2P, но в заключение заявлено, что возможное сотрудничество с сетевыми провайдерами может быть выгодным с точки зрения контроля возможностей, доступных на «последней миле» (не управляемой поставщиком услуг).

² Сервис Xbox Live может использовать возможности QoS для того, чтобы улучшить QoE конечного пользователя.

³ Компании Juniper и Cisco недавно выпустили SDK для своих операционных систем.

со своими стратегиями), чтобы определить правила объединения для инфраструктуры управления.

Рекомендация 6: реализация предварительных версий некоторых интерфейсов. Как отмечалось ранее, одной из основных проблем разработки архитектуры NGN является составление спецификаций интерфейсов и их реализация. Для их успешной реализации необходимо провести тестирование взаимодействия. По этой причине можно рекомендовать создание базовых модулей для последующего тестирования на совместимость.

Рекомендация 7: общая дорожная карта сетей следующего поколения. Для обеспечения согласованности действий в процессе стандартизации NGN, ITU-T, ETSI/TISPAN и 3GPPP требуется представить четкий план развития технологий, бизнес-моделей, условий пользователей и пр., которые должны учитываться или будут учтены в ближайшем будущем. Это позволит согласовать исследовательские работы по стандартизации, а также усилия основных поставщиков по внедрению новых технологий.

В целом этот план должен помочь различным участникам (операторам, вендорам, регуляторам и пр.) определить, когда можно ожидать появления стандартов и каких именно.

1.3. Дорожная карта сетей следующего поколения

Для согласованного и эффективного развития сетей NGN как ключевой компоненты Интернета будущего, согласно рекомендациям, представленных в предыдущем разделе, необходимо подробно изложить план, который определит развитие технологий NGN. В рамках проекта EuQoS такая дорожная карта была разработана с учетом состояния технологий на тот момент. Она представлена в [16], позже она была обновлена с учетом последних исследований (рис. 1.3).

Дорожная карта развития технологий учитывает технологические перспективы и перспективы для бизнеса. В частности, были рассмотрены следующие направления развития: бизнес-модели, требования пользователей, плоскость услуг, плоскость управления, базовые сетевые технологии и операционные возможности.

Тенденция развития 1: анализ различных бизнес-моделей. При определении путей развития сетей NGN анализ подходящих бизнес-моделей является обязательным. Важно четко определить, как можно стимулировать разработку новых возможностей в различных заинтересованных кругах.

Для того, чтобы построить Интернет будущего с дополнительными возможностями, важно понять, какие стороны получают от этого преимущества и какую прибыль можно будет получить как в прямой форме (например, если клиенты непосредственно оплачивают услуги), так и косвенно (доходы за счет рекламы). Это могло бы привести к описанию требований, предъявляемых к открытым интерфейсам (с экономической точки зрения) и к развитию существующих моделей взаимодействия.

Тенденция развития 2: анализ требований конечных пользователей. Как отмечено в рекомендациях, анализ поведения конечных пользователей и оценка их будущих предпочтений являются необходимыми для успеха сетей NGN. Это требование может охватывать многие аспекты, такие как безопасность, удобство интерфейса и т.д.

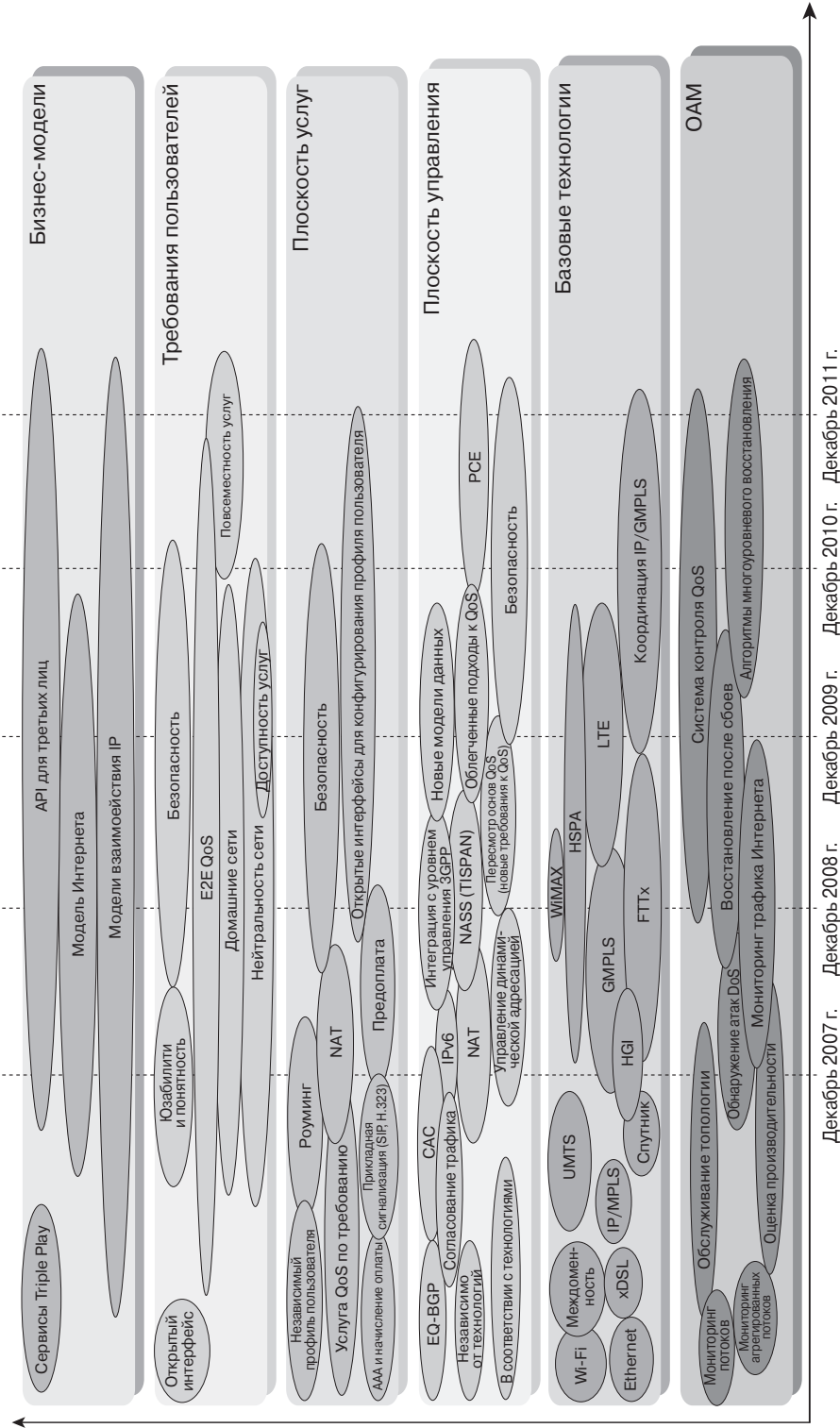


Рис. 1.3. Дорожная карта сетей NGN

Тенденция развития 3: эволюция плоскости услуг. Это направление развития сосредоточено на анализе функций, которые должна обеспечивать плоскость управления сетей NGN. Технические функции разрабатываются согласно бизнес-моделям и требованиям пользователей.

В данной теме рассматриваются вопросы управления профилями пользователей и механизмами AAA.

Тенденция развития 4: эволюция плоскости управления. Необходимо провести анализ механизмов и возможностей, которые должны быть разработаны и интегрированы для внедрения услуги гарантированного QoS. При развитии плоскости необходимо учитывать операции с точки зрения разных масштабов времени (например, для резервирования всех потоков или действий, совершаемых по запросу пользователя).

Тенденция развития 5: эволюция базовых сетевых возможностей (транспортные возможности). По мере появления новых сетевых технологий важно определить момент, когда будут созданы решения, способные взаимодействовать с новым сетевым оборудованием, и использовать их встроенные механизмы QoS.

Кроме того, важно убедиться, что различные сетевые технологии могут взаимодействовать и работать согласованно. Примером может служить согласование работы оптических систем и магистральных IP-маршрутизаторов.

Тенденция развития 6: эволюция OAM (Управление, администрирование и обслуживание [Operation, Administration and Maintenance]). Понятие OAM включает в себя все функции, которые должна выполнять коммерческая система, главным образом в области безопасности и аудита. Это ключевое требование для гарантированного отслеживания доставки услуг, использующих механизмы QoS.

Литература

1. <http://www.geni.net/>.
2. <http://www.nets-find.net/>.
3. <http://www.future-internet.eu/>.
4. <http://akari-project.nict.go.jp/eng/index2.htm>.
5. The generation Z connection: Teaching information literacy to the newest net generation, Teacher Librarian. Available online. February 2006.
6. Cisco, Global IP traffic forecast and methodology 2006–2011, January 2008.
7. ITU-T Y.2001, General overview of NGN, December, 2004.
8. ITU-T Y.2012, Functional requirements and architecture of the NGN release 1, June 2006.
9. <http://www.etsi.org/tispan/>.
10. <http://www.3gpp.org/>.
11. <http://www.itu.int/en/pages/default.aspx>.
12. <http://www.euqos.eu/>.
13. M. A. Callejo, J. Enriquez, et al., EuQoS: End-to-end QoS over heterogeneous networks, *ITU-T Innovations in NGN – Future Network and Services*, Geneva, pp. 177–184. May 2008.

14. X. Masip, J. Enriquez, M. A. Callejo, et al., The EuQoS system: A solution for QoS routing in heterogeneous networks. *IEEE Communi. Maga.*, Vol. 45, pp. 96–103, February 2007.
15. D. D. Clark, J. Wroclawski, K. Sollins, and R. Braden, Tussle in cyberspace: Defining tomorrow's Internet, SIGCOMM 2002.
16. M. A. Callejo and J. Enriquez, Bridging the standardization Gap to provide QoS in current NGN architectures, *IEEE Communi. Maga.*, Vol. 46, pp. 132–137, October 2008.

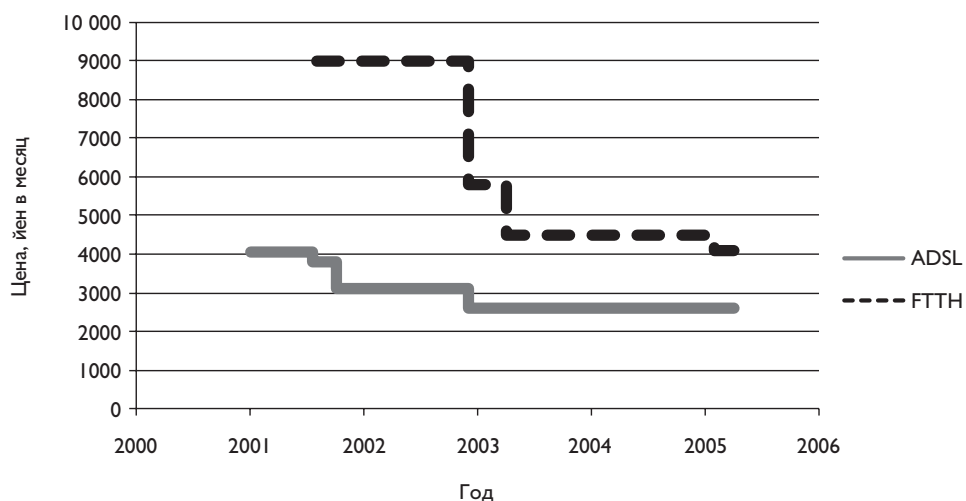
ГЛАВА 2

ГЛОБАЛЬНАЯ СЕТЬ СО СПЛОШНЫМ ПОКРЫТИЕМ: ИНФРАСТРУКТУРА СЕТИ ДАТЧИКОВ И ИСПОЛНИТЕЛЬНЫХ МЕХАНИЗМОВ

*Хироши Сайто, Масато Мацуо, Осами Кагами, Шигеру Кувано,
Дайсэй Учида и Юйчи Кадо*

2.1. Введение

Рост трафика Интернета был обеспечен возрастающим темпом создания проводных и беспроводных линий доступа, что явилось следствием конкуренции между провайдерами в предоставлении услуг высокоскоростной связи, например, при переходе от ADSL к FTTH или от третьего поколения сотовых сетей к четвертому. Как результат этой сильной конкуренции число абонентов широкополосной связи быстро увеличивалось, цены на услуги связи снижались, хотя скорость доступа увеличивалась (рис. 2.1).



Источник данных:

<http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h17/html/H1401000.html>

Рис. 2.1. Стоимость широкополосного доступа в Японии (указаны цены типичных услуг ADSL/FTTH, предоставляемых компанией NTT-East). Источник данных: <http://www.johotsusintokei.soumu.go.jp/whitepaper/html/H1401000.html>

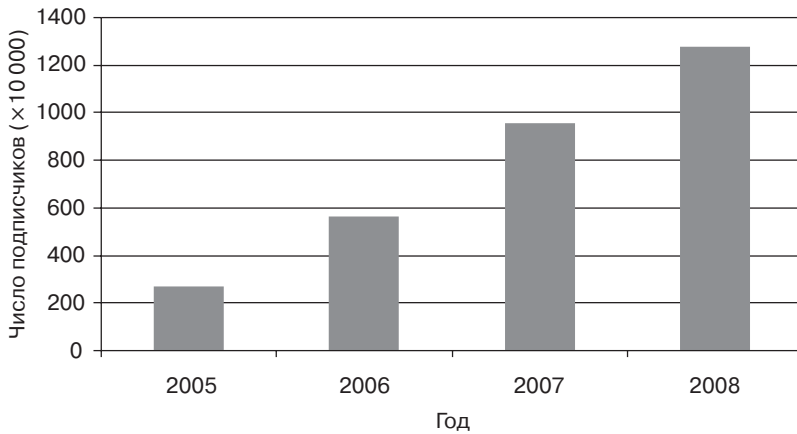


Рис. 2.2. Число подписчиков на тарифы с постоянной абонентской платой. Число подписчиков на пакет услуг rake-houdai компании NTT docomo, в котором установлена фиксированная цена, не зависящая от числа переданных и полученных пакетов данных. Источник данных: <http://www.ntt.co.jp/ir/library/annual/pdf/08/p9.pdf>

Кроме того, многие провайдеры установили фиксированные тарифы на услуги связи. Такая оплата использовалась в сетях проводной связи, но провайдеры услуг сотовой связи также стали ее вводить преимущественно для услуг передачи данных (рис. 2.2). При такой системе оплаты выручка операторов связи не увеличивается, даже если объем трафика значительно растет. Однако тем провайдерам, которые уже ввели безлимитные тарифы, сложно от них отказаться, поскольку они привлекательны для клиентов с большим объемом трафика и являются важным фактором для их удержания.

Безлимитные тарифы и снижение цен подразумевают снижение доходов провайдеров, когда прекращается рост числа подписчиков на услуги широкополосного доступа. Таким образом, провайдерам необходимо искать другие источники доходов, требующих новых механизмов подключения, не через существующие уже способы широкополосного доступа к сети. Это обусловлено тем, что уже известные способы не могут стать новыми источниками дохода.

Одной из концепций компьютерных технологий является идея «вездесущих (повсеместных) вычислений» (ubiquitous computing) [1]. Эта концепция требует, чтобы компьютеры постоянно находились на службе у людей в их повседневном окружении. В обществе, где эта концепция претворена в жизнь, компьютеры встроены во множество устройств/объектов с датчиками и исполнительными устройствами (актюаторами) незаметно (прозрачно) для общества. Они работают и взаимодействуют друг с другом для предоставления различных услуг. Концепция «вездесущих вычислений», созданная в 1980-х годах, является в настоящее время не только мечтой. Последние исследования в области компьютерных технологий, электроники и микромеханики дают возможность создавать маленькие, дешевые, потребляющие мало энергии от встроенных батарей датчики и исполнительные устройства с вычислительными возможностями. Такие

компоненты могут быть подключены к чему угодно и размещены везде, где потребуется. Мы будем создавать сети с использованием таких узлов, способных обеспечивать подключение в любое время благодаря использованию беспроводных каналов, обнаруживать и распознавать интересные нас события, а также управлять машинами и устройствами [2–4]. Связывание общества такими глобальными сетями — это технический вызов для работников отрасли связи и компьютерных специалистов, а технологии, необходимые для создания подобного общества, имеют большой потенциал нового источника доходов для сетевых операторов.

В этой главе описывается сеть, получившая название глобальной сети со сплошным покрытием (*wide area ubiquitous network, WAUN*) [5]. Объективной целью создания этой сети была повсеместная реализация сетевой инфраструктуры датчиков и исполнительных для создания объединенного сетями общества.

2.2. Целевое применение и рынок сбыта

Сеть WAUN может быть полезна для реализации приложений с интерфейсом «машина–машина». Области применения включают следующие направления:

- 1) безопасность: дом, оборудованный датчиками, обнаруживающими вторжение через сад или окна;
- 2) обеспечение здравоохранения: дом, оборудованный датчиками движения и контролирующим сердцебиение, дает возможность быстро отреагировать на внезапные недомогания, такие как сердечный приступ во время приема ванны;
- 3) уход: дом-«сиделка» с: а) датчиками, определяющими положение каждого человека в нем и подающими сигнал тревоги, если человек входит в опасную зону или покидает дом; б) датчиками, обнаруживающими падение или недержание;
- 4) управление хранилищами: баки (емкости для бензина или пива) с датчиками, измеряющими количество оставшейся жидкости и посылающими данные в систему управления хранилищами, которая составляет график пополнения этих баков;
- 5) защита окружающей среды: датчики температуры, влажности и содержания различных химических веществ в лесу, обнаруживающие лесные пожары и другие нарушения безопасности окружающей среды и вычисляющие количество поглощаемого деревьями углекислого газа;
- 6) отслеживание стихийных бедствий: датчики ускорения и нагрузок, отслеживающие смещения земли и землетрясения, чтобы перекрыть подачу газа в дом, остановить высокоскоростные поезда или включить красный свет на светофорах;
- 7) управление инфраструктурой: датчики, подключенные к зданиям, мостам, туннелям и транспортным эстакадам для обнаружения износа конструкций в результате старения и принятия необходимых мер по ремонту этих сооружений;

- 8) управление логистикой: датчики определяют местонахождение грузов и отслеживают их состояние, например температуру замороженных грузов;
- 9) обслуживание автомобилей: датчики следят за состоянием деталей автомобиля и дают рекомендации по их замене;
- 10) уход за детьми: датчики определяют местонахождение детей и предоставляют информацию об этом, такую как «пришел в школу»;
- 11) управление местами для парковки: датчики отслеживают занятость парковочных мест, чтобы направить автомобиль к свободному.

Большинство этих задач может быть решено с помощью существующих сетей, но некоторые из них не могут быть реализованы повсеместно из-за высокой стоимости сетевых соединений, небольшой продолжительности работы от батарей и ограниченного сетевого покрытия. Если технология WAUN сможет преодолеть эти проблемы, то это позволит занять ей свою долю рынка на начальном этапе развития.

В дополнение к этому можно предложить ряд новых услуг, в случае если товары, в том числе из списка ежедневных покупок, были включены в сеть [6]:

- 1) управление приемом лекарств, а именно: отслеживание расхода таблеток из упаковки, данные пересылаются лечащему врачу. Лечение было бы эффективным, если бы врач проверял правильность и регулярность приема лекарств пациентом. Такая услуга особенно важна для пожилых людей, которые могут забыть принять лекарства вовремя. В Японии рынок медикаментов имеет объем около 6,7 триллионов йен в год [7]. Если управление приемом лекарств будет применено к 10% этого рынка, стоимость этой доли составит 670 миллиардов йен. Такое управление помогло бы снизить расходы на лекарства;
- 2) усовершенствование визитных карточек. Содержащаяся на них информация со временем устаревает. Визитки, имеющие простой дисплей на электронных чернилах, приемник беспроводной связи и тонкопленочную батарею, могли бы обновлять отображаемую информацию;
- 3) управление личными печатями можно реализовать, если отслеживать их применение. Во многих деловых и личных ситуациях японцы используют личные печати подобно подписям в западных странах. При отслеживании использования личной печати в деловых целях можно достичь значительного прогресса в компьютеризации офисной работы. В дополнение к управлению личными печатями многообещающим выглядит отслеживание местоположения различных офисных предметов и важных документов;
- 4) использование каких-либо вещей может быть отслежено по открытию упаковки. Это дало бы нам возможность определять, был ли использован тот или иной товар. К примеру, данную услугу могли бы применять налоговые агенты и работники хранилищ. Службы доставки ежегодно оперируют в Японии более чем тремя миллиардами пакетов [8], а японская почта доставляет свыше ста миллионов заказных отправок в год [9].

Стоит отметить, что эти новые сценарии можно реализовать, используя крохотные датчики и исполнительные механизмы, подключенные к сети. Они в данном случае будут являться самыми низкоуровневыми телекоммуникационными терминалами. Это может привести к новой концепции сети будущего: большинство терминалов будут иметь множество функций и высокую производительность, то есть быть чем-то наподобие персональных компьютеров. Однако такие сценарии потребуют чрезвычайно большого количества терминалов и откроют новые рынки для сетевых провайдеров, поскольку в существующих проводных и беспроводных широкополосных сетях не реализовано подключение такого количества устройств.

2.3. Требования, концепция и система

Для обеспечения упомянутых выше сценариев использования и получения новых источников доходов предлагается использовать сеть WAUN. Она должна удовлетворять следующим требованиям: низкая стоимость и энергопотребление (большой срок службы батарей), обеспечение мобильности, поддержка дешевых терминалов с ограниченными техническими характеристиками, безопасность, масштабируемость в соответствии с количеством терминалов и сплошное (вездесущее) покрытие.

Для того, чтобы обеспечить выполнение этих требований, предложенная нами архитектура использует беспроводную связь на большом расстоянии, которая должна служить в качестве первого транзитного участка для беспроводных терминалов (wireless terminal, WT), хотя основные исследовательские усилия направлены на создание сети датчиков с несколькими транзитными участками, наподобие беспроводной самоорганизующейся сети (ad hoc сети). Такая архитектура была выбрана в основном потому, что последний вариант имеет недостатки, такие как потребление энергии, когда терминал используется как мобильный узел коммутации, подход к безопасности мобильных узлов коммутации и нестабильность зоны покрытия или маршрутизации из-за того, что слишком много мобильных узлов имеют чрезмерную свободу передвижения. К тому же дешевые терминалы не поддерживают сложные протоколы маршрутизации.

Поскольку мы выбрали архитектуру, которая не использует для установленного беспроводного соединения несколько транзитных участков, для экономичного покрытия больших зон важно иметь достаточно протяженные соединения (соты большого размера). Фактические расстояния составили несколько километров. Это объясняется двумя причинами. Во-первых, по мере того как увеличивается радиус соты r , количество точек доступа (access point, AP) может быть уменьшено в $1/r^2$ и размер вложений в беспроводную систему связи уменьшится примерно в той же степени, поскольку основную часть этих расходов составляет стоимость точек доступа. Во-вторых, большинство провайдеров имеют свои сооружения, имеющие энергоснабжение и линии передачи данных, через каждые несколько километров. Таким образом, если радиус соты сети WAUN будет больше, чем несколько километров, существующие провайдеры смогут использовать эти сооружения для размещения точек доступа, что минимизирует раз-

мер необходимых капитальных вложений. Однако радиосвязь на большем расстоянии требует терминалов большей мощности. Таким образом, необходимо удовлетворить противоречивые требования с помощью технологий, описанных в этой главе. Основной темой исследований является «сота радиусом 5 километров при мощности передатчика 10 мВт и сроке службы батареи терминала 10 лет».

Масштабируемость также является важным фактором. Для обеспечения масштабируемости сети WAUN используются следующие правила. Соединение устанавливается между парой «беспроводной терминал – проводной терминал», для каждого беспроводного терминала соответствующий проводной терминал является единственным и фиксированным (в реальности один виртуальный проводной терминал может состоять из множества распределенных проводных терминалов). Таким образом, сеть WAUN не поддерживает подключение произвольных терминалов служб общего пользования, так как большинство приложений предусматривает использование терминалов в границах предприятия или жилого района. К тому же реализация этого правила дает значительное повышение уровня безопасности (на практике службы более высокого уровня поддерживают установление соединения с другими терминалами). В результате сеть WAUN может поддерживать множество частных сетей датчиков. Общая схема сети WAUN показана на рис. 2.3.

Чтобы удовлетворять сформулированным требованиям, сеть WAUN имеет следующие возможности:

- 1) она служит промежуточным звеном между проводными и беспроводными терминалами и не обеспечивает прозрачности сессий между ними;
- 2) беспроводная связь имеет большую дальность (около 5 км), обеспечиваемую разнесением приема на основе суммирования дифференциально взвешенных сигналов. Это даст возможность сетевому провайдеру покрыть значительную территорию небольшим количеством точек доступа и, тем самым, предложить услугу по приемлемой цене;

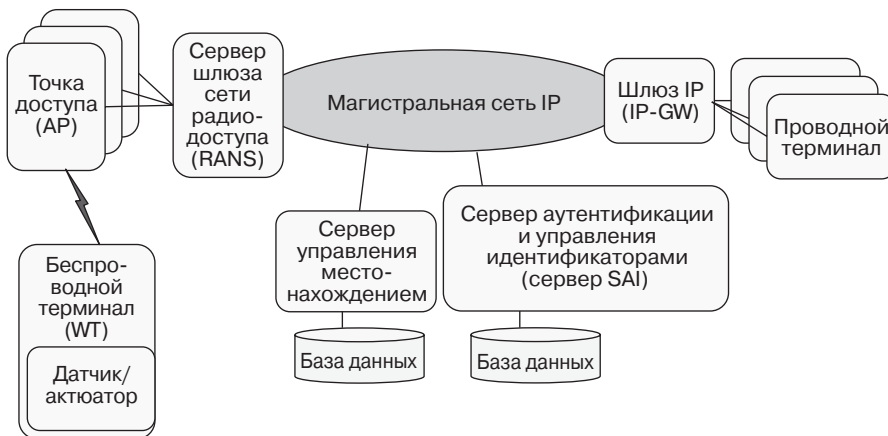


Рис. 2.3. Глобальная сеть со сплошным покрытием (WAUN)

- 3) беспроводные терминалы не являются IP-терминалами и не используют протокол передачи данных TCP/IP, поскольку он является протоколом слишком высокого уровня, а терминалы имеют слабый процессор и малое количество памяти. Точки доступа, организуемые сетевым провайдером, преобразуют протокол беспроводной связи, созданный для беспроводных терминалов сети WAUN, в протоколы, разработанные сообществом IP. Точки доступа также преобразуют идентификаторы беспроводных терминалов, используемые в соединениях с ними, в те, которые применяются в сети фиксированной связи. Серверы шлюзов сети радиодоступа (radio access network gateway server, RANS) выделяют сигналы (то есть пользовательские данные и запрос авторизации) от каждого терминала и перенаправляют их по соответствующему адресу;
- 4) беспроводные терминалы могут перемещаться. Функция управления мобильностью охватывает всю область, в которой они работают, и реализуется с помощью технологий регистрации местонахождения, подобных используемым в сетях сотовой связи;
- 5) проводные терминалы являются терминалами IP, взаимодействуют с беспроводными терминалами в сети WAUN и подключены через шлюзы IP (IP gateway, IP-GW). Их интерфейс с сетью WAUN – это широко используемый обычный интерфейс, такой как TCP/IP, но проводные терминалы IP лишены прямого доступа к таким компонентам сети WAUN, как RANS, по соображениям безопасности. Сеть WAUN не поддерживает установление соединения между проводными терминалами IP;
- 6) несколько идентификаторов в сети WAUN используются для того, чтобы сделать обслуживание удобным, безопасным и эффективным. Сеть WAUN включает функции безопасности, преобразования и разрешения идентификаторов. В частности, чтобы предотвратить отслеживание перемещений посторонними лицами, идентификаторы назначаются беспроводным терминалам лишь на ограниченное время и часто обновляются. Управление идентификаторами с взаимной аутентификацией между терминалом и сетью позволяет обеспечить безопасность передачи данных. Сервер аутентификации и управления идентификаторами (subscriber authentication and ID management, SAI) хранит информацию о профиле подписчика, включая информацию беспроводных и проводных терминалов для целей аутентификации и управления идентификаторами.

2.4. Опорная сеть

Базовая (опорная) сеть WAUN контролирует обмен данными между парами «проводной терминал – мобильный терминал» и обеспечивает функции управления идентификаторами, определения местоположения, безопасности и контроля доступа. Для того, чтобы эти функции работали с огромным количеством беспроводных терминалов, необходимо обеспечить высокую масштабируемость. При разработке базовой сети WAUN имеется два важных момента. Во-первых, объем вычислений, необходимых для управления обменом с беспроводными термина-

лами, должен быть сокращен как можно больше, поскольку эти терминалы потребляют мало энергии и имеют низкие характеристики. Во-вторых, ограниченная полоса пропускания радиоканала должна эффективно использоваться большим количеством беспроводных терминалов совместно. Таким образом, для того, чтобы сеть WAUN могла обслужить больше беспроводных терминалов, необходимо уменьшить объем передаваемых служебных данных.

2.4.1. Коммуникационный протокол

Протокол обмена сети WAUN для передачи данных между проводным и беспроводным терминалами показан на рис. 2.4. Точка доступа преобразует протокол беспроводной связи с терминалом в TCP/IP, используемый в базовой сети WAUN, и наоборот. Между точкой доступа и беспроводным терминалом должна использоваться облегченная версия протокола обмена, приемлемая для терминалов с малым уровнем энергопотребления и низкими вычислительными мощностями, тогда как для экономичной реализации базовой сети WAUN используется обычный протокол, такой как TCP/IP.

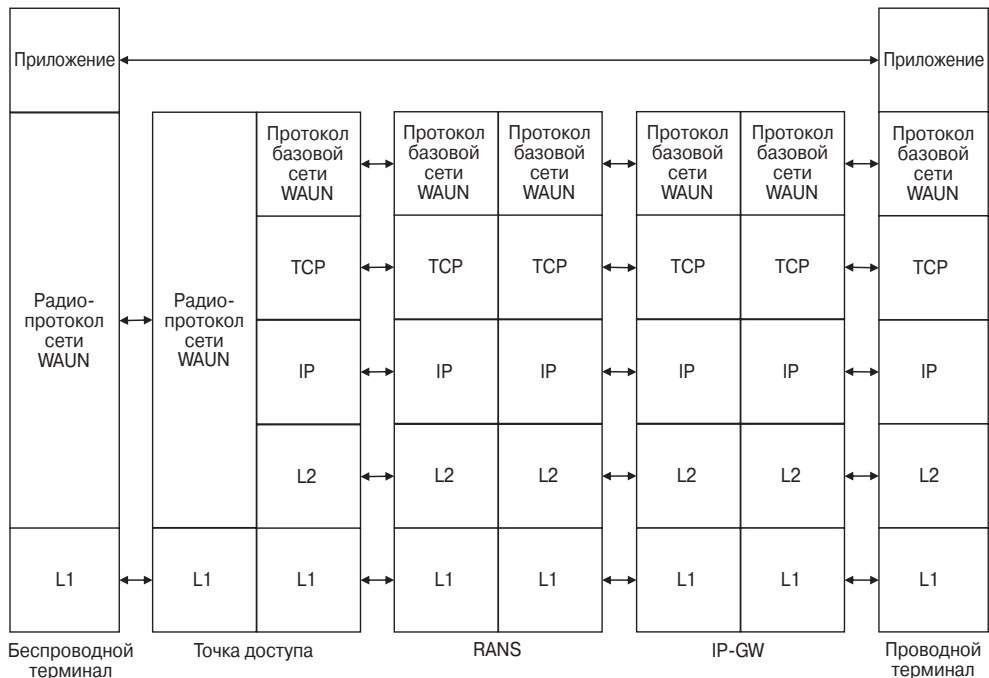


Рис. 2.4. Коммуникационный протокол сети WAUN

Базовая сеть WAUN определяет адрес назначения пакета, принятого от беспроводного терминала, основываясь на его идентификаторе, поскольку соответствующий проводной терминал неподвижен и зарегистрирован на сервере SAI. Таким образом, отсутствует необходимость сообщать в пакете адрес назначения (когда бес-

проводной терминал отправляет пакет проводному терминалу) или адрес источника (когда проводной терминал отправляет пакет беспроводному). Такое решение дает три преимущества. Во-первых, уменьшается нагрузка на терминалы с малым уровнем потребления энергии и низкими вычислительными мощностями и пресекаются как намеренные, так и ошибочные соединения с неподходящим проводным терминалом. Во-вторых, повышается эффективность использования канала. Например, адрес IPv6 имеет 128 разрядов. В сети WAUN, где многие терминалы совместно используют ограниченную полосу пропускания, такой 128-разрядный адрес оказывается слишком обременительным для беспроводного канала. В-третьих, соответствующий проводной терминал может быть заменен без необходимости изменять программное обеспечение (ПО) в беспроводном терминале. В противном случае при необходимости замены проводного терминала потребовалось бы изменять ПО в большом числе беспроводных терминалов, разбросанных по разным местам.

2.4.2. Управление идентификаторами

Сеть WAUN пересылает данные к беспроводным терминалам и от них, основываясь на их идентификаторах. В зависимости от назначения терминала используются следующие три типа идентификаторов:

- 1) постоянный идентификатор назначается на весь период обслуживания, чтобы уникально идентифицировать беспроводной терминал. Он используется только внутри базовой сети WAUN для обеспечения безопасности. Вместо постоянного идентификатора беспроводной терминал может применять временный, а проводной для идентификации беспроводного – служебный идентификатор. Таким образом, точка доступа выполняет преобразование временного идентификатора в постоянный и обратно, а шлюз IP – служебного и временного идентификаторов. Сервер SAI управляет тем, как взаимосвязаны эти три идентификатора;
- 2) временный идентификатор используется для аутентификации беспроводного терминала до момента установления соединения. Таким образом, этим идентификатором управляют и беспроводной терминал, и сервер SAI. Временный идентификатор часто обновляется синхронно на обоих этих устройствах, чтобы избежать отслеживания терминала посторонними наблюдателями. Этот идентификатор может быть использован повторно, если при обновлении он оказывается уникальным, то его длина уменьшается по сравнению с постоянным для более эффективного применения полосы пропускания беспроводного канала;
- 3) служебный идентификатор используется для того, чтобы беспроводной терминал мог быть идентифицирован проводным. Он дает возможность прозрачно заменить беспроводной терминал на другой, например, в случае его поломки.

Количество этих идентификаторов огромно, и они должны управляться серверами SAI, а их преобразование выполняется в точках доступа и шлюзах IP для каждого случая обмена данными. Следовательно, управление данными и преобразования должны выполняться децентрализованно.

2.4.3. Безопасность

Существующие технологии обеспечения безопасности с высокой надежностью в сетях IP, такие как виртуальная частная сеть (virtual private network, VPN), могут быть применены в проводной части сети WAUN. Для беспроводных соединений требуются особые методы, поскольку их полоса пропускания ограничена, а беспроводные терминалы имеют ограниченные возможности и низкое энергопотребление. Подобно телефонной сотовой сети, сеть WAUN имеет функции безопасности, которые предотвращают перехват данных, отслеживание, кражу идентификаторов и их фальсификацию. Однако эти функции обеспечиваются при более чем вдвое меньшей длине сообщений, чем в телефонных сотовых сетях. Например, чтобы обновить временный идентификатор, в телефонной сотовой сети новый временный идентификатор в зашифрованном виде переходит к беспроводному терминалу, тогда как сеть WAUN для его одновременного обновления на концах соединения передает не сам идентификатор, а уменьшенное количество информации.

Беспроводной терминал при установлении соединения с точкой доступа аутентифицируется сервером RANS, кэширующим временный идентификатор (который выдан сервером SAI). Сервер RANS аутентифицирует беспроводной терминал, когда тот включается и перемещается за границы зоны связи. Аналогичным образом, проводной терминал аутентифицируется шлюзом IP, который назначен этому терминалу.

2.4.4. Управление доступом (авторизация)

Определение загруженности сети WAUN может основываться на числе обменов данными, и она может ограничивать частоту обмена с каждым терминалом, например, один раз в час или в сутки. Разрешенная частота обменов данными для каждого беспроводного терминала первоначально определяется договором на абонентское обслуживание и регистрируется на сервере SAI. Сервер RANS и шлюз IP временно хранят эти сведения, получая их при аутентификации, и проверяют частоту соединений. Если частота, с которой беспроводной терминал отправляет и получает данные, выходит за рамки установленного лимита, сервер RANS и шлюз IP отказываются устанавливать соединение.

2.4.5. Протоколы приема и передачи данных

Протоколы передачи данных в восходящем (передача из беспроводного терминала в проводной) и нисходящем (в обратном направлении) каналах показаны на рис. 2.5 и 2.6 [10]. В протоколе восходящей связи процедура аутентификации и авторизации выполняется сервером RANS перед каждой передачей данных.

Последовательность аутентификации, показанная на рис. 2.5 и 2.6, включает процедуру обновления информации в беспроводном терминале. После аутентификации сервер RANS обновляет информацию о беспроводном терминале (включая зону пейджинга, в которой он находится) на сервере управления местоположением и кэширует эту информацию у себя. Сервер RANS может хранить информацию о беспроводном терминале, находящемся в зонах покрытия точек доступа,

которые обслуживаются этим сервером. Затем он передает информацию шлюзу IP, обслуживающему проводной терминал и соответствующему этому беспроводному терминалу, а также обновленную информацию о зоне пейджинга, включая свой адрес. (Шлюз IP кэширует эту информацию, она дает возможность выбрать нужный сервер RANS, если протокол передачи данных в нисходящем канале выполняется без запроса информации о зоне пейджинга, в которой находится беспроводной терминал. Таким образом, использование кэшированной информации снижает нагрузку на сервер управления местоположением и сервер SAI и сокращает время, необходимое для обмена данными.)

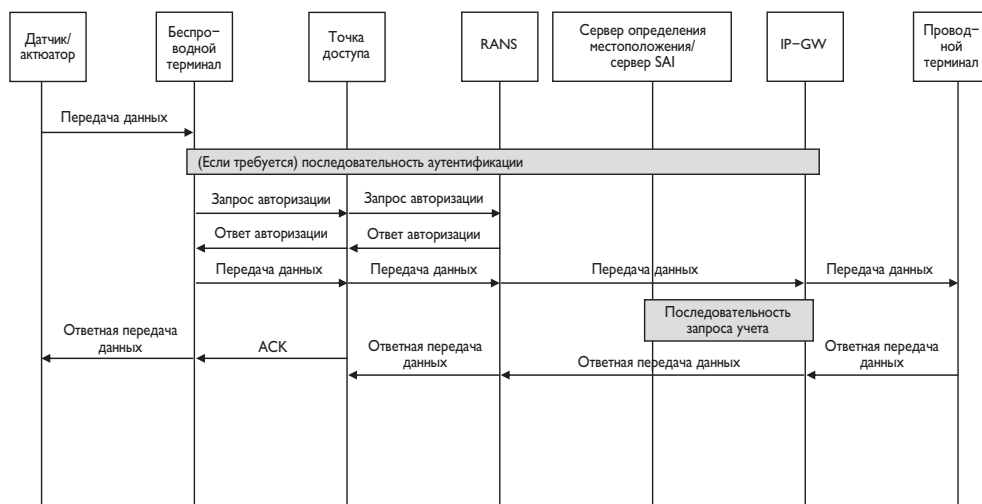


Рис. 2.5. Протокол передачи данных в восходящем канале WAUN

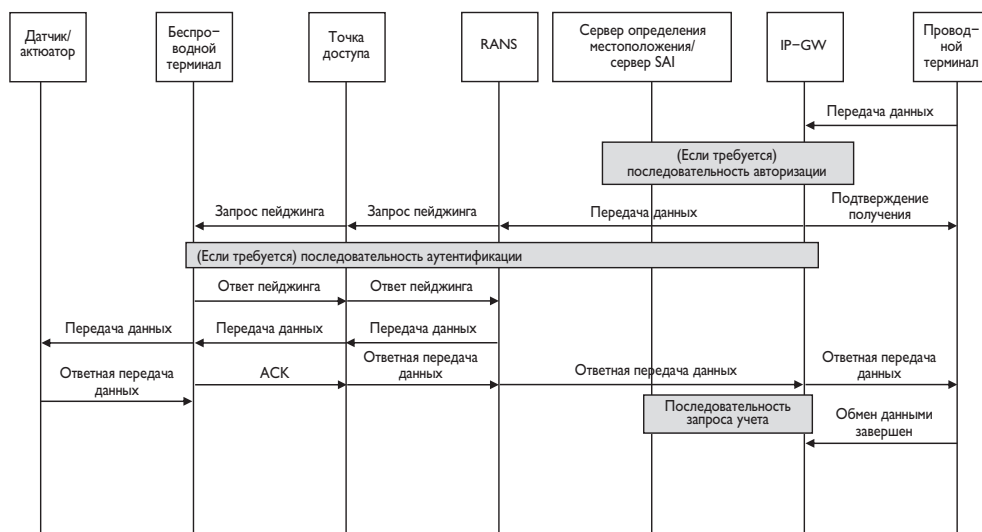


Рис. 2.6. Протокол передачи данных в нисходящем канале WAUN

В протоколе нисходящей связи сеть WAUN использует четырехходовую последовательность обмена между проводным терминалом и шлюзом IP. Сообщение «уведомление о приеме» показывает, что шлюз IP авторизовал передачу и начал процедуру обмена данными. Сообщение «ответ данных» информирует, что беспроводной терминал был аутентифицирован и принял данные.

2.5. Беспроводная сеть доступа [35]

2.5.1. Основы построения сети

Поскольку сеть WAUN является сетью нового типа, требования [6] к системам беспроводного доступа, такие как масштабируемость в соответствии с количеством терминалов, мобильность терминалов и поддержка терминалов с низкой производительностью, не могут быть обеспечены существующими технологиями беспроводного доступа. Для сетей WAUN необходимо разработать новые методы организации беспроводного доступа. С точки зрения сетевой инфраструктуры сотовая конфигурация больше, чем организация соединения с несколькими транзитными участками, подходит для обеспечения стабильности работы и низкого энергопотребления беспроводных терминалов [6]. Базовый анализ связей [6] позволяет выдвинуть предположение, что для таких терминалов с мощностью передатчика 10 мВт можно использовать соты радиусом 5 км. В этом случае уровень принимаемого сигнала крайне низок, поэтому создание системы беспроводного доступа с использованием современных беспроводных технологий является сложной задачей.

Таким образом, необходимо разработать сложную технологию, объединяющую такие методы беспроводной передачи, как модуляция/демодуляция, исправление ошибок и разнесение. Так как беспроводные терминалы должны иметь простую конструкцию и низкий уровень энергопотребления, точка доступа должна выполнять сложные операции, чтобы компенсировать простоту терминалов. Важным является также использование технологии управления доступом, которая могла бы обеспечивать работу десятков тысяч беспроводных терминалов с разными уровнями обслуживания и в то же время снижала бы энергопотребление этих терминалов, поддерживая прерывистый режим их работы. Кроме того, необходимо разработать метод управления сетью для стабильного и эффективного функционирования системы беспроводного доступа, гарантирующего мобильность терминалов и их подключение к базовой сети.

Следующие разделы описывают архитектуру системы и ключевые технологии сети беспроводного доступа WAUN.

2.5.2. Архитектура системы

Схема сети беспроводного доступа приведена на рис. 2.7. Эта сеть состоит из двух сетевых элементов: точек доступа и беспроводных терминалов. Они связаны беспроводными каналами связи. И точка, и терминал включают три функции: интерфейс физического уровня (physical layer interface, РНУ), протокол управления доступом (medium access control) и функцию сетевого управления (network control, CNT).

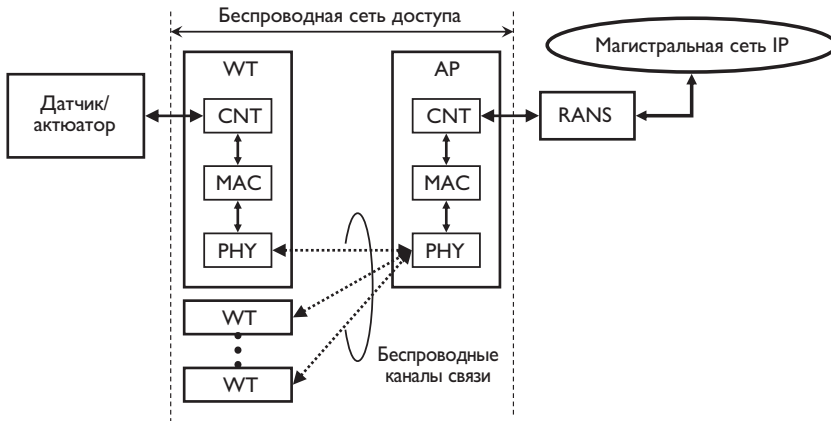


Рис. 2.7. Схема беспроводной сети доступа

Физический уровень предоставляет функции беспроводных передачи и приема и модуляции/демодуляции. Протокол управления доступом реализован для обеспечения управления множественным доступом и должен поддерживать различные уровни QoS сетевой инфраструктуры со сплошным покрытием. Точка доступа соединяется с магистральной сетью WAUN по протоколу IP через сервер RANS с использованием CNT. Подключение к беспроводному терминалу с датчиками или исполнительными механизмами также устанавливается с использованием CNT. Функция CNT управляет функциями PHY и MAC точки доступа и беспроводного терминала. Ключевые вопросы, касающиеся этих трех функций, описаны ниже.

Пример сотовой архитектуры показан на рис. 2.8. Каждая сота является шестиугольником размером в несколько километров, их совокупность образует структуру, подобную пчелиным сотам. В трех вершинах каждой соты размещены трехсекторные антенны, излучающие радиосигналы в направлении центра сот. Чтобы избежать помех от смежных сот, им назначаются разные частотные каналы.

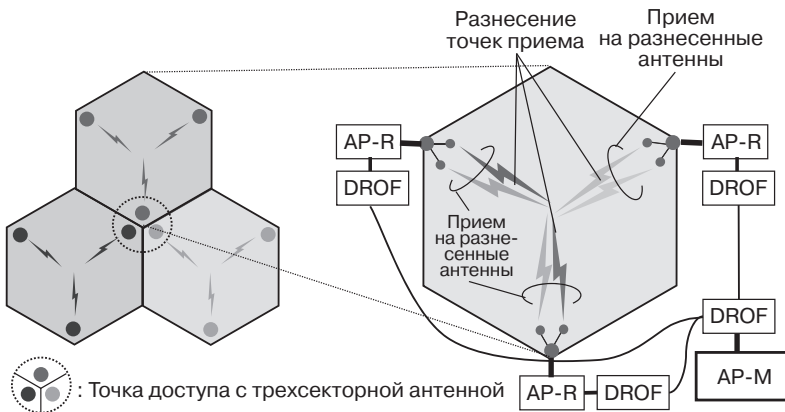


Рис. 2.8. Конфигурация беспроводной соты

Для достижения высокой степени покрытия в сети используются методы приема на разнесенные антенны и разнесение точек приема. Функция РНУ в сети физически разделена между модулями двух типов: модуль модуляции/демодуляции и радиочастотный модуль приема/передачи. Модули первого типа представляют собой главное оборудование точки доступа (master equipment of the AP, AP-M), модули второго – размещены вместе с антенной удаленно (remote equipment of the AP, AP-R). Обработка всех видов сигналов реализована в AP-M. Передаваемые радиосигналы направляются в модули AP-R, а принимаемые этими модулями сигналы собираются в AP-M. Для передачи радиосигналов между AP-M и AP-R используется подсистема цифровой передачи радиосигнала по кабелю (digitized radio over fiber, DROF) [11]. Оцифрованные радиосигналы передаются между AP-M и AP-R по сети Ethernet.

2.5.3. Основные особенности системы

2.5.3.1. Интерфейс физического уровня

2.5.3.1.1. *Требования к интерфейсу физического уровня.* Интерфейс РНУ является основой сети беспроводного доступа. Требования к нему изложены ниже:

- 1) передача на большое расстояние. Цель разработки системы – сота радиусом 5 километров при мощности передатчика беспроводного терминала 10 мВт;
- 2) использование типа модуляции, который эффективно утилизирует выделенную полосу пропускания. Ограниченные частотные ресурсы должны обеспечивать работу огромного количества терминалов;
- 3) низкие накладные расходы. Поскольку в трафике сети WAUN преобладают короткие пакеты, служебная часть каждого пакета должна быть минимальной, чтобы избежать снижения эффективности передачи;
- 4) компактные, малопотребляющие терминалы. Беспроводные терминалы должны быть компактными, иметь как можно больший срок службы батареи и как можно меньшую стоимость.

2.5.3.1.2. *Функции РНУ.* Чтобы обеспечить выполнение указанных выше требований, функции РНУ реализованы следующим образом.

- 1) **Характеристики радиоканала.** Метровый и дециметровый диапазоны были выбраны в связи с малыми задержками при распространении и низкими потерями при экранировании. Мощность передатчика беспроводного терминала ограничена 10 мВт, что является пределом, не требующим лицензирования в Японии. Точки доступа являются лицензируемыми станциями и могут излучать сигналы более высокой мощности.
- 2) **Коммуникационная схема.** Для повышения чувствительности при приеме сигналов терминалов используется режим множественного доступа с разделением по времени (time division multiple access, TDMA), поскольку приемник может использовать для синхронизации антенну с узкой апертурой в условиях, когда мощность излучения ограничена. Принята схема дуплексирования с временным разделением (time division duplex, TDD), поскольку она дает возможность использовать одни и те же узлы в радиомодуле беспроводного терминала и для приема, и для передачи.

- 3) **Схема модуляции/демодуляции.** Для оптимального использования полосы пропускания выбрана квадратурная фазовая модуляция со сдвигом $\pi/4$ ($\pi/4$ -shift quadrature phase shift keying, QPSK). Для демодуляции в беспроводных терминалах используется дифференциальное детектирование, поскольку его можно реализовать в простых устройствах, а в точках доступа – синхронное детектирование из-за его высокой чувствительности. Для прямой коррекции ошибок выбраны сверточное кодирование и декодирование по алгоритму Витерби с мягким решением, так как они обеспечивают высокую эффективность кодирования и сравнительно просты для аппаратной реализации.
- 4) **Структура пакета PHY.** Структура пакета PHY показана на рис. 2.9. Пакет принимаемых терминалом сигналов (downlink, DL) состоит из символов заголовка (преамбулы) и символов данных. Символы заголовка находятся в начале пакета и используются для синхронизации пакета. Пакет данных, передаваемых терминалом (uplink, UL), состоит из нескольких пилотных символов и символов данных. Пилотные символы равномерно помещаются в пакете и используются для синхронизации пакета и отслеживания канала при синхронном детектировании.

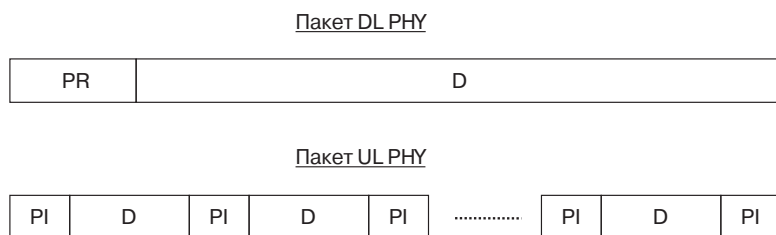


Рис. 2.9. Структура пакета PHY: PR – заголовок; PI – пилотный символ; D – символ данных

- 5) **Синхронизация сигналов в нисходящем канале.** Синхронизация беспроводного терминала с принимаемым сигналом выполняется путем дифференциального детектирования и взаимной корреляции с заголовком пакета. Если говорить подробнее, синхронизация частоты осуществляется оценкой смещения частоты несущей по фазовой компоненте значения взаимной корреляции, а тактовая и кадровая синхронизация выполняются оценкой их временной позиции по пику того же значения. Дифференциальное детектирование позволяет вычислить сдвиг несущей частоты, даже если возникающий из-за этого сдвиг фазы в пределах заголовка превышает π , что позволяет уменьшить стоимость генератора WT. Схема взаимной корреляции может обнаружить временные отсчеты даже в случае низкого отношения сигнал–шум (ОСШ). Таким образом, этот метод обеспечивает синхронизацию в пределах одного пакета с высокой точностью. Это сокращает отрезок времени, в течение которого терминал выполняет прием и уменьшает накладные расходы на передачу пакета.

- 6) **Синхронизация передачи в восходящем канале.** В беспроводном терминале используется метод автоматического контроля частоты передачи, чтобы уменьшить накладные расходы на синхронизацию частот [12]. Точка доступа хранит весь пакет, принятый с определенного направления, синхронизация тактовой частоты и пакетов основана на дифференциальном детектировании и взаимной корреляции тестовых символов для отслеживания канала, что требуется для синхронного детектирования. Это также позволяет уменьшить размер служебной информации при тактовой синхронизации и синхронизации пакетов, тем самым достигается высокая эффективность передачи.
- 7) **Схема разнесения.** Точка доступа поддерживает разнесение приема и передачи для улучшения чувствительности в условиях затуханий и экранирования окружающей средой. При разнесении приема и передачи для компенсации затуханий и экранирования применяются разнесение приемных антенн и мест приема. При нисходящей передаче используется разнесение со смещением частоты, принятое в японских пейджинговых системах. При этом методе антеннами передаются одинаковые сигналы со слегка отличающимися несущими частотами, так что уровень приема меняется во времени по всей территории соты благодаря интерференции сигналов с разных антенн, таким образом, сота не имеет мертвых точек. Метод разнесения обеспечивает качество передач, которые соответствуют числу антенн у точки доступа. При приеме сигналов, передаваемых терминалом, используется метод суммирования дифференциально взвешенных сигналов каждого канала (maximal ratio combining, MRC). Метод разнесения улучшает пропускную способность канала простым увеличением числа антенн у точки доступа.

2.5.3.2. Функции MAC. Протокол MAC управляет десятками тысяч беспроводных терминалов, поддерживает качественную связь с помощью автоматических запросов повтора (automatic repeat request, ARQ) независимо от ошибок, возникающих в радиоканале, и управляет QoS, используя изменение размера окна задержки случайного доступа и динамическое выделение слотов [13]. Кроме того, протокол MAC эффективно поддерживает работу беспроводных терминалов, передающих небольшие объемы данных через длительные интервалы времени. Он включает функцию поддержки прерывистого приема беспроводными терминалами соответственно требованиям к трафику. Такая схема приема снижает потребление энергии терминалами и продлевает срок службы батарей.

2.5.3.2.1. Логические каналы и структура фрейма. Структура фрейма MAC в беспроводной системе показана на рис. 2.10. Логические каналы, используемые на уровне MAC, перечислены в табл. 2.1. Чтобы добиться хорошей производительности при синхронизации фреймов даже в условиях плохой радиосвязи с беспроводным терминалом, на уровне MAC используется механизм TDMA/TDD. Длина фрейма MAC выбрана равной 9600 символам с учетом общей эффективности и уровня задержек при передаче. Первая часть фрейма предназначена для данных, передаваемых на терминал, вторая — для данных, принимаемых от терминала. Граница между ними изменяется динамически в соответствии с результатами планирования распределения пакетов, которое меняется от фрейма к фрейму.

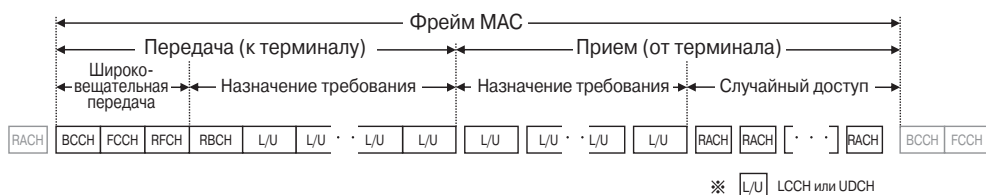


Рис. 2.10. Структура фрейма MAC

Таблица 2.1. Логические каналы

Название	Использование
BCCH	Управление каналом передачи используется при приеме и передает информацию об этом канале, относящуюся ко всей соте. Он содержит фиксированное количество данных
FCCH	FCCH посылается при приеме и передает информацию, описывающую структуру фрейма MAC в радиointерфейсе
RFCH	Назначение канала обратной связи со случайным доступом – информировать терминалы о параметрах случайного доступа
RBCH	Канал передачи RLC используется во входящем соединении и передает управляющую информацию, относящуюся ко всей соте
UDCH	Канал данных пользователя используется для передачи данных между точкой доступа и беспроводным терминалом
LCCH	Канал контроля соединения является двунаправленным и используется для передачи информации о работе ARQ
RACH	Канал случайного доступа предоставляет беспроводному терминалу возможность отправить управляющую информацию точке доступа, используя случайный доступ

Фрейм MAC включает каналы контроля передачи (broadcast control channel, BCCH), контроля фрейма (frame control channel, FCCH), обратной связи со случайным доступом (random access feedback channel, RFCH), управления радиоканалом (radio link control broadcast channel, RBCH), данных пользователя (user data channel, UDCH), логического управления (logical control channel, LCCH), случайного доступа (random access channel, RACH). Каналы BCCH используются для сообщения атрибутов точки доступа и посылаются в начале каждого фрейма MAC. Каналы FCCH показывают структуру фрейма MAC, то есть позицию и длину других каналов, следующих за FCCH. Каналы RFCH применяются для передачи информации, связанной со случайным доступом, то есть результатов случайного доступа в предыдущем фрейме MAC, размера окна задержек для каждого класса QoS, позиций слотов случайного доступа и их количества в текущем фрейме MAC, каналы RBCH – для широковещательной передачи управляющих сообщений о радиоканале, каналы UDCH – для передачи данных пользователя, а LCCH – управляющей информации MAC, например ARQ-ACK (подтверждение).

2.5.3.2.2. *Последовательности доступа.* Последовательность передачи данных пользователя с использованием случайного доступа и назначения по требованию, когда данные посылаются от беспроводного терминала к точке доступа, показана на рис. 2.11. В этой системе беспроводной связи точка доступа посылает каналы BCCH, FCCH и RFCH в соответствующем порядке в начале фрейма MAC. Если терминал имеет данные для отправки, он принимает канал RFCH, чтобы определить начальную позицию и число слотов случайного доступа. Чтобы избежать

конфликтов с каналами RACH других терминалов, терминал выполняет задержку. Количество пропускаемых при такой задержке слотов выбирается терминалом случайно в интервале от нуля до размеров окна. При первой попытке случайного доступа размер окна устанавливается согласно значению, заданного точкой доступа в качестве начального и указанного в RFCH. После выполнения задержки терминал посылает RACH, чтобы сделать запрос точке доступа на назначение UDCH для передачи пользовательских данных. Канал RACH содержит MAC-ID. Уникальный MAC-ID назначается каждому беспроводному терминалу и дает возможность точке доступа идентифицировать терминал. В прототипе системы длина MAC-ID равна 16 разрядам. Таким образом, точка доступа может управлять более чем 60 000 терминалами.

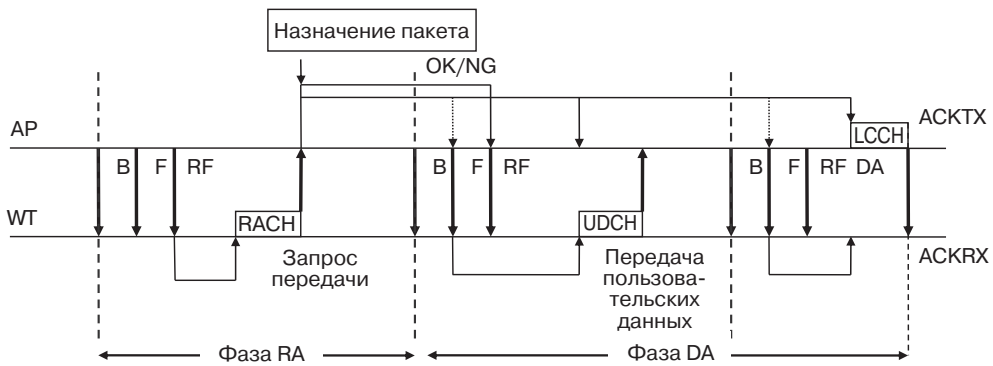


Рис. 2.11. Последовательность передачи данных пользователя В, ВССН; F, FCCH; RF, RFCH

После передачи RACH терминал снова принимает RFCH в следующем фрейме MAC. Если в предыдущем фрейме попытка случайного доступа была успешной, точка доступа посылает терминалу подтверждение (ACK) в RFCH. В противном случае точка доступа не посылает ничего. Если терминал не смог получить подтверждение, он удваивает размер окна и вычисляет задержку для слота отправки согласно этому размеру. После задержки терминал снова пытается отправить RACH. Такие попытки повторяются, пока RACH не будет успешно принят или пока количество попыток не достигнет заранее заданного предела.

После получения подтверждения от точки доступа терминал ждет назначенного ему UDCH, о котором оповещается через FCCH. Когда UDCH будет назначен терминалу, он посылает в нем свои данные пользователя. После того как точка доступа примет UDCH, если прием прошел без ошибок, она посылает обратно LCCH с подтверждением ARQ-ACK. В противном случае она возвращает LCCH с ARQ-NAK (negative acknowledgment, отказ подтверждения), который информирует беспроводной терминал об ошибке при передаче UDCH.

2.5.3.2.3. Управление QoS. В системе определены три класса QoS. Точка доступа предлагает службы, основанные на этих трех классах, и беспроводные терминалы могут их использовать одновременно. Сервисы различаются по соединениям уп-

равления каналами данных (data link control, DLC), и каждый WT устанавливает не более трех соединений DLC. Кроме того, в каждом соединении DLC используется ARQ, чтобы исправлять битовые ошибки, возникающие в радиоканале, и обеспечивать качество обмена данными. Управление QoS в восходящем канале обеспечивается точкой доступа путем задания размера окна задержки случайного доступа. Таким образом, точка задает размер окна задержки в соответствии с каждым классом QoS и оповещает терминалы посредством RFCH. Затем терминалы выполняют случайный доступ, используя полученный в уведомлении размер окна задержки, пытаясь отправить данные пользователя. Когда точка доступа принимает решение о размере окна задержки, меньший размер назначается классу QoS с высоким приоритетом и больший – классу с низким приоритетом.

2.5.3.2.4. Механизм сна. Беспроводные терминалы имеют два режима приема BCCH: последовательный и прерывистый. В режим прерывистого приема они переключаются, если отсутствуют данные для передачи. В этом режиме терминал принимает BCCH только один раз из N (N может быть от 2 до 128). Тем самым терминал снижает свое энергопотребление и продлевает срок службы батарей. Пример перехода терминала в режим прерывистого приема BCCH показан на рис. 2.12. В этом случае терминал переходит в режим прерывистого приема BCCH, при отсутствии назначенных ему каналов, таких как UDCH и LCCH, в течение трех последовательных фреймов MAC. Беспроводной терминал устанавливается в режим прерывистого приема только каждого четвертого BCCH.

2.5.3.3. Функция сетевого управления

2.5.3.3.1. Конфигурация CNT. Функция сетевого управления точки доступа (AP-CNT) управляет беспроводным каналом связи точки и каналом связи с магистральной сетью WAUN через RANS. Беспроводные терминалы также используют эту функцию (WT-CNT), управляющую беспроводным каналом связи и взаимодействием с радиомодулем и внешним оборудованием: датчиками и исполнительными механизмами.

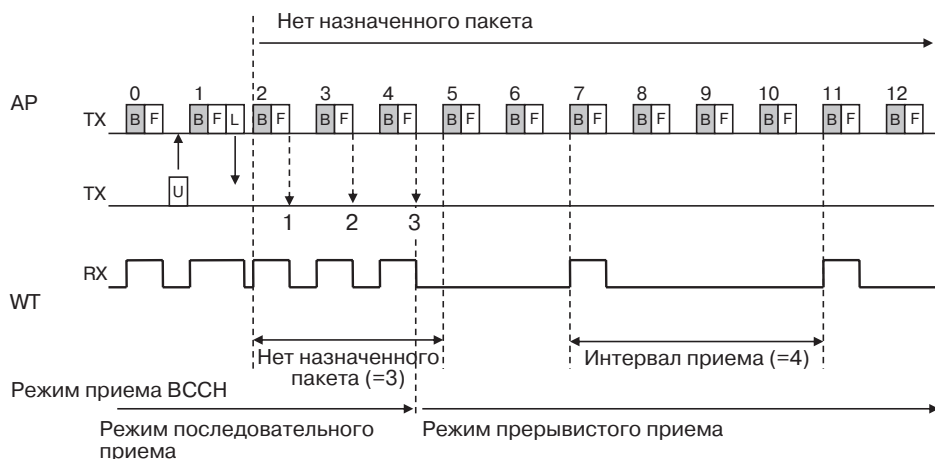


Рис. 2.12. Смена режима приема B, BCCH; F, FCCH; U, UDCH; L, LCCH.

AP-CNT подключена к RANS по стеку TCP/IP. AP-CNT передает сообщения пользователя и управляющие сообщения по соединению TCP/IP. В случае сети WAUN оборудование беспроводного терминала должно быть компактным и иметь низкое энергопотребление, поэтому стек протоколов TCP/IP в нем реализовать нельзя, к тому же объем служебных данных TCP/IP слишком велик для узкого беспроводного канала сети WAUN. Поэтому точка доступа должна работать как преобразователь между использующей TCP/IP магистральной сетью и сетью беспроводной связи.

2.5.3.3.2. Функция CNT :

- 1) *управление оборудованием.* AP-CNT контролирует оборудование точки доступа. Когда на точку доступа подается питание, AP-CNT пытается соединиться с RANS. После соединения с RANS AP-CNT начинает широковещательную передачу информации точки доступа на несущей управления. После завершения этой передачи беспроводные терминалы могут выполнять поиск точки доступа, с которой они должны устанавливать соединение;
- 2) *управление несущей.* Поскольку точка доступа может использовать несколько несущих, AP-CNT должна обладать возможностью управлять ими. Точка доступа использует одну несущую управления и несколько несущих для обмена данными. Несущая управления используется для передачи служебной информации, такой как идентификатор точки доступа. Когда беспроводной терминал определяет несущую управления точки доступа, он получает из ВССН ее идентификатор, сведения о загрузке каналов передачи данных на несущих и другую информацию. Информационная несущая используется для передачи сообщений между терминалами и магистральной сетью. Когда беспроводной терминал, выбравший коммуникационную несущую, запрашивает UDCH для отправки информации в магистральную сеть, для отправки этого запроса используется RACH. Если запрос может быть принят, терминалу назначается UDCH на той же несущей. AP-CNT также управляет информацией о трафике на каждой несущей, то есть частотой несущей, загрузкой ее трафиком, информацией об ошибках и уровне шумов. Сначала беспроводной терминал ищет несущую управления и синхронизируется с ней. Затем он выбирает точку доступа, с которой должен соединиться;
- 3) *управление терминалом.* AP-CNT управляет информацией о беспроводных терминалах, используя таблицу управления терминалами, хранящуюся в памяти. Первоначально информация о терминале заносится в таблицу после его аутентификации. Затем заполняются элементы таблицы, которые необходимы для установления соединения с терминалом, такие как идентификатор терминала, идентификатор соединения, статус терминала и информация, относящаяся к безопасности. Точка доступа получает значения этих элементов от магистральной сети после аутентификации терминала и удаляет их, когда очищается соединение, назначенное терминалу. Некоторые элементы периодически обновляются по соображениям безопасности;

- 4) *управление соединениями*. AP-CNT и WT-CNT устанавливают связь между магистральной сетью и терминалом при приеме данных из сети или от терминалов.

Сначала AP-CNT оценивает использование пропускной способности беспроводной сети. Результаты оценки объявляются беспроводным терминалам по широкополосному каналу. WT-CNT, пытаясь соединиться с магистральной сетью, может выбирать точку доступа на основе класса своего трафика и объявленной емкости. Если объявленная пропускная способность превышает заданный пороговый уровень, WT-CNT отказывается от создания нового соединения с точкой доступа и выбирает другое доступное соединение.

Затем, при передаче в восходящем канале WT-CNT, пытающийся отправить пакет, пробует установить соединение. Если соединение уже было установлено, он запрашивает канал связи. В противном случае для установления соединения требуется аутентификация беспроводного терминала. Даже если соединение установлено, для выделения канала требуется наличие в магистральной сети сервера аутентификации и управления идентификаторами. Этот сервер оценивает, должна ли точка доступа удовлетворять требование выделения канала, отправленное терминалом. На основе этой оценки AP-CNT разрешает или запрещает терминалу доступ к сети. Посылать свои пакеты с данными точке доступа могут только терминалы, прошедшие аутентификацию и имеющие радиосоединение и канал связи.

В случае передачи данных в нисходящем канале AP-CNT ожидает поступления данных или пейджинговых сообщений из магистральной сети. Когда сообщение поступает, AP-CNT проверяет таблицу управления терминалами, чтобы найти соединение, по которому следует переправить это сообщение. Если терминал найден в таблице, AP-CNT выделяет коммуникационный канал для передачи сообщения беспроводному терминалу. Если же терминал в таблице не найден, AP-CNT пытается послать ему пейджинговое сообщение через широкополосный канал. WT-CNT, который отслеживает широкополосный канал, но не имеет соединения, обнаруживает это пейджинговое сообщение. После этого WT-CNT пробует установить соединение.

2.6. Беспроводной терминал

Этот раздел описывает методы снижения мощности, потребляемой беспроводными терминалами сети WAUN. В нем обсуждается важность работы в режиме низкого энергопотребления и влияние прерывистой работы на потребление энергии беспроводным терминалом. Представлена значительно снижающая энергопотребление многопороговая КМОП-схема, которая может существенно увеличить срок службы батарей.

2.6.1. Требования к беспроводным терминалам

На рис. 2.13 показана упрощенная блок-схема беспроводного терминала сети WAUN [14]. Терминал состоит из радиочастотных цепей (передатчик T_x и приемник R_x),

петли фазовой автоподстройки частоты (ФАПЧ), тактового генератора, цифровых групповых трактов, батареи, интерфейса датчиков и исполнительных механизмов (актюаторов) и антенны. Для создания терминала с низкой стоимостью необходимо интегрировать почти все активные цепи в однокристалльную микросхему большой степени интеграции (БИС). Интегрирование в БИС приемника дает возможность исключить множество навесных деталей, поэтому такая технология является многообещающей для создания маленьких и дешевых терминалов. Не удастся интегрировать в БИС батареи питания, датчик или исполнительный механизм, а также антенну. Антенна может быть реализована в виде печатных проводников на той же плате, где размещена БИС, ее расчетный коэффициент усиления составляет -15 дБи. Интерфейс датчика или исполнительного механизма обычно является последовательным и низкоскоростным, порядка 9600 бит/с. Полагая, что датчик или исполнительный механизм (например, однокристалльный датчик температуры) являются малоразмерными, они могут быть встроены в терминал с помощью модификации интерфейса.

Благодаря своему малому размеру беспроводной терминал сети WAUN, содержащий датчик или исполнительный механизм, может быть установлен в самых разных местах. Однако если датчик или исполнительный механизм достаточно велики, беспроводной терминал сети WAUN может быть встроены в них и подключаться к ним с помощью адаптера, преобразующего используемые ими протоколы в протоколы беспроводного терминала сети WAUN. В этом случае терминал должен быть достаточно малым, чтобы его можно было встроить в другое устройство.

Таким образом, минимизация размера беспроводного терминала сети WAUN очень важна независимо от того, является ли датчик или исполнительный механизм простым или сложным, маленьким или большим. Цель работы заключалась в разработке терминала объемом не более 10 см^3 . Основным препятствием такой минимизации явился размер батареи. В сети WAUN чрезвычайно большое количество терминалов будет располагаться в самых разных средах, в том числе вне помещений. Беспроводной терминал должен иметь малогабаритные элементы питания, такие как дисковые или тонкопленочные, со сроком службы несколько лет, поскольку они не могут быть подзаряжены или заменены. Следовательно, снижение потребления энергии (и, тем самым, уменьшение размера батареи) является критическим фактором в разработке беспроводного терминала сети WAUN.

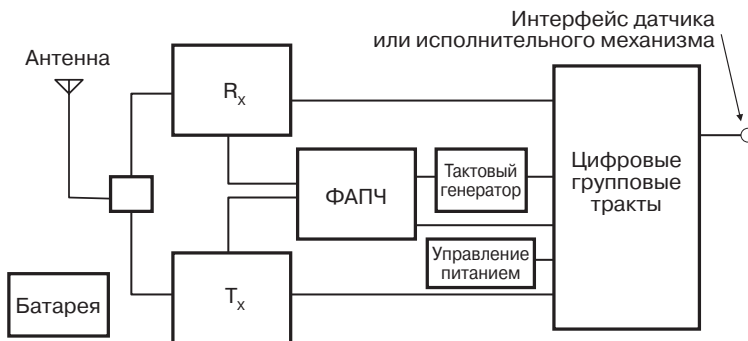


Рис. 2.13. Упрощенная блок-схема терминала сети WAUN

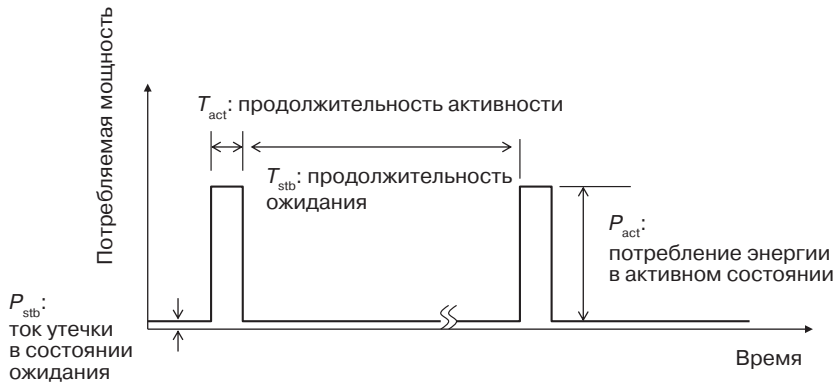


Рис. 2.14. Прерывистая работа (если при нахождении в режиме ожидания можно пренебречь током утечки, среднее потребление энергии пропорционально степени активности)

2.6.2. Прерывистая работа

Очевидно, что работа беспроводного терминала сети WAUN с крайне низким потреблением не может быть достигнута в непрерывном режиме. Этому терминалу не обязательно работать часто, как это делают терминалы сотовой связи, следовательно, энергопотребление можно снизить за счет снижения доли активности. Уровень активности был установлен на несколько порядков меньше, чем в обычных телефонных системах сотовой связи, где он составляет примерно 10^{-2} . Мы стремились достичь отношения, меньшего, чем 10^{-4} , который соответствует нескольким секундам работы в день. Типичная прерывистая работа показана на рис. 2.14, где P_{act} и P_{stb} — мощности потребления в активном режиме и режиме ожидания, T_{act} и T_{stb} — продолжительность этих периодов. Средняя потребляемая мощность P_{av} определяется как:

$$P_{av} = R_{act} \times P_{act} + P_{stb}. \quad (2.1)$$

Коэффициент активности R_{act} , определяемый как $T_{act}/(T_{act} + T_{stb})$ и является важной характеристикой. Предположим, что T_{act} равно 10 мс, а T_{stb} — 100 с, то P_{av} и R_{act} окажутся равными 5 мкВт и 10^{-4} . Было принято, что P_{act} равно 50 мВт, что является типичным значением для маломощного беспроводного терминала. Заметим, что это вычисление верно, только если P_{stb} достаточно мало, оно не должно превышать нескольких микроватт. На основе этих вычислений получен график срока службы батарей разных типов, приемлемых для беспроводных терминалов WAUN (рис. 2.15). Размер этих батарей существенно меньше, чем заданный объем терминала 10 см³. Ясно, что для обеспечения работы батарей в течение нескольких лет доля активности должна быть весьма малой. Расчеты были выполнены, исходя из предположения, что сумма $T_{act} + T_{stb}$ постоянна и равна 100 с, что соотносится с интервалом прерывистой работы. Таким образом, если снижается R_{act} , то следует уменьшить и T_{act} . Чтобы сделать возможным использование в беспроводном терминале WAUN тонкопленочных элементов питания, T_{act} необ-

ходимо уменьшить до 1 мс. Один из методов, позволяющих обеспечить такое короткое T_{act} , – использование ФАПЧ с быстрым захватом [15].

Описанный выше сценарий, в котором можно пренебречь P_{stb} , является идеальным и в настоящее время находится вне возможностей доступных нам технологий. С учетом этого в следующем разделе обсуждается ключевая для проекта многопороговая КМОП-технология (multithreshold complementary metal oxide semiconductor, МТСМОS) [16], позволяющая снизить P_{stb} .

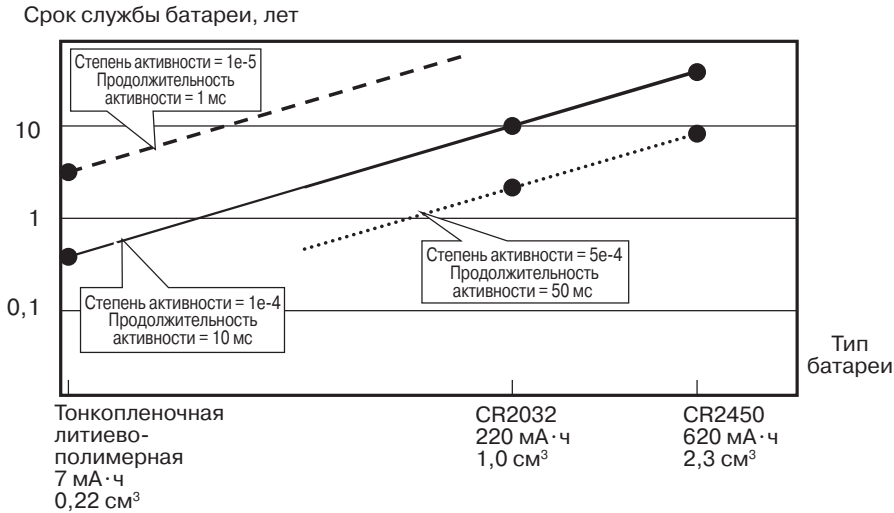


Рис. 2.15. Зависимость времени службы батареи от степени активности для различных типов батарей (потребление в активном режиме – 50 мВт)

2.6.3. Технология МТСМОS

В общем случае потребление энергии ожидается пропорциональным коэффициенту активности R_{act} . Однако нельзя полагаться на эти предположения, поскольку имеющийся ток утечки может оказаться доминирующим в потреблении энергии. Достичь заданного R_{act} с использованием обычных КМОП-технологий очень сложно. Требуемые R_{act} и токи утечки показаны на графике, построенном исходя из предположения, что потребление энергии в активном режиме составляет 50 мВт (рис. 2.16). В некоторых случаях беспроводной терминал должен иметь отдельные блоки, работающие с низкой тактовой частотой, для продолжения функционирования в периоды ожидания, что может оказать влияние на потребление энергии в эти периоды. Однако схемы, работающие с низкой тактовой частотой, обычно содержат небольшое количество вентилях, имеющих вполне удовлетворительный ток потребления порядка 0,1 мкА [17]. Напротив, основные цепи беспроводного терминала содержат большое количество вентилях, поскольку должны обеспечивать выполнение сложных операций. Следовательно, их мощности утечки будут большими. К тому же статический ток утечки всегда увеличивается на один-два порядка при повышении температуры окружающей среды от комнатной до при-

мерно 85 °С [18]. Поскольку беспроводные терминалы могут быть расположены в разных местах вне помещений, важным фактором становится их устойчивость к изменениям окружающей температуры. Это означает, что необходимо обеспечить низкую величину тока утечки, даже при ее возрастании на два порядка.

Среднее энергопотребление, мВт

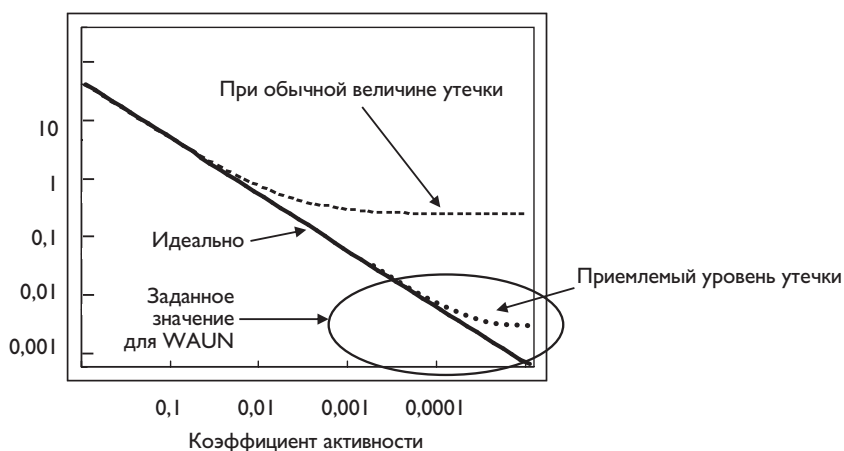


Рис. 2.16. Потребление энергии терминалом WAUN и нижний предел этого значения, определяемый током утечки (мощность в активном режиме принята равной 10 мВт)

Одним из наиболее многообещающих решений является использование технологии МТСМОС «кремний на изоляторе», КНИ (silicon-on-insulator, SOI) [16, 19]. В этой технологии низко- и высокопороговые полевые транзисторы МОП (metal oxide semiconductor field effect transistors, MOSFET) объединены в одной БИС. Низкопороговые транзисторы улучшают скоростные характеристики, особенно в радиочастотных цепях, тогда как высокопороговые снижают ток утечки в покое во время периода ожидания. Транзистор управления питанием подает напряжение в схему во время активного периода и отключает во время периода ожидания, исключая, тем самым, влияние тока утечки.

Принципиальная схема МТСМОС для беспроводного терминала показана на рис. 2.17. Основные цепи собраны на низкопороговых полевых МОП-транзисторах. Они подключены не напрямую к цепи питания (V_{DD}), а к цепи виртуального источника питания (V_{DDV}). Виртуальная цепь питания подключена к реальной через МОП-транзистор управления питанием, пороговое напряжение которого достаточно велико, чтобы сделать ток утечки в выключенном состоянии крайне низким. Была экспериментально исследована эффективность отключения питания, с использованием заказной КМОП/КНИ БИС, с заявленным током утечки менее 1 нА при комнатной температуре и сравнительно высокой нагрузочной способностью более 30 мА. Зависимость ее тока утечки от температуры изображена на рис. 2.18. Результаты показывают, что данная микросхема имеет достаточно большой запас в 1 мкА относительно заданного порогового значения.

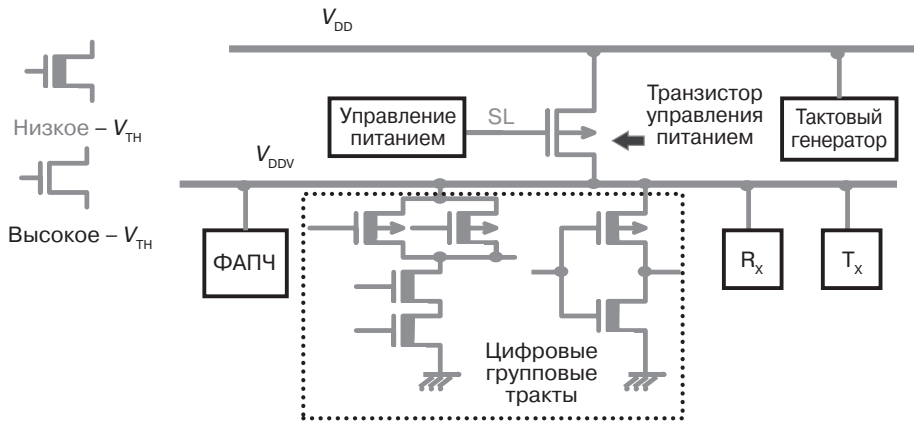


Рис. 2.17. Схема МТСМОС (блок, непрерывно работающий с низкой тактовой частотой, подключен к VDD напрямую)

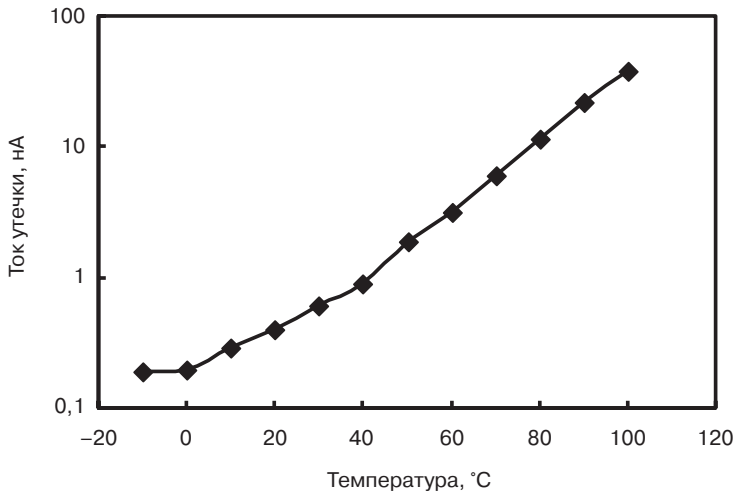


Рис. 2.18. Зависимость измеренного тока утечки переключателя питания от температуры

2.6.4. Результаты обеспечения низкого энергопотребления

Были представлены основные элементы схемотехники беспроводных терминалов сети WAUN. Поскольку эти терминалы работают в прерывистом режиме, общее потребление энергии терминалом сильно зависит от величины тока утечки, следовательно, его уменьшение является важным фактором. Было показано, что многопороговые КМОП-цепи могут обеспечить очень низкие значения потребления в периоды ожидания (менее 1 мкВт). Построенные таким образом схемы имеют высокую эффективность в прерывистых режимах работы, и их использование может продлить срок работы от батарей до 10 лет, даже если используются дисковые или тонкопленочные элементы.

2.7. Интерфейс прикладного программирования и промежуточное ПО

Сеть WAUN объединяет датчики и исполнительные механизмы множества типов, разбросанные по большой территории. Это открывает возможности создания мира, в котором территориально-распределенные прикладные программы регистрируют физическое состояние окружающей среды, считывая данные с датчиков, и управляют этим состоянием, отправляя команды исполнительным механизмам. Прикладные программы сети WAUN размещаются и на проводных терминалах (серверные приложения), и на беспроводных терминалах, оборудованных датчиками или исполнительными механизмами (приложения устройства), и работают благодаря обмену данными. Серверная программа в проводном терминале собирает, обрабатывает и анализирует данные с датчиков, накопленные программами устройств, или управляет этими программами. Для того, чтобы облегчить разработку подобных программ, предоставлены соответствующая библиотека и промежуточное ПО.

2.7.1. Коммуникационная библиотека в проводных и беспроводных терминалах

Прикладным программистам нет необходимости подробно изучать протоколы сети WAUN, поскольку коммуникационная библиотека WAUN обеспечивает простой и удобный интерфейс приема/передачи данных для программ на сервере и на устройствах. Пример ее использования приведен на рис. 2.19. Функция `ubi_send_blk` вызывает последовательность загрузки данных WAUN. Эта функция посылает данные, указанные в `msg.payload`, программе устройства, которое определяется служебным идентификатором в `msg.service_id`, и возвращает управление, получив от шлюза IP сообщение «ответная передача данных», как показано на рис. 2.6. Функция `ubi_send_nbk` возвращает управление, не ожидая получения ответного сообщения от шлюза IP. Серверная программа получает ответные сообщения, используя функцию `ubi_recv_nbk`.

```
char* buffer;
struct send_message msg;
int ret;

buffer = (char*)malloc(BUFFER_SIZE + 1);
strcpy(msg.service_id,
       "0x0100000000000000000000000000000000000000000000000000000000000001");
msg.len = BUFFER_SIZE;
msg.payload = buffer;

ret = ubi_send_blk(UBI_DL_IMM, &msg);
if (ret < 0)
{
    fprintf(stderr, "ubi_send_blk NG: %d\n", ret);
    ubi_finalize();
    free(buffer);
    exit(1);
}
```

Рис. 2.19. Пример кода серверной программы, использующей коммуникационную библиотеку WAUN

Библиотека также содержит следующие дополнительные функции для улучшения удобства пользования и повышения качества программного обеспечения: 1) псевдомногогосеансовая функция строит очередь запросов на передачу данных от программы и последовательно обрабатывает эти запросы, чтобы освободить приложение от управления сеансами; 2) для повышения надежности передачи данных, если передача данных оказывается неудачной, функция повторной передачи и удаления дубликатов автоматически повторяет отправку (и удаляет повторно полученные данные); 3) для передачи данных, превышающих размер максимального блока данных для передачи (maximum transmission unit, MTU), имеется функция фрагментирования и обратной сборки; 4) для снижения частоты передачи небольших объемов данных поддерживается функция упаковки/распаковки. Это повышает эффективность работы беспроводных терминалов, частота коммуникации которых ограничена системой управления доступа WAUN. Прикладной программный интерфейс (API) для обоих типов терминалов был реализован на языке C, а также на версии языка nesC [20] для беспроводных терминалов, работающих под управлением TinyOS [21].

2.7.2. Промежуточное ПО: *uTupleSpace*

Разработка серверного ПО может оказаться сложной задачей по разным причинам. Во-первых, форматы данных, используемые для обмена с каждой программой устройства, могут отличаться, поскольку такой формат часто зависит от датчика или исполнительного механизма. Во-вторых, одна программа устройства может одновременно использоваться двумя или более серверными программами. В-третьих, программы не всегда доступны для коммуникации, так как беспроводные терминалы работают в прерывистом режиме, а также могут покинуть зону обслуживания. К тому же не все адреса доступных программ устройств известны, поскольку эти программы добавляются и удаляются динамически. Таким образом, необходимо промежуточное программное обеспечение (middleware), которое позволяет серверным программам связываться с различными типами ПО устройств единообразно и на равных условиях, а также прозрачно общаться с ними, не имея информации об их существовании и адресах, даже если они перемещаются в зоне обслуживания и покидают ее. В качестве промежуточного ПО, удовлетворяющего этим условиям, предложено ПО *uTupleSpace* [22].

Программа *uTupleSpace* основана на модели пространства кортежей (tuple space) [23], концепции, используемой в параллельных и распределенных вычислениях. Буква *u* означает повсеместность (ubiquitous). Модель пространства кортежей — это модель с разделяемой памятью, которую программы используют для сообщения между собой путем чтения и записи данных, называемых кортежами, в или из логически общей памяти, называемой пространством кортежей (рис. 2.20). Программа, выполняющая запись в пространство кортежей, регистрирует кортеж, называемый «содержимое» (entry), который содержит данные, тогда как программа, выполняющая чтение, регистрирует кортеж, именуемый «шаблон» (template), в который включены образцы, сопоставляемые с «содержимым», и читает сопоставленные данные из пространства кортежей. Путем такого сопоставления достигается единообразное, равноправное и непрямое сообщение, при котором неизвестны существование адресата и его адрес.

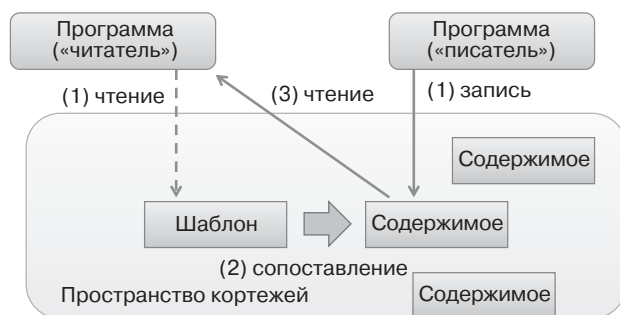


Рис. 2.20. Модель пространства кортежей

Было изучено множество областей применения пространства кортежей в среде со сплошным покрытием [24–27]. Хотя они поддерживают избирательное чтение, в глобальной среде избирательная запись не поддерживается. Возможность избирательной записи является важной для исполнительных механизмов, поскольку она позволяет указать условия, при которых разрешается чтение, для запрета возможности чтения этих данных неавторизованными программами управления. Кроме того, шаблоны в их исходном определении не могут задавать пространственно-временной диапазон для программ устройств (беспроводных терминалов). Однако положение и время являются важным фактором для повсеместности работы прикладных программ. Поэтому модель `uTupleSpace` расширяет модель шаблонов пространства кортежей для поддержки избирательной записи и эффективного диапазона поиска для многомерных ключей.

Модель `uTupleSpace` расширяет обычный кортеж до кортежа `uTuple`, который в дополнение к участку данных, соотносящихся с обычным кортежем, имеет участок с метаданными. Он содержит информацию о типе устройства, адресе (служебном идентификаторе беспроводного терминала), позиции и времени, в которых работает «читатель» или «писатель» (т.е. беспроводной терминал), и типе данных в участке данных. Кроме того, `uTupleSpace` поддерживает два типа коммуникаций. Коммуникация по событию выполняет избирательное чтение по совпадению шаблона «читателя» с содержимым, записанным «писателем», тогда как коммуникация по команде выполняет избирательную запись по соответствию шаблона «писателя» с содержимым «читателя». Эти коммуникационные модели показаны на рис. 2.21. При коммуникации по событию «писатель» (программа устройства датчика) регистрирует `uTuple (eventActual)`, состоящее из собственных сообщений «писателя» в каждой части. Затем «читатель» (серверная программа) регистрирует `uTuple (eventFormal)`, состоящее из шаблонов в каждой части, которые должны соответствовать желаемому «писателю» и его данным. При коммуникации по команде «читатель» (программа устройства) регистрирует `uTuple (commandFormal)`, состоящее из собственных сообщений «писателя» в части метаданных и шаблона в части данных, который соответствует ожидаемым командным данным. Затем «писатель» (серверная программа) регистрирует `uTuple (commandActual)`, состоящее из сообщения в части данных и шаблона в части метаданных, который соответствует желаемым «читателям».



а) коммуникация в результате события б) коммуникация по команде

Рис. 2.21. Коммуникационная модель uTupleSpace

Для применения модели uTupleSpace в сети WAUN она была реализована в проводных терминалах в виде uTupleServer (рис. 2.22). Такое решение было принято в связи с тем, что проводные терминалы имеют достаточно ресурсов и все чувствительные данные выгружаются на эти терминалы. Программы, которые пишут или читают кортежи uTuple с uTupleServer, реализованы в виде uTupleClient, предоставляющие API доступа к uTupleSpace.

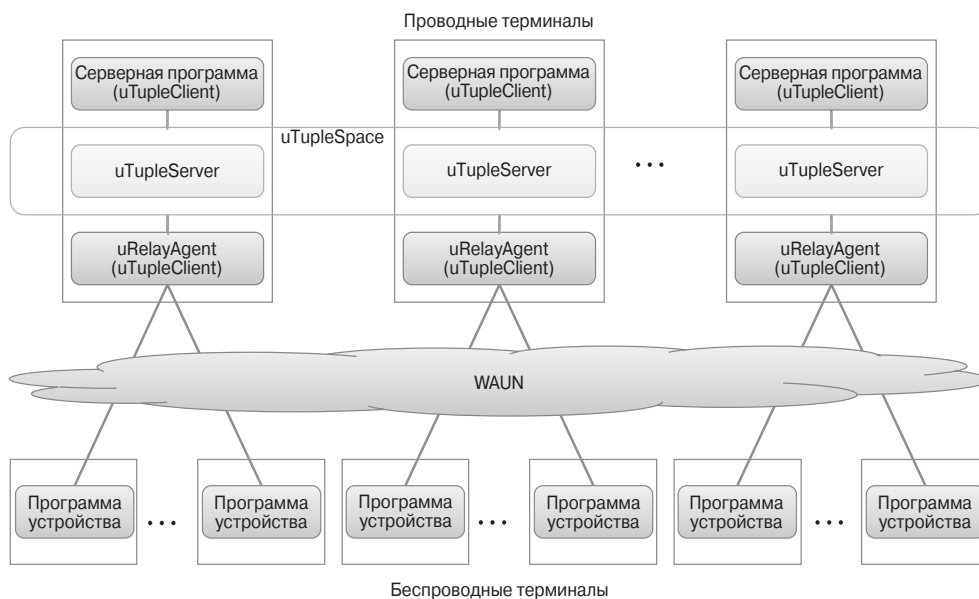


Рис. 2.22. Архитектура промежуточного ПО uTupleSpace

Программы устройств в беспроводных терминалах, подключенных к WAUN, загружают и выгружают данные на прокси `uRelayAgent`, расположенный на более высоком уровне для чтения и записи кортежей `uTuple`. `uRelayAgent` использует коммуникационную библиотеку для обмена с программами устройств и управляет информацией об этих устройствах, чтобы сформировать метаданные для `eventActual` и `commandFormal` для каждой программы устройства. Эта информация заблаговременно регистрируется в `uRelayAgent` с соответствующим служебным идентификатором и обновляется с использованием информации, полученной из WAUN. Для данных, выгружаемых программой устройства, `uRelayAgent` создает `eventActual` и записывает его в `uTupleServer`. Чтобы загрузить данные в программу устройства, `uRelayAgent` создает `commandFormal`, читает `commandActual`, соответствующий этому `commandFormal`, и обрабатывает этот набор из `commandFormal` и `commandActual` вместе с соответствующим им служебным идентификатором. Этот идентификатор является идентификатором того беспроводного терминала, в который будут загружаться данные. Используя служебный идентификатор, `uRelayAgent` формирует и посылает данные. Такой механизм позволяет серверным программам общаться с программами устройств в нужном беспроводном терминале через сеть WAUN, просто читая и записывая кортежи `uTuples` в `uTupleServer`.

Хотя модель пространства кортежей обеспечивает гибкую коммуникацию в среде со сплошным покрытием, она должна иметь достаточную масштабируемость, чтобы обеспечить работу многих экземпляров программ с огромными количествами данных, поскольку при каждой коммуникации происходит сопоставление данных. Для достижения масштабируемости пространство кортежей создается путем использования большого количества серверов с функциями распределения хранилища данных и нагрузки по обработке сопоставлений. То есть `uTupleSpace` распределяет кортежи `uTuple` по серверам `TupleServer`, используя распределенную хэш-таблицу (*distributed hash table*, DHT) для быстрого сопоставления больших количеств разнообразных данных. Обработка соответствий распределена по серверам `uTupleServer` в соответствии с ключом распределения, который состоит из информации о типе устройства и типе данных, записанной в метаданных кортежа `uTuple`.

Таким образом, поиск в многомерном диапазоне с использованием положения и времени, адреса и значений данных для кортежей `uTuple`, имеющих одинаковые тип устройства и тип данных, может осуществляться на одном сервере `uTupleServer` [28]. Чтобы улучшить пропускную способность сопоставления данных даже при увеличении количества пишущих и читающих `uTuple`, используется технология масштабирования [29]. Когда количество кортежей `uTuple`, записанных в соответствующий `uTupleServer` возрастает, другой `uTupleServer` автоматически начинает разделять эти кортежи. Когда количество выполняемых сопоставлений для `uTuple` на определенном `uTupleServer` превышает допустимый уровень нагрузки, новый `uTupleServer` копирует шаблоны `uTuple` с первого и выполняет сопоставление данных параллельно.

Одна из причин, по которой концепция «пространства кортежей» не используется широко, является ее масштабируемость. Эффективность обработки была

измерена на системе-прототипе, использующей Mac OS X Server (2,8 ГГц Quad-Core Xeon, 2 ГБ ОЗУ), а затем была выполнена оценка масштабируемости. Ее результаты показаны на рис. 2.23. Приведено число обработанных в секунду кортежей uTuple, начиная с регистрации кортежа и заканчивая возвращением результатов сопоставления. Тестируемое приложение поддерживает только коммуникацию по команде и имеет 10 млн беспроводных терминалов, записывающих 500 млн uTuples (eventActual) в день. Серверы uTupleServer хранят 3,5 млрд eventActual и 1000 eventFormal и выполняют сопоставление 6000 eventActual, вновь регистрируемых каждую секунду, и 1 eventFormal, вновь регистрируемое каждые 10 с. Каждый из новых eventActual соответствует одному уже зарегистрированному eventFormal, а каждый новый eventFormal соответствует 100 уже зарегистрированным eventActual. Рис. 2.23 показывает, что uTupleSpace может достичь масштабируемости даже несмотря на увеличение количества данных и процессов сопоставления.

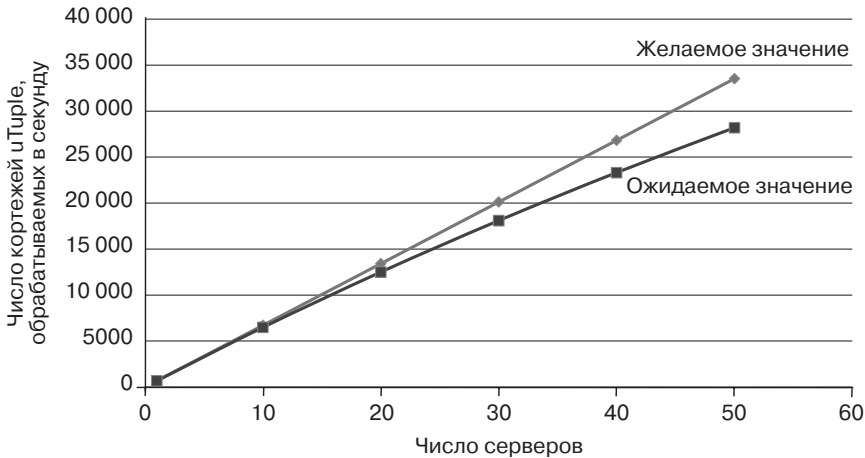


Рис. 2.23. Оценка производительности сопоставления данных

2.8. Экспериментальная часть [36]

2.8.1. Предпосылки к проведению экспериментов

Передача данных в восходящем канале в сети WAUN является ключевым техническим препятствием, поскольку мощность передачи беспроводных терминалов сильно ограничена, что позволяет снизить стоимость беспроводного доступа. Поэтому исследования методов беспроводной связи на большие расстояния были сосредоточены на восходящей передаче данных из терминалов [12]. Непосредственной целью было реализация соты радиусом 5 км при мощности передатчика беспроводного терминала 10 мВт, что в Японии является максимальным значением, не требующим получения разрешения при использовании вне помещений [30].

Для достижения этой цели необходимо дополнить прием на разносенные антенны разносением точек приема для компенсации снижения производи-

тельности из-за отражений и затуханий сигнала. Традиционный подход при разнесении мест приема заключается в использовании схем комбинированной селекции [31, 32]. Тем не менее, сеть WAUN должна иметь меньшую вероятность потерь сигнала, чем телефонные сотовые системы, поскольку она обязана поддерживать преимущественно неподвижные объекты. Для разнесенного приема наиболее подходящим является метод суммирования дифференциально взвешенных сигналов (MRC). Для разнесения точек приема применяется подсистема цифровой передачи радиосигнала по оптоволокну (DROF). Она может соединять радиочастотный и групповой тракты точки доступа оптоволоконным кабелем. Это позволяет расположить радиокомпоненты на расстоянии друг от друга.

Для того, чтобы доказать пригодность подсистемы DROF и выполнимость разнесенного приема, были проведены испытания в Токио (Япония). В данном разделе приводятся результаты этих испытаний. Прежде всего перед их проведением была оценена теоретически выполнимость требования к радиусу соты в 5 км при мощности беспроводного терминала 10 мВт. Затем была проведена оценка уровня приема наших прототипов, разработанных на основе экспериментов с проводными системами. Далее, используя прототипы, оценен уровень приема и производительность передачи при разнесенном приеме. В ходе испытаний было обнаружено, что метод MRC как средство обеспечения разнесенного приема вполне реализуем. По итогам исследований сделан вывод, что точка доступа может использовать как разнесение приемных антенн, основанное на использовании MRC, так и пространственное разнесение, основанное на том же методе. Таким образом, радиус соты в 5 км при мощности передатчика беспроводного терминала 10 мВт является реализуемым.

2.8.2. Параметры беспроводного восходящего канала сети WAUN

Характеристики беспроводного восходящего канала сети WAUN приведены в табл. 2.2. Для несущей частоты выбраны метровый (УКВ) и дециметровый (ДМВ) диапазоны, поскольку потери при распространении в них радиосигнала сравнительно малы, а сеть WAUN не требует широкой полосы пропускания. Было принято, что антенна точки доступа будет расположена на крыше здания NTT, так как высокий коэффициент усиления антенны требует и большего ее размера. Учитывая желание сделать размер антенны разумным, и для ее использования и в УКВ-, и ДМВ-диапазонах, ее коэффициент усиления равен 10 дБи. Коэффициент усиления антенны беспроводного терминала был выбран равным -10 дБи для внутренней антенны и 0 дБи — для внешней. Помимо этого, коэффициент шума принят равным 4 дБ — значение, которое может быть получено при размещении малошумящих усилителей (low-noise amplifier, LNA) рядом с антенной на крыше для компенсации потерь в соединительном кабеле. В качестве схемы модуляции и метода прямого исправления ошибок выбраны квадратурная фазовая модуляция со сдвигом $\pi/4$ (QPSK) и сверточное кодирование и декодирование по алгоритму Витерби с мягким решением, описанные в разд. 2.5. Скорость передачи данных равна 9600 бит/с. Полагаем, что этой скорости достаточно для работы сервисов WAUN.

Таблица 2.2. Параметры беспроводного восходящего канала связи сети WAUN

Диапазон несущей частоты	УКВ/ДМВ
Мощность передатчика беспроводного терминала	10 мВт
Усиление антенны	AP: 10 дБи WT: –10 дБи (внутренняя антенна) 0 дБи (внешняя антенна)
Уровень шума	4 дБ (в точке доступа)
Модуляция/демодуляция	Квадратурная фазовая модуляция со сдвигом $\pi/4$ /синхронное детектирование
Прямая коррекция ошибок	Сверточное кодирование (ограничение длины – 7, скорость кодирования – 1/2). Декодирование по алгоритму Витерби с мягким решением
Глубина чередования	16 бит
Скорость передачи	9600 бит/с
Требуемый уровень приема	–126 дБм (чтобы достичь уровня ошибок 0,01 в условиях аддитивного белого гауссова шума)
Схема разнесения	Разнесение приемных антенн и точек приема

Такая полоса является узкой, следствием чего является плоское замирание. Следовательно, для того, чтобы увеличить эффективность прямого исправления ошибок в такой среде, используется интерливер–деинтерливер. Требуемый уровень приема составляет –126 дБм при коэффициенте ошибочных пакетов менее 0,01 в условиях аддитивного белого гауссова шума (additive white Gaussian noise, AWGN). Кроме того, для компенсации снижения производительности в условиях экранирования и затуханий в точке доступа используется разнесение антенн и точек приема.

2.8.3. Теоретическое исследование реализуемости 5-километровой соты на местности

2.8.3.1. Конфигурация соты. Чтобы реализовать разнесение приемных антенн и точек приема, используется конфигурация соты, показанная на рис. 2.8 и описанная в разд. 2.5. Радиочастотные блоки точки доступа (AP-R) размещены в трех равноудаленных местах на границе соты с угловыми интервалами 120° . Модули AP-M точки доступа могут быть расположены где угодно, поскольку AP-R связаны с ними посредством DROF. Каждая точка включает три блока AP-R, каждый из которых оснащен секторной антенной с углом раскрытия на половинной мощности 120° , использует свою частоту и покрывает зону другой соты с углом 120° . Такая конфигурация обеспечивает разнесение приема по трем точкам без увеличения количества зданий, на которых установлены блоки AP-R. Кроме того, если AP-R имеет несколько секторных, направленных в одну сторону антенн, AP сможет применить метод разнесения приемных антенн.

2.8.3.2. Теоретическая оценка. Теоретическая реализуемость беспроводной передачи данных на 5 км с использованием передатчика беспроводного терминала мощностью 10 мВт путем вычисления интегральной функции распределения (cumulative distribution function, CDF) уровня приема. Сигналы, принимаемые

каждым AP-R, объединяются с использованием MRC в случае, если AP-R имеет несколько антенн секторного типа, что соответствует возможности AP реализовать прием на разнесенные антенны. Исходя из этого предположения, вычисляем CDF уровней приема для двух схем разнесенного приема: 1) объединенные сигналы со всех точек приема в соте дополнительно объединяются с использованием MRC (трехточечный MRC); 2) выбирается объединенный сигнал, имеющий наивысший уровень приема среди точек приема соты (выбор из трех точек); 3) кроме того, также вычисляется CDF уровня приема, когда все антенны точки доступа находятся в центре соты, антенны точки доступа являются всенаправленными, и принятые сигналы объединяются с помощью MRC (одноточечного), если точка доступа имеет несколько антенн. Принимаем, что в первом и втором случаях каждый AP-R имеет одну или две антенны (с одним или двумя ответвлениями при использовании трехточечного MRC (1B3S-MRC или 2B3S-MRC) либо трехточечного выбора (1B3S-sel или 2B3S-sel)), в третьем случае точка доступа имеет три или шесть антенн (три или шесть ответвлений на точку приема (3B1S или 6B1S)). Несущая частота равна 280 МГц. Высоты расположения антенн точки доступа и беспроводного терминала принимаются равными 30 м и 1 м соответственно. Коэффициент усиления антенны беспроводного терминала равен -10 дБи (внутренняя антенна). Были использованы следующие модели распространения: Окамура–Хата [33], логарифмически нормального распределения и рэлеевская как модели распространения на большое расстояние, экранирования и затухания соответственно. Также были проведены исследования распространения радиоволн в том же районе Токио. Измеренные значения были использованы для получения следующих параметров: стандартного отклонения логарифмически нормального распределения, корреляции экранирования и корреляции затухания. Оценки CDF приведены на рис. 2.24. Вероятность ошибки принята равной 1%, что меньше, чем примерно 10% в обычных телефонных сетях сотовой связи [34]. Как показано на рис. 2.25, конфигурация 2B3S-MRC имеет преимущество в 6 дБ перед 6B1S, если обе они имеют равное число антенн. Кроме того, конфигурация 2B3S-MRC эффективнее на 4,5 и 2,5 дБ по сравнению с 1B3S-MRC и 2B3S-sel. Поэтому использование разнесения точек приема с использованием MRC и разнесения антенн с MRC дают заметное улучшение уровня покрытия соты.

Далее была оценена высота расположения антенны точки доступа, необходимая для достижения требуемого уровня ошибок в первом варианте соты, трехточечном MRC. В частности, рассчитана вероятность ошибки при требуемом уровне приема как функция от высоты расположения антенны точки доступа. Кроме того, при этой оценке считается, что каждый AP-R имеет одну, две или три антенны (1B3S-MRC, 2B3S-MRC и 3B3S-MRC), а коэффициент усиления антенны беспроводного терминала – как 0 дБ и -10 дБ для внешней и внутренней антенны. На рис. 2.25 показана вероятность ошибки в зависимости от высоты расположения антенны точки доступа. При работе беспроводного терминала с внешней антенной конфигурация 2B3S-MRC может обеспечить вероятность ошибки 1% при высоте расположения антенны 20 м, что соответствует высоте здания NTT. При работе беспроводного терминала с внешней антенной конфигурация 2B3S-MRC

может обеспечить вероятность ошибки 1% при высоте расположения антенны 20 м, что соответствует высоте здания NTT с учетом размещения на крыше стальной мачты. Поэтому радиус соты в 5 км на местности при мощности передатчика беспроводного терминала 10 мВт может быть получен при использовании конфигурации соты 2B3S-MRC. Это означает, что если реализуется разнесение точек приема с использованием MRC и разнесенные приемные антенны с использованием MRC, то можно обеспечить радиус соты 5 км.

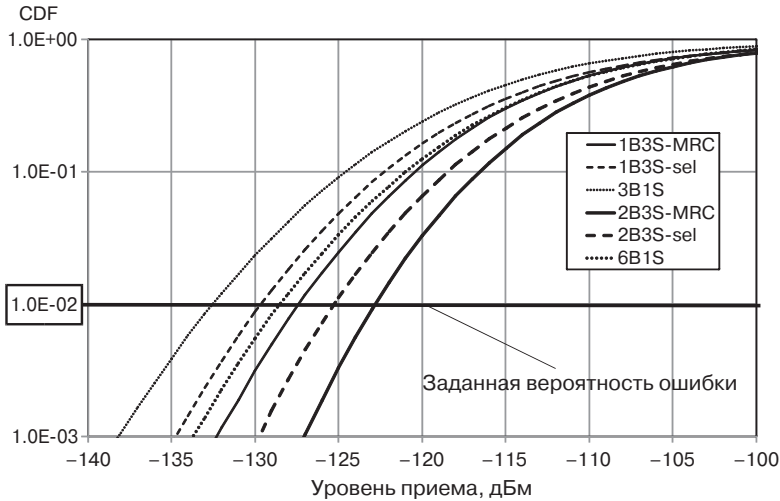


Рис. 2.24. Интегральная функция распределения уровня приема

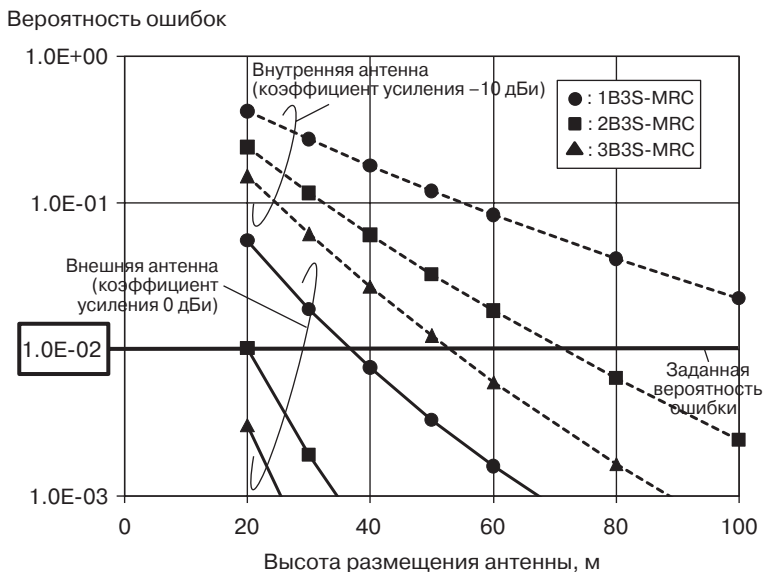


Рис. 2.25. Вероятность ошибки как функция высоты размещения антенны точки доступа

2.8.4. Оценка прототипа

Были разработаны прототипы точки доступа и беспроводного терминала, в которых реализованы функции РНУ, описанные в разд. 2.5. Их характеристики приведены в табл. 2.3. Чувствительность приема прототипов была оценена на основе экспериментов с проводными устройствами при передаче 16-байтовых пакетов данных. Конфигурации с одно- и двухкратным разнесением были протестированы в среде AWGN и в условиях затухания с независимыми и тождественно распределенными рэлеевскими каналами соответственно.

Частота появления ошибочных пакетов (коэффициент пакетных ошибок) (packet error ratio, PER) показана на рис. 2.26. Для сравнения пунктирными линиями показаны результаты компьютерного моделирования, при котором уровень шума был принят равным 4 дБ – значение, используемое при разработке беспроводной системы связи. Требуемый уровень приема определен как уровень, при котором в среде AWGN PER составляет 0,01. Как показано на рис. 2.26, чувствительность приема прототипа точки доступа соответствует результатам моделирования, а уровень приема в восходящем канале при PER = 0,01 соответствует заданному для беспроводного канала уровню –126 дБм (табл. 2.2). Таким образом, эффективность передачи данных прототипом может считаться удовлетворяющей требованиям. Кроме того, из рис. 2.26 видно, что эффективность при передаче в нисходящем канале на несколько децибел хуже, чем при передаче в восходящем канале (с одно- и двухкратным разнесением). Эти результаты обусловлены неизбежной разницей в чувствительности между дифференциальным и синхронным детектированием, используемым при приеме и передаче. Следовательно, мощность передатчика точки доступа должна быть выше, чем передатчика беспроводного терминала.

Таблица 2.3. Характеристики прототипа

Параметр	Точка доступа	Беспроводной терминал
Несущая частота	286,4625 МГц	
Мощность передачи	100 мВт	10 мВт
Символьная скорость	9600 бод	
Скорость передачи данных	9600 бит/с	
Режим передачи	TDMA-TDD	
Схема модуляции	Квадратурная фазовая модуляция со сдвигом $\pi/4$	
Схема демодуляции	Синхронное детектирование	Дифференциальное детектирование
Информация для синхронизации	Только пилотные символы	Только один заголовок
Прямая коррекция ошибок	Сверточное кодирование и декодирование по алгоритму Витерби с мягким решением (ограничение длины – 7, скорость кодирования – 1/2)	
Схема разнесения	В восходящем канале: MRC В нисходящем канале: сдвиг частоты	

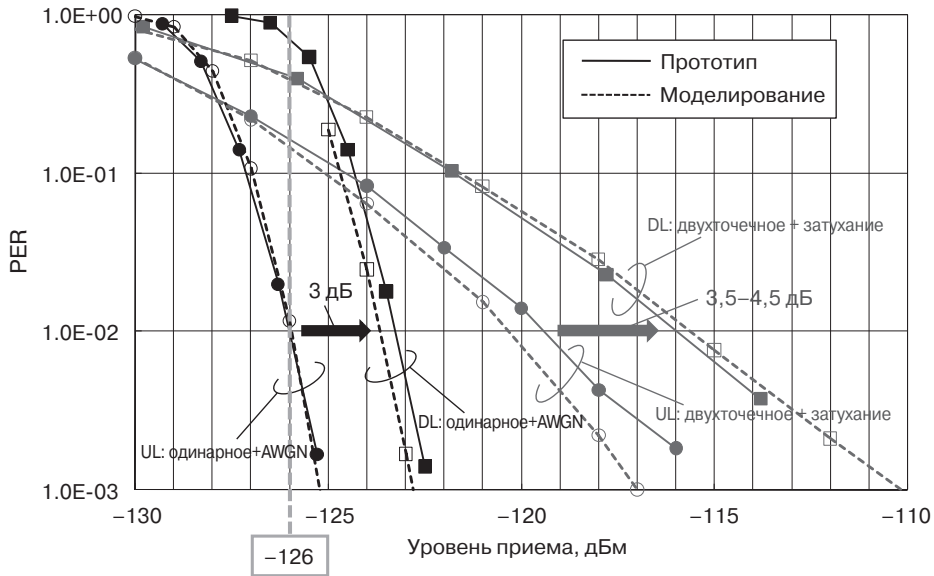
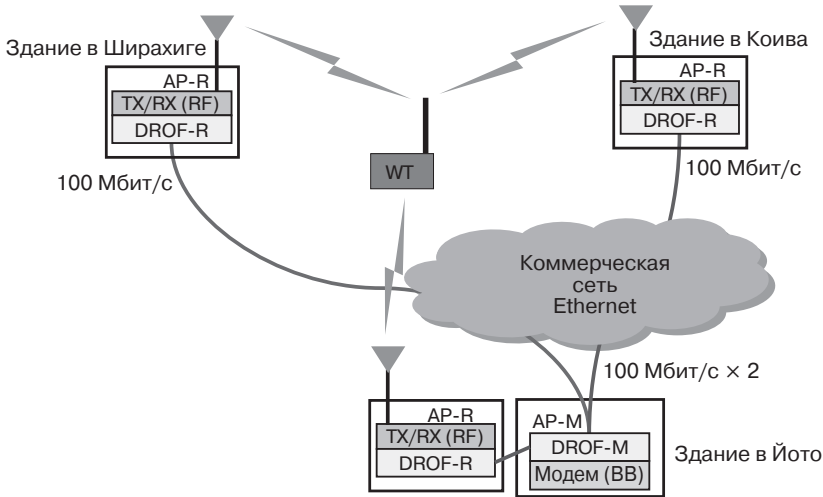


Рис. 2.26. Доля ошибок передачи прототипа



WT – беспроводной терминал

Рис. 2.27. Схема подсистемы DROF и разнесения точек приема при полевом тестировании

2.8.5. Полевые испытания

2.8.5.1. Краткое описание. Прототип был испытан в полевых условиях. Для соединения AP-M и AP-R использовалась подсистема DROF. Схема этой подсистемы показана на рис. 2.27. По одному AP-R было размещено на каждом из трех зданий NTT (в Ширахиге, Йото и Коива) в Большом Токио, AP-M – на здании в Йото. Здания были соединены с помощью подсистемы DROF, работающей поверх ком-

мерческой сети Ethernet. В подсистеме DROF оцифрованные радиосигналы с радиоинтерфейса помещались в пакеты Ethernet и передавались между главным DROF (DROF-M) и удаленным DROF (DROF-R) в обоих направлениях. Чтобы обеспечить синхронизацию времени и частоты между DROF-M и DROF-R, тактовый сигнал DROF-M подавался на AP-R. Такая синхронизация позволяет обеспечить временное согласование сигналов, принятых AP-R и AP-M. Таким образом, использование подсистемы DROF может обеспечить основанный на MRC прием в разнесенных точках.

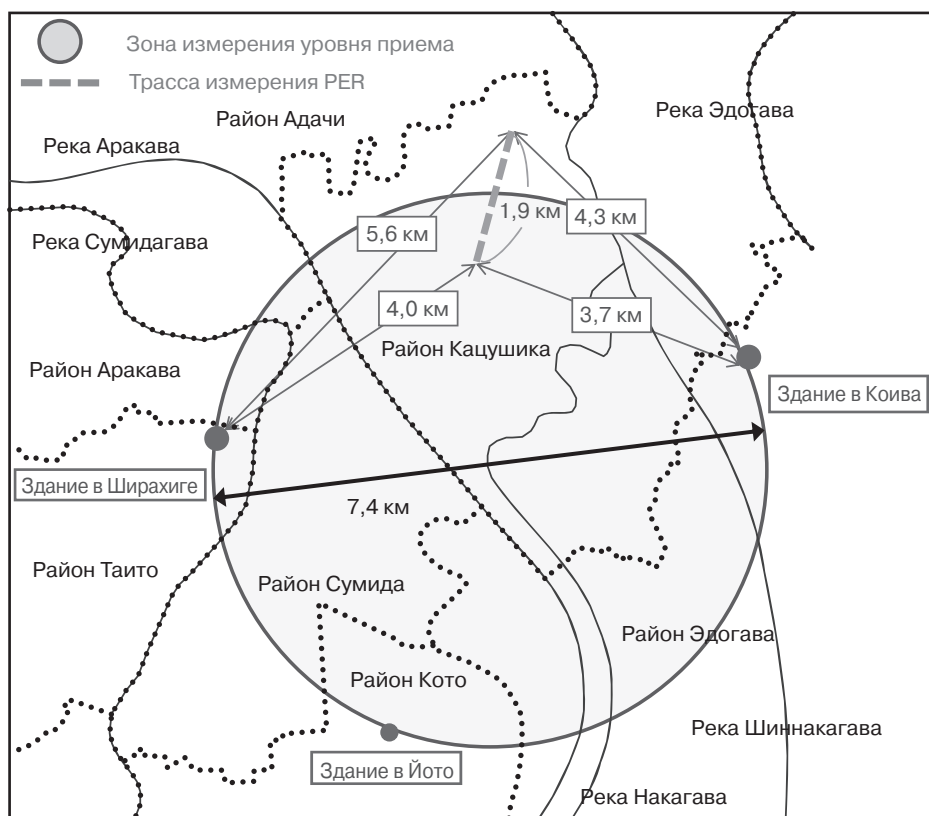


Рис. 2.28. Карта уровней приема и измерения коэффициента пакетных ошибок в ходе полевых испытаний

Для оценки уровня приема при работе трех разнесенных точек без использования разнесенных антенн (1B3S-MRC) использовались три AP-R и AP-M. Кроме того, две AP-R (в Ширахиге и Коива) и AP-M использовались для оценки уровня ошибок при приеме в двух точках без разнесения антенн (1B2S-MRC). Все антенны точки доступа были размещены на крышах зданий NTT. Каждая антенна являлась уголковым отражателем с коэффициентом усиления 7 дБи, размещались они на высоте 35, 29 и 25 м на зданиях в Ширахиге, Йото и Коива. Беспроводной терминал размещался в транспортном средстве, оборудованном измерительной

аппаратурой, а его дипольная антенна с коэффициентом усиления 2 дБи была установлена на крыше. Уровень потерь между антенной и беспроводным терминалом изменялся с помощью ступенчатого аттенюатора таким образом, чтобы общий коэффициент усиления соответствовал принятому при расчетах. Антенна беспроводного терминала была внутренней с усилением -10 дБи. Измерительное транспортное средство перемещалось по Токио, передавая фиксированное количество данных (16 байт), прием проводился как с разнесением точек приема с MRC, так и без разнесения. Схема зоны полевых испытаний представлена на рис. 2.28. Окружность соответствует зоне измерений уровня приема. Трасса фактического перемещения изображена пунктирной линией. Она выбиралась таким образом, чтобы в районе зданий в Ширахиге и Коива уровни приема были примерно равны.

2.8.5.2. Результаты полевых испытаний. Функции CDF уровней приема приведены на рис. 2.29. Толстые и тонкие непрерывные линии соответствуют измеренным значениям CDF вариантов 3B1S-MRC и 1B1S-MRC, в последнем случае AP-R находилась на здании в Ширахиге. Для сравнения пунктирными линиями обозначены рассчитанные значения CDF, полученные в ходе компьютерного моделирования, результаты которого представлены на рис. 2.24. Измеренные величины CDF совпадают с рассчитанными теоретически. Это доказывает, что рассчитанные величины CDF уровней приема (рис. 2.24) и теоретическая вероятность ошибок (рис. 2.25) соответствуют действительности.

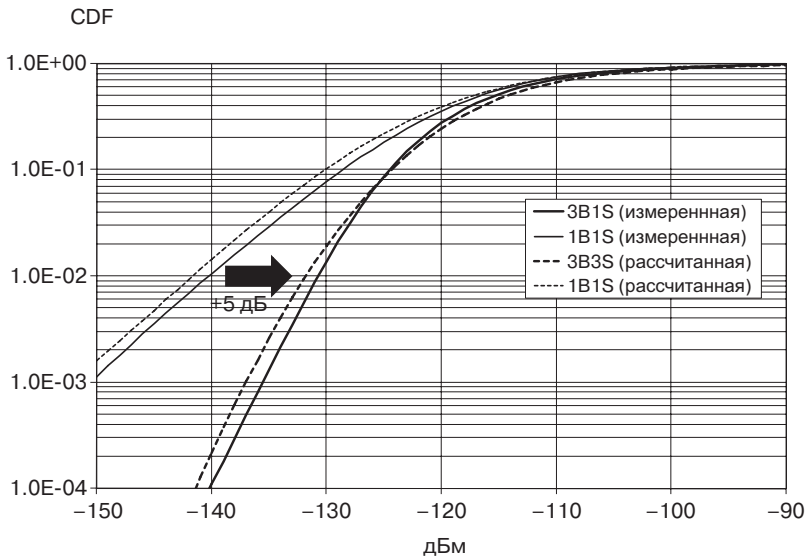


Рис. 2.29. Интегральная функция распределения уровней приема

Зависимость PER от уровня приема показана на рис. 2.30. Уровень приема при разнесенных точках приема определен как среднее значение для двух зданий. Для сравнения сплошными и пунктирными линиями показаны полученные с помощью компьютерного моделирования значения PER для многоточечного при-

ема с использованием MRC и одноточечного приема. Уровень шума предполагался равным 6 дБ. В качестве модели замираний использовались независимые и тождественно распределенные рэлеевские каналы с одинаковой мощностью по всем путям. Измеренные величины PER в основном соответствуют полученным в ходе компьютерного моделирования для случаев многоточечного и одноточечного приемов (рис. 2.30). Этим подтверждается, что подсистема DROF, использующая разнесение точек приема, может обеспечить теоретический выигрыш от MRC в реальных условиях распространения радиоволн. Разнос точек приема может обеспечить величину PER на порядок меньшую, чем для одной точки приема. Результаты подтверждают реализуемость разноса точек приема на основе использования подсистемы DROF и показывают, что схема MRC позволяет обеспечить разнос точек приема в сочетании с подсистемой DROF.

Из приведенных выше результатов можно сделать вывод, что точка доступа может использовать разнесение точек приема с MRC, так же как и разнесение приемных антенн с MRC. Следовательно, с учетом данных технологий можно реализовать соту радиусом 5 км при мощности передатчика 10 мВт.

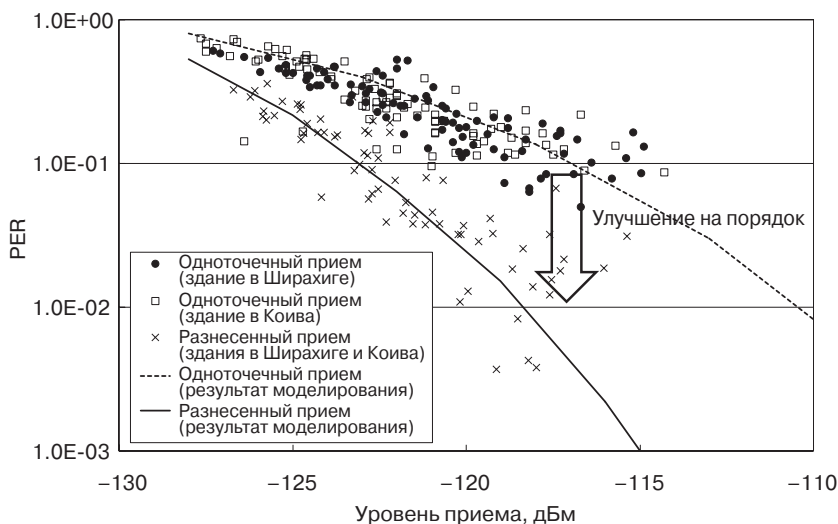


Рис. 2.30. Зависимость коэффициента пакетных ошибок от уровня приема в ходе полевых испытаний

2.9. Выводы

В этой главе описана распределенная сеть со сплошным покрытием (WAUN), которая является сетевой инфраструктурой, предназначенной для датчиков и исполнительных механизмов. Был разработан прототип системы, а также было подтверждено, что можно получить заданную при исследованиях и разработке цель реализовать соту радиусом 5 км с использованием беспроводных терминалов мощностью 10 мВт со сроком службы батарей 10 лет. Можно предполагать, что существует большой и перспективный рынок для сетей датчиков и исполнительных механизмов или соеди-

нений «машина—машина», и этот рынок является важным для развития сетевых операторов. Для дальнейшего развития рынка вместе с бизнес-партнерами проводятся испытания прикладных сервисов с использованием системы-прототипа.

Кроме того, для увеличения числа партнеров описываемая сеть предлагается органам стандартизации. Например, на заседании ITU-R/WP-5A, проходившем с 23 октября по 6 ноября 2008 года, началось предварительное обсуждение новой концепции «Мобильные беспроводные сети доступа, обеспечивающие обмен с большим числом территориально-распределенных датчиков и исполнительных механизмов, в наземных мобильных устройствах обслуживания», к числу которых относится и сеть WAUN. Посредством международной стандартизации и переговоров с бизнес-партнерами планируется развивать коммерческое использование предложенной системы для повсеместного применения.

Также широкое использование сети WAUN приведет к созданию вторичного рынка, на котором реализуются данные с датчиков, собранных операторами WAUN. Используя эти данные, вторичные пользователи смогут создавать продукты или услуги с добавленной стоимостью. По существу сеть WAUN является шагом к новому рынку распространения информации.

Литература

1. <http://www.ubiq.com/hypertext/weiser/UbiHome.html>.
2. G. J. Pottie and W. J. Kaiser, Wireless integrated network sensors, *Commun. ACM*, Vol. 43, No. 5, pp. 551–558, May 2000.
3. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, A survey on sensor networks, *IEEE Commun. Mag.*, Vol. 40, No. 8, pp. 102–114, 2002.
4. B. W. Cook, S. Lanzisera, and K. S. J. Pister, SoC issues for RF smart dust, *Proce. IEEE*, Vol. 94, No. 6, pp. 1177–1196, June 2006.
5. H. Saito, O. Kagami, M. Umehira, and Y. Kado, Wide area ubiquitous network: The network operator's view of a sensor network, *IEEE Commun. Mag.*, Vol. 46, No. 12, pp. 112–120, 2009.
6. H. Saito, M. Umehira, and T. Ito, Proposal of the wide area ubiquitous network, in *Telecommunications World Congress*, Budapest, Hungary, 2006.
7. <http://www.kantei.go.jp/jp/singi/bt/dai2/2siryou10-3-3-4.pdf> (на японском языке).
8. http://www.mlit.go.jp/kisha/kisha07/09/090704_.html (на японском языке).
9. <http://www.zaimu.japanpost.jp/tokei/2004/excel/yuubin/ya040002.xls> (на японском языке).
10. H. Toshinaga, K. Mitani, H. Shibata, K. Takasugi, M. Ishizuka, S. Kotabe, S. Ishihara, H. Tohjo, and H. Saito, Wide area ubiquitous network service system, *NTT Technical Rev.*, Vol. 6, No. 3, 2008. <https://www.ntt-review.jp/>.
11. S. Kuwano, Y. Suzuki, Y. Yamada, and K. Watanabe, Digitized radio-over-fiber (DROF) system for wide-area ubiquitous wireless network, in *Proceedings, Topical Meeting on Microwave Photonics*, Grenoble, France, October 2006.
12. T. Fujita, D. Uchida, Y. Fujino, O. Kagami, and K. Watanabe, A short-burst synchronization method for narrowband wireless communications systems, *IEEE ISWPC 2007*, Puerto Rico, February 2007.
13. F. Nuno, Y. Shimizu, and K. Watanabe, A new QoS control scheme using dynamic window size control for wide area wireless networks, *ICSNC 2007*, French Riviera, France, August 2007.

14. H. Saito, M. Umehira, and M. Morikura, Considerations of global ubiquitous network infrastructure, *IEICE Trans. Commun.*, Vol. J88-B, No. 11, pp. 2128–2136, 2005 (на японском языке).
15. M. Nakamura, A. Yamagishi, M. Harada, M. Nakamura, and K. Kishine, Fast-acquisition PLL using fully digital natural-frequency-switching technique, *Electron. Lett.*, Vol. 44, No. 4, pp. 267–269, 2008.
16. S. Mutoh, T. Douseki, Y. Matsuya, T. Aoki, S. Shigematsu, and J. Yamada, 1-V power supply high-speed digital circuit technology with multithreshold-voltage CMOS, *IEEE J. Solid-State Circuits*, Vol. 30, No. 8, pp. 847–855, 1995.
17. <http://www.okisemi.com/eu/Products/RTC/ml907x.html>.
18. T. Douseki, M. Harada, and T. Tsuchiya, Ultra-low-voltage MTCMOS/SIMOX technology hardened to temperature variation, ScienceDirect, *Solid-State Electron.*, Vol. 41, No. 4, pp. 519–525, 1997.
19. T. Ohno, Y. Kado, M. Harada, and T. Tsuchiya, Experimental 0.25- μ m-gate fully depleted CMOS/SIMOX process using a new two-step LOCOS isolation technique, *IEEE Trans. Electron Devices*, Vol. 42, No. 8, pp. 1481–1486, 1995.
20. <http://nescs.sourceforge.net/>.
21. <http://www.tinyos.net/>.
22. T. Nakamura, M. Nakamura, A. Yamamoto, K. Kashiwagi, Y. Arakawa, M. Matsuo, H. Minami, uTupleSpace: A bi-directional shared data space for wide-area sensor network, in *Proceedings of the 2009 International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT2009)*, pp. 396–401, December 2009.
23. D. Gelernter, Generative communication in Linda, *ACM Trans. Prog. Lang. Syst.*, Vol. 7, No. 1, pp. 80–112, January 1985.
24. C. Curino, M. Giani, M. Giorgetta, A. Giusti, A. Murphy, and G. Picco, TinyLIME: Bridging mobile and sensor networks through middleware, in *Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications (PerCom2005)*, pp. 61–72, March 2005.
25. P. Costa, L. Mottola, A. L. Murphy, and G. P. Picco, TeenyLIME: Transiently shared tuple space middleware for wireless sensor networks, in *Proceedings of the International Workshop on Middleware for Sensor Networks (MidSens '06)*, ACM, pp. 43–48, 2006.
26. G. Castelli, A. Rosi, M. Mamei, and F. Zambonelli, A simple model and infrastructure for context-aware browsing of the world, in *Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom2007)*, pp. 229–238, March 2007.
27. G. Hackmann, C.-L. Fok, G.-C. Roman, and C. Lu, Agimone: Middleware support for seamless integration of sensor and IP networks, in *Lecture Notes in Computer Science*, Vol. 4026, Springer, Berlin, pp. 101–118, 2006.
28. Y. Arakawa, A. Yamamoto, H. Minami, M. Matsuo, H. Tohjo, and H. Saito, Implementation of wide-area ubiquitous platform considering scalability, in *Proceedings of IEICE General Conference '08*, B-7-149, 2008 (на японском языке).
29. Y. Arakawa, K. Kashiwagi, T. Nakamura, M. Nakamura, and M. Matsuo, Evaluation of dynamic scaling method for real-world data sharing mechanism, IEICE Technical Report IN2009-21 (на японском языке).
30. M. Umehira, H. Saito, O. Kagami, T. Fujita, and Y. Fujino, Concept and feasibility study of wide area ubiquitous network for sensors and actuators, *IEEE VTC-Spring*, pp. 165–169, 2007.
31. Y. Yeh, J. C. Wilson, and S. C. Schwartz, Outage probability in mobile telephony with directive antennas and macrodiversity, *IEEE Trans. Vehicular Technol.*, Vol. vt-33, No. 3, pp. 123–127, 1984.

32. S. Fukumoto, K. Higuchi, A. Morimoto, M. Sawahashi, and F. Adachi, Combined effect of site diversity and fast transmit power control in W-CDMA mobile radio, *IEEE VTC-Spring*, pp. 1527–1534, Tokyo, 2000.
33. M. Hata, Empirical formula for propagation loss in land mobile radio services, *IEEE Trans. Vehicular Technol.*, Vol. 29, pp. 317–325, 1980.
34. M. Sakamoto, Location probability estimation of services availability in portable radio telephone systems, *IEEE VTC*, pp. 575–581, 1988.
35. S. Kuwano, D. Uchida, F. Nuno, and M. Takahashi, Wireless access system for wide area ubiquitous networks, *NTT Technical Rev.*, Vol. 6, No. 3, 2008. <https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200803sp3.html>.
36. D. Uchida, S. Kuwano, T. Fujita, and Y. Fujino, Field test results for wide area ubiquitous networks, *NTT Technical Rev.*, Vol. 6, No. 3, 2008. <https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200803sp3.html>.

ГЛАВА 3

ПРОВОДНЫЕ СЕТИ ДОСТУПА

Скотт Рейнольдс

3.1. Введение

Под проводными сетями доступа понимается набор технологий передачи данных на «последней миле», которые соединяют деловые и жилые здания с сетями общего доступа. Исторически сложилось так, что сети доступа были увязаны с характером предоставляемых услуг. Каждый знаком с парами медных проводов, по которым осуществлялась телефонная связь, многие до настоящего времени принимают развлекательные программы по радиочастотным коаксиальным кабелям. Широкополосный или высокоскоростной доступ в Интернет (high-speed Internet, HSI) послужил стимулом для провайдеров сетевого доступа (access network providers, ANP) в совершенствовании и развитии их сети на участках «последней мили».

В конце прошлого столетия благодаря популярности Всемирной паутины операторы сетей доступа осознали, что их сети должны предоставлять больше услуг, а не только передачу сигнала. Проводные сети доступа уже стали каналом связи между домом и бизнесом, в них предлагался набор услуг, за который и собиралась плата. Этот набор обычно описывался понятием «тройная услуга» (triple play) и включал в себя передачу голоса, видео и скоростной доступ к Интернету. Провайдеры вступили в стадию масштабной модернизации своих сетей, сосредотачиваясь на обеспечении все большей полосы пропускания, исходя из предположений, что пропускная способность — это средство увеличения доходов и чем больше она будет, тем больше окажется средний доход в расчете на одного абонента (average revenue per user, ARPU). Телефонные сети были модернизированы для поддержки высокоскоростного Интернета с помощью технологии DSL (digital subscriber line), а комбинированные оптические коаксиальные сети (hybrid-fiber coaxial, HFC) были перестроены для того, чтобы поддерживать полнодуплексный обмен, обеспечивающий высокоскоростной доступ в Интернет. Некоторым сетевым провайдерам оказалось недостаточно постепенного улучшения существующих сетей «последней мили». Единственным адекватным направлением развития стала перепрокладка «последней мили» к жилым домам и деловым зданиям с заменой ее на волоконно-оптические линии, сулившие почти неограниченную пропускную способность.

В этой главе будут рассмотрены три распространенные технологии доступа: DSL, HFC и появляющиеся сейчас пассивные оптические сети (passive optical network, PON), в настоящее время используемые в сетях «оптика в каждый дом» (fiber-to-the-home, FTTH). Будут описаны технологии, лежащие в основе этих сетей, текущее положение дел и тенденции развития каждой из этих технологий.

Мы живем в продуктивное для информационных технологий время. Сети доступа и Интернет сформировали симбиоз, в котором огромная доступная полоса пропускания улучшенной сетевой инфраструктуры может быть использована новыми услугами и приложениями. Обмен музыкой и коммерческие службы наподобие iTunes™ были бы невозможны без масштабного распространения широкополосного доступа к Интернету. Проводные сети перестраиваются для поддержки сервисов потокового видео: YouTube™, Netflix и других. Вещание с высокой четкостью поднимает требования к пропускной способности еще выше. Но одно можно утверждать с уверенностью. Эта тенденция не показывает признаков ослабления. Рост пропускной способности открывает все новые возможности. Услуги и приложения, к которым будет получен доступ завтра, станут возможными только потому, что сегодня сети предоставляют необходимый широкополосный доступ.

3.2. Сети доступа на основе медных кабелей

Мало кто мог предположить, что изобретенная Александром Грэхемом Беллом и запатентованная им в 1881 году замкнутая двухпроводная телефонная цепь [1], приведет к появлению практически вездесущей сети телефонии и передачи данных, которая продолжит использоваться и развиваться более чем столетие спустя. В мире насчитывается свыше 650 млн оконечных медных пар [2]. Из-за колоссальной стоимости их замены провайдеры сетевого доступа имеют мотивы для миграции от низкоскоростной, но высоконадежной передачи голоса, к расширению потенциально имеющейся у медной пары пропускной способности, для предоставления новых услуг и создания новых источников доходов. Раскрытие возможностей «последней мили» по расширению пропускной способности за счет эксплуатации неиспользованных ранее частот, улучшенных методов обработки сигнала для кодировки цифрового сигнала в аналоговую форму становится все более трудным из-за шумовых ограничений, свойственных такому носителю сигнала, как витая пара. Тем не менее, удалось преодолеть множество препятствий и расширить пропускную способность с нескольких десятков килобит в секунду до десятков мегабит в секунду в современных сетях с возможным увеличением до сотен мегабит в секунду в недалеком будущем [3]. Медная витая пара, существующая уже свыше ста лет, сейчас может передавать несколько каналов телевидения высокой четкости, видео по требованию (VOD) и другие услуги, насыщенные возможностями мультимедиа, непосредственно в жилые дома или деловые здания по всему миру. Такие расширяемые возможности гарантируют, что скромная медная витая пара останется доминирующим звеном в технологиях обозримого будущего.

3.2.1. Сеть на медном кабеле

Медная витая пара – тип кабеля, в котором два изолированных медных проводника, обычно диаметром 24 или 26 AWG (0,51 или 0,40 мм), свиты друг с другом для снижения электромагнитных помех. Первоначально проводники для изоляции обертывались бумагой, однако недостаточная влагозащищенность этого мате-

риала делала кабели малопригодными для использования вне помещений. Поэтому основным изолирующим материалом стал и продолжает быть полиэтилен [4]. Многочисленные изолированные витые пары группируются в кабели, называемые «группой пучков» («binder group»), которые расходятся от центральной станции провайдера сетевого доступа к жилым и деловым районам. Длина линий изменяется в значительных пределах в зависимости от плотности населения в обслуживаемой зоне. Линии в городских районах обычно короткие (менее 900 м), в пригородах их длина составляет от 900 до 2700 м и увеличивается до 5,4 км в сельских районах [4].

Проводная линия между центральной станцией и пользователем обычно включает в себя пары из разных кабелей, что может означать разный диаметр жил на разных участках и наличие мостов-ответвлений. Мост-ответвление – разомкнутая телефонная линия, намеренно проложенная вдоль основного маршрута кабеля для будущего подключения или оставшаяся от старого подключения после переноса или отключения абонента (рис. 3.1). Изменения в толщине проводов и наличие мостов-ответвлений сказываются на частотных характеристиках линии, что может привести к уменьшению максимальной пропускной способности отдельных витых пар. Хотя сетевые провайдеры постепенно оптимизируют инфраструктуру своих линий, между различными линиями все еще остаются значительные отличия в длине и качестве, что создает сложности для обеспечения максимальной ширины канала.

Витую пару часто описывают как среду для передачи, ограниченную шумами, из-за большого количества разнообразных источников помех, оказывающих на нее влияние (рис. 3.2), в том числе:

- затухание сигнала, которое зависит от типа используемого диэлектрика, диаметра провода, типа свивки и общей длины линии. Затухание увеличивается по мере увеличения частоты сигнала и длины линии;
- нелинейные фазовые сдвиги вызывают межсимвольную интерференцию;
- отраженный сигнал появляется из-за полнодуплексного обмена по одной паре проводников;

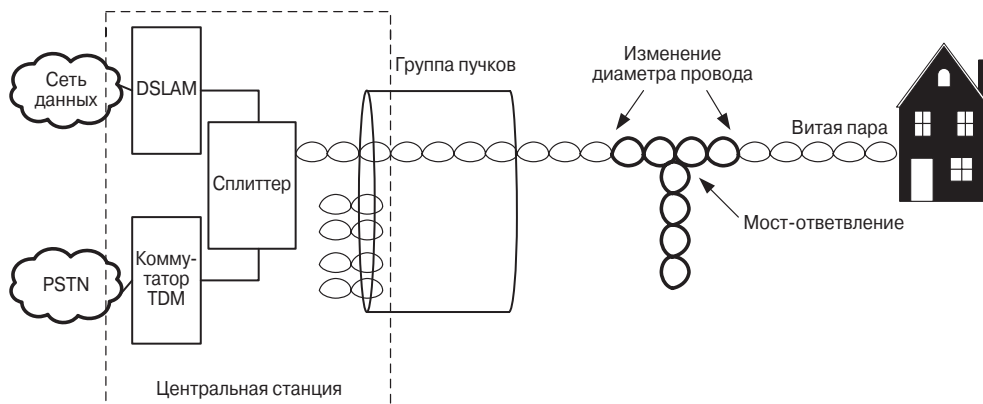


Рис. 3.1. Линия на медной витой паре

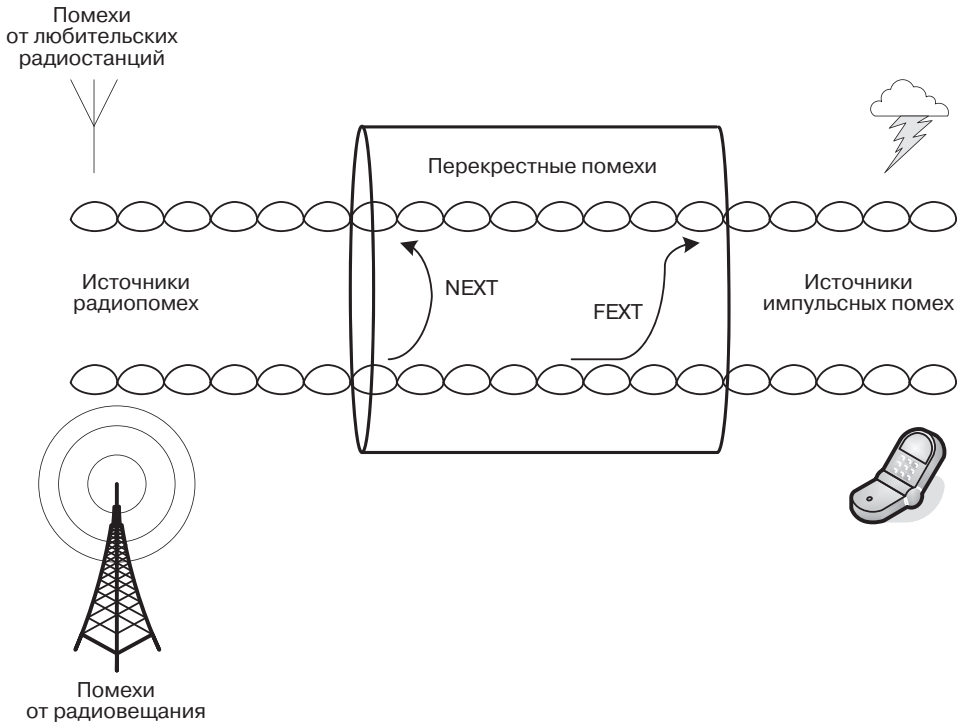


Рис. 3.2. Ухудшение качества линии

- мосты-ответвления создают провалы в передаточной характеристике линии;
- между парами в пучках существуют перекрестные наводки. Эти наводки являются основным фактором, ухудшающим параметры передачи DSL [5]. Такая интерференция обусловлена электромагнитным излучением других пар, расположенных в непосредственной близости. Наводка увеличивается с ростом частоты, что делает ее более вредной по мере роста пропускной способности. На пару могут действовать два вида перекрестных наводок: перекрестная наводка на ближнем конце (near-end crosstalk, NEXT), вызванная сигналами, распространяющимися в противоположном направлении, и перекрестная наводка на дальнем конце (far-end crosstalk, FEXT), вызванная сигналами, передаваемыми в том же направлении. Для линии большей длины наводка на дальнем конце самоограничивается из-за затухания в линии, однако для того, чтобы поддерживать новое поколение услуг, требующих большой пропускной способности, длина линий постоянно уменьшается, тем самым увеличивая отрицательный эффект такой наводки;
- радиопомехи (radio-frequency interference, RFI) – помехи, генерируемые радиопередатчиками, например, любительскими или переносными радиостанциями. Частоты этих передатчиков определяются нормативными документами и хорошо известны, что позволяет соответствующим образом планировать использование спектра частот для высокоскоростной передачи данных по медным проводам;

- фоновый шум — аддитивный белый гауссов шум, определяет шумовой порог;
- Импульсный шум — случайным образом возникающие дискретные шумовые «пики», узкополосные или широкополосные в зависимости от своей природы.

Международные органы стандартизации, такие как: Американский национальный институт стандартов (ANSI), Европейский институт стандартов электросвязи (ETSI) и Международный союз электросвязи (ITU), определяют различные типы ослабления сигнала и предоставляют математические модели для оценки влияния шумов на различные схемы передачи данных DSL [6].

3.2.2. Обзор DSL

Цифровая абонентская линия — модемная технология, в которой для передачи данных с высокой скоростью используется медная витая пара. Термин xDSL объединяет несколько вариантов этой технологии, которые обеспечивают сочетание скорости передачи данных, расстояния передачи и частотной совместимости. В качестве примера можно привести асимметричную DSL (ADSL), симметричную DSL (SDSL), высокоскоростную DSL (high-bit-rate DSL, HDSL) и сверхвысокоскоростную DSL (very-high-bit-rate DSL, VDSL). Варианты xDSL, их скорости, расстояние связи и используемые стандарты приведены в табл. 3.1.

Таблица 3.1. Сравнение DSL

Технология	Стандарт ITU-R (год ратификации)	Максимальная пропускная способность нисходящего канала	Максимальная пропускная способность восходящего канала (расстояние)	Максимальное расстояние ¹	Диапазон частот
ADSL	G.992.1 (1999)	1,3 Мбит/с	12 Мбит/с (300 м)	~ 5,5 км	1,1 МГц
ADSL2	G.992.3 (2002)	1 Мбит/с	12 Мбит/с (300 м)	2,4 км	1,1 МГц
ADSL2+	G.992.5 (2005)	1 Мбит/с	26 Мбит/с (300 м)	3,6 км	2,2 МГц
ADSL-RE	G.992.3 (2003)	0,8 Мбит/с	5 Мбит/с	6,9 км	~1,8 МГц
SHDSL	G.991.2 (2002)	5,6 Мбит/с	5,6 Мбит/с	2,7 км	1,1 МГц
VDSL	G.993.1 (2004)	16 Мбит/с	52 Мбит/с (300 м)	1200 м	12 МГц
VDSL2	G.993.2 (2005)	100 Мбит/с	100 Мбит/с	4,5 км	30 МГц

¹ Максимальное расстояние — не расстояние, на котором может быть получена максимальная скорость. На практике наибольшее расстояние, на котором достигается максимальная скорость обмена данными, оказывается заметно меньше, чем максимальное расстояние, на котором возможна работа. Например, VDSL2 обеспечивает скорость 100 Мбит/с на расстоянии ~450 м, 50 Мбит/с на расстоянии 900 м и около 1 Мбит/с на расстоянии 4,5 км.

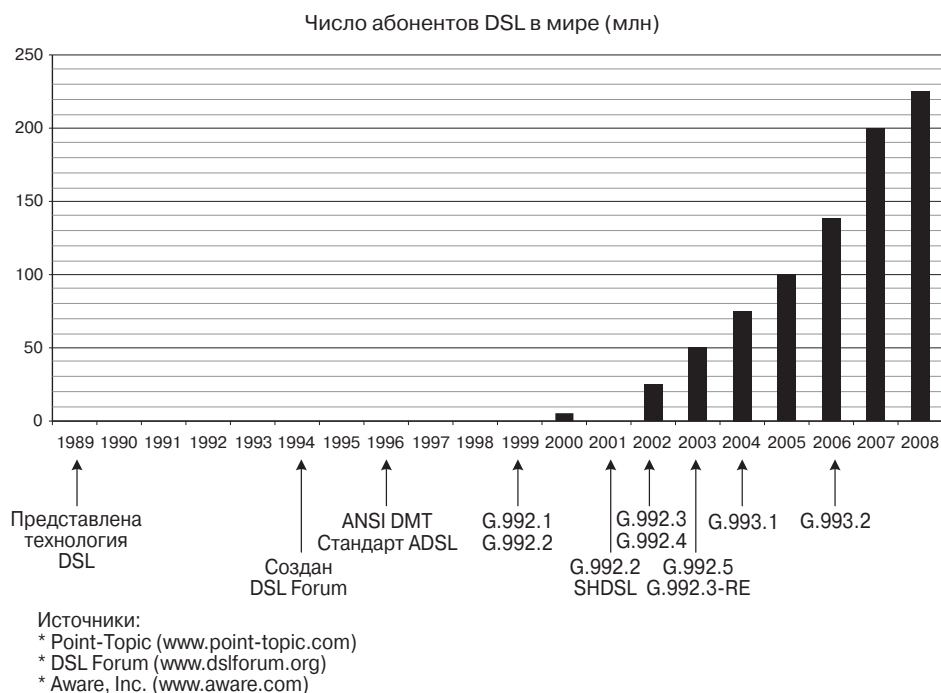


Рис. 3.3. График стандартизации DSL и внедрения технологии

Технология ADSL была первым вариантом DSL, который прошел международную стандартизацию и получил широкое распространение в мире. График, иллюстрирующий появление стандартов и масштабы распространения разных вариантов технологии, приведен на рис. 3.3. Вследствие необходимости доставки видеосигнала нисходящий канал ADSL имеет большую ширину, чем восходящий, этим характеризуются также многие последующие варианты DSL. Степень асимметричности пропускной способности позволила уменьшить NEXT, что увеличило практическую дальность линии, это, в свою очередь, сделало услугу более качественной с экономической точки зрения и ускорило ее внедрение.

Другим важным фактором внедрения ADSL стала возможность ее работы совместно с традиционной телефонной сетью (Plain Old Telephone Service, POTS). ADSL может работать вместе с POTS (и узкополосной ISDN) благодаря разнесению частот, причем сеть POTS использует частоты от 0 до 4 кГц, а ADSL – от 25 кГц до 1,1 МГц¹. Благодаря применению разделителей частот (сплиттеров) и в конечной точке, и на центральной станции низкочастотный сигнал POTS направляется в PSTN, а высокочастотный сигнал DSL поступает на мультиплексор доступа цифровой абонентской линии (digital subscriber line access multiplexer, DSLAM). Технология дуплексирования с разделением частот (frequency division duplexing, FDD) определяет доступную пропускную способность ADSL между нисходящим и восхо-

¹ Точные значения используемых частот зависят от типа используемого оборудования и местных условий.

дящим каналами. Передача восходящего канала занимает низкочастотную часть диапазона, от 25 до 138 кГц, а частоты нисходящего канала начинаются со 138 кГц и доходят до 1,1 МГц (рис. 3.4). Поскольку затухание увеличивается по мере увеличения длины линии и повышения частоты, частотный диапазон нисходящего канала более подвержен влиянию длины линии, снижающей ширину канала.

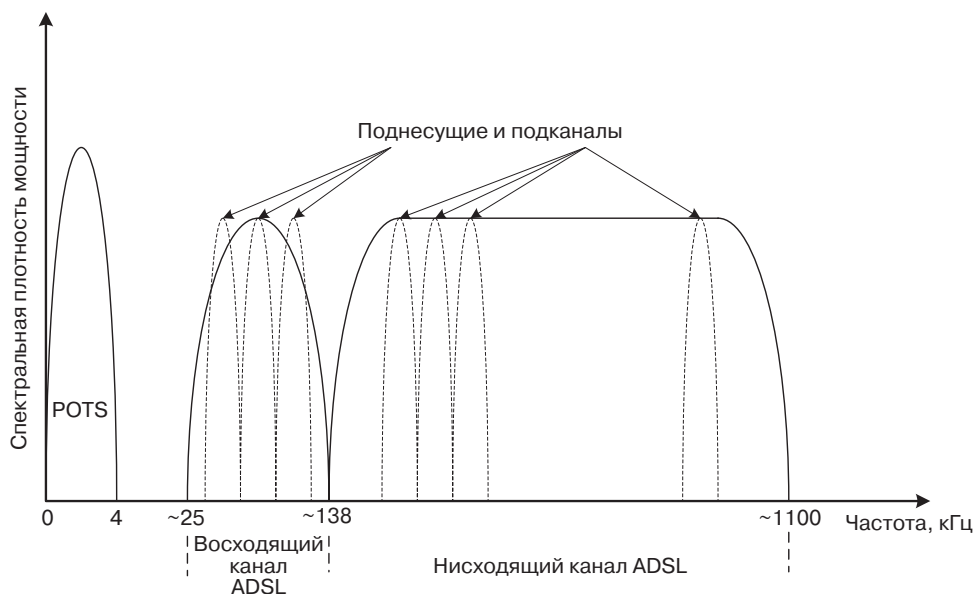


Рис. 3.4. Спектр ADSL

В ранних реализациях ADSL использовались различные и несовместимые между собой методы модуляции. В качестве примеров можно привести амплитудно-фазовую модуляцию без несущей (carrierless amplitude phase, CAP) и дискретную многотональную модуляцию (discrete multitone, DMT). Модуляция CAP является нестандартным вариантом квадратурной амплитудной модуляции (quadrature amplitude modulation, QAM). Тогда как при QAM модулируется амплитуда двух квадратурных несущих¹, CAP использует сочетание двух сигналов с импульсной амплитудной модуляцией, которые фильтруются для получения квадратурно-модулированного сигнала. Модуляция CAP использует широкий диапазон частот, деля его на три области: POTS (от 0 до 4 кГц), восходящий канал (от 25 до 160 кГц) и нисходящий канал (от 240 кГц до 1,1 МГц). Модуляция DMT, наоборот, использует большое количество узкополосных каналов (224 – для нисходящего канала и 25 – для восходящего в случае ADSL), каждый со своей собственной несущей. Канал модулируется индивидуально с использованием модуляции, подобной QAM и кодирующей в одном символе несколько битов. В модуляции QAM каждая комбинация амплитуды и фазы соответствует определенному сочетанию битов.

¹ Квадратурные несущие – синусоиды, сдвинутые по фазе на 90°.

64-символьное соевзедие (64-QAM) содержит 64 однозначно определяемых сочетания амплитуды и фазы, способных представить любое двоичное число, состоящее из шести разрядов. Каждый канал имеет ширину 4 кГц и способен передавать до 32 кбит/с. DMT обладает следующими преимуществами по сравнению с другими способами модуляции: более простое выравнивание амплитуды в отдельных каналах, эффективное использование пропускной способности благодаря возможности перераспределения битов в другие подканалы, бесфильтровое мультиплексирование частотных поддиапазонов, хорошая устойчивость к перекрестным наводкам, а также высокая производительность в условиях рассогласования линии из-за различий в диаметре проводов на отдельных участках или наличия мостов-ответвлений.

Использование адаптивных фильтров приводит к проявлению основного недостатка DMT – необходимости обучения фильтров для обеспечения стабильности. Обучение выполняется как часть процедуры инициализации линии, прежде чем она будет готова к приему и передаче данных пользователя и может периодически повторяться при изменении условий. Дополнительные улучшенные методы обработки сигналов, такие как треллис-кодирование и прямая коррекция ошибок с чередованием, используются для повышения устойчивости к шумам, тем самым улучшая ОСШ, и, увеличивая практически достижимую длину линии при номинальной ширине канала. Цифровая технология передачи сигналов по медным парам, впервые разработанная компанией Bell Labs в середине 1980-х годов, стала применяться только после ратификации основанного на DMT международного стандарта G.992.1 [7], уменьшившего значение систем ADSL с модуляцией CAP.

Хотя развитие ADSL было обусловлено необходимостью передачи видеосигнала, эта технология не могла обеспечить ширину полосы пропускания, достаточную для распространенных в то время видеокодеков. Чтобы преодолеть это ограничение, стандартом G.992.3 [8] была определена технология ADSL2, повысившая скорость передачи данных и расстояние, достигая 12 Мбит/с на дистанции 180 м и поддерживающая меньшие скорости на расстояниях до 4,5 км. Технология ADSL2 предоставляла возможность более эффективного использования линии путем снижения полосы неиспользуемых частот (обеспечивая полностью цифровой режим работы линии, без аналоговой телефонии), поддерживая механизмы как асинхронной (asynchronous transfer mode, ATM), так и синхронной передачи данных, дающей возможность дальнейшего расширения пропускной способности путем объединения каналов с использованием метода инверсного мультиплексирования ATM (inverse multiplexing for ATM, IMA). Однако ADSL2 была спектрально несовместимой с ADSL, что делало невозможным использование ADSL и ADSL2 на разных парах одного и того же пучка. Спектральная совместимость позже была обеспечена в ADSL2+ [9], в которой полоса частот нисходящего канала была увеличена до 2,2 МГц с использованием 512 поднесущих, что позволило достичь пропускной способности до 24 Мбит/с на расстоянии до 900 м.

Технологии VDSL [10] и VDSL2 [11] представляют собой последнее слово в продолжающейся эволюции DSL. Оба стандарта обеспечивают значительное повышение скорости передачи данных за счет увеличения диапазона используемых частот до 12 МГц в VDSL и до 30 МГц в VDSL2. Такое повышение частоты обеспе-

чивает пропускную способность нисходящего канала до 50 Мбит/с, что достаточно для потокового видео в форматах HD и SD. Как показано на рис. 3.5, в VDSL предусмотрено использование сегментированного спектра частот, где частотные диапазоны для нисходящего и восходящего каналов не являются больше непрерывными, что позволяет сделать VDSL более совместимым по используемому спектру частот с существующими реализациями xDSL.

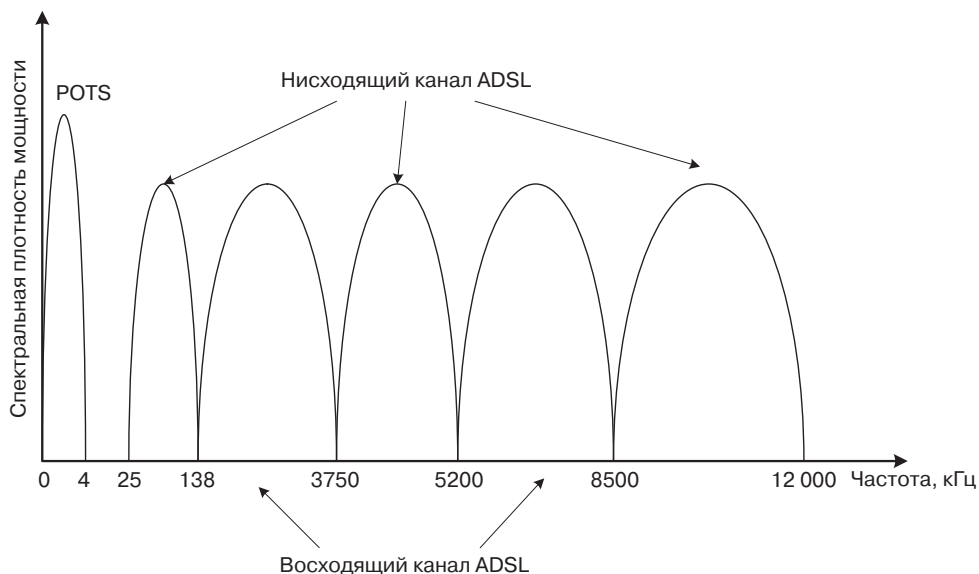


Рис. 3.5. Спектр VDSL

Переход к естественной инкапсуляции Ethernet в VDSL, использующий результаты, полученные рабочей группой «Ethernet на первой миле» и оформленные в виде стандарта Института инженеров по электротехнике и электронике (IEEE) 802.3ah, признает рост значимости Ethernet в сетях, не относящихся к локальным, снижая время преобразований при обеспечении взаимодействия домашних сетей и основанных на Ethernet магистральных сетей и сетей агрегации. Асинхронный режим передачи и синхронная передача данных остаются стандартными возможностями. Хотя скорость передачи данных в VDSL и VDSL2 выглядит привлекательно, эти технологии для достижения такой впечатляющей производительности накладывают значительные ограничения на длину линии. В обоих вариантах скорость передачи данных заметно падает после 1200 м [12], а поскольку в сельских районах длина телефонной линии 5,4 км не является чем-то необычным, снижение длины линии путем установки активных электронных устройств в сети становится необходимым условием ее развития, обеспечивающим скорости связи, близкие к этим заявленным максимумам.

В мае 2006 года VDSL2 как стандарт G.993.2 была одобрена Международным союзом электросвязи. Она разрабатывалась для увеличения скорости передачи данных и достижения дальности связи, сравнимой с той, которая обеспечивалась бо-

лее ранними технологиями. VDSL2 предлагает впечатляющую скорость передачи данных – свыше 25 Мбит/с на относительно длинных линиях (1200–1800 м) и симметричную скорость 100 Мбит/с, важную для высокоскоростного обмена данными в бизнес-приложениях – на коротких (менее 300 м) [12]. Многие из усовершенствований, впервые появившихся в ADSL2+, в том числе улучшенная диагностика, способность динамически изменять скорость передачи данных канала и превосходящая устойчивость к воздействию импульсных шумов, также реализованы в VDSL2. Устойчивость к воздействию импульсных шумов является особенно важной при пакетной передаче видеосигнала. Важно, что VDSL2 имеет возможность взаимодействия с широким набором более ранних вариантов этой технологии, включая исходную ADSL, ADSL2 и ADSL2+. VDSL2 использует тот же тип модуляции, что и ADSL, DMT, но с увеличением числа каналов до 4096. Чрезвычайно важной особенностью стандартизации VDSL2 стала разработка плана использования частот, который учитывает региональные особенности распределения частотного диапазона при обеспечении как симметричной, так и асимметричной скорости передачи в разных линиях одного кабеля.

3.2.3. Эталонная сетевая архитектура DSL

Хотя медный кабель является важным элементом современных сетей проводного доступа, это не единственный компонент, необходимый для предоставления услуг DSL. В этом разделе будет представлен более сетецентричный взгляд на современные сети DSL, описано оборудование и дополнительные сети, требующиеся для предоставления услуг широкополосного доступа в жилых районах.

Архитектурные решения сетей DSL принадлежат организации DSL Forum [13], сейчас известной как Broadband Forum, ассоциации, обеспечивающей распространение технологии DSL во всем мире путем разработки технических спецификаций. Имея в своих членах преимущественно сетевых провайдеров и изготовителей оборудования, Broadband Forum разрабатывает спецификации, содержащие требования к оборудованию, используемому в широкополосных сетях DSL, и определяющие типовую архитектуру сетей, которая помогает провайдерам проектировать такие сети. Эта организация имеет богатый опыт разработки технических условий, охватывающих всю историю эволюции технологии широкополосного доступа DSL. Также в этом разделе будет более подробно описан один из документов – технический доклад TR-101 «Переход к агрегации DSL на основе Ethernet» («Migration to Ethernet-based DSL Aggregation») [14], поскольку он содержит обзор тенденций, оказывающих влияние на внедрение проводного широкополосного доступа в жилых районах.

Распространенные в таких районах широкополосные подключения DSL в качестве технологии агрегирования использовали асинхронную передачу. Каждый абонент подключается к Интернету по протоколу IP, инкапсулированным в одну или несколько постоянных виртуальных цепей, использующих ATM. Трафик многих тысяч абонентов агрегируется сетью маршрутизаторов ATM, которая передает трафик далее концентраторам BRAS (broadband remote access concentrator). Эти концентраторы являются точками централизованного принятия решений о политике

обслуживания пользователей, ответственных за их аутентификацию, авторизацию и ведение учета (authentication, authorization, and accounting, AAA). BRAS является первым элементом сети на уровне IP, шлюзом по умолчанию. На рис. 3.6 показан пример организации широкополосного доступа в жилых районах с использованием ATM-агрегации.

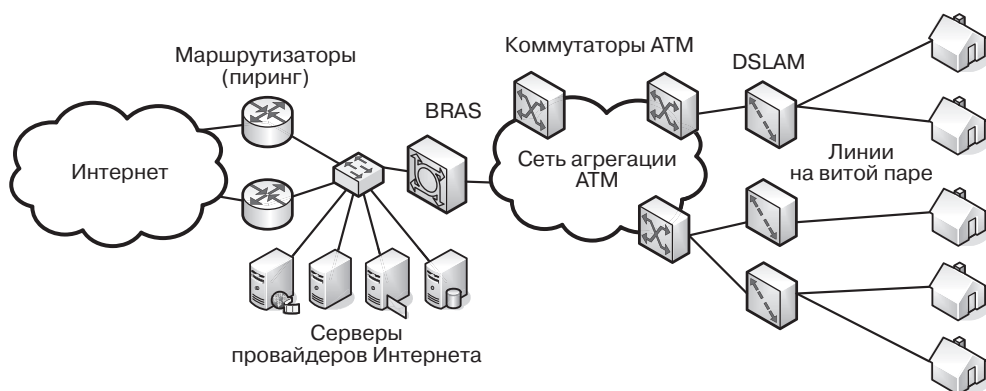


Рис. 3.6. Сетевая архитектура DSL жилого района, основанная на ATM

Требование поддержки передачи видеоданных привело к необходимости расширения пропускной способности медной линии, что повлекло другие изменения, в частности, в сети агрегации. Для эффективной передачи видеосигнала и сеть доступа, и сеть агрегации для масштабного распространения такого пакетированного сигнала требуют значительной ширины каналов связи, гарантированного качества обслуживания и эффективного использования пропускной способности. Сеть Ethernet хорошо изучена в части предоставления высоких скоростей соединений, обеспечения качества услуг на базе передачи пакетов, простой и эффективной подготовки технических средств к работе, исходно обладает способностями многоадресной передачи, ее сетевая избыточность вполне удовлетворяет использованию в качестве транспортной сети. Технические возможности современной транспортной сети Ethernet и ее убедительное преимущество в стоимости привели к повсеместной миграции на нее с сетей ATM во вновь создаваемых и модернизируемых широкополосных сетях в жилых районах. Спецификация Broadband Forum TR-101 определяет эталонную архитектуру сети (рис. 3.7) и требования к сетевым элементам в этой архитектуре.

Эталонная сеть состоит из ряда сетевых элементов (широкополосный шлюз сети, узел доступа, устройства сетевого интерфейса и др.), сетей (местной, агрегации, доступа, абонентского оборудования) и опорных точек (T, U, V и A10). Данные точки являются границами: точками демаркации, административными границами или сетеспецифичными точками скопления трафика.

Шлюз широкополосного доступа (broadband network gateway, BNG) – основанный на Ethernet маршрутизатор IP с функциями обеспечения абонентского AAA, качества обслуживания, многоадресной передачи и безопасности. Кроме

того, BNG требуется, чтобы реализовать многие из возможностей, обычно присутствующих сейчас в устройствах BRAS, в том числе обеспечение пользовательских PPP-сессий поверх Ethernet с помощью протокола PPPoE [15] и поддержку L2TP-туннелирования (Layer 2 Tunneling Protocol) [16]. Шлюз BNG занимает в сети критически важное место, обрабатывая весь восходящий и нисходящий абонентский трафик, что делает его точкой, ответственной за принятие решений и исполнение установленных в сети правил. Такая управляющая точка выполняет функции идентификации служебных сессий и функции управления трафиком, обеспечивая отсутствие перегрузок в сетях доступа и агрегации, включая абонентскую линию тем самым гарантируя, что приложения пользователя получают требуемые услуги с приемлемым качеством.

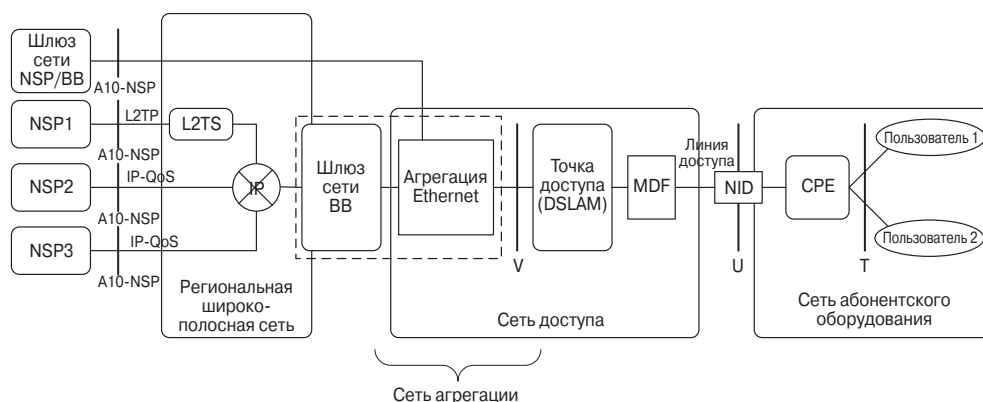


Рис. 3.7. Архитектура сети агрегации TR-101 Ethernet

Принципиальной целью создания сети агрегации является сохранение неизменными имеющихся сетей Ethernet, что обеспечивается объединением трафика от тысяч абонентов, проживающих в микрорайоне, и передачей агрегированного трафика в BNG. Сеть агрегации состоит из групп соединенных между собой коммутаторов Ethernet, соединяющих между собой BNG и DSLAM. Коммутаторы Ethernet по сравнению с аналогичными устройствами ATM обладают гораздо большей производительностью и относительно низкой ценой. Такие коммутаторы обеспечивают т.н. IGMP snooping [14], при котором коммутатор выборочно переконфигурирует таблицы многоадресных пересылок, основываясь на сообщениях протокола IGMP, посылаемых абонентом. Этот протокол (Internet Group Management Protocol) используется приложениями для передачи видео по IP, чтобы сигнализировать о событиях «смена канала», получаемых от телеприставок абонента. Благодаря поддержке IGMP snooping в сети агрегации обеспечивается эффективное использование пропускной способности путем выборочной репликации каналов (групп IGMP), которые просматривают один или несколько абонентов. Сеть агрегации может служить точкой, в которой в сеть вводится содержимое «огороженного сада», например, видеотрафик определенного оператора. Обычно это выполняется путем прямого включения серверов видео в сеть агрегации.

Такой ввод трафика в нисходящий канал, минуя BNG, потенциально сводит на нет решения, принимаемые BNG, поскольку он не может видеть и учитывать такой трафик. В подобной архитектуре необходимо отделять трафик «огороженного сада» от трафика высокоскоростного Интернета с помощью VLAN и такой организацией трафика, которая гарантировала бы отсутствие влияния трафика Интернета на приоритетный видеосигнал в периоды пиковых нагрузок. Архитектура, противоположная описанной, заключается в том, чтобы пропускать весь трафик, в том числе от «огороженного сада» через BNG, где он может правильно учитываться, что обеспечит точное принятие решений и отсутствие перегрузок нисходящего канала.

Мультиплексор DSLAM – элемент сети, который связывает при помощи проводной линии внутреннюю сеть провайдера и абонента. Он реализует физический уровень технологии DSL и служит адаптером между протоколом канального уровня и протоколом сети агрегации, что подразумевает взаимное преобразование ATM и Ethernet. Мультиплексоры DSLAM также выступают в роли терминаторов линий DSL, увеличивая тем самым скорость линии, обеспечивают дополнительные протокольные функции (IGMP snooping и отчет об использовании прокси), улучшенные возможности удаленного управления и диагностики, а также возможности QoS для доставки по проводной линии различных видов услуг.

Документ TR-101 и его предшественники определяют опорную точку U как расположенную на пользовательском конце проводной линии. Устройство сетевого интерфейса (network interface device, NID) реализует физический уровень DSL и инкапсуляцию канального уровня, такие как: IP через PPP через ATM или IP через PPP через Ethernet через ATM или просто IP через Ethernet. Рис. 3.8, заимствованный из TR-101, иллюстрирует некоторые из возможностей.

Интерфейс U

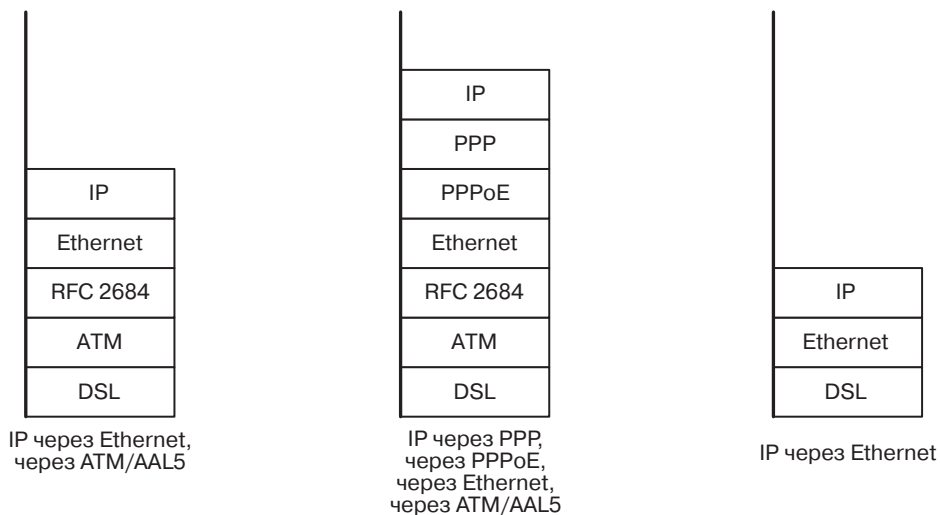


Рис. 3.8. Стеки пакетных протоколов

Опорная точка U представляет собой границу между сетью провайдера и домашней сетью пользователя. Оборудование конечного пользователя (Customer Premises Equipment, CPE) взаимодействует с элементами домашней сети через Ethernet или другие проводные соединения (витая пара, коаксиальный кабель, электрическая сеть или беспроводное соединение). Оно может подключаться к различным устройствам: телеприставке, телефону (обычному через переходное устройство, а также VoIP), домашнему компьютеру, шлюзу (маршрутизатору).

Часто сети DSL воспринимаются как простые линии из медного провода, но в действительности — это сложные сети, объединяющие множество разнородных сетевых технологий и элементов и обеспечивающие доставку услуг с помощью транспорта IP.

3.2.4. Будущее

В последние десять лет наблюдался значительный рост пропускной способности на имеющих столетнюю историю медных проводных линиях. Но действительно ли мы достигли предела тех возможностей, которые можно извлечь из этой старой технологии? К счастью, кое-кто с этим не согласен и активно исследует способы получения от медных проводов неявных возможностей, обещающих повысить скорость передачи данных даже больше, чем в существующих и разрабатываемых пассивных оптических сетях [3, 5].

Ключевой стратегией такого повышения является снижение влияния шумов, в частности, перекрестных помех. Это достигается управлением спектром всех передатчиков в пучке. Существует ряд методов управления спектром, которые обеспечивают дополнительные преимущества за счет повышения сложности. Простейший метод — это статическое управление спектром, которое определяет правила, применяемые для того, чтобы гарантировать спектральную совместимость между всеми службами и технологиями, которые используют пары в одном пучке исходя из наихудших сочетаний использования. Такое управление включает использование предопределенных масок распределения спектральной мощности (power spectrum density, PSD) для управления максимально разрешенными уровнями мощности передачи на любой частоте системы DSL. Оба стандарта — VDSL и VDSL2 — содержат описания таких масок и определяют уровень сигнала, генерируемого соответствующим передатчиком во всей полосе рабочих частот.

Статическое распределение спектра используется в настоящее время для гарантии того, что существующее поколение служб является совместимым и не послужит препятствием для будущих вариантов технологии DSL. При таком распределении не делается попыток динамически управлять мощностью передачи в зависимости от особенностей местных условий развертывания сети. Динамическое управление спектром [17] — форма адаптивного управления, которая оптимизирует спектр различных систем DSL, которые могут использовать линии одного пучка путем подстройки мощности каждого передатчика так, чтобы требования к пропускной способности удовлетворялись с приемлемым запасом. Целью явля-

ется снижение мощности сигнала в линии до уровня, при котором обеспечивается ее приемлемое функционирование и уменьшается наводка на другие линии и интерференция.

Динамическое управление спектром требует возможности определять характеристики линии: затухание, мощность передачи, плотность бит на тон и вносимые потери на тон. Эти параметры в сочетании с другой информацией о линии, такой как длина, наличие мостов-ответвлений и идентификации пучков пар, являются исходными данными для принятия решений по динамическому управлению спектром, оценке ожидаемой скорости передачи данных, рекомендованных параметров работы и позволяют управлять отдельными параметрами линии, такими как значение маски PSD и параметры прямого исправления ошибок (forward error correction, FEC). Эта работа включает вычисление мощности передачи, необходимой для регулирования ОСШ как функции от частоты ($NSF(f)$). Увеличение мощности передачи сверх этих оптимальных значений требует улучшения параметров линии, но не дает выигрыша в пропускной способности, вместо этого оно увеличивает наводки на другие пары. Такой подход дает наибольший выигрыш на более коротких линиях, поскольку при этом для достижения той же скорости требуется меньшая мощность.

Заключительным шагом в динамическом управлении спектром является конфигурирование каждого передатчика в соответствии с рассчитанными параметрами. Трехступенчатая процедура «определение параметров – расчет – обновление настроек» может быть выполнена при инициализации линии и затем проводится периодически с изменением настроек по мере варьирования характеристик линии. Поскольку динамическое управление спектром автоматизирует значительную долю работ по поддержанию и обслуживанию линии DSL, оно предоставляет дополнительный выигрыш в величине операционных расходов на поддержание работы линии [17].

Наконец, новый способ передачи сигнала DSL, который называется векторизованной передачей [3, 5, 17], подразумевает исключение возможности возникновения эффекта перекрестных наводок и реализацию свободной от шумов среды передачи, способной потенциально обеспечить огромную скорость передачи данных, ограниченную лишь возможностями аналого-цифровых (АЦП) и цифро-аналоговых преобразователей (ЦАП). Цель векторизованной передачи – исключить перекрестную наводку на дальнем конце (свойственную другим вариантам DSL, путем введения совместной обработки сигналов. Наводка FEXT, DSL, является преимущественной причиной ограничения производительности, особенно при уменьшении длины линии, что приводит к меньшему затуханию в ней. Векторизованная передача координирует передачу по нисходящему и восходящему каналу, создает вектор сигнала, передаваемого в прямом направлении, принимает вектор обратного сигнала и концептуально рассматривает группу витых пар в связке как систему с несколькими входами и выходами (multiple-input-multiple-output, MIMO). Такая координированная передача может обеспечить скорость свыше 400 Мбит/с на линиях длиной до 360 м [3].

В основе векторизованной передачи лежит способность координировать (в пределах отрезка времени) все передачи в нисходящем канале. Модемы, располо-

женные в мультиплексах DSLAM линий DSL, синхронизируются общим дискретным многотоновым символьным сигналом. При передаче сигнала в восходящем канале благодаря использованию опорной синхронизации в DSL все абонентские модемы синхронизируют свою передачу с тем же сигналом. Приемники в DSLAM могут исключить влияние перекрестных наводок в восходящем канале как на дальнем, так и на ближнем концах, формируемых другими источниками DSL, за счет обратной связи с решением в каждом тоне. При передаче в восходящем канале один из пользователей вообще не будет иметь перекрестных наводок ни в одном тоне. Передача этого пользователя декодируется первой. Затем рассчитывается влияние этой передачи на передачу для другого пользователя и вычитается из передач для всех последующих пользователей для каждого тона в передаче DMT. Перекрестные помехи в нисходящем канале удаляются путем вычисления влияния других (координированных) передатчиков и внесения предсказаний в передаваемый сигнал. Векторизованная передача требует подробной информации о точных значениях перекрестных помех матрицы автокорреляции шумов для линий обрабатываемого пучка, для чего необходимы дополнения к существующим обучающим последовательностям, для генерации этих данных вдобавок к вносимым потерям и информации об усилении и фазе сигнала, получаемой в ходе инициализации линии.

Векторизованная передача не является аналогом механизма bonding, стандартизованного в ADSL2. Этот механизм представляет из себя метод мультиплексирования и демультимплексирования канального уровня, который агрегирует нескольких физических линий, создавая одно виртуальное соединение, пропускная способность которого складывается из пропускной способности составляющих его линий. Векторизование – совместное генерирование и обработка сигнала физического уровня и поэтому не зависит от использования каких-либо схем агрегирования.

3.2.5. Гибридные оптико-проводные сети

Для обеспечения высокой пропускной способности, необходимой для насыщенных видео-сервисов triple play, провайдерам сетей доступа необходимо уменьшить длину проводных линий, что делает необходимым добавление в сеть распределения активных элементов. Это приводит к внедрению оптических каналов от центральной станции к устройствам DSLAM, расположенных вблизи мест проживания абонентов. Такие сети обычно называют «оптоволокно до сетевого узла» (fiber-to-the-node, FTTN), «оптоволокно до микрорайона» (fiber-to-the-curb, FTTC) или «оптоволокно до здания» (fiber-to-the-building, FTTB), указывая расположение DSLAM относительно зданий абонентов. Затем DSLAM соединяются короткими проводными линиями с жилыми помещениями. На рис. 3.9 приведены различные модели FTTx.

Решение развернуть сеть FTTN или же полностью оптическую сеть «оптоволокно до квартиры» (fiber-to-the-home, FTTH) во многом определяется экономической конъюнктурой и учитывает стоимость установки, эксплуатации и ожидаемых доходов от услуг. Однако в некоторых случаях прокладка новых кабельных

сетей к зданиям может оказаться невозможной по эстетическим или историческим соображениям. В качестве общего положения отметим, что сеть FTTN с линиями VDSL2, позволяющая эксплуатировать имеющиеся проводные линии, экономически эффективней по сравнению с существующей сетевой инфраструктурой и обеспечивает более быстрый выход на рынок. Сеть FTTN может оказаться более выгодной по стоимости в случае прокладки новых сетей и обещает более низкую стоимость эксплуатации [18].

Одной из основных задач сети со смешанной архитектурой xDSL/FTTN является управление спектром, в частности, предупреждение наложения в одном пучке сигналов существующих в настоящее время сервисов DSL (длинные линии) на сигналы от DSLAM, подключенных к оптоволокну (короткие линии) [17]. Пока не регламентированы какие-либо методы управления спектром, более высокоскоростные линии будут создавать большое количество наводок на длинные, менее скоростные, идущие от центральной станции. Без динамического управления спектром передатчик короткой линии может использовать сигнал большей мощности, чем это необходимо для достижения требуемой скорости передачи данных.

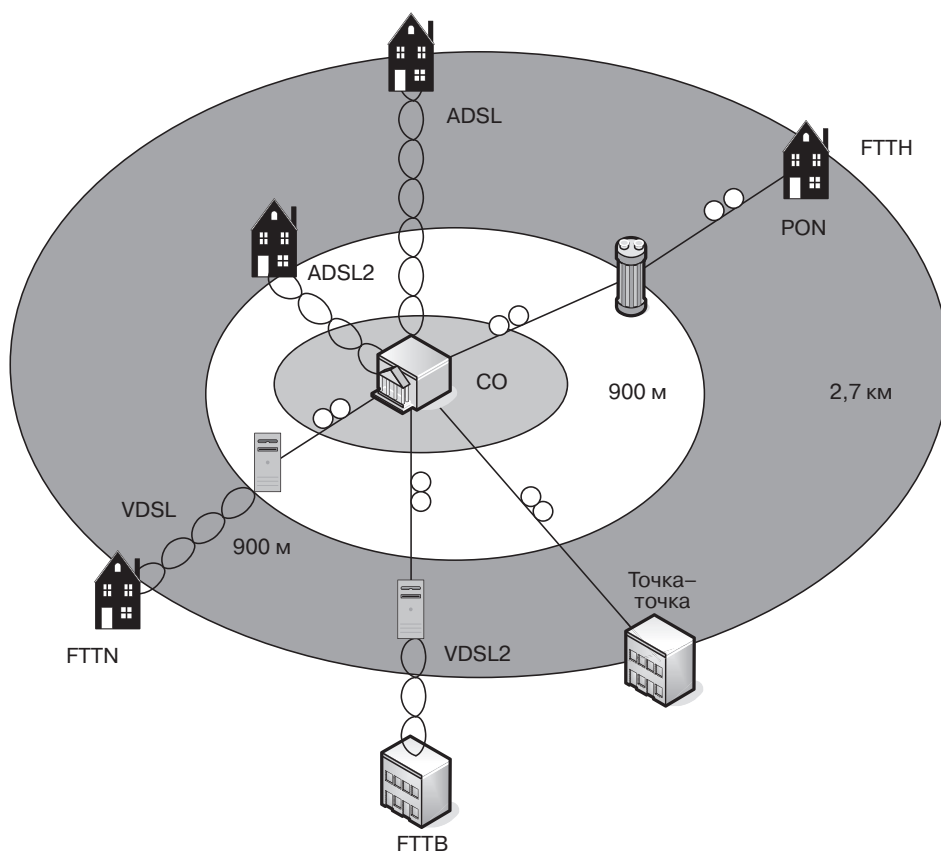


Рис. 3.9. Модели FTTx

Другие аспекты внедрения FTTH являются менее теоретическими и более приземленными. Как подавать питание на удаленные DSLAM? Какие средства контроля окружающей среды требуются и нужны ли вообще? Какие решения предусмотрены в POTS на случай перебоев в энергоснабжении? Оборудование, размещенное на центральной станции, защищено с точки зрения безопасности, находится в хороших температурных условиях с кондиционированием, имеет источники бесперебойного питания и другие системы поддержания работоспособности, но ничто из вышеперечисленного не применимо к оборудованию в металлическом шкафу, который установлен на углу улицы. Проблемы, возникающие при размещении такого сложного активного электронного оборудования вне контролируемой среды станции, довольно многочисленны и требуют, чтобы оно было специально разработано устойчивым к условиям окружающей среды при работе в металлическом шкафу без кондиционирования или при установке на столбе или опоре.

Наконец, часто не учитывается обслуживание таких устройств техническими службами оператора сети. Размещение большого количества меньших по емкости DSLAM на обслуживаемой территории может привести к повышенным затратам на подготовку их к работе, управление и обслуживание. Такие операционные расходы имеют тенденцию расти пропорционально числу установленных сетевых элементов. Эти расходы уже являются довольно значительными, и провайдеры ищут способы снизить их влияние на прибыльность бизнеса.

Но даже в таких условиях архитектура FTTH представляет собой обычную эволюцию сетей, идущую по пути повышения пропускной способности для доставки услуг будущего по обычной медной линии.

Линии из медной витой пары формировали костяк проводных сетей доступа в течение более чем столетия. Эта долгоживущая среда передачи, дополненная передовыми достижениями в технологии обработки сигналов, эволюционировала от обычной телефонной связи до предоставления телепередач высокой четкости, видео по требованию и других услуг, насыщенных мультимедийным содержанием, что гарантирует продолжение использования таких проводных сетей еще в течение долгого времени.

3.3. Пассивные оптические сети

В этом разделе описывается новая разновидность сетей проводного доступа — пассивные оптические сети. Они являются распределительными сетями с древовидной топологией «одна точка ко многим» (point-to-multipoint, P2MP), не имеющими активных элементов в каналах передачи. Их высокая пропускная способность и свойства, присущие топологии P2MP, делают сети PON идеальной технологией для проводных сетей доступа будущего. Также будут представлены различные варианты PON, причем особое внимание будет уделено технологии Ethernet PON (EPON). Технология PON была стандартизирована Международным союзом электросвязи [19, 20–23] и Институтом инженеров электротехники и электроники (IEEE) [24], предоставившими альтернативы, оптимизированные для передачи традиционного трафика и кадров Ethernet. Созданная IEEE технология EPON и ее вариант со ско-

ростью 10 Гбит/с обеспечивают огромную пропускную способность при сохранении преимуществ Ethernet, вероятно, самой удачной сетевой технологии в мире.

3.3.1. Принцип построения пассивных оптических сетей

Сети PON состоят из волоконно-оптических кабелей для передачи данных, оптических соединителей для распределения данных и активных элементов, ответственных за преобразование сигналов из оптической формы в электрическую и обратно.

Оптическое волокно — это очень тонкая стеклянная нить, которая работает как волновод, позволяя свету распространяться с очень малыми потерями за счет принципа полного внутреннего отражения. Оптический сигнал передается в ответвления с использованием оптических разветвителей, которые повторяют оптический сигнал, пришедший к ним на вход, на несколько выходов. Поскольку разветвители являются пассивными элементами, оптическая мощность любого выходного сигнала составляет лишь часть мощности, поступившей на входной порт. Такое снижение оптической мощности ограничивает возможности разветвления сети. Объединители выполняют обратную функцию, соединяя оптические сигналы от нескольких источников и передавая дальше объединенный сигнал. Объединители являются «высоконаправленными» устройствами, в них теряется очень небольшая часть оптической мощности, это свойство характеризуется коэффициентом направленности. Функции разветвления и объединения интегрированы в одном элементе, называемом оптической муфтой. Основными элементами базовой архитектуры PON являются оптические терминалы (optical line terminal, OLT) и устройства оптической сети (optical network unit, ONU)¹. Эти активные элементы устанавливаются внутри центральной станции и рядом с местонахождением абонента, соответственно. Устройства OLT и ONU «замыкают» оптическую распределительную сеть, являясь интерфейсом между ее электрическим и оптическим участками, и обычно выполняют функции канального уровня модели OSI. Базовая архитектура сети PON показана на рис. 3.10.

Большинство разновидностей PON в значительной степени технически подобны друг другу, и их главным отличием является используемый протокол передачи данных. Организация ИТУ-T стандартизировала две архитектуры PON: широкополосную PON (broadband PON, BPON), основанную на режиме асинхронной передачи (ATM), и более позднюю, гигабитную PON (GPON), которая использует общий метод инкапсуляции (Generic Encapsulation Method, GEM) для присущего данной среде мультиплексирования с разделением по времени (time division multiplex, TDM), ATM и инкапсуляции кадров Ethernet с малыми накладными расходами. Технология Ethernet PON, стандартизованная IEEE, предоставляет полностью совместимый со стандартом 802.3 интерфейс MAC для передачи и приема кадров Ethernet.

¹ В терминологии ИТУ также называется терминалом оптической сети (optical network terminal, ONT).

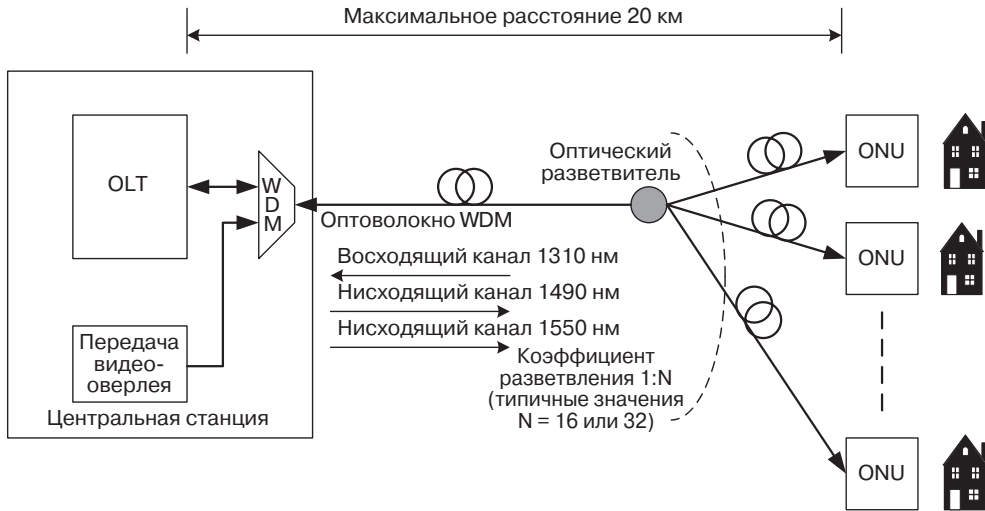


Рис. 3.10. Базовая архитектура распределительной сети PON

В связи со свойствами оптической репликации и направленностью оптических муфт сети PON по своей природе асимметричны. В нисходящем канале кадры OLT широковещательно передаются всем ONU, но выделяются и обрабатываются только кадры, адресованные непосредственно данному ONU. Если использовать в качестве аналогии Ethernet, то в восходящем канале PON окажется подобной LAN с общей средой передачи. При передаче в обратном направлении пропускная способность также разделяется между ONU благодаря оптическим объединителям, собирающим воедино передачи каждого ONU. При этом требуется схема арбитража для координации использования пропускной способности восходящего канала, чтобы предотвращать коллизии. Из-за направленности оптических муфт ONU не в состоянии обнаружить коллизию, поэтому, несмотря на то, что восходящий канал PON и похож на общую среду, обычные состязательные механизмы арбитража ресурсов, такие как множественный доступ с контролем несущей и обнаружением коллизий (carrier sense multiple access with collision detection, (CSMA/CD) и множественный доступ с контролем несущей и предотвращением коллизий (carrier sense multiple access with collision avoidance, CSMA/CA), оказываются сложно реализуемыми.

Вместо того, чтобы разрабатывать громоздкий состязательный алгоритм, и ITU-T, и IEEE для предотвращения коллизий на оптическом уровне использовали схему множественного доступа с разделением по времени (TDMA). BPON, GPON и EPON используют общий подход к разделению обратного канала на кванты времени, хотя в деталях эти реализации различаются. Каждый квант времени представляет собой окно передачи, определяемое временем начала и продолжительностью или временем окончания. Затем OLT выделяет ONU квант на передачу, используя особый алгоритм распределения пропускной способности. OLT может распределять пропускную способность между ONU произвольным образом, начиная от статического выделения до динамического распределения, основан-

ного на количестве данных, которое ONU собирается передать. Сравнение этих алгоритмов будет представлено ниже.

Когда окно передачи будет выделено ONU, это устройство выполнит передачу данных в виде пакета данных на полной скорости физического канала (1 Гбит/с в случае GPON). После передачи данных ONU полностью останавливает все передачи и выключает лазер. Он остается выключенным в течение периода молчания, чтобы избежать случайного излучения в восходящий канал шумов, которые потенциально могут вызвать появление битовых ошибок в ведущихся в этот момент передачах.

3.3.2. Пассивные оптические сети Ethernet

Сеть Ethernet PON (EPON) возникла в результате работ исследовательской группы IEEE «Ethernet на первой миле» (Ethernet in the First Mile, EFM). Эта группа была создана в 2001 году для развития технологии Ethernet в сетях доступа, пригодной для использования как домашними абонентами, так и в бизнес-целях и покрывающей как архитектуру «точка–точка» (P2P), так и архитектуру «точка–много точек» (P2MP), а также управление, администрирование и обслуживание (OAM) сетей Ethernet. В соответствии с процедурами IEEE исследовательская группа в сентябре 2001 года стала целевой группой 802.3ah, за этим последовало одобрение запроса на авторизацию проекта (Project Authorization Request, PAR) [26]. Одна из ее задач – реализация сервиса Ethernet со скоростью 1 Гбит/с с использованием пассивной оптической сети P2MP, поддерживающей минимальный коэффициент расщепления (разветвления) 1:16 с сохранением существующего формата кадров, уровня управления доступом к среде передачи (MAC) и не зависящего от среды интерфейса (media independent interface, MII) стандарта Ethernet 802.3, работающего на расстояниях до 10 км (табл. 3.2).

Придерживаясь этих целей и стараясь минимизировать изменения на физическом уровне и подуровне, зависящем от физической среды (physical medium-dependent, PMD), можно было бы достичь быстрого одобрения стандарта благодаря использованию дешевых и доступных в массовых объемах оптических и полупроводниковых компонентов, поддерживающих работу со скоростью 1 Гбит/с [26].

Целевая группа 802.3ah успешно завершила свою работу по стандартизации выпуском документа 802.3ah-2004. Эта работа была включена в секцию 5 издания 2005 года стандарта IEEE 802.3 [24] (рис. 3.11). Документ 802.3ah EPON стандартизирует гигабитную симметричную (1 Гбит/с в нисходящем и восходящем каналах) сеть PON, которая использует две длины волны в одном волокне (1490 нм для нисходящего канала и 1310 нм для восходящего) для передачи данных с возможностью резервирования дополнительной длины волны нисходящего канала (1550 нм) для предоставления дополнительных услуг, например, аналогового телевидения. При энергетическом потенциале 24 дБ максимальная протяженность соединения составляет до 20 км при коэффициенте разветвления 1:16. Кадры инкапсулируются в формат стандарта 802.3 и кодируются с использованием линейного кодирования 8b/10b.

Таблица 3.2. Цели запроса на авторизацию проекта EPON

Параметр	Значение
Формат кадра	Формат и кодирование по стандарту 802.3
Скорость линии	Стандартная скорость Ethernet, 1000 Мбит/с
Оптоволокно	Одно одномодовое волокно (SMF)
Расстояние	Не менее 10 км
Типы PMD	Исследуются 1310/1310, 15xx/1310 и ITU 983.3
Коэффициент разветвления	Мин. 1:16
Коннектор	Коннектор SC, исследуются коннекторы с высокой плотностью размещения, подобные LC

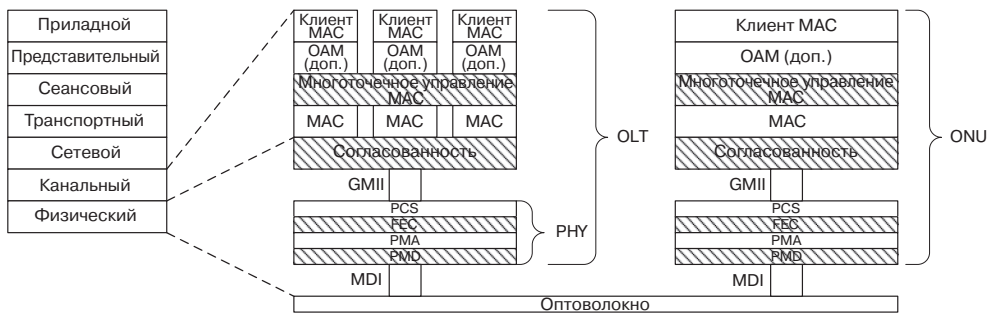


Рис. 3.11. Протокольный стек и характеристики сети IEEE EPON

Стандарт 802.3 Ethernet MAC поддерживает два режима работы: с общей средой передачи и единичными коллизиями и полнодуплексную технологию «точка–точка». Восходящий канал PON обладает признаками обоих режимов. IEEE специфицировал схему TDMA в сочетании с эмуляцией логической топологии P2P для эмуляции P2P-соединения на базе разделяемой полосы пропускания восходящего канала PON. Ключевым расширением, предложенным целевой группой и одобренным в качестве стандарта, является создание дополнительного протокола управления MAC – многоточечного протокола управления MAC (Multipoint MAC Control Protocol, MPCP). Протокол MPCP является протоколом управления в реальном времени, который отвечает за манипулирование операциями подуровня MAC. Он расширяет существующий, основанный на паузах метод управления потоком подуровня управления MAC и добавляет возможно-

сти синхронизации, управление ресурсами ONU и обнаружение, регистрацию и инициализацию этих устройств. Кадры протокола управления MAC выделяются среди других кадров MAC по особому значению (шестнадцатеричное 88-08) в поле «длина/тип». Кадры MPCP выделяются по особому 16-разрядному значению, которое идет вслед за полем «длина/тип». Описанный процесс показан на рис. 3.12.

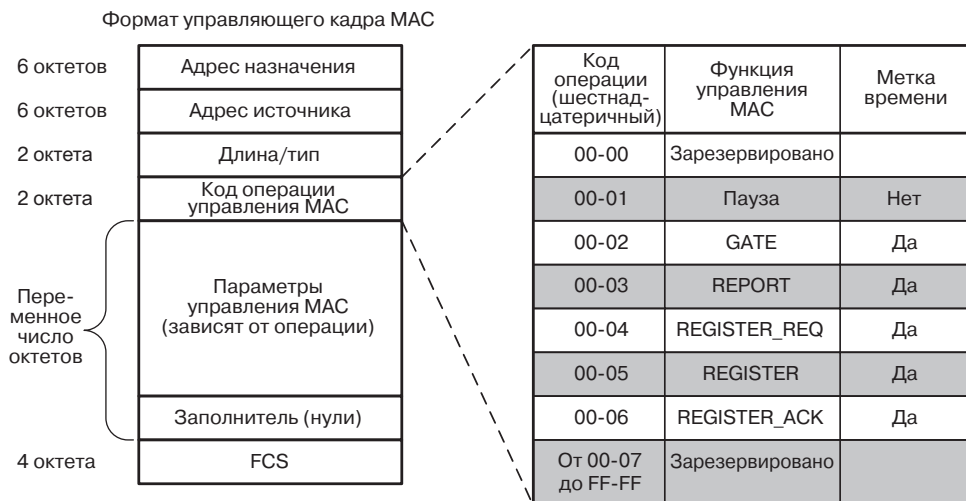


Рис. 3.12. Формат управляющего кадра MAC

MPCP определяет пять дополнительных кадров управления MAC:

- GATE: получателю выделяется окно передачи.
- REPORT: уведомление об ожидающей передаче данных от отправителя.
- REGISTER_REQ: запрос от отправителя о признании его участвующим в передаче.
- REGISTER: уведомление, что получатель признан участвующим в передаче.
- REGISTER_ACK: уведомление, что станция-отправитель подтвердила свое участие в передаче.

Механизм выделения пропускной способности TDMA требует, чтобы все передающие узлы были синхронизированы с общим источником времени во избежание коллизий. Поскольку каждый ONU хранит кадры, принятые из абонентской сети, ожидая выделения ему возможности передачи, он должен иметь согласованное с другими устройствами «восприятие» времени. Устройства ONU выполняют синхронизацию с помощью отметок времени, которые вставляются в передаваемое OLT сообщение MPCP GATE. Отметка времени — это монотонно изменяющийся 32-разрядный счетчик, увеличивающий свое значение каждые 16 нс (отрезок времени, называемый временным квантом). Поле отметки времени заполняется OLT и соответствует времени передачи первого байта адреса назначения в сообщении GATE. Как только это сообщение принимается, ONU устанавливает

локальные часы MPCP согласно значению в поле отметки времени. Эти часы ведут счет времени по тактам, восстанавливаемым из входного потока данных. Поскольку в линии в периоды молчания передаются символы IDLE, часы постоянно корректируются, минимизируя уход вперед или отставание. Хотя описываемый метод требует строгого контроля отклонения времени задержки внутри OLT, которое не может быть больше чем 2^{16} квантов времени в подслоях RS, PCS и PMA, он позволяет использовать в OLT стандартные источники времени с точностью $\pm 10^{-4}$.

Управление ресурсами состоит из назначения ONU пропускной способности, планирования загрузки восходящего канала для определения, в каком порядке ONU будут передавать данные и выделения пропускной способности этого канала для задания длины кванта времени. MPCP использует управляющие сообщения GATE и REPORT для управления ресурсами и координации доступа к восходящему каналу. Сообщение GATE посылается в нисходящем канале от OLT к конкретному ONU, разрешая ему определенную возможность передачи. Квант времени задается временем его начала и продолжительностью передачи. Получив сообщение GATE, ONU синхронизирует свои локальные часы MPCP и выбирает кадр (или последовательность кадров) для передачи. Выделение квантов времени тщательно конвейеризуется, чтобы минимизировать время обхода всех ONU и максимально использовать пропускную способность. Конвейеризация эффективно исключает избыточную передачу и обработку сообщений GATE, однако она требует знания времени прохождения сигнала в обоих направлениях (round-trip time, RTT) для каждого ONU. Устройство ONU передает сообщение REPORT к OLT, чтобы запросить возможность последующей передачи. Временной график конвейеризованной передачи сообщений GATE и REPORT показан на рис. 3.13.

Сообщение REPORT содержит информацию о заполненности очереди (в квантах времени), показывающую размер пропускной способности для передачи, которую ONU запрашивает. OLT может использовать эту информацию при выполнении алгоритма выделения пропускной способности. Сообщение REPORT может указывать состояние до восьми очередей в группе, называемой «набор очередей». Одно сообщение может содержать до 13 таких наборов. Сам алгоритм распределения пропускной способности стандартом IEEE не описывается и зависит от реализации. Это открыло большую область для исследований. Были проведены работы по попыткам сбалансировать противоречащие друг другу требования по максимизации использования сети, обеспечению качества обслуживания и уменьшению сложности [27–30].

Третья область ответственности MPCP – координация автообнаружения ONU. Исходя из того, что ONU предписано не передавать никаких данных без явного выделения кванта времени, необходима процедура, по которой выделяющие эти кванты OLT могло бы обнаруживать вновь активированные ONU. Этот протокол отвечает за выполнение первоначального обнаружения, квитирования при активации, измерения периода кругового обращения, определение индивидуального 48-разрядного MAC-адреса ONU и предоставление конфигурационной информации, которая делает возможным эффективный двунаправленный обмен данными. Для этого предусмотрена четырехступенчатая процедура квитирования, использующая описанные выше управляющие сообщения MPCP:

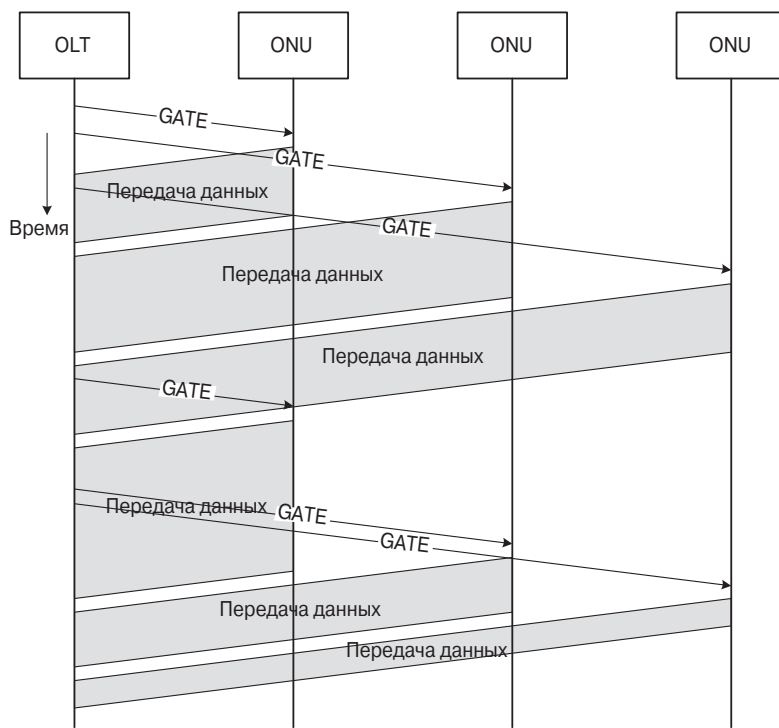
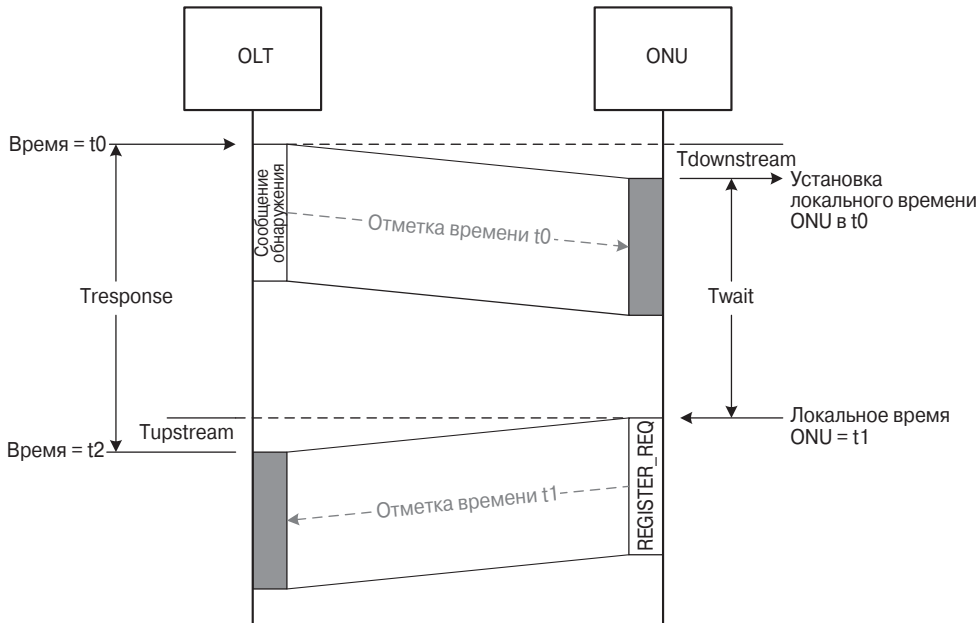


Рис. 3.13. Конвейеризованная передача данных

- на первом шаге OLT выделяет квант времени для обнаружения. Этот квант имеет специальную семантику, обычный квант предоставляет возможность передачи данных конкретному ONU, а квант обнаружения – всем неинициализированным подобным устройствам. Во время кванта обнаружения OLT выполняет широкополосную передачу сообщения обнаружения GATE, объявляя время начала кванта обнаружения и его продолжительность. Сообщение обнаружения GATE содержит также метку времени OLT;
- все известные и инициализированные ONU отбрасывают сообщение обнаружения GATE. Все неинициализированные ONU принимают такое сообщение, синхронизируют свои локальные часы MPCP и ждут времени, назначенного для передачи. Чтобы избежать коллизий, которые ожидаются в случае, если больше одного неинициализированного ONU начнут передачу сразу после начала кванта времени обнаружения, протокол требует, чтобы каждое ONU перед началом передачи выжидало в течение случайного отрезка времени. Устройство ONU передает сообщение REGISTER_REQ, содержащее адрес источника и отметку времени из первого байта MAC-адреса получателя. OLT принимает это сообщение, которое дает возможность вычислить период кругового обращения. Он равен разнице между временем приема сообщения REGISTER_REQ и меткой времени, включенной в сообщение. Описанный процесс показан на рис. 3.14;



$T_{\text{downstream}}$ – задержка прохождения сигнала по нисходящему каналу.

T_{upstream} – задержка прохождения сигнала по восходящему каналу.

T_{wait} – время ожидания ONU; равно $t_1 - t_0$.

T_{response} – время ответа OLT; равно $t_2 - t_0$.

Период кругового обращения (RTT) = $T_{\text{downstream}} + T_{\text{upstream}} = T_{\text{response}} - T_{\text{wait}} = (t_2 - t_0) - (t_1 - t_0) = t_2 - t_1$.

Рис. 3.14. Вычисление периода кругового обращения

- OLT отвечает на сообщение REGISTER_REQ сообщением REGISTER, назначающим идентификатор логического соединения (logical link identifier, LLID). Этот идентификатор дает ONU возможность выделять среди передаваемых кадров те, которые адресованы ему. OLT немедленно посылает вновь активированному ONU одноадресное сообщение GATE;
- когда ONU принимает адресованные ему сообщения REGISTER и GATE, оно отвечает сообщением REGISTER_ACK (в кванте времени, отведенном для сообщений GATE), что завершает процесс. Процедура автообнаружения показана на рис. 3.15.

Процесс обнаружения представляет собой накладные расходы, которые используют часть общей пропускной способности, уменьшая полезную полосу пропускания. Размер и периодичность выделения квантов времени обнаружения должны быть сбалансированы так, чтобы и время обнаружения и инициализации новых ONU было невелико и не сильно падала пропускная способность сети из-за отвлечения части квантов времени на процесс обнаружения.

Стандарт IEEE [24] предусматривает наличие функции эмуляции логической топологии (logical topology emulation, LTE), чтобы полностью соответствовать требованиям документа 802.1D, описывающего мосты Ethernet. В дополнение к варианту «общая среда – единственная коллизия» и полнодуплексному режиму работы «точка–точка», описанному в 802.3 MAC, совместимые с 802.1D мосты не

пересылают кадры обратно в порт-источник. Если рассматривать OLT как мост, совместимый с 802.1D, сеть PON должна представлять собой либо полнодуплексную топологию «точка–точка» или топологию «общая среда – единственная коллизия». Стандарт 802.3 [24] описывает функцию эмуляции логической топологии, которая находится ниже подуровня MAC (и поэтому прозрачна для MAC), что дает PON возможность имитировать любую из этих топологий. Стандарт 802.3 [24] описывает поведение только полнодуплексной модели «точка–точка». Однако нежелательно терять значительный выигрыш от передачи в нисходящем канале единственной копии сигнала в режиме широковещания; это добавляет в архитектуру порт MAC широковещательной передачи одной копии (a single-copy broadcast, SCB), используемый для логической широковещательной передачи кадров всем ONU в нисходящем канале.

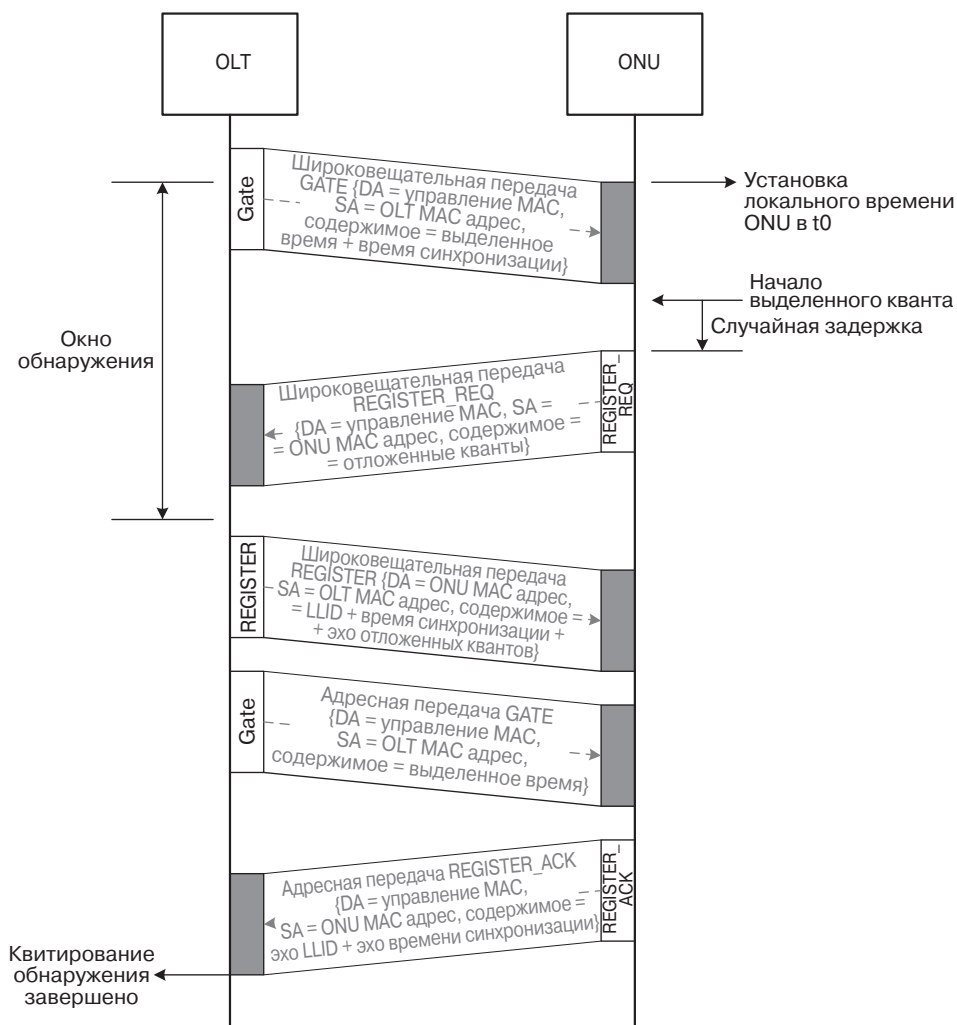


Рис. 3.15. Квитирование при обнаружении

LTE обеспечивает назначение идентификатора логического соединения каждому ONU в ходе процесса автообнаружения. Кадры передаются с 16-разрядным LLID, содержащимся в модифицированном заголовке (защищен контрольной суммой). Кадры, соответствующие назначенному LLID (или ширококвещательному LLID), ONU принимает, а все остальные отбрасывает. При передаче в обратном направлении ONU вставляет LLID в заголовок, давая OLT возможность направить кадр к виртуальному MAC, соответствующему ведущему передаче ONU, тем самым эмулируя полнодуплексную топологию «точка–точка».

Для увеличения пределов физической досягаемости оптической распределительной сети, повышения коэффициента разветвления и надежности коммуникационного канала, IEEE включил в стандарт необязательный механизм прямой коррекции ошибок (FEC). Он обеспечивает способность обнаруживать и исправлять битовые ошибки, которые происходят в процессе передачи. Кодировщик добавляет в кадр информацию о четности для того, чтобы декодер мог определить ошибки и реконструировать правильную информационную последовательность. Процедура FEC, выбранная целевой группой 802.3ah, идентична той, которая используется в других технологиях PON, в том числе в GPON, и представляет блочный алгоритм Рида–Соломона, добавляющий 16 байтов четности к каждому 239-байтному блоку кадра данных [22]. Стандарт IEEE определяет процедуру сегментирования кадра 802.3 Ethernet на последовательность 239-байтных блоков. Последний блок при необходимости дополняется нулями для упрощения вычисления кода четности FEC. Эти дополняющие байты не входят в состав кадра и не передаются. Символы четности группируются вместе и передаются в конце кадра, оставляя формат кадра 802.3 неизменным. Это решение демонстрирует главное преимущество стандартизированных, основанных на передаче кадра технологий, допуская взаимодействие с устройствами, не поддерживающих коррекцию ошибок.

Последняя тема, заслуживающая обсуждения, относится к защите данных в EPON. Полагая, что все кадры пассивно передаются ONU в нисходящем канале и эти устройства полагаются на логические, а не физические механизмы для фильтрации кадров, игнорирование этих логических ограничений даст ONU возможность подслушивать все передачи в нисходящем канале. В отличие от локальных сетей, сети доступа обслуживают не сотрудничающих между собой абонентов, что требует обеспечения конфиденциальности, поэтому удивительно, что целевая группа 802.3ah не требовала наличия дополнительного компонента шифрования. Тем не менее, многие производители сетевого оборудования включают возможность шифрования нисходящего и восходящего канала благодаря широкой доступности полупроводниковых компонентов, которые реализуют 128-разрядное шифрование AES [31, 32].

Быстрая разработка спецификаций и коммерциализация технологии EPON являются свидетельством гибкости и жизнеспособности стандарта 802.3. Ethernet является повсеместно распространенной сетевой технологией, выбором для телекоммуникационных сетей будущего, а EPON – важный шаг к наведению мостов между домашними сетями и региональными и магистральными сетями Ethernet. Коммерческое будущее выглядит многообещающим благодаря усилиям целевой группы IEEE 802.3ah по поддержанию обратной совместимости с множеством устройств Ethernet.

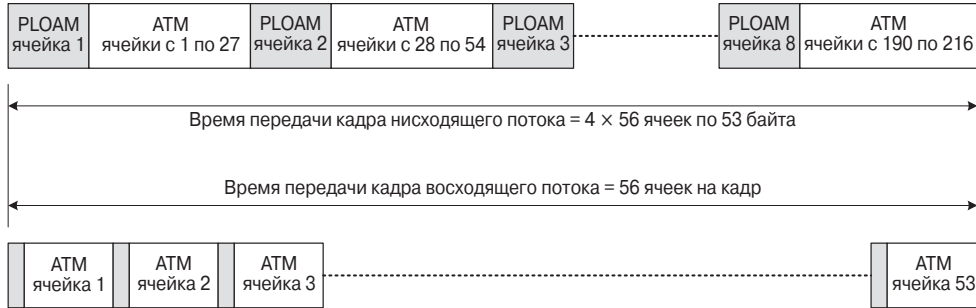
3.3.3. Пассивные оптические сети ITU-T

Некоторые технологии PON опередили работу IEEE по стандартизации EPON. Эти более ранние технологии создавались под эгидой ITU-T. В 1995 году группа, состоящая из семи ведущих сетевых провайдеров, сформировала специальное объединение, названное «Сеть доступа с полным обслуживанием» (Full Service Access Network, FSAN) [33]. Эта группа имела достойную цель: создать унифицированный набор технических спецификаций для сетей доступа будущего, способных предоставлять расширенный перечень пакетных услуг в дополнение к стандартным транспортным схемам мультиплексирования с разделением по времени и асинхронного режима передачи. Члены FSAN разработали спецификацию сети PON с использованием ATM в качестве транспортного протокола, ставшую известной как асинхронная PON или APON. В 1997 году ITU-T передал спецификацию APON, переименованную в широкополосную PON (BPON), на рассмотрение для принятия в качестве стандарта, и эта спецификация стала основой для рекомендаций серии G.983 [19]. Первоначальная спецификация PON обеспечивала симметричную скорость 155 Мбит/с (155 Мбит/с в нисходящем канале и 155 Мбит/с в восходящем), которая позже была расширена, включив асимметричную скорость 622–155 Мбит/с и симметричную 622 Мбит/с.

Группа FSAN продолжила работу по определению минимально функционального набора возможностей, реализованного в виде рекомендаций, названных «Общая техническая спецификация» (Common Technical Specification, CTS). Предлагая общий ограниченный набор возможностей, группа FSAN стремилась добиться снижения расходов на оборудование и эксплуатацию за счет уменьшения сложности этого оборудования и увеличения объемов его выпуска. Хотя цель была достойной, требования к эффективной передаче традиционного трафика (TDM и ATM) привели к формированию схемы, неудобной для обеспечения требований доминирующего вида трафика, а именно Ethernet. Преодоление этого ограничения стало целью создания последовавшей за BPON технологии гигабитной PON (GPON).

3.3.3.1. Широкополосная PON. Рекомендации семейства G.983 [19] описывают сеть PON с дальностью работы до 20 км с использованием либо одноволоконного кабеля (две длины волны), либо двухволоконного с максимальным коэффициентом расщепления 1:32. Как упоминалось выше, сеть BPON поддерживает симметричные скорости передачи 155 и 622 Мбит/с и несимметричную 622/155 Мбит/с. BPON отличалась от EPON тем, что имела асимметричную структуру кадров. Форматы кадров, использовавшиеся в нисходящем и восходящем каналах, различались (рис. 3.16). Нисходящий канал (от OLT к ONU) основан на псевдокадре из 56 ячеек ATM. Каждый псевдокадр состоит из 54 «пользовательских» ячеек и двух ячеек для OAM физического уровня (physical layer operations, administration and maintenance, PLOAM). Так же, как и в других разновидностях PON, нисходящий канал пассивно дублируется на все ONU, а конкретное ONU извлекает ячейки с совпадающим VPI/VCI. Кадр нисходящего канала состоит из 56-байтных ячеек, 3 байта являются заголовком, а 53 – ячейкой ATM.

Кадр нисходящего канала



Кадр восходящего канала

Рис. 3.16. Формат кадра BPON со скоростью 622/155 Мбит/с

Широкополосные сети PON управляют пропускной способностью восходящего канала с помощью механизма TDMA, в котором OLT выделяет кванты времени ONU, передавая ячейки GRANT PLOAM. Как часть процедуры обнаружения и настройки ONU OLT выполняет операцию определения дальности до него, которая оценивает период кругового обращения для каждого ONU. OLT вычисляет выравнивающую задержку, нормализующую задержки всех ONU к единому для всех значению, эквивалентному расстоянию в 20 км. OLT обеспечивает особую выравнивающую задержку для каждого ONU, тем самым гарантируя работу восходящего канала без коллизий.

Благодаря своей ранней разработке сеть BPON была успешно внедрена корпорациями NTT в Японии и бывшей Bell South (ныне AT&T) в США, которые предлагали коммерческие услуги, основанные на использовании BPON начиная с 1999 года [34]. Однако в новых решениях PON используются более новые технологии EPON и GPON. Хотя другие технологии ее и обогнали, BPON представляет собой важный вклад в развитие, поскольку она обеспечила фундамент для сменивших ее GPON и EPON.

3.3.3.2. Гигабитная PON. Группы FSAN и ITU-T продолжили развивать свое первоначальное детище – BPON для достижения гигабитных скоростей, представив серию рекомендаций G.984, стандартизирующую гигабитные PON (GPON). Общие характеристики и особенности физического уровня GPON были определены в рекомендациях G.984.1 [20] и G.984.2 [21]. Эти рекомендации содержали спецификации скоростей передачи 1,244 Гбит/с и 2,488 Гбит/с для восходящего и нисходящего каналов. С учетом скорости передачи уже существующих сетей BPON стало доступно семь разных скоростей передачи данных, что предоставило провайдерам сетевого доступа достаточную гибкость при создании их сетей. В спецификациях GPON определяются двухволоконные и одноволоконные (1490 нм для нисходящего канала и 1310 нм для восходящего) системы. Обычная для других вариантов PON длина волны 1550 нм выделялась для оказания дополнительных услуг. Протоколы GPON поддерживают коэффициент разветвления до 1:128 и логическую протяженность канала до 60 км, однако

физически данные параметры были ограничены энергетическим потенциалом оптической линии до 1:64 и 20 км.

Рекомендация G.984.3 [22] определяет функцию конвергенции передачи (transmission convergence, TC). Конвергенция передачи определяет, как пользовательские данные адаптируются к подуровню PMD и включает синхронизацию времени по сети, форматы кадров, процедуры измерения расстояния, а также функциональность уровня MAC. Эта рекомендация также описывает основные функции управления и контроля MAC, включая автообнаружение, наблюдение за исправностью узлов и их производительностью, а также конфигурацию дополнительных возможностей, таких как прямая коррекция ошибок и шифрование. Рассмотрим G.983.3 более подробно.

3.3.3.2.1. Конвергенция передачи GPON. Спецификация уровня конвергенции передачи GPON определяет GPON TC (GPON transmission convergence, GTC) – механизм передачи пользовательского трафика службами GPON (рис. 3.17). В настоящее время стандарты обеспечивают использование методов передачи, основанных на использовании как кадров, так и ячеек. И хотя GPON и BPON поддерживают подуровень конвергенции передачи ATM, эти системы не могут взаимодействовать на обычных скоростях передачи. Введение общего метода инкапсуляции (Generic Encapsulation Method, GEM) устранило имевшую место неэффективность сегментации и последующей сборки кадров переменной длины, что требовалось для систем, основанных на использовании ячеек. Метод GEM многое позаимствовал от общей процедуры кадрирования (Generic Framing Procedure, GFP), определенной в рекомендациях ITU-T G.7041 [35]. GFP – метод мультиплексирования, который позволяет передавать пользовательские данные переменной длины через сети SONET/SDH или аналогичные транспортные сети.

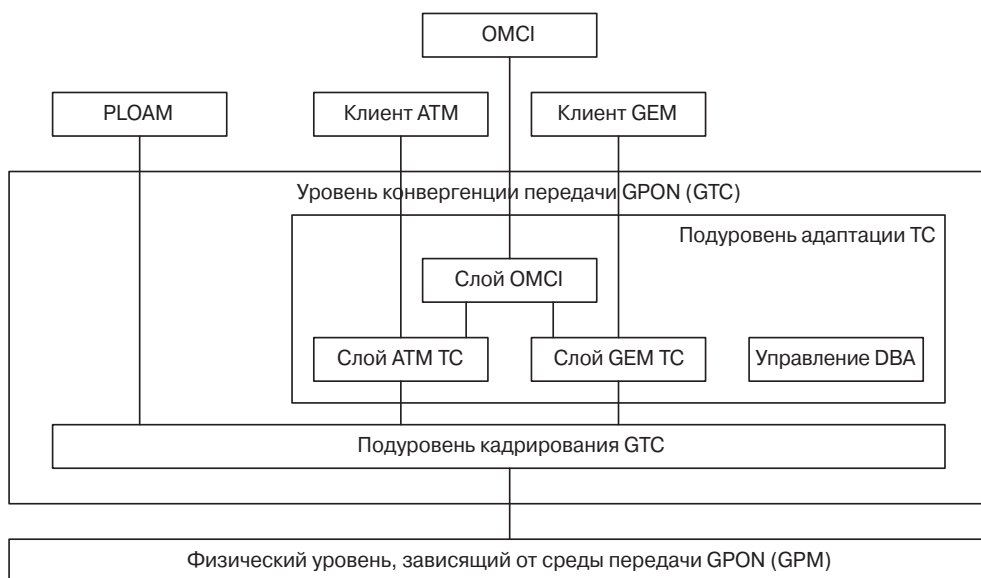


Рис. 3.17. Подуровень конвергенции передачи GPON

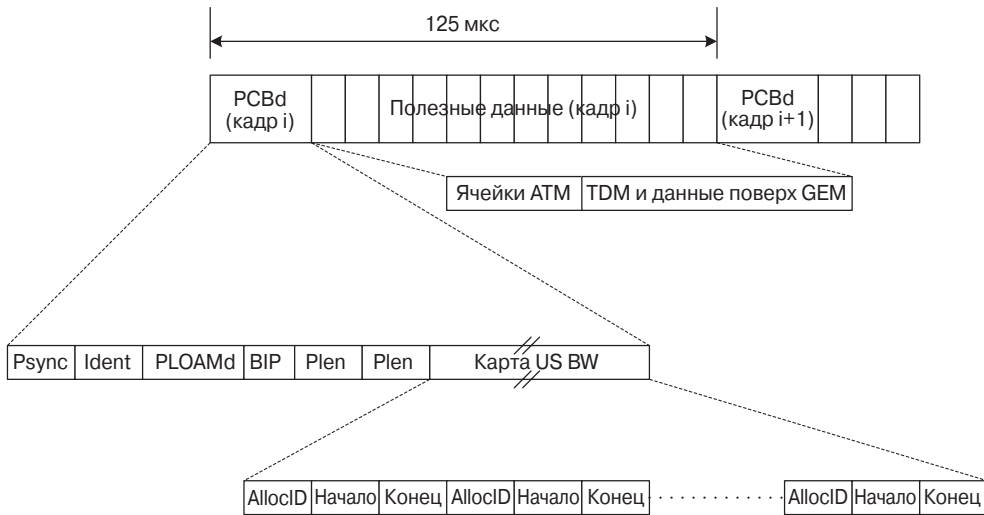


Рис. 3.18. Формат кадра нисходящего канала

Уровень GTC, в свою очередь, разделен на два подуровня: кадров GTC и адаптации TC. Подуровень кадров отвечает за синхронизацию, шифрование, FEC, MAC и PLOAM. Подуровень адаптации описывает две схемы TC: динамическое распределение пропускной способности и определение интерфейса контроля и управления ONU (management and control interface to the ONU, OMCI). Описание особенностей управления ONU содержится в G.984.4 [23].

Сеть GPON, подобно BPON, поддерживает асимметричную структуру кадров, при которой формат кадров в нисходящем канале отличается от формата в восходящем. Кадр нисходящего канала состоит из участка заголовка (physical control block downstream, PCBd) и участка полезных данных. Продолжительность кадра составляет 125 мкс независимо от скорости передачи, что приводит к уменьшению доли полезной нагрузки в кадре при более низкой скорости. Периодичность в 125 мкс дает возможность ONU использовать опорный генератор с частотой 8 кГц, что удобно, в частности, при взаимодействии с сервисами TDM. Рекомендация G.984.3 содержит процедуру определения расстояния, подобно BPON, при которой OLT выравнивает задержки для ONU по значению, эквивалентному расстоянию в 20 км. Такое выравнивание выполняется ONU в ходе процесса активации.

Как показано на рис. 3.18, PCBd содержит поле преамбулы и заголовка для обеспечения синхронизации на физическом уровне. Это поле не шифруется. Четырехбайтовое поле Ident используется как часть системы шифрования данных. Поле PLOAM содержит 13-байтовое сообщение PLOAM, а поле PCBd – скалярный массив распределения пропускной способности, называемый картой пропускной способности (BWmap). Эта карта содержит массив структур выделения. Каждая структура выделения состоит из идентификатора очереди (alloc_ID) и пары указателей – начала и конца. Каждая запись защищена контрольной суммой, которая дает возможность обнаруживать двойные ошибки и исправлять одиночные.

Кадр восходящего канала состоит из переменного числа полей заголовка и секции полезной нагрузки (рис. 3.19). Его продолжительность равна продолжительности кадра нисходящего канала независимо от скоростей передачи. В каждый кадр включается несколько передач от одного или нескольких ONU, координированных с помощью передаваемой в нисходящем канале карты BWmap. Секция полезной нагрузки кадра в нисходящем канале содержит ячейки ATM, фреймы GEM или и то, и другое.

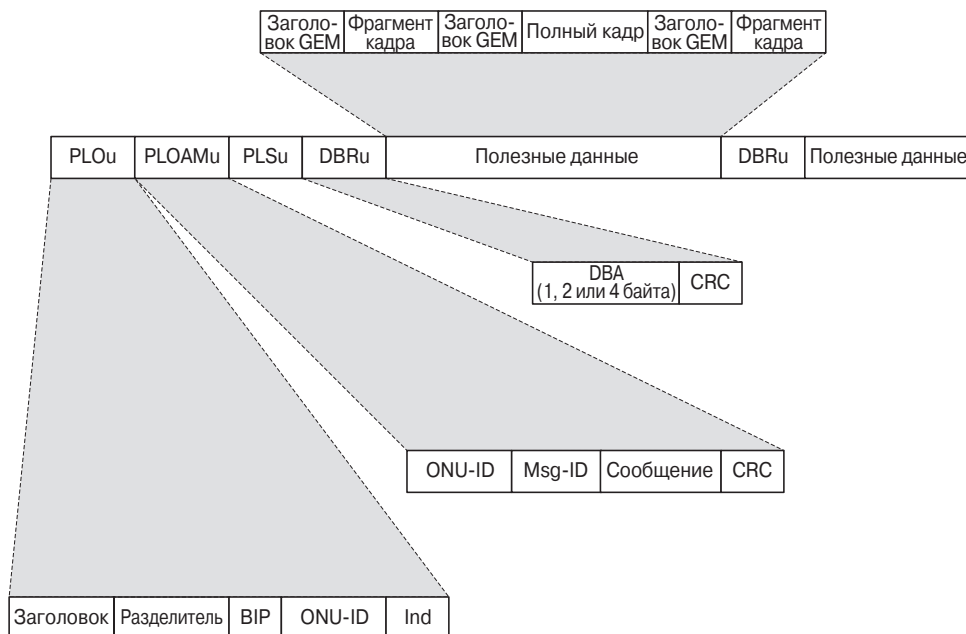


Рис. 3.19. Формат кадра восходящего канала GPON

Формат кадра восходящего канала обеспечивает включение в передачу переменного числа заголовков. В записи размещения BWmap содержатся поля флагов, определяющих включенные в кадр заголовки. Существует четыре типа таких заголовков:

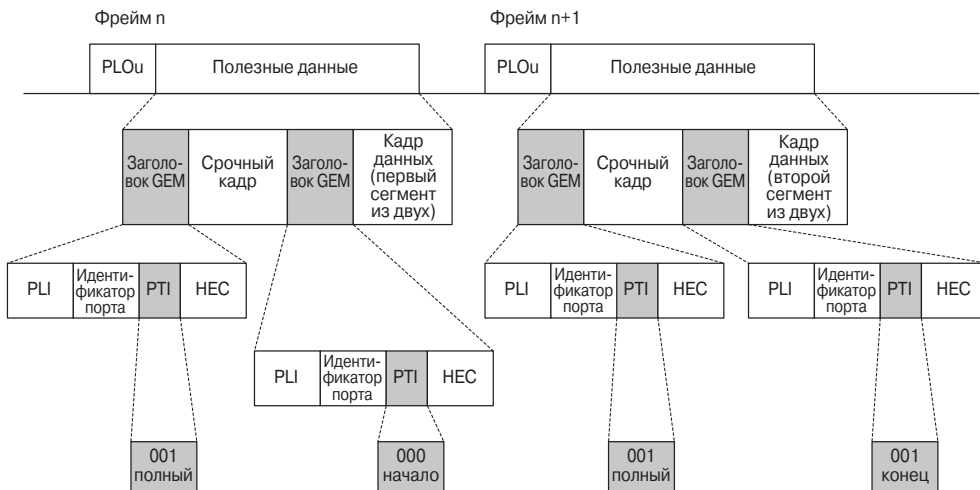
- *заголовок физического уровня (Physical Layer Overhead, PLOu):* обязателен и содержит преамбулу, разделители и информацию идентификации ONU. Различные поля в этом заголовке защищены с помощью четности чередования битов (bit interleaved parity, BIP);
- *ОАМ физического уровня (Physical Layer Operations, Administration, and Maintenance, PLOAMu):* необязательный, если включается, то содержит 13-байтовое сообщение PLOAM;
- *последовательность уровня мощности (Power Level Sequence, PLSu):* этот необязательный заголовок предназначен для регулировки мощности передачи ONU с целью уменьшения динамического диапазона оптического сигнала, поступающего на OLT;

- *отчет о динамической пропускной способности (Dynamic Bandwidth Report, DBRu):* дополнительный заголовок, сообщающий о требованиях ONU к пропускной способности. Он может быть одно-, двух- или четырехбайтовым в зависимости от типа трафика, о котором сообщает. В нем указывается размер запроса (в квантах по 48 байт), или значение согласованной/максимальной скорости передачи, либо и та, и другая информация.

Секция полезной нагрузки кадра в восходящем канале содержит ячейки ATM, фреймы GEM или и то, и другое.

3.3.3.2.2. Инкапсуляция GEM. Общий метод инкапсуляции – основанный на кадрах механизм, способный передавать данные Ethernet, TDM и ATM в едином транспортном контейнере, сохраняя используемые в этих сетях форматы кадров. Фрейм GEM состоит из пятибайтного заголовка GEM и участка полезной информации. Заголовок GEM включает поле длины полезной нагрузки, 12-разрядный идентификатор порта (который облегчает мультиплексирование потока), индикатор типа полезной нагрузки (payload-type indicator, PTI), а также 13-разрядное поле HEC, которое обеспечивает возможность обнаружения и исправления ошибок, а также разграничение фреймов.

Важным различием между EPON- и GEM-инкапсулированными кадрами Ethernet в GPON является то, что GEM разрешает фрагментацию клиентского кадра в данные нескольких фреймов GEM, тогда как стандарт 802.3 не допускает такой фрагментации. Эта способность дает возможность GEM выступать в роли транспорта для TDM, удовлетворяя жестким требованиям к задержкам и джиттеру путем приоритетной обработки критичных ко времени доставки данных TDM за счет несрочного трафика. Эта фрагментация показана на рис. 3.20.



PLI: индикатор длины полезных данных (12 битов).

Идентификатор порта: 12-разрядный идентификатор, позволяющий использовать 4096 идентификаторов трафика.

PTI: индикатор типа полезных данных (3 бита).

HEC: контроль ошибок заголовка (13 битов).

Рис. 3.20. Заголовок GEM и пример фрагментации

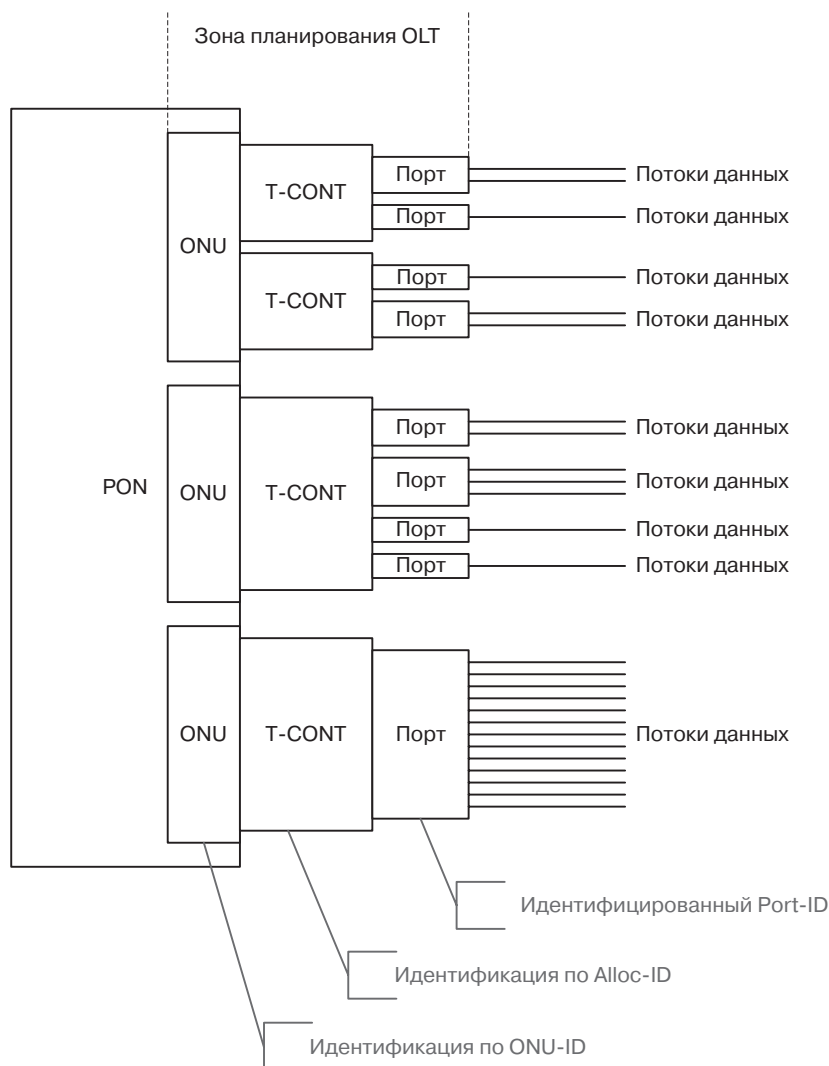


Рис. 3.21. Иерархия классификации трафика GEM

GEM обеспечивает ориентированный на соединение двунаправленный канал передачи данных, определяемый идентификатором порта (port ID). Он используется для транспортировки пользовательского потока данных между ONU и OLT. Порты GEM агрегируются в логические сущности, называемые транспортными контейнерами (T-Cont), которые определяются идентификаторами выделения (Allocation ID, alloc-ID). На рис. 3.21 показана иерархия потоков, портов и контейнеров.

Так же, как и в других вариантах PON, в GPON за планирование передачи по восходящему каналу отвечает OLT, а схема управления обеспечивает точное управление трафиком. Вместо того, чтобы разрешать передачу конкретному ONU с тем, чтобы ONU выбирало, какой именно кадр из набора ожидающих передачу передавать в данный момент, OLT в сети GPON отвечает за планирование переда-

чи каждым ONU каждого контейнера трафика. Такое тонкое (fine-grained) планирование облегчается за счет того, что ONU сообщает о занятости буфера каждого контейнера. Контейнеры трафика аналогичны классам обслуживания, которые агрегируют в одну или несколько физических очередей трафик, требующий сходной обработки. Контейнер рассматривает агрегированные данные как единую сущность с особыми требованиями, такими как пропускная способность, задержки, джиттер. Преимущества такой схемы деления данных: повышенная эффективность сети, снижение сложности (и, тем самым, стоимости) ONU и способность обеспечить уровни качества обслуживания для всех абонентов. Обратной стороной такого подхода становится потенциально значительная доля пропускной способности восходящего и нисходящего каналов, расходуемая на отчеты и запросы выделения пропускной способности для каждого T-Cont от всех ONU. Рекомендации G.984.3 определяют пять типов T-Cont, относящихся к разным классам обслуживания, или уровням планирования:

- TCONT 1: унаследованная эмуляция TDM, обеспечивающая выделение пропускной способности без запроса в виде фиксированного размера полезных данных, запланированных к передаче через определенные интервалы. Доля пропускной способности, используемая TCONT1, исключается из динамического распределения, выполняемого OLT;
- TCONT 2: применяется для трафика с переменной скоростью (VBR), предъявляющего требования как к пропускной способности, так и к задержкам. Этот тип контейнера удобен для пакетизированной передачи речи и видео;
- TCONT 3: тип контейнера предназначен для трафика, обслуживаемому по принципу «Better-Than-Best-Effort», он получает весь избыток пропускной способности, доступный в данный момент, но гарантируется выделение только минимальной ее доли во избежание «зависания» процесса;
- TCONT 4: предназначен для трафика, обслуживаемому по принципу негарантированного обслуживания («Best-Effort»), без выделения гарантированного минимума пропускной способности;
- TCONT 5: сочетание двух или более видов контейнеров. Он предназначен для агрегирования полосы пропускания, выделенной каждому ONU. Порядок передачи различных alloc-ID определяется по усмотрению ONU.

Количество данных, ожидающих передачи в буфере T-Cont, ONU сообщает в поле DBRu кадра восходящего канала. Режим таких отчетов определяется типом TCONT. Режим 0 передает один байт, который соответствует числу 48-байтных блоков, ожидающих передачи. Этот режим полезен для трафика, обслуживаемого без гарантий (TCONT4), и является единственным обязательным режимом, предусмотренным рекомендациями. Режим 1 предназначен для запроса пропускной способности для передачи TCONT3 и TCONT5. Он использует два байта, первый содержит требование к максимальной скорости передачи, второй байт — к средней скорости. Устройство ONU должно управлять входящим потоком данных, используя механизм корзины маркеров. Режим 2 использует четырехбайтовый отчет, оптимальный для TCONT5. В этом режиме ячейки TCONT2 кодируются в первом байте. Второй и третий байты содержат требования к пиковой и средней скоро-

сти передачи TCONT3, а четвертый — длину очереди TCONT4. OLT MAC принимает решения о планировании, исходя из отчетов о динамическом распределении пропускной способности, полученных ранее, и долгосрочных ограничений, принятых для каждого ONU, таким образом, чтобы каждый ONU получил минимальный уровень обслуживания даже при значительной нагрузке на канал.

3.3.4. Управление ресурсами в сетях PON

Механизм распределения пропускной способности восходящего канала в PON затрудняет обеспечение ее справедливого разделения между ONU при соблюдении гарантий качества обслуживания и непрерывного высокого уровня использования сети. В большом количестве исследований [27–30] предлагались различные алгоритмы для решения этой проблемы. В данном разделе будет рассмотрена концепция управления ресурсами в сети PON.

Еще в ранних описаниях EPON и GPON управление ресурсами начиналось с согласования.

EPON и GPON разрешают ONU запрашивать требуемую пропускную способность восходящего канала, тогда как OLT выделяет запрошенные ресурсы в соответствии с некоторыми заранее установленными правилами. В сетях EPON, соответствующих 802.3ah, это достигается обменом сообщениями REPORT/GATE по протоколу MPCP, а в сетях GPON, соответствующих G.984, той же цели служит механизм DBRu/BWmap.

Второй аспект управление ресурсами заключается в выборе ONU, которому предоставляется возможность передачи. Решение может определяться классом обслуживания, который ONU запрашивает для передачи данных, как это имеет место в случае GPON, или быть полностью оторванным от него, например в случае использования алгоритма кругового обслуживания. Но один аспект управления ресурсами не является полностью определенным ни в стандарте EPON, ни в GPON: точное выделение пропускной способности для ONU или класс обслуживания трафика конкретного ONU. Также данный механизм называется динамическим выделением пропускной способности (dynamic bandwidth allocation, DBA). Алгоритмы такого выделения учитывают количество и тип данных, буферизованных в ONU и ожидающих передачи, они дают OLT возможность динамически изменять долю пропускной способности, выделяемую ONU для обслуживания этих данных. Алгоритмы DBA являются важным механизмом повышения эффективности использования пропускной способности восходящего канала, так как они увеличивают общую производительность.

Сети доступа по своей природе характеризуются пульсирующим характером трафика из-за сравнительно умеренного уровня агрегации трафика, генерируемого сравнительно небольшим количеством абонентов. В отличие от них, городские и магистральные сети, объединяющие большое количество источников трафика, эффективно сглаживают суммарную нагрузку. Изучение профилей классического трафика Ethernet [36] показывает, что трафик, генерируемый каждым отдельным источником, носит ярко выраженный пульсирующий характер, что приводит к значительным изменениям потребности в пропускной способности в

разные моменты времени. Статическое выделение пропускной способности входящего канала приводит к его недоиспользованию, что выражается в невысокой пропускной способности в целом, увеличенным задержкам пакетов и потенциально возможным потерям пакетов даже при низкой загрузке. Применение алгоритмов DBA позволяет сети адаптироваться к требованиям к пропускной способности, существующим в данный момент, обеспечивая большую степень статистического мультиплексирования, а следовательно к более высокой пропускной способности, меньшим задержкам и потерям пакетов.

3.3.4.1. Алгоритм IPACT. Классическим алгоритмом статистического мультиплексирования, является алгоритм чередующихся опросов с адаптивным временем цикла (Interleaved Polling with Adaptive Cycle Time, IPACT), описанный в [28, 30]. При использовании этого алгоритма каждый ONU опрашивается индивидуально и получает разрешения на передачу по простому циклическому алгоритму. Размер выделенного окна передачи равен запрошенному в предыдущем цикле, тем самым гарантируя, что пропускная способность распределяется динамически в зависимости от заполненности очереди. Чтобы предотвратить монопольное использование всей полосы одним ONU, каждому из них назначается максимальный размер окна передачи (maximum transmission window, MTW). После того как ONU использует свое MTW, оно не получит больше возможностей передачи до следующего цикла опроса. Существует несколько разновидностей этого алгоритма, различающихся трактовкой понятия MTW:

- фиксированный: DBA игнорирует запрошенный размер окна, вместо этого выделяя MTW с постоянным интервалом опроса;
- ограниченный: DBA выделяет окно запрошенного размера, но не более установленного для него предела;
- доверительный: DBA выделяет окно, размер которого превышает размер запрошенного на некую постоянную величину (пропорциональную размеру окна);
- эластичный: DBA пытается преодолеть ограничение выделения MTW в цикле опроса, при этом OLT накапливает данные об успешных циклах опроса, что гарантирует, что в течение последних N выделений назначенная пропускная способность не превысит $N \times \text{MTW}$, где N – число ONU.

3.3.4.2. Схемы классов обслуживания. Другие алгоритмы распределения пытаются учесть тип трафика, который отправляет ONU. В некоторых случаях предоставление ONU агрегированной пропускной способности может оказаться недостаточным для того, чтобы весь трафик был обработан согласно потребности. Например, голосовой трафик накладывает на сети доступа строгие ограничения по задержкам. Рекомендация ITU-T G.114 «Время передачи в одном направлении» [37] устанавливает задержку в 1,5 мс для распространения сигнала в одном направлении в пределах сети доступа. Безотносительно к тому, какая доля пропускной способности выделена данному ONU, если такие данные будут задержаны более чем на 1,5 мс, качество передаваемого звука может ухудшиться. Семейства алгоритмов планирования, которые учитывают не только использование пропускной способности, но и задержки; джиттер и требования к потере пакетов могут быть классифицированы на обеспечивающие абсолютное качество обслуживания или относи-

тельное. Абсолютные гарантии являются количественными, и они описывают требования соглашения о предоставлении услуги (Service Level Agreement, SLA) к трафику в терминах пропускной способности, задержек и доли потерянных пакетов. Относительные гарантии QoS характеризуют гарантию обслуживания в качественных терминах, таких как «низкие потери», «малые задержки», обеспечение заданной пропускной способности. Обслуживание разных классов планируется таким способом, что их относительная важность сохраняется. Если говорить в общем, то схема с абсолютной гарантией может быть сложной и может включать элементы контроля доступа и профилирования для каждого класса.

Хотя в этой области было проведено немало исследований, давших ценные результаты, важно вернуться назад и проанализировать необходимость использования таких сложных методов в восходящем канале, в частности, учитывая особенности сетей широкополосного доступа в жилых районах. Очевидно, что в нисходящем канале требуются услуги передачи голоса (низкие задержки и низкая пропускная способность), видеосигнала (гарантированная полоса пропускания и малые потери) и обязательства по доступу в Интернет. Для восходящего канала простых высокоприоритетных услуг (передача голоса) и обязательств по предоставлению доступа в Интернет будет, по всей видимости, достаточно для большинства абонентов. Другие часто упоминаемые классы услуг для приложений – игры и ориентированные на пользователей видеоконференции – дают невысокий доход и имеют низкий потенциал его роста. Известно, что услуги, ориентированные на бизнес, могут потребовать более тщательно продуманного выделения пропускной способности, чтобы обслуживать трафик учреждений АТС, основанный на TDM, и большое разнообразие классов услуг. Эти сценарии могут привести к возрастанию сложности и стоимости, связанному с интеллектуальными механизмами обеспечения QoS в восходящем канале, позволяющими PON заменить одни услуги другими.

3.3.5. Тенденции будущего

Пассивные оптические сети обещают на порядок большую пропускную способность, чем существующие сейчас сети доступа, использующие медные провода. Однако эти сети находятся в процессе развития и изучения областей для применения в будущем.

Сети PON, основанные на TDM, могут развиваться в различных направлениях. Повышенный энергетический потенциал мог бы позволить добиться большего коэффициента разветвления или большей протяженности, значительно увеличив количество пользователей, обслуживаемых одним оптоволоконном. Это важный фактор в определении экономической целесообразности сети PON, поскольку он позволяет разнести амортизационные расходы на большее число пользователей, снижая стоимость услуг в расчете на одного абонента. Тех же целей можно достичь усилением сигнала, но ценой потери ценного качества оптических сетей доступа (optical distribution network, ODN) – их пассивного характера. Другим направлением масштабирования является скорость передачи. Международные органы стандартизации активно работают над описаниями более высокоскоростных сетей PON.

IEEE силами рабочей группы P802.3av [25] готовит стандарт 10-гигабитной сети Ethernet PON, имея целью обеспечить как симметричную 10 Гбит/с сетевую архитектуру, так и несимметричную – 10 Гбит/с в нисходящем канале и 1 Гбит/с – в восходящем. ITU-T рассматривает подобные расширения к рекомендациям GPON, чтобы увеличить скорость до 10 Гбит/с и выше. Постепенное развитие PON за счет повышения скорости передачи данных сохраняет средства, вложенные в существующую PDN, повышает ее пассивную природу и независимость от скорости, требуя при модернизации только замены оптоэлектроники в OLT и ONU.

Сети PON с поддержкой спектрального уплотнения каналов (мультиплексированием с разделением по длине волны) (wave division multiplexing, WDM) [38] превосходят современные сети TDM PON, равно как и разрабатываемые в настоящее время высокоскоростные сети PON. Сети WDM-PON обещают достичь гораздо большей пропускной способности. В них каждая пара ONU и OLT использует отдельную пару длин волн, что обеспечивает соединение «точка–точка». Разделение по длинам волн обеспечивает улучшенную защиту конфиденциальности, может гарантировать коэффициент расщепления в 10 раз больший, чем достигнутый в настоящее время, и увеличить дальность связи до 100 км. Возникающие при этом проблемы вполне преодолимы при условии использования рентабельной и надежной настраиваемой оптики.

Сети PON имеют значительный потенциал роста, что делает их идеальными кандидатами для сетей доступа будущего, которые необходимы для предоставления новых, зачастую еще неизвестных услуг в следующие десятилетия. Конечно, это серьезный вызов, но сети WDM-PON и гибридная архитектура TDM/WDM сулят достичь практически неограниченных скоростей. Безусловно, будущее будет ярким – с оптической точки зрения, разумеется.

3.4. Гибридные коаксиально-оптические сети

Операторы телевизионных кабельных сетей (CATV) перенесли свою основную деятельность из сферы предоставления видеоконтента в область предоставления полного набора услуг – видео, голосовой связи и телекоммуникационных. Это повлекло за собой техническую эволюцию кабельных сетей доступа с включением в сетевую структуру оптоволоконных каналов и значительной модернизацией того, что раньше было однонаправленной широкоэвещательной сетью, в двунаправленную сеть со многими услугами. Операторы кабельных сетей (называемые также многосистемными операторами – multiple system operators, MSO) агрессивно расширяли свои сети, чтобы обеспечить распространение многих сотен каналов телевидения высокой четкости, видео по заказу, персонализированных видеослужб и высокоскоростного доступа к Интернету в ответ на конкурентное давление со стороны операторов телекоммуникационных сетей. В этом разделе будут рассмотрены основы построения гибридных коаксиально-оптических (hybrid fiber coaxial, HFC) сетей доступа, особое внимание будет уделено стандарту DOCSIS 3.0 [39–42] – новейшему из серии стандартов, описывающих передачу данных по коаксиальному кабелю.

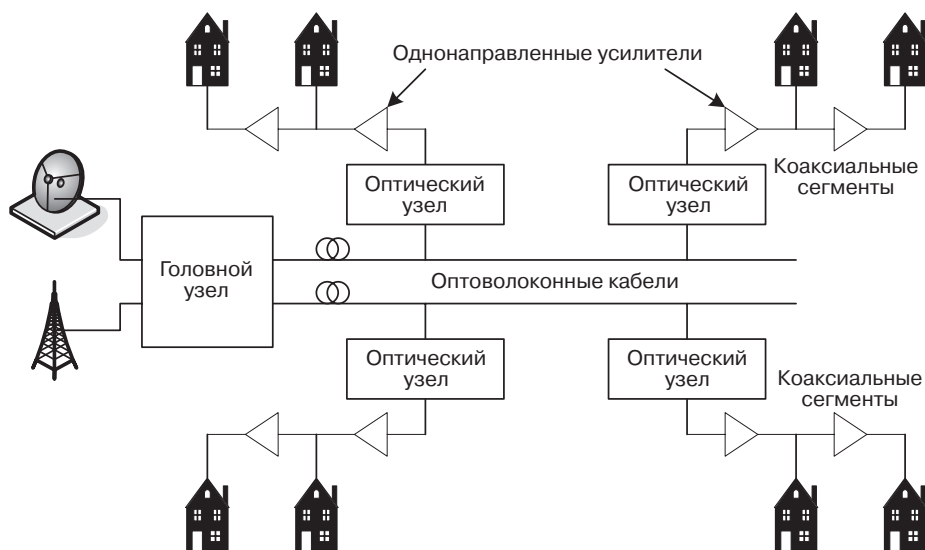


Рис. 3.22. Сетевая архитектура однонаправленной гибридной коаксиально-оптической сети

3.4.1. Архитектура гибридных коаксиально-оптических сетей

Сети кабельного телевидения являлись, по существу, однонаправленными сетями, способными передавать видеосигнал. Сети были спроектированы специально с учетом местных стандартов телевидения, передача сигнала велась на радиочастотах, характеристики каналов были близкими к характеристикам эфирного телевидения в данной местности, в частности, Северной Америке это привело к использованию вещания в стандарте NTSC с полосой пропускания 6 МГц. Чтобы улучшить протяженность сети и качество сигнала, в головных узлах (head end, HE) использовалось оптоволокно с низкими потерями. Эта архитектура известна как гибридная коаксиально-оптическая сеть (рис. 3.22).

В такой сети головной узел получает видеоконтент от телевизионных спутников, местного эфирного вещания или других источников. Затем он смешивается с местным контентом и модулируется в аналоговую форму для передачи по оптоволоконной распределительной сети. Оптоволоконные кабели оканчиваются в оптических узлах, которые обслуживают жилые зоны с числом абонентов от нескольких сотен до нескольких тысяч. В них выполняется преобразование оптического сигнала в электрический, и аналоговый радиосигнал передается по сегментам сети из коаксиального кабеля. Оптоволокно практически не имеет потерь в диапазоне частот от мегагерц до гигагерц, чего нельзя сказать о коаксиальном кабеле, требующем использования усилителей для обеспечения всех абонентов сигналом приемлемого качества. Гибридная коаксиально-оптическая сеть обеспечивает передачу полного спектра сигналов видеовещания в диапазоне 54–550 МГц.

Чтобы обеспечить полнодуплексный обмен, сети HFC были модернизированы для поддержки передачи в обе стороны. Оптическая часть сети может использовать для восходящего канала отдельные волокна, но коаксиальный сегмент должен пе-

редавать и прямой, и обратный сигналы. Для передачи восходящего канала используется диапазон частот от 5 до 42 МГц. Кроме того, усилители в коаксиальных сегментах были модернизированы, чтобы поддерживать двунаправленное усиление. В прямом направлении для передачи данных используется один канал шириной 6 МГц. При использовании 64-символьной квадратурной амплитудной модуляции пропускная способность может составлять до 30 Мбит/с. При передаче в восходящем канале в связи с большим уровнем шумов в диапазоне частот 5–42 МГц используются более устойчивые методы модуляции: квадратурная с фазовым сдвигом (QPSK) и 16-символьная QAM.

Помимо модернизации сети для обеспечения полнодуплексной работы в сетях HFC требуется дополнительное оборудование. У абонентов устанавливаются кабельные модемы, преобразующие цифровую информацию (обычно кадры Ethernet) в модулированный радиосигнал, передаваемый в восходящем канале, и сигнал в нисходящем канале, в цифровой вид. Оконечная станция кабельного модема (Cable Modem Termination System, CMTS), устанавливаемая на головных узлах, выполняет обратное преобразование. Оно включает в себя преобразование шестимеггерцового канала, объединение его с другими каналами и преобразование сигналов для работы с оптической частью сети. На рис. 3.23 показана сеть HFC, которая поддерживает цифровую передачу данных.

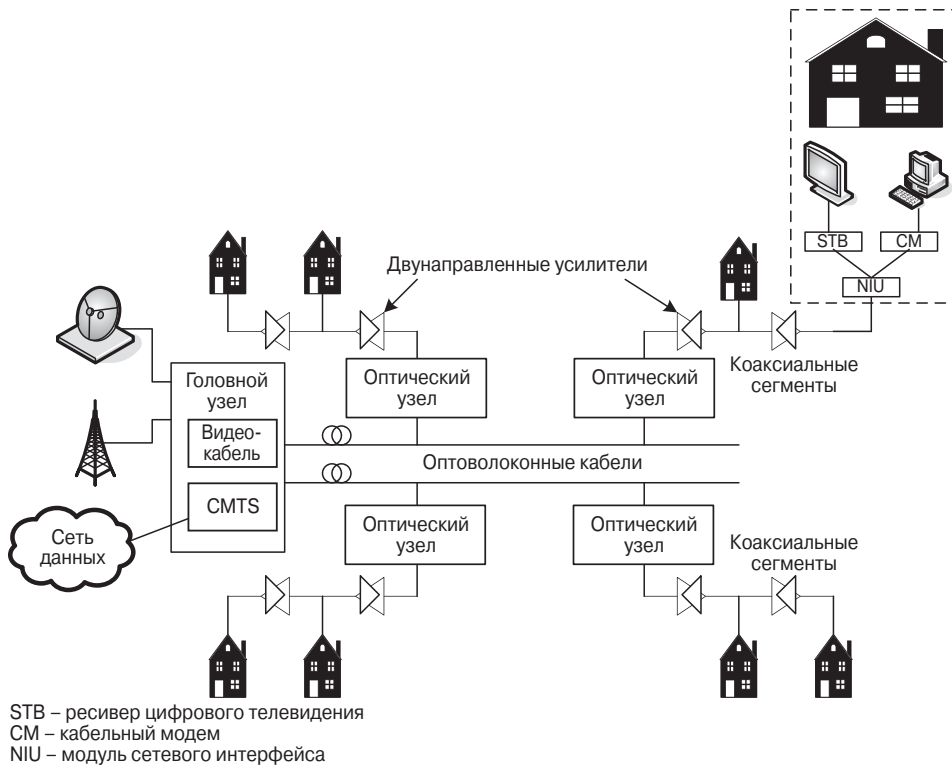


Рис. 3.23. Сетевая архитектура двунаправленной гибридной коаксиально-оптической сети

Поскольку пропускная способность этой сети разделяется между абонентами, все передачи в обратном канале должны координироваться. Двухнаправленные усилители в коаксиальных сегментах не дают кабельным модемам возможности обнаруживать коллизии, препятствуя использованию механизмов, определяющих наличие несущей, таких как CSMA/CD. Передачу данных в обратном канале, свободную от коллизий, обеспечивает механизм TDMA канального уровня, подобный тем, что используются в сетях PON. Головная станция регулярно посылает широкоэвещательные запросы. Недавно добавленные станции отвечают на них, процедура определения длины линии вычисляет дополнительную задержку, и головная станция назначает кабельному модему квант времени для передачи.

3.4.2. Стандарты DOCSIS

Стандарты передачи данных по коаксиальному (телевизионному) кабелю (Data Over Cable Service Interface Specification, DOCSIS) описывает физический, MAC и сетевой уровни взаимодействия между кабельным модемом и головной станцией. Эти стандарты также содержат описание методов обеспечения безопасности (абонентских данные в разделяемой среде передачи) и службы управления сетью. Стандарт DOCSIS 1.0, выпущенный в 1997 году [43], предоставлял базовые возможности соединения с Интернетом. Он поддерживает в нисходящем канале схемы модуляции 64 и 256-QAM и в восходящем – QPSK и 16-QAM. Ценность первого варианта заключалась в том, что он обеспечил стандартизацию оборудования, это улучшило способности к взаимодействию, снизило стоимость оборудования и увеличило распространенность этой системы. Стандарт DOCSIS 1.1, оформленный в 2001 году [44], улучшил меры безопасности и добавил возможности QoS. Благодаря этому кабельные операторы получили возможность предлагать дополнительные услуги, такие как игры и передача голоса.

Стандарт DOCSIS 2.0, представленный в 2002 году [45], увеличил пропускную способность (до 30 Мбит/с в восходящем канале и 50 Мбит/с в нисходящем) и расширил набор схем модуляции QAM в восходящем канале. Последняя версия DOCSIS 3.0 [39–42] предусматривает связывание каналов (channel bonding) для увеличения скорости передачи как в нисходящем, так и восходящем каналах, чтобы обеспечить возможность конкуренции с сетями VDSL/VDLS2 и FTТх. При связывании четырех каналов достигается пропускная способность 120 Мбит/с в восходящем канале и 160 Мбит/с – в нисходящем. Объединением большего числа каналов можно достичь большей пропускной способности. Связывание каналов является логическим объединением нескольких радиочастотных каналов. В нисходящем канале мультиплексирование осуществляется на уровне пакетов, каждый пакет передается по одному каналу. В восходящем канале пакет «нарезается» и передается через все доступные в группе каналы. Например, если кабельному модему требуется отправить пакет Ethernet размером 1000 байт, он запрашивает у головной станции тысячебайтовый квант времени. В случае связывания каналов головная станция отвечает выделением квантов для передачи фрагментов пакетов в связанных каналах: это может быть 500-байтовый квант в восходящем кана-

ле № 1, 200-байтовый в восходящем канале № 2 и 300-байтовый в восходящем канале № 3. Кабельный модем сегментирует пакет на 500-байтовый, 200-байтовый и 300-байтовый фрагменты и отправляет их по трем восходящим каналам. Каждый фрагмент содержит последовательный номер и указатель, что дает головной станции возможность выполнить необходимую сборку фрагментов, воссоздав исходный 1000-байтовый пакет. Связывание каналов в DOCSIS 3.0 имеет обратную совместимость с кабельными модемами стандартов DOCSIS 1.x/2.0, что гарантирует прозрачную миграцию на большую пропускную способность. Другими заметными улучшениями в DOCSIS 3.0 стали возможность физического переключения диапазона частот восходящего канала (к стандартным 5–42 МГц добавились 5–65 МГц и 5–85 МГц), позволившая расширить пропускную способность, поддержка IPv6, QoS для многоадресного IP-вещания, отслеживание абонентом многоадресного IP-вещания и повышенная безопасность.

3.4.3. Тенденции будущего

Многосистемные операторы остро ощущают угрозу, исходящую от архитектуры FTTH, внедряемой телекоммуникационными компаниями. Сети FTTH имеют то преимущество, что сигналы видеовещания (1550 нм) и нисходящего и восходящего каналов данных (1490/1310 нм) передаются на разных длинах волн. Для того, чтобы многосистемные операторы смогли предоставить такую же пропускную способность, необходимо дальнейшее развитие сетей HFC. Они активно добиваются следующих эволюционных улучшений:

- отвлечение части пропускной способности уменьшает количество телепрограмм, доступных в аналоговом виде. Исключенные каналы могут быть демодулированы и приняты с помощью телеприставок. Это требует преобразования их в цифровую форму и сжатия видеосигнала в формат MPEG-4. Для декодирования требуется установка ресивера или наличие функции декодирования, встроенной в телевизор;
- технология коммутируемого цифрового видео (switched digital video, SDV) переходит от широкоэвещательной передачи к модели многоадресного распределения. В системах SDV абонентам доставляются только те каналы, которые они в данный момент смотрят;
- расширение используемого спектра частот. Верхняя частота спектра, используемого в HFC, увеличилась с 550 до 750 МГц и до 860 МГц в настоящее время. Ведутся работы по ее увеличению до 1002 МГц;
- упрощение плана распределения частот объединением всех специальных услуг, таких как цифровое телевидение обычного стандарта, видео по запросу и высокоскоростной доступ в Интернет, в один широкополосный канал (> 200 МГц) и доставкой их с использованием IP-транспорта. Такая архитектура требует расширения и усложнения возможностей управления IP-трафиком в головных станциях и кабельных модемах, чтобы гарантировать доставку с требуемым уровнем QoS.

Гибридные коаксиально-оптические сети и использующие их операторы занимают прочные позиции на рынке, предоставляя услуги по доставке видеокон-

тента огромному количеству людей по всему миру. Тем не менее, они вынуждены усовершенствовать свои сети, чтобы предложить пропускную способность и услуги не хуже тех, что предлагают телекоммуникационные операторы. Под давлением финансовых соображений, заставляющих выживать и конкурировать, сети HFC будут оставаться важной частью проводных сетей доступа, предоставляя высокую пропускную способность и богатый выбор услуг множеству абонентов.

3.5. Заключение

Несмотря на свои технические различия, проводные сети доступа эволюционировали от уровня физических соединений, предназначенного для предоставления одной-единственной услуги, к сложным сетям со множеством услуг, в которых весь трафик, включая голосовой и видео, использует в качестве транспорта протокол IP. Чтобы обеспечить такое развитие, создатели проводных сетей доступа сконцентрировались на увеличении пропускной способности физического уровня, доступной абонентам, и росте «интеллектуальности» сетей, гарантирующей, что любое приложение или услуга при передаче по протоколу IP получит необходимое качество обслуживания, необходимое для удовлетворения ожиданий абонентов. Широкополосные сети будущего смогут предоставить скорость в сотни мегабит в секунду (потенциально гигабиты) в каждый дом или офис. Доступность такой полосы пропускания сделает возможными недоступные сейчас услуги, и даже те, которые сегодня трудно представить.

Литература

1. US Patent and Trade Mark Office, Patent # 244,426, A. G. Bell, July 19 1881.
2. Chris Hellberg et al., *Broadband Network Architectures: Designing and Deploying Triple Play Services*, Prentice-Hall, 2007.
3. J. Cioffiet al., CuPON: The copper alternative to PON 100 Gb/s DSL networks, *IEEE Commun. Mag.*, Vol. 45, No. 6, pp. 132–139, June 2007.
4. D. Waring, J. Lechleider, and T. Hsing, Digital subscriber line technology facilitates a graceful transition from copper to fiber, *IEEE Commun. Mag.*, Vol. 29, No. 3, pp. 96–104, March 1991.
5. J. Cioffi and G. Ginis, Vectored transmission for digital subscriber line systems, *IEEE JSAC Special Issue on Twisted Pair Transmissions*, Vol. 20, No. 5, pp. 1085–1104, March 2001.
6. ITU-T, ITU-T Recommendation G.992.2: Single-Pair High-Speed Digital Subscriber Line (SHDSL) Transceivers, ITU-T, December 2003.
7. ITU-T, ITU-T Recommendation G.992.1: Asymmetric Digital Subscriber Line (ADSL) Transceivers, July 1999.
8. ITU-T, ITU-T Recommendation G.992.3: Asymmetric Digital Subscriber Line Transceivers 2 (ADSL2), January 2005.
9. ITU-T, ITU-T Recommendation G.992.5: Asymmetric Digital Subscriber Line (ADSL) Transceivers – Extended Bandwidth ADSL2 (ADSL2+), January 2009.
10. ITU-T, ITU-T Recommendation G.993.1: Very High Speed Digital Subscriber Line Transceivers, June 2004.
11. ITU-T, ITU-T Recommendation G.993.2: Very High Speed Digital Subscriber Line Transceivers 2 (VDSL2), February 2006.

12. Broadband Forum, DSL Technology Evolution – ADSL2/ADSL2plus/ADSL-RE/VDSL2, http://www.broadband-forum.org/downloads/About_DSL.pdf.
13. Broadband Forum, www.broadband-forum.com.
14. Broadband Forum, Technical Report TR-101, Migration to Ethernet-Based DSL Aggregation, April 2006.
15. IETF, RFC 2516 – A Method for Transmitting PPP Over Ethernet (PPPoE), February 1999.
16. IETF, RFC 2661 – Layer Two Tunneling Protocol «L2TP», August 1999.
17. Telenor Group, dynamic spectrum management – A methodology for providing significantly higher broadband capacity to the users, *Telektronikk*, No. 4, pp. 126 –137, 2004.
18. L. Hutcheson, FTTx: Current status and the future, *IEEE Commun. Mag.*, July 2008.
19. ITU-T, ITU-T Recommendation G.983.1: Broadband Optical Access Systems Based on Passive Optical Networks (PON), January 2005.
20. ITU-T, ITU-T Recommendation G. 984.1: Gigabit-Capable Passive Optical Networks (GPON): General Characteristics, March 2003.
21. ITU-T, ITU-T Recommendation G.984.2: Gigabit-Capable Passive Optical Networks (GPON): Physical Media Dependent (PMD) Layer Specification, March 2003.
22. ITU-T, ITU-T Recommendation G. 984.3: Gigabit-Capable Passive Optical Networks (GPON): Transmission Convergence Layer Specification, February 2004.
23. ITU-T, ITU-T Recommendation G. 984.4: Gigabit-Capable Passive Optical Networks (GPON): ONT Management and Control Interface Specification, June 2004.
24. IEEE, IEEE 802.3 Local and Metropolitan Area Networks – Specific Requirements, Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, December 2005.
25. IEEE P802.3av task force (<http://www.ieee802.org/3/av/>).
26. IEEE, Ethernet PON (EPON) and the PAR + 5 Criteria, May 2001, www.ieee802.org/3/efm/public/may01/pesavento_1_0501.pdf.
27. G. Kramer, *Ethernet Passive Optical Networks*, McGraw-Hill, New York, 2005.
28. Y. Luo et al., Resource management for broadband access over time-division multiplexed passive optical networks, *IEEE Network*, Vol. 21, No. 5, pp. 20–27, September/October 2007.
29. J. Angelopoulos et al., Efficient transport of packets with QoS in an FSAN-aligned GPON, *IEEE Commun. Mag.*, Vol. 42, No. 2, pp. 92–98, February 2004.
30. M. McGarry, M. Maier, and M. Reisslein, Ethernet PONs: A survey of dynamic bandwidth allocation (DBA) algorithms, *IEEE Optical Commun. Mag., Special Supplement Optical Communications*, Vol. 42, No. 8, pp. 8–15, August 2004.
31. PMC-Sierra Inc. PAS6301 device, www.pmc-sierra.com.
32. Teknovus Inc. TK3701 device, www.teknovus.com.
33. Full Service Access Network (FSAN), <http://www.fsanweb.org/>.
34. H. Ueda et al., Deployment status and common technical specifications for a B-PON system, *IEEE Commun. Mag.*, Vol. 39, No. 12, pp. 134 –141, December 2001.
35. ITU-T, ITU-T Recommendation, G.7041: Generic Framing Procedure (GFP), February 2003.
36. W. Leland, M. Taqqu, W. Willinger, and D. Wilson, On the self-similar nature of Ethernet traffic (extended version), *IEEE/ACM Trans. Networking*, Vol. 2, No. 1, pp. 1–15, February 1994.
37. ITU-T, ITU-T Recommendation, G.114: One-Way Transmission Time, May 2003.
38. K. Grobe and J.-P. Elbers, PON in adolescence: From TDMA to WDM-PON, *IEEE Commun. Mag.*, Vol. 46, No. 1, pp. 26–34, January 2008.
39. CableLabs, Data-over-cable service interface specifications, cable modem to customer premise equipment, interface specification, CM-SP-CMCIv3.0-I01-080320, March 2008.

40. CableLabs, Data over cable service interface specifications, DOCSIS 3.0, physical layer specification, CM-SP-PHYv3.0-I08-090121, January 2009.
41. CableLabs, Data-over-cable service interface specifications, DOCSIS 3.0, MAC and upper layer protocols interface specification, CM-SP-MULPIv3.0-I09-090121, January 2009.
42. CableLabs, Data-over-cable service interface specifications, DOCSIS 3.0, security specification CM-SP-SECv3.0-I09-090121, January 2009.
43. CableLabs, DOCSIS 1.0, <http://www.cablemodem.com/specifications/specifications10.html>.
44. CableLabs, DOCSIS 1.1, <http://www.cablemodem.com/specifications/specifications11.html>.
45. CableLabs, DOCSIS 2.0, <http://www.cablemodem.com/specifications/specifications20.html>.