ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ
Государственное образовательное учреждение высшего профессионального образования
«**ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**»

А.В. Марчуков

БЕСПРОВОДНЫЕ ИНФОРМАЦИОННЫЕ СЕТИ

Рекомендовано в качестве учебного пособия
Редакционно-издательским советом
Томского политехнического университета

Издательство
Томского политехнического университета
2009

УДК 681.327.8(075.8)
ББК 32.973.202я73
М30

Марчуков А.В.

М30 Беспроводные информационные сети: учебное пособие / А.В. Марчуков; Томский политехнический университет. – Томск: Изд-во Томского политехнического университета, 2009. – 84 с.

В учебном пособии рассматриваются современные беспроводные сети (БС), их архитектура, топология, методы управления, сетевые стандарты и системы безопасности.

Разработано в рамках реализации Инновационной образовательной программы ТПУ по направлению «Информационно-коммуникационные системы и технологии» и предназначено для студентов, изучающих дисциплины «Вычислительные сети, системы и телекоммуникации», «Сетевые операционные системы».

УДК 681.327.8(075.8)
ББК 32.973.202я73

Рецензенты

Кандидат технических наук,
доцент кафедры КСУП ТУСУРа
В.П. Коцубинский

Главный инженер фирмы «Интант»
С.Н. Кузмичев

ОГЛАВЛЕНИЕ

Введение

Технология беспроводных сетей WLAN (Wireless LAN) развивается довольно быстро. Эти сети удобны в первую очередь для подвижных средств, но находят применение и в других областях (динамичные сети фирм, больницы и т. д.). В данной работе собран и систематизирован опыт проектирования, построения и эксплуатации беспроводных сетей и беспроводных систем передачи данных за период 2000–2008 годы. Наиболее перспективным представляется проекты IEEE 802.11 и IEEE 802.16, которые должны играть для радиосетей такую же интегрирующую роль, как 802.3 для сетей Ethernet. В системах передачи данных на основе мобильной телефонной связи перспективными направлениями являются стандарты 3G и 4G. Беспроводные сети и системы передачи данных на основе радиоканала не могут конкурировать по качеству услуг, производительности, помехозащищённости с системами передачи данных на основе оптоволокна в глобальных и региональных сетях, а с сетями на основе витой пары в локальных сетях. Но они являются единственной альтернативой в подвижных системах, в условиях труднодоступной местности и временно развёртываемых сетевых фрагментах. Дополнительные возможности пользователям, нуждающимся в услугах беспроводной связи, предоставляет стандарт bluetooth, который призван освободить руки клиенту и покончить с телефонными проводами. Домашние беспроводные сети на основе с ZigBee – стандарта беспроводной передачи данных на короткие расстояния объединяют между собой большинство бытовых устройств. Но одним стандартом ZigBee на малых расстояниях дело не ограничивается. Уже разработан и утвержден конкурирующий стандарт ультра-широкополосного доступа, получивший название беспроводного USB – WUSB. WUSB представляет собой беспроводное расширение стандарта USB 2.0 и позволяет передавать информацию со скоростью 480 Мбит/с в радиусе 10 м. Бурно растущий рынок сетевых услуг на основе мобильной телефонии требует определённого внимания с точки зрения понимания того, какой сервис можно получить с данного рынка. Административные аспекты построения беспроводных сетей также необходимо знать при их проектировании. Наконец, стандарты, которые положены в основу разработки и эксплуатации беспроводных систем, служат основным руководящим и стартовым документом при принятии решения о развёртывании мобильных систем. Рынок систем и устройств для беспроводной передачи данных развивается столь динамично, что требует пристального внимания специалистов по автоматизации практически всех областей нашей деятельности.

1. ПОНЯТИЕ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ПРЕДПРИЯТИЯ

1.1. Структурно-функциональная модель информационной инфраструктуры предприятия, формирование системного определения информационной инфраструктуры

Понятие инфраструктуры с течением времени претерпевало значительные изменения. Более того, в настоящее время это понятие в виде определения не содержится ни в одном международном стандарте. Действительно, во времена больших ЭВМ инфраструктура представляла собой линии связи, модемы, системы энергообеспечения и кондиционирования. В период развития локальных сетей LAN инфраструктура осталась прежней, однако сложность ее элементов возросла. Переход к глобальным сетям еще более усложнил это понятие. При этом сложность возрастала не только за счет увеличения числа элементов и связей между ними, но и за счет усложнения внутренней структуры элементов и перераспределения функций. Например, программы управления каналами переместились на управления сетевыми устройствами. То есть параллельно усложнению аппаратуры усложнялась математика – программы управления инфраструктурой. Все это не могло найти своего отражения в современных методологиях информационных технологий. Появилась новая методология моделирования информационных систем, представляющая информационную систему как всю инфраструктуру предприятия, задействованную в процессе управления всеми информационно-документальными потоками. Это методология ITIL, позволяющая привести системы к единому стандарту и обеспечивающая их эффективное функционирование. Сегодня стандартом де-факто в области управления обслуживанием информационных систем считается библиотека ITIL (Information Technology Infrastructure Library), разработанная в конце 80-х годов по заказу английского правительства и ставшая сборником лучшего мирового опыта в области управления качеством предоставляемых IT-услуг. Ключевая концепция ITIL – информационные технологии сегодня – это прежде всего управление сервисом или услугами. На нем сфокусирована вся методология, и оно объединяет остальные компоненты для достижения цели – выполнения сервисных соглашений с пользователями. В стандарте ITIL деятельность по обеспечению IT-сервисов представляется в виде отдельных процессов, имеющих

входные и выходные параметры и четко определенные цели. Все процессы разделены на две большие категории:

1. Предоставление сервисов (Service Delivery). В эту категорию входят такие функции, как управление уровнем сервисов (Service Management), производительностью (Capacity Management), доступностью (Availability Management), затратами (Cost anagement) и непрерывностью (Contingency Management).
2. Поддержка сервисов (Service Support) – управление конфигурациями (Configuration Management), проблемами (Problem Management), изменениями (Change Management), разработкой и распространением программного обеспечения (Software Control & Distribution), а также взаимодействие с пользователями (Service Desk).

Под информационной инфраструктурой предприятия понимают: оборудование, программное обеспечение, процедуры, коммуникации, связанные с компьютерной техникой, необходимые для поддержки IT-сервисов. Управление инфраструктурой рассматривается при этом как сложное понятие, в которое входят: управление сетями, распределение программного обеспечения, управление рабочими станциями, управление операционными системами, управление базами данных и приложениями, управление безопасностью, управление изменениями, управление инцидентами. Управление инфраструктурой рассматривается при этом как сложное понятие, в которое входят: управление сетями, распределение программного обеспечения, управление рабочими станциями, управление операционными системами, управление базами данных и приложениями, управление безопасностью, управление изменениями, управление инцидентами. Информационная инфраструктура, модель которой мы рассмотрели, так же, как и любой продукт, имеет жизненный цикл и так же, как жизненный цикл информационной системы, описывается с помощью соответствующих стандартов. На каждой фазе жизненного цикла информационной инфраструктуры существуют методологии и инструментарии для поддержки соответствующей фазы, начиная от формирования требований к инфраструктуре и заканчивая выводом ее из эксплуатации.

1.2. Место беспроводных сетей в информационной инфраструктуре предприятия. Основные классы беспроводных сетей и систем передачи данных на основе радиоканала. Архитектура систем передачи данных по радиоканалу и беспроводных сетей

1.2.1. Беспроводные локальные сети

Основой информационной инфраструктуры любого предприятия на данный момент являются структурированные кабельные сети (СКС), позволяющие свести в единую систему множество информационных сервисов разного назначения: локальные вычислительные и телефонные сети, системы безопасности, видеонаблюдения и контроля доступа. СКС представляет собой иерархическую кабельную систему здания или группы зданий, разделенную на структурные подсистемы. Структурированные кабельные системы являются тем «базисом», на котором строятся все основные компоненты информационно-вычислительных комплексов компаний. Но там, где разворачивать СКС не выгодно или невозможно, применение беспроводных сетей (БС) остается единственной альтернативой. Общедоступная беспроводная локальная сеть (public wireless LAN) позволяет любому пользователю, имеющему пользовательское устройство с платой интерфейса беспроводной сети, получить доступ к Internet. Общедоступные беспроводные локальные сети могут быть развернуты во многих людных местах по всему миру – в аэропортах, торговых центрах, гостиницах. Места, которые постоянно посещают люди, лишь ненадолго задерживаясь в них и сохраняя возможность доступа к сетевым услугам, принято называть «горячими точками» (hotspots). Общедоступной беспроводной локальной сетью может пользоваться любой из нас. Она может служить и источником прибыли, потому что владелец «горячей точки» выставляет счета своим абонентам. Однако иногда владельцы таких точек предоставляют доступ к беспроводной сети бесплатно с целью привлечения посетителей. Беспроводные локальные сети небольших «горячих точек» устроены просто. Например, владелец кафе может установить одну точку доступа беспроводной локальной сети, позволяющей пользоваться широкополосным Internet-соединением, подобно тому, как это происходит в условиях дома или небольшого офиса. Свободный доступ привлекает посетителей, которые при просмотре Web-страниц и работе с электронной почтой заказывают кофе и какие-то блюда. Если владелец «горячей точки» намерен получать плату за доступ к сети, в систему беспроводной локальной сети включаются контроллер доступа и узел выставления счетов абонентам. Когда пользователь запускает свой Web-браузер, контроллер доступа автоматически перенаправляет его на Web-страницу, на кото-

рой ему предлагается зарегистрироваться или подписаться на услуги. Счета абонентам выставляют по различным тарифным планам: поминутно, за день или за месяц пользования. Система выставления счетов отслеживает степень использования сервиса и автоматически снимает нужные суммы с кредитных карт. В крупных «горячих точках» необходимо устанавливать несколько точек доступа, что делает их сети сравнимыми с беспроводными локальными сетями предприятий. Общедоступные беспроводные локальные сети, охватывающие сразу несколько мест, нуждаются в сложных системах контроля доступа и выписки счетов. Крупная сеть гостиниц может, например, развернуть общедоступные беспроводные локальные сети в сотнях различных мест, а пользователи – подписаться на несколько месяцев предоставления услуг и пользоваться ими из любой гостиницы. Здесь для выполнения функций контроля доступа потребуется централизованный сервер, способный обеспечивать аутентификацию, авторизацию и учет (authentication, authorization and accounting, AAA; принцип трех А). На предприятии развертывание беспроводных сетей обусловлено конкретными причинами – наличие труднодоступных мест для монтажа СКС, временные рабочие места, удаленные подразделения, не подключенные к общественной сети передачи данных, потребность в корпоративной сети передачи данных на основе радиоканалов, независимой от внешних провайдеров. Типичный пример организации офисной беспроводной сети представлен на рис. 1. Беспроводный сегмент используется для подключения КПК (карманный переносной компьютер), ноутбуков сотрудников предприятия, экспедиторов, складских работников и гостей к информационной инфраструктуре предприятия.

Рис. 1. Типовая схема организации беспроводной сети сегмента SOHO

1.2.2. Цифровые радиорелейные линии (РРЛ)

Радиорелейные линии на основе цифровых радиорелейных станций (РРС) стали важной составной частью цифровых сетей электросвязи – ведомственных, корпоративных, региональных, национальных и даже международных. Предназначены для организации связи и передачи данных между населенными пунктами, удаленными подразделениями предприятия и пр., применяются в основном в тех местах, где прокладка оптоволоконного кабеля не целесообразна по экономическим или техническим причинам. Каждая РРС имеет две направленные приемопередающих антенны – одна антенна служит для связи с предыдущей, а вторая с последующей станцией. Сигнал, принимаемый первой антенной, усиливается и передается на следующую РРС и т. д. Как правило, ствол данных представляет собой сборку из нескольких двух мегабитных каналов передачи данных. Основную часть потока, предназначенного для данной станции, используют подключенные к ней абоненты.

РРЛ классифицируют по следующим взаимосвязанным признакам:

1) скорость передачи данных (цифрового потока) – пропускная способность, в зависимости от которой различают РРЛ:
   - высокоскоростные (скорость передачи свыше 140 Мбит/с);
   - среднескоростные (до 52 Мбит/с);
   - низкоскоростные (до 8 Мбит/с);
2) емкость радиорелейной линии (количество стволов и каналов в них), в зависимости от которой различают РРЛ:
   - большой емкости;
   - средней емкости;
   - малоканальные.
3) количество пролетов в радиорелейной линии, по которому различаются РРЛ:
   - однопролетные;
   - многопролетные.

Высокоскоростные большой емкости радиорелейные линии применяются в глобальных сетях передачи данных и называются магистральными. Среднескоростные средней емкости радиорелейные линии – для создания региональных, зоновых сетей передачи данных и называются зоновыми. Наконец, малоканальные широко используются для организации связи на железнодорожном транспорте, газопроводах, нефтепроводах, линиях электропередачи и т. п. Малоканальные радиорелейные линии с подвижными РРС применяются в военных целях. Полосы радиочастот РРЛ расположены в диапазоне от 2 до 50 ГГц и жестко регламентируются внутри каждой полосы как рекомендациями ITU (Меж-

дународного союза электросвязи), так и Радиорегламентом Российской Федерации. При организации связи по цифровой радиорелейной линии должна быть решена проблема выделения частот приема и передачи. Ее решение относится к компетенции ГКРЧ России, и для РЭС всех назначений эта процедура осуществляется в соответствии с «Положением о порядке выделения полос (номиналов) радиочастот...» и результатами рассмотрения в установленном порядке радиочастотных заявок, поступающих от заявителей. Принципиальная схема фрагмента РРЛ представлена на рис. 2.

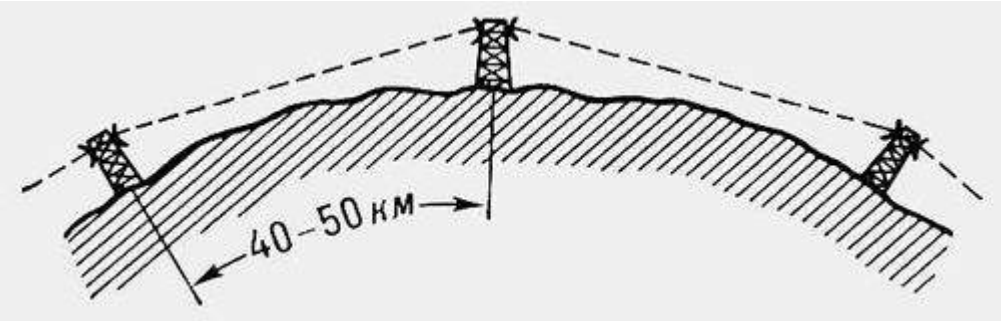


Рис. 2. Принципиальная схема организации радиорелейной линии связи

Антенны соседних приемопередающих станций РРЛ должны находиться в зоне прямой видимости друг друга. Как правило, РРЛ применяются в труднодоступной местности и используются для доступа удаленных подразделений к информационной инфраструктуре предприятия.

Основные характеристики:

- точка-точка;
- в пределах прямой видимости 10…100 км;
- низкая защищенность от помех;
- легкий перехват, низкая секретность;
- большие затраты на установку, требуется лицензирование;
- скорость передачи данных 12…274 Мбит/с;
- вероятность ошибки 10^{-4}.

1.2.3. Спутниковые беспроводные сети и системы передачи данных

Для создания постоянных каналов телекоммуникаций служат геостационарные спутники, висящие над экватором на высоте около 36 000 км. Спутник, выведенный на геостационарную орбиту, висит практически все время над данным участком земной поверхности. Обычно спутники помечаются географической долготой мест, над которыми они висят. На практике геостационарный спутник не стоит на месте, а выполняет движение по траектории, имеющей вид цифры 8. Угловой размер этой восьмерки должен

укладываться в рабочую апертуру антенны, в противном случае антенна должна иметь сервопривод, обеспечивающий автоматическое слежение за спутником. Из-за энергетических проблем телекоммуникационный спутник не может обеспечить высокого уровня сигнала. По этой причине наземная антенна должна иметь большой диаметр, а приемное оборудование – низкий уровень шума. Это особенно важно для северных областей, для которых угловое положение спутника над горизонтом невысоко (это особенно существенно для широт более 70 °), а сигнал проходит довольно толстый слой атмосферы, заметно ослабляясь. Спутниковые каналы могут быть рентабельны для областей, отстоящих друг от друга более чем на 400…500 км (при условии что других средств не существует). Правильный выбор спутника (его долготы) может заметно снизить стоимость канала. Спутниковый канал может быть настроен оптимально с учетом необходимой его пропускной способности для передачи в едином цифровом потоке каналов телефонии и передачи данных, включая трафик Internet (при условии, что других средств не существует). Число позиций для размещения геостационарных спутников ограничено. В последнее время для телекоммуникаций планируется применение так называемых низколетящих спутников (<1000 км; период обращения ~1 ч). Эти спутники движутся по эллиптическим орбитам, и каждый из них по отдельности не может гарантировать стационарный канал, но в совокупности эта система обеспечивает весь спектр услуг (каждый из спутников работает в режиме «запомнить» и «передать» Из-за малой высоты полета наземные станции в этом случае могут иметь небольшие антенны и малую стоимость. Каждый телекоммуникационный спутник снабжен несколькими антеннами. Нисходящий луч может быть сфокусирован на достаточно ограниченную область на земле (с диаметром несколько сот километров), что также упрощает осуществление двунаправленного обмена. Фрагмент корпоративной сети предприятия с использованием спутникового канала представлен на рис. 3.

Таблица 1

Частотные диапазоны, используемые для спутниковых телекоммуникаций

Диапазон	Канал снижения (downlink) [ГГц]	Канал подъема (uplink) [ГГц]	Источники помех
C	3,7...4,2	5,925...6,425	Наземные помехи
ku	11,7...12,2	14,0...14,5	Дождь
ka	17,7...21,7	27,5...30,5	Дождь

Из таблицы видно, что передача ведется на более высокой частоте, чем прием сигнала со спутника. Спутник принимает сообщение на одной частоте, затем конвертирует сигнал в другую частоту и передает на землю. Это

необходимо для разделения потоков информации на спутник и со спутника. Обычный спутник обладает 12–20 транспондерами (приемопередатчиками), каждый из которых имеет полосу 36…50 МГц, что позволяет сформировать поток данных 50 Мбит/с. Такая пропускная способность достаточна для получения 1600 высококачественных телефонных каналов (32 кбит/с) или скоростного Интернета. Современные спутники используют узкоапертурную технологию передачи vsat (very small aperure terminals).

Основные характеристики спутниковых каналов:

- топология точка-точка;
- для спутников выделены 4 полосы (4/6 ГГц и 12/14 ГГц);
- низкая защищенность от помех;
- легкий перехват, низкая секретность;
- большие затраты на развертывание;
- требуется лицензирование;
- вероятность ошибки 10^{-4}.

Спутник связи типа «Горизонт» или «Ямал»

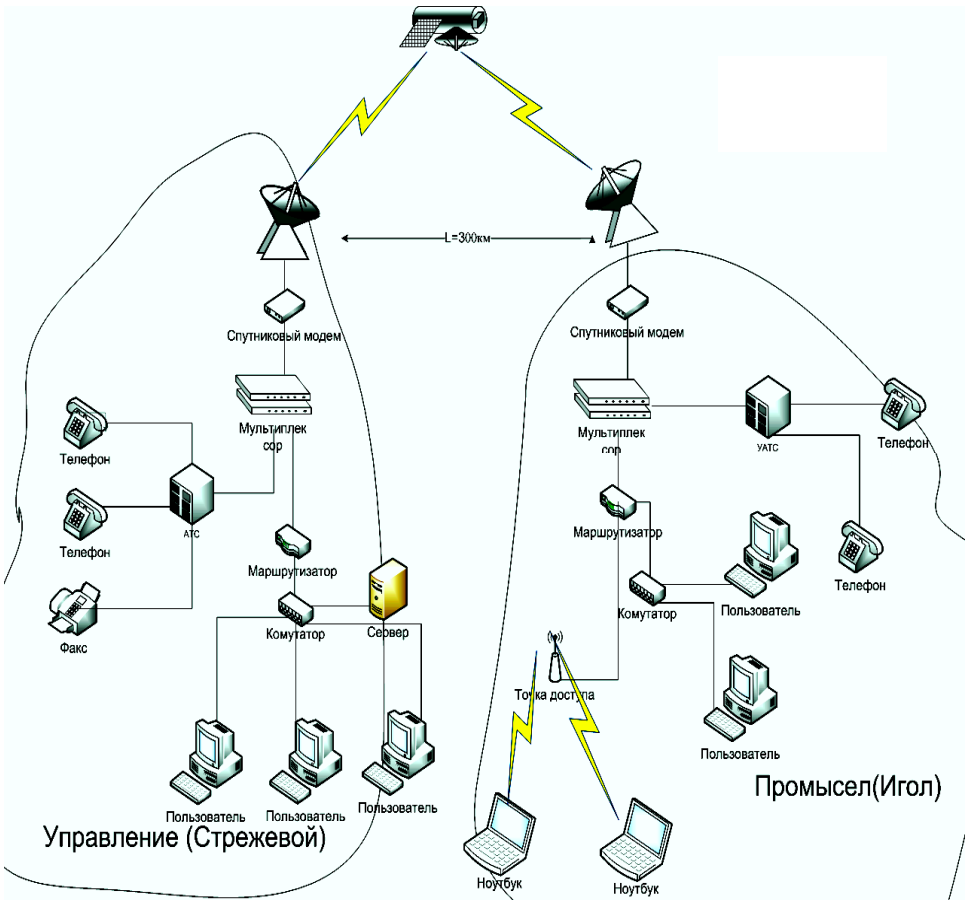


Рис. 3. Фрагмент корпоративной сети передачи данных с использованием спутникового сегмента

2.ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПЕРЕДАЧИ ДАННЫХ ПО РАДИОКАНАЛУ

2.1. Методы построения радиосигнала в WiFi-сетях

В настоящее время при разработке аппаратуры для беспроводных сетей используются два метода построения сигнала:

1. *С непосредственной модуляцией несущей частоты* (Direct-Sequence Spread Spectrum – DSSS).

Информационный сигнал домножается на псевдослучайный код (Pncode – Pseudo Random Noise Code). Полученный результат используют для модуляции несущей. В приемнике полученный сигнал умножают на тот же код и выделяют полезный сигнал.

Основной проблемой, возникающей при использовании метода прямой последовательности, является эффект близко расположенного передатчика, т. е. уровень сигнала мешающего передатчика гораздо выше уровня нужного передатчика, что может привести к потере связи.

2. *Со скачкообразной перестройкой частоты* (Frequency-Hopping Spread Spectrum – FHSS).

Частота несущей изменяется согласно уникальной последовательности. Для реализации этого метода необходим скоростной синтезатор частот.

Недостаток: сложность получения высокого значения базы сигнала, что необходимо для увеличения числа пользователей, помехоустойчивости, повышения конфиденциальности.

Достоинство: меньшая подверженность эффекту близкого передатчика.

Оба метода основаны на принципе приемопередачи с «расширенным спектром», который обеспечивает защиту от помех и конфиденциальность передаваемой информации. Обычно при выборе сетевого продукта учитываются следующие факторы: скорость передачи данных, дальность устойчивой связи, соответствие стандартам, эксплуатационные характеристики и стоимость. Выбор типа аппаратуры для беспроводной сети определяется как условиями эксплуатации, так и стоимостью изделия. Следует отметить, что устройства, работающие по методу FHSS, более дешевы и потребляют меньше энергии. Взяв за основу FHSS, можно получить миниатюрный и недорогой адаптер для портативного ПК.

Расчет радиолинии

При развертывании беспроводных сетей и систем СВЧ-диапазона необходим расчет радиолиний, что является традиционной радиорелейной задачей.

При расчете радиолинии требуется найти соотношение выходной мощности передатчика и входной мощности приемника. Принципиальная схема соединения двух устройств с помощью радиолинии приведена на рис. 4.

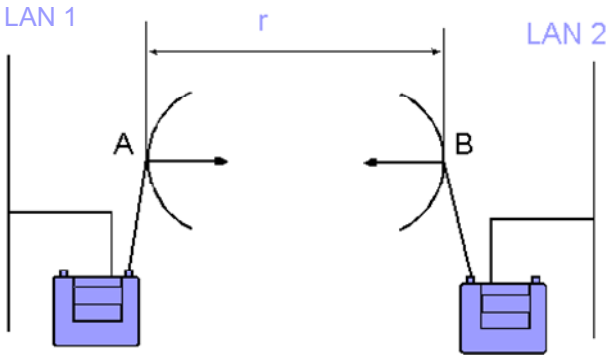


Рис. 4. Схема соединения двух локальных сетей с помощью радиолинии

Это соотношение можно описать с помощью формулы идеальной радиосвязи:

$$P_{пр} = P_{прд} \cdot D_{прд} \cdot D_{пр} \cdot l^2/(4 \cdot p \cdot r^2),$$

где $P_{пр}$ – действующая мощность, поступающая на вход приемника;

$P_{прд}$ – действующая мощность, развиваемая передатчиком на зажимах антенны;

$D_{прд}$ – коэфициент направленного действия (КНД) передающей антенны;

$D_{пр}$ – коэфициент направленного действия (КНД) приемной антенны;

l – длина волны;

p – 3,14;

r – расстояние между приемником и передатчиком.

Эта формула достаточно точно описывает энергетические соотношения в радиоканале при отсутствии потерь за счет среды распространения.

Для учета влияния среды распространения (атмосфера земли), в формулу радиосвязи вводят *множитель ослабления* ($F_{среды}$):

$$F_{среды}=10^{-r \cdot D/10},$$

где D – погонное затухание волны в атмосфере.

Тогда формула радиосвязи приобретает вид:

$$P_{пр}= P_{прд} \cdot D_{прд} \cdot D_{пр} \cdot F_{среды} \cdot l^2/(4 \cdot p \cdot r^2).$$

Для сантиметровых волн типичным значением затухания в дожде средней интенсивности $D = 0{,}3$ дБ/км. Тогда $F_{среды} = 0{,}5$ для расстояния 10 км.

Оценивая реальное качество работы радиоканала, следует иметь в виду, что на входе приемника всегда есть шум, складывающийся из шума окружающей среды и внутренних шумов приемника. Для надежного функционирования системы надо иметь запас по мощности, т. е.

превышение уровня принятого сигнала над чувствительностью приемника. Коэффициент запаса (M):

$M = P_{пр} / P_{пр\ мин.}$, где

$P_{пр.\ мин} = K \cdot T \cdot DF \cdot (E/N_o)_{треб}$ – чувствительность приемной системы:

K – постоянная Больцмана;

T – шумовая температура приемной системы с учетом шумовой характеристики окружающей среды;

DF – полоса пропускания приемника до детектора;

$(E/N_o)_{треб}$ – отношение энергии сигнала к спектральной плотности шума.

Данные расчеты являются довольно приблизительными и приведены для демонстрации того, что проектирование радиолиний является очень сложной технической задачей и доверять это дело можно только профессионалам-проектировщикам.

2.2. Частотная сетка в беспроводных сетях, регистрация WiFi-сетей

Применение электромагнитных волн для телекоммуникаций имеет уже столетнюю историю. Спектр используемых волн делится на ряд диапазонов, приведенных в табл. 2.

Таблица 2

Название	Стандарт	Частота
WiFi	802.11a	5 ГГц.
WiFi	802.11b	2,4 МГц...2,4835
WiFi	802.11g	2,4 МГц...2,4835
WiFi	802.11n	2,4 Ггц и 5 ГГц.
WiMax	802.16	2…66 ГГц
WiMax	802.16a	2…11 ГГц
WiMax	802.16e	2…6 ГГц
Bluetooth	802.11	2,4 ГГц
ZigBee	802.15.4.	2,4 ГГц

Если не используется направленная антенна и на пути нет препятствий, радиоволны распространяются по всем направлениям равномерно и сигнал падает пропорционально квадрату расстояния между передатчиком и приемником (удвоение расстояния приводит к потерям 6 дБ). Радио каналы для целей передачи информации используют частотные диапазоны:

- 902…928 МГц (расстояния до 10 км, пропускная способность до 64 кбит/с);
- 2,4 ГГц и 12 ГГц (до 50 км, до 8 Мбит/с).

Они используются там, где не существует кабельных или оптоволоконных каналов или их создание по каким-то причинам невозможно или

слишком дорого. Более низкие частоты (например, 300 МГц) мало привлекательны из-за ограничений пропускной способности, а большие частоты (>30 ГГц) работоспособны для расстояний не более или порядка 5 км из-за поглощения радиоволн в атмосфере. При использовании диапазонов 4, 5 и 6 (табл. 2) следует иметь в виду, что любые препятствия на пути волн приведут к их практически полному поглощению. Для этих диапазонов заметное влияние оказывает и поглощение в атмосфере.

В России использование частот регламентируется **«Положением о порядке использования на территории Российской Федерации внутриофисных систем передачи данных в полосе частот от 2400 до 2483,5 МГц»**, выдержки из которого приведены далее. *«Стандартом IEEE 802.11b и IEEE 802.11g (WiFi) предусмотрено использование частотного диапазона от 2,4 до 2,4835 ГГц, который предназначен для безлицензионного использования в промышленности, науке и медицине (Industry, Science and Medicine – ISM). Поэтому для получения разрешения на этой частотной полосе применяется упрощенный порядок. Разрешения оформляются ФГУП «Главный радиочастотный центр» на основе сделанных заявок от физических и юридических лиц. В течение 30 дней заявки рассматриваются и, если нет никаких замечаний, в адрес заявителя направляются финансовые документы для оплаты за проведенные работы. При поступлении средств на расчетный счет заявителю выдается разрешение на использование частоты. Затем ФГУП «Главный радиочастотный центр» информирует соответствующие ведомства по месту установки РЭС (ФГУП Радиочастотный центр федерального округа и «Управление государственного надзора за связью и информатизацией в Российской Федерации»). Однако на частотах 2,4 ГГц могут возникать проблемы из-за помех, создаваемых другими бытовыми беспроводными устройствами, например микроволновыми печами или радиотелефонами. Чтобы получить разрешение на использование радиочастот в других диапазонах, в том числе в диапазоне 5 ГГц (стандарт 802.11a), необходимо предварительно получить частное решение ГКРЧ (Государственная Комиссия по радиочастотам)».* Что касается стандарта WiFi 802.11a, работающего в диапазоне 5 ГГц, то в России такое оборудование использовать не разрешено, поскольку его применяет для своих целей ряд государственных служб. А для стандартов 802.11b/g разрешительный порядок был изменен на уведомительный. Необходимо помнить также, что при реализации радиорелейных и спутниковых линий связи необходимы разрешение на использование частот и лицензия на услуги связи.

3. ТЕХНОЛОГИЯ БЕСПРОВОДНЫХ ИНФОРМАЦИОННЫХ WiFi-СЕТЕЙ

3.1. Определение, термины WiFi, общие сведения

Беспроводная сеть – это система передачи данных, в которой в качестве носителя используются радиоволны. Беспроводная сеть позволяет предоставить пользователям доступ к информационным ресурсам там, где развертывание кабельной системы невозможно или экономически нецелесообразно. WiFi (англ. *Wireless Fidelity* – «беспроводная точность») – стандарт на оборудование Wireless LAN. Разработан консорциумом WiFi Alliance на базе стандартов IEEE 802.11, «WiFi» – торговая марка «WiFi Alliance». Технологию назвали Wireless-Fidelity (дословно «беспроводная точность») по аналогии с HiFi. Подключение нового пользователя к сети выполняется очень быстро, т. к. не требует прокладки проводов и установки информационных розеток. Средства безопасности на базе протоколов WEP, WPA и 802.1x обеспечивают надежное шифрование данных при передаче по радиоканалу и предоставляют функции аутентификации пользователей. Для дополнительной безопасности сеть может быть настроена на использование VPN.

Беспроводные сети имеют ряд существенных преимуществ перед обычными кабельными сетями:

- в отличие от обычной проводной LAN-сети, WLAN-сеть можно очень быстро развернуть, что очень удобно при проведении презентаций или в условиях работы вне офиса;
- пользователи мобильных устройств при подключении к локальным беспроводным сетям могут легко перемещаться в рамках действующих зон сети;
- скорости современных сетей довольно высоки (до 54 Мб/с), что позволяет их использовать для очень широкого спектра задач;
- с помощью дополнительного оборудования беспроводная сеть может быть успешно соединена с кабельными сетями;
- WLAN-сеть может оказаться единственным выходом, если не возможна или не желательна прокладка кабеля внутри здания, которая влечет за собой неизбежное сверление стен и прокладку кабельных каналов.

Но нужно иметь ввиду, что кроме описанных достоинств беспроводных сетей, есть еще и некоторые недостатки, а именно:

- чувствительность к радиопомехам;
- в некоторых случаях, в условиях крайне тяжелой радиочастотной обстановки, нормальная работа сети практически невозможна;

- скорость соединения плавает, соединение может прерываться;
- происходит сильное поглощение радиоволн железобетоном и некоторыми другими материалами, что приводит к ослаблению сигнала, а в итоге к снижению скорости передачи данных.

3.2. Топология и оборудование беспроводных сетей WiFi

Стандартом WiFi предусмотрено несколько вариантов топологии беспроводной сети.

Простейшей структурой является локальная сеть «каждый с каждым» **Ad-hoc** – Independent Basic Service Set (IBSS – независимый основной набор услуг) или Peer-to-Peer (точка–точка), которую можно считать беспроводным аналогом одноранговой сети Ethernet, при которой узлы сети связываются напрямую друг с другом. Такая структура удобна для быстрого развертывания сетей. Для ее организации требуется минимум оборудования – каждое устройство просто должно быть снабжено адаптером WLAN. Пример данной сети приведен на рис. 5.

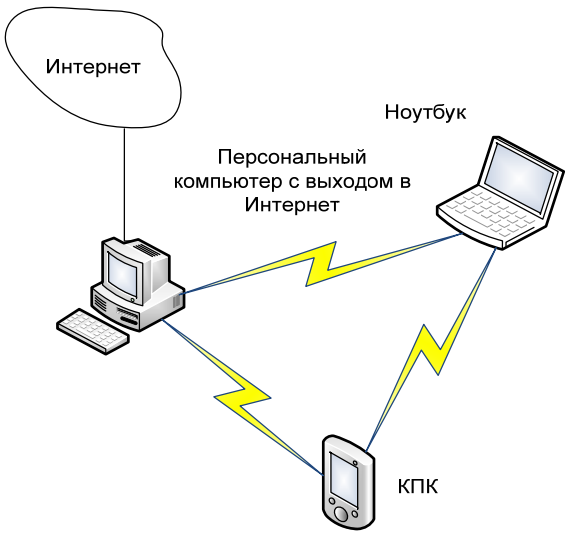


Рис. 5. Фрагмент одноранговой беспроводной сети

Данная топология предназначена для развертывания временных сетей на выставках, проведения различных семинаров и совещаний, а также для использования дома или в офисах малых компаний. Этот способ позволит соединить до восьми устройств в одноранговую сеть, где каждое устройство будет связано с другим. Но на самом деле его стоит использовать для соединения в сеть двух или трех устройств. Большее количество узлов объединять по этой схеме непрактично и неудобно. К примеру, чтобы Ваш КПК получил доступ к глобальной сети, вам по-

требуется постоянно держать компьютер включенным, с выходом в Интернет. Чаще используется другой вид организации беспроводных сетей, получивший название Infrastructure Mode – инфраструктурный режим (рис. 6). В этом режиме узлы сети связаны друг с другом не напрямую, а через точку доступа – Access Point. Различают два режима взаимодействия с точками доступа – BSS (Basic Service Set – базовый набор услуг) и ESS (Extended Service Set – расширенный набор услуг).

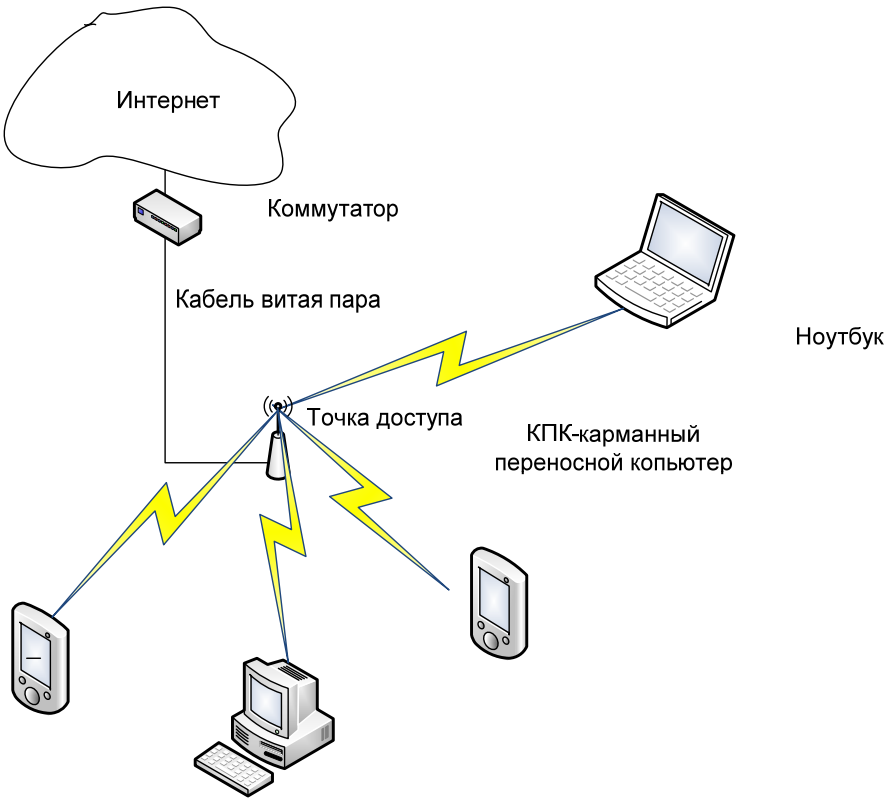


Рис. 6. Базовый режим связи через одну точку доступа

В базовом режиме BSS все узлы связаны между собой через одну точку доступа, которая может также играть роль моста для соединения с Интернетом и внешней кабельной сетью.

Расширенный режим ESS представляет собой объединение нескольких точек доступа, т. е. нескольких сетей BSS. В этом случае точки доступа могут взаимодействовать и друг с другом, а пользователь может переходить от одной точки доступа к другой. Расширенный режим удобно использовать тогда, когда необходимо объединить в одну сеть достаточно удаленных друг от друга пользователей или подключить несколько проводных сетей. Точки доступа соединяются между собой либо по радиоканалу, либо проводами (Ethernet-соединение) при отсутствии радиовидимости, например при наличии разделяющих помещение бетонных стен или межэтажных перекрытий.

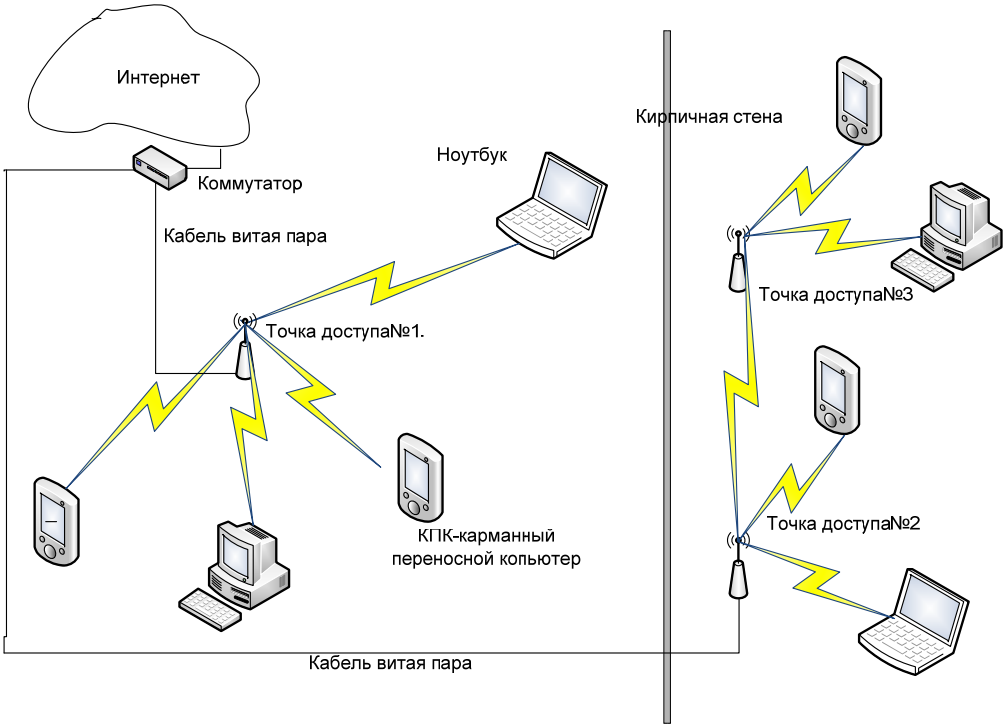


Рис. 7. Расширенный режим связи через несколько точек доступа

3.3. Домашние сети WiFi

Рано или поздно перед каждым активным пользователем Интернета встает проблема построения домашней сети.

Подключение при помощи витой пары подразумевает прокладку кабеля – а это короба, дрель, пыль, грязь и все прочие радости, связанные со сверлением стен. Да и не всегда ясно, где будет любимое рабочее место и где устанавливать розетки. Есть простой выхода из этой ситуации – организовать беспроводную сеть WiFi, позволяющую получать доступ к Интернету из любой комнаты в квартире и соединение между компьютерами и мобильными устройствами. Оптимальная схема вашей сети, к примеру, может выглядеть так, как показано на рис. 8.

Устанавливаем в прихожей, около телефонной розетки, одно небольшое устройство, которое одновременно является ADSL-модемом и точкой доступа WiFi, например ZyXEL P-660HTW EE. Снабжаем настольный компьютер адаптером WiFi, ноутбуки и КПК обычно имеют встроенные WiFi-адаптеры, настраиваем все оборудование – сеть готова. Если у Вас уже есть домашний компьютер, подсоединенный к Интернет, и появилось новое мобильное устройство, с которого также нужно выходить в мировую сеть, то очевидным решением будет установка точки доступа WiFi, которую надо подсоединить к компьютеру через Ethernet-порт. Тут могут быть два разных варианта. Первый –

точка доступа соединяется напрямую со встроенным в компьютер Ethernet-портом. В этом случае для того, чтобы все пользователи WiFi-сети могли выходить в Интернет, необходимо, чтобы компьютер был включен, что не всегда удобно (рис. 9).

Рис. 8. Подключение домашней беспроводной сети через точку доступа

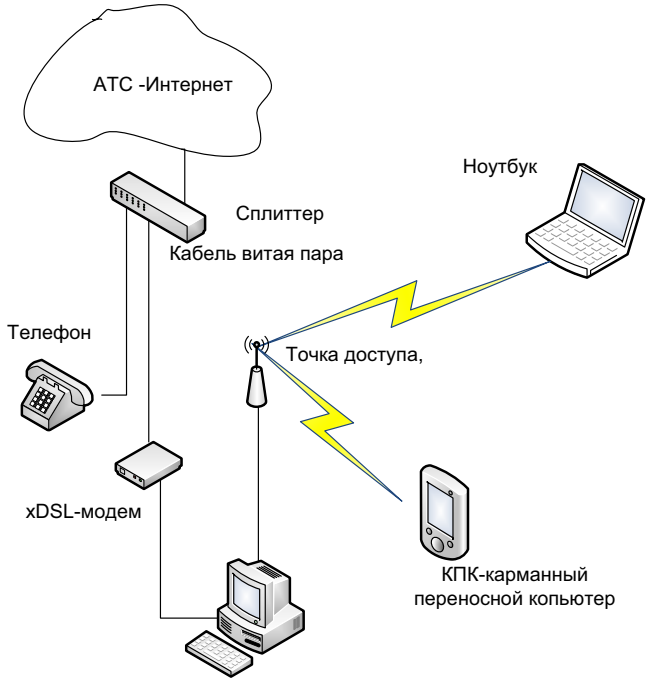


Рис. 9. Подключение домашней беспроводной сети через компьютер

Если Ваш модем имеет Ethernet-порт, то более технологичным будет второй способ подключения. Точка доступа WiFi подсоединяется не к компьютеру, а к небольшому Ethernet-коммутатору, к которому, в свою очередь, подключены также компьютер и модем. В этом случае все устройства могут работать с сетью независимо друг от друга (рис. 10).

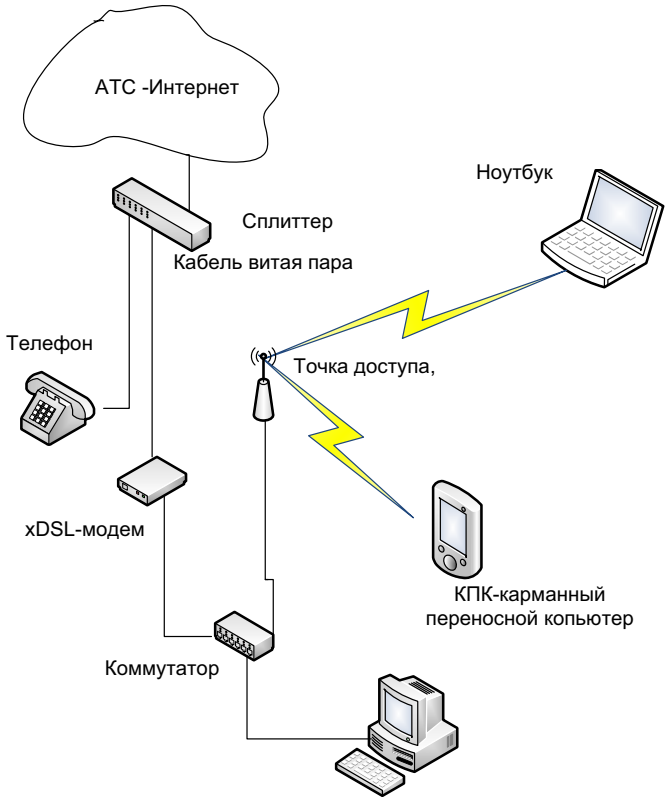


Рис. 10. Подключение домашней беспроводной сети через коммутатор

Если речь идет о создании беспроводной сети в пределах небольшой квартиры, то одной точки доступа будет вполне достаточно. Если же требуется реализовать задачу создания беспроводной сети в большом помещении, состоящем из комнат, разделенных бетонными стенами с арматурой, то одной точки доступа может оказаться явно недостаточно.

Для того чтобы расширить радиус действия беспроводной сети, проще всего развернуть распределенную беспроводную сеть на базе двух или более точек доступа. В худшем случае все же придется воспользоваться дрелью, чтобы соединить между собой точки доступа Ethernet-кабелем.

Перед развертыванием беспроводной сети рекомендуется определить степень поглощения радиоволн во всех возможных местах размещения клиентских устройств. Для этого потребуется беспроводная точка доступа и ноутбук или КПК, снабженные беспроводными адаптерами.

Методика планирования сети примерно следующая: устанавливаем точку доступа в месте предполагаемого размещения и включаем электропитание (ни в какой Интернет не включаем, никакие параметры беспроводной сети не настраиваем). Берем мобильное устройство и запускаем мастер установки беспроводной сети или просто включаем беспроводный адаптер, где сразу же начнется процедура поиска локальных беспроводных сетей, которые находятся в радиусе действия беспроводного адаптера. Большинство производителей устанавливают идентификатор сети SSID в значение «default», поэтому среди всех найденных сетей нас интересует именно эта.

Если ваше устройство нашло несколько сетей с таким именем, и вы смогли подключиться к одной из них – поздравляем! Вы подключились к соседу, который по недосмотру или неопытности забыл защитить свою беспроводную сеть, тем самым, давая Вам и всей округе возможность пользоваться своей сетью и доступом в Интернет за его счет.

Необходимо походить с ноутбуком по помещениям, в которых вы предполагаете работать через WiFi, и понаблюдать за уровнем сигнала и информацией об изменении скорости работы сети. Анализ картины на местности поможет выбрать необходимую схему сети и оптимальные места расположения точек доступа.

4. СТАНДАРТЫ WiFi-СЕТЕЙ

4.1. Базовый стандарт IEEE 802.11. Спецификации уровня доступа к среде и физического уровня для беспроводных сетей

Стандарт RadioEthernet IEEE 802.11 – это стандарт организации беспроводных коммуникаций на ограниченной территории в режиме локальной сети, т. е. когда несколько абонентов имеют равноправный доступ к общему каналу передач. 802.11 – первый промышленный стандарт для беспроводных локальных сетей (Wireless Local Area Networks), или WLAN. Стандарт был разработан Institute of Electrical and Electronics Engineers (IEEE), 802.11 может быть сравнен со стандартом 802.3 для обычных проводных Ethernet-сетей.

Стандарт RadioEthernet IEEE 802.11 определяет порядок организации беспроводных сетей на уровне управления доступом к среде (MAC-уровне) и физическом (PHY) уровне. В стандарте определен один вариант MAC (Medium Access Control)-уровня и три типа физических каналов.

Подобно проводному Ethernet, IEEE 802.11 определяет протокол использования единой среды передачи, получивший название carrier sense multiple access collision avoidance (CSMA/CA). Вероятность коллизий беспроводных узлов минимизируется путем предварительной посылки короткого сообщения, называемого ready to send (RTS). Оно информирует другие узлы о продолжительности предстоящей передачи и адресате. Это позволяет другим узлам задержать передачу на время, равное объявленной длительности сообщения. Приемная станция должна ответить на RTS посылкой clear to send (CTS). Передающий узел узнает, свободна ли среда и готов ли приемный узел к приему. После получения пакета данных приемный узел должен передать подтверждение (ACK) факта безошибочного приема. Если ACK не получено, попытка передачи пакета данных будет повторена.

В стандарте предусмотрено обеспечение безопасности данных, которое включает аутентификацию для проверки того, что узел, входящий в сеть, авторизован в ней, а также шифрование для защиты от подслушивания.

На физическом уровне стандарт предусматривает два типа радиоканалов и один инфракрасного диапазона.

В основу стандарта 802.11 положена сотовая архитектура. Сеть может состоять из одной или нескольких ячеек (сот). Каждая сота управляется базовой станцией, называемой точкой доступа (Access Point, AP). Точка доступа и находящиеся в пределах радиуса ее действия рабочие станции образуют базовую зону обслуживания (Basic Service Set, BSS). Точки доступа многосотовой сети взаимодействуют между собой через распределительную систему (Distribution System, DS), представляющую собой эквивалент магистрального

сегмента кабельных ЛС. Вся инфраструктура, включающая точки доступа и распределительную систему, образует расширенную зону обслуживания (Extended Service Set). Стандартом предусмотрен также односотовый вариант беспроводной сети, который может быть реализован и без точки доступа, при этом часть ее функций выполняется непосредственно рабочими станциями.

В настоящее время существует множество стандартов семейства IEEE 802.11:

1. 802.11 – первоначальный основополагающий стандарт. Поддерживает передачу данных по радиоканалу со скоростями 1 и 2 (опционально) Мбит/с.
2. 802.11a – высокоскоростной стандарт WLAN. Поддерживает передачу данных со скоростями до 54 Мбит/с по радиоканалу в диапазоне около 5 ГГц.
3. 802.11b – самый распространенный стандарт. Поддерживает передачу данных со скоростями до 11 Мбит/с по радиоканалу в диапазоне около 2,4 ГГц.
4. 802.11c – стандарт, регламентирующий работу беспроводных мостов. Данная спецификация используется производителями беспроводных устройств при разработке точек доступа.
5. 802.11d – определял требования к физическим параметрам каналов (мощность излучения и диапазоны частот) и устройств беспроводных сетей с целью обеспечения их соответствия законодательным нормам различных стран.
6. 802.11e – создание данного стандарта связано с использованием средств мультимедиа. Он определяет механизм назначения приоритетов разным видам трафика, таким как аудио- и видеоприложения. Требование качества запроса, необходимое для всех радиоинтерфейсов IEEE WLAN.
7. 802.11f – стандарт, связанный с аутентификацией, определяет механизм взаимодействия точек связи между собой при перемещении клиента между сегментами сети. Другое название стандарта – Inter Access Point Protocol. Стандарт, описывающий порядок связи между равнозначными точками доступа.
8. 802.11g – устанавливает дополнительную технику модуляции для частоты 2,4 ГГц. Предназначен для обеспечения скоростей передачи данных до 54 Мбит/с по радиоканалу в диапазоне около 2,4 ГГц.
9. 802.11h – разработка данного стандарта связана с проблемами при использовании 802.11a в Европе, где в диапазоне 5 ГГц работают некоторые системы спутниковой связи. Для предотвращения взаимных помех стандарт 802.11h имеет механизм «квазиинтеллектуального» управления мощностью излучения и выбором несущей частоты передачи. Стандарт, описывающий управление спектром частоты 5 ГГц для использования в Европе и Азии.

10. 802.11i (WPA2) – целью создания данной спецификации является повышение уровня безопасности беспроводных сетей. В ней реализован набор защитных функций при обмене информацией через беспроводные сети, в частности технология AES (Advanced Encryption Standard) – алгоритм шифрования, поддерживающий ключи длиной 128, 192 и 256 бит. Предусматривается совместимость всех используемых в данное время устройств, в частности Intel Centrino с 802.11i-сетями. Затрагивает протоколы 802.1X, TKIP и AES.

11. 802.11j – предназначена для Японии и расширяет стандарт 802.11a добавочным каналом 4,9 ГГц.

12. 802.11n – позволяет поднять пропускную способность сетей до 100 Мбит/сек.

13. 802.11r – предусматривает создание универсальной и совместимой системы роуминга для возможности перехода пользователя из зоны действия одной сети в зону действия другой.

Из всех существующих стандартов беспроводной передачи данных IEEE 802.11 на практике наиболее часто используются всего три, определенных Инженерным институтом электротехники и радиоэлектроники (IEEE), – 802.11b, 802.11g и 802.11a.

Сравнение стандартов беспроводной передачи данных:

Стандарт 802.11b

- Частотный диапазон – 2,4 ГГц.
- Количество используемых радиоканалов – 3 не перекрывающихся.
- Макс. скорость передачи данных – 11 Мб/с.
- Примерная дальность действия – 30 м при 11 Мб/с.

Стандарт 802.11g

- Частотный диапазон – 2,4 ГГц.
- Количество используемых радиоканалов – 3 не перекрывающихся.
- Макс. скорость передачи данных – 54 Мб/с.
- Примерная дальность действия – 100 м при 1 Мб/с, 15 м при 54 Мб/с.

Стандарт 802.11a (в России не сертифицирован)

- Частотный диапазон – 5 ГГц.
- Количество используемых радиоканалов – 8 не перекрывающихся.
- Макс. скорость передачи данных 54 Мб/с.
- Примерная дальность действия – 50 м при 11 Мб/с, 12 м при 54 Мб/с, 100 м при 6 Мб/с.

В окончательной редакции широко распространенный стандарт 802.11b был принят в 1999 г. и благодаря ориентации на свободный от ли-

цензирования диапазон 2,4 ГГц завоевал наибольшую популярность у производителей оборудования. Пропускная способность (теоретическая – 11 Мбит/с, реальная – от 1 до 6 Мбит/с) отвечает требованиям большинства приложений. Поскольку оборудование 802.11b, работающее на максимальной скорости 11 Мбит/с, имеет меньший радиус действия, чем на более низких скоростях, то стандартом 802.11b предусмотрено автоматическое понижение скорости при ухудшении качества сигнала. К началу 2004 года в эксплуатации находилось около 15 млн радиоустройств 802.11b.

В конце 2001 г. появился стандарт беспроводных локальных сетей 802.11a, функционирующих в частотном диапазоне 5 ГГц (диапазон ISM). Беспроводные ЛВС стандарта IEEE 802.11a обеспечивают скорость передачи данных до 54 Мбит/с, т. е. примерно в пять раз быстрее сетей 802.11b, и позволяют передавать большие объемы данных, чем сети IEEE 802.11b.

К недостаткам 802.11a относятся большая потребляемая мощность радиопередатчиков для частот 5 ГГц, а также меньший радиус действия (оборудование для 2,4 ГГц может работать на расстоянии до 300 м, а для 5 ГГц – около 100 м). Кроме того, устройства для 802.11a дороже, но со временем ценовой разрыв между продуктами 802.11b и 802.11a будет уменьшаться.

802.11g является новым стандартом, регламентирующим метод построения WLAN, функционирующих в нелицензируемом частотном диапазоне 2,4 ГГц. Максимальная скорость передачи данных в беспроводных сетях IEEE 802.11g составляет 54 Мбит/с. Стандарт 802.11g представляет собой развитие 802.11b и обратно совместим с 802.11b. Соответственно ноутбук с картой 802.11g сможет подключаться и к уже действующим точкам доступа 802.11b, и ко вновь создаваемым 802.11g. Теоретически 802.11g обладает достоинствами двух своих предшественников. В числе преимуществ 802.11g надо отметить низкую потребляемую мощность, большую дальность действия и высокую проникающую способность сигнала.

Стандарт 802.11n утверждён в сентябре 2009 г. Ключевой компонент стандарта под названием MIMO (Multiple Input, Multiple Output – много входов, много выходов) предусматривает применение пространственного мультиплексирования с целью одновременной передачи нескольких информационных потоков по одному каналу, а также многолучевое отражение, которое обеспечивает доставку каждого бита информации соответствующему получателю с небольшой вероятностью влияния помех и потерь данных. Именно возможность одновременной передачи и приема данных определяет высокую пропускную способность устройств 802.11n. Беспроводные адаптеры и точки доступа, реализованные в данном стандарте, передают и получают данные по схеме 4 × 4, то есть используют 4 разделенных потока для доставки голосовой

информации, видео и данных по любому из двух каналов – 5-ГГц или 2,4-ГГц. Устройства будут иметь несколько антенн.

4.2. Организация беспроводной сети

Стандарт IEEE 802.11 работает на двух нижних уровнях модели ISO/OSI: физическом и канальном. Другими словами, использовать оборудование WiFi так же просто, как и Ethernet: протокол TCP/IP накладывается поверх протокола, описывающего передачу информации по каналу связи. Расширение IEEE 802.11b не затрагивает канальный уровень и вносит изменения в IEEE 802.11 только на физическом.

В беспроводной локальной сети есть два типа оборудования: клиент (обычно это компьютер, укомплектованный беспроводной сетевой картой, но может быть и иное устройство) и точка доступа, которая выполняет роль моста между беспроводной и проводной сетями. Точка доступа содержит приемопередатчик, интерфейс проводной сети, а также встроенный микрокомпьютер и программное обеспечение для обработки данных.

4.3. 802.11 – спецификация физического уровня

Стандарт IEEE 802.11 предусматривает передачу сигнала одним из двух методов – прямой последовательности (Direct Sequence Spread Spectrum, DSSS) и частотных скачков (Frequency Hopping Spread Spectrum, FHSS), различающиеся способом модуляции, но использующие одну и ту же технологию расширения спектра. Основной принцип технологии расширения спектра (Spread Spectrum, SS) заключается в том, чтобы от узкополосного спектра сигнала, возникающего при обычном потенциальном кодировании, перейти к широкополосному спектру, что позволяет значительно повысить помехоустойчивость передаваемых данных.

Метод FHSS предусматривает изменение несущей частоты сигнала при передаче информации. Для повышения помехоустойчивости нужно увеличить спектр передаваемого сигнала, для чего несущая частота меняется по псевдослучайному закону и каждый пакет данных передается на своей несущей частоте. При использовании FHSS конструкция приемопередатчика получается очень простой, но этот метод применим, только если пропускная способность не превышает 2 Мбит/с, так что в дополнении IEEE 802.11b остался один DSSS. Из этого следует, что совместно с устройствами IEEE 802.11b может применяться только то оборудование стандарта IEEE 802.11, которое поддерживает DSSS, при этом скорость передачи не превысит максимальной скорости в «узком месте» (2 Мбит/с), коим является оборудование, использующее старый стандарт без расширения.

В основе метода DSSS лежит принцип фазовой манипуляции (т. е. передачи информации скачкообразным изменением начальной фазы сигнала). Для расширения спектра передаваемого сигнала применяется преобразование передаваемой информации в так называемый код Баркера, являющийся псевдослучайной последовательностью. На каждый передаваемый бит приходится 11 бит в последовательности Баркера. Различают прямую и инверсную последовательности Баркера. Из-за большой избыточности при кодировании вероятность того, что действие помехи превратит прямую последовательность Баркера в инверсную, близка к нулю. Единичные биты передаются прямым кодом Баркера, а нулевые – инверсным.

Под беспроводные компьютерные сети в диапазоне 2,4 ГГц отведен довольно узкий «коридор» шириной 83 МГц, разделенный на 14 каналов. Для исключения взаимных помех между каналами необходимо, чтобы их полосы отстояли друг от друга на 25 МГц. Несложный подсчет показывает, что в одной зоне одновременно могут использоваться только три канала. В таких условиях невозможно решить проблему отстройки от помех автоматическим изменением частоты, поэтому в беспроводных локальных сетях используется кодирование с высокой избыточностью. В ситуации, когда и эта мера не позволяет обеспечить заданную достоверность передачи, скорость с максимального значения 11 Мбит/с последовательно снижается до одного из следующих фиксированных значений: 5,5; 2; 1 Мбит/с. Снижение скорости происходит не только при высоком уровне помех, но и если расстояние между элементами беспроводной сети достаточно велико.

4.4. Канальный уровень IEEE 802.11

Подобно проводной сети Ethernet, в беспроводных компьютерных сетях WiFi канальный уровень включает в себя подуровни управления логическим соединением (Logical Link Control, LLC) и управления доступом к среде передачи (Media Access Control, MAC). У Ethernet и IEEE 802.11 один и тот же LLC, что значительно упрощает объединение проводных и беспроводных сетей. MAC у обоих стандартов имеет много общего, однако есть некоторые тонкие различия, принципиальные для сравнения проводных и беспроводных сетей.

В Ethernet для обеспечения возможности множественного доступа к общей среде передачи (в данном случае кабелю) используется протокол CSMA/CD, обеспечивающий выявление и обработку коллизий (в терминологии компьютерных сетей так называются ситуации, когда несколько устройств пытаются начать передачу одновременно).

В сетях IEEE 802.11 используется полудуплексный режим передачи, т. е. в каждый момент времени станция может либо принимать, либо пе-

редавать информацию, поэтому обнаружить коллизию в процессе передачи невозможно. Для IEEE 802.11 был разработан модифицированный вариант протокола CSMA/CD, получивший название CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Работает он следующим образом. Станция, которая собирается передавать информацию, сначала «слушает эфир». Если не обнаружено активности на рабочей частоте, станция сначала ожидает в течение некоторого случайного промежутка времени, потом снова «слушает эфир» и, если среда передачи данных все еще свободна, осуществляет передачу. Наличие случайной задержки необходимо для того, чтобы сеть не зависла, если несколько станций одновременно захотят получить доступ к частоте. Если информационный пакет приходит без искажений, принимающая станция посылает обратно подтверждение. Целостность пакета проверяется методом контрольной суммы. Получив подтверждение, передающая станция считает процесс передачи данного информационного пакета завершенным. Если подтверждение не получено, станция считает, что произошла коллизия и пакет передается снова через случайный промежуток времени.

Еще одна специфичная для беспроводных сетей проблема – две клиентские станции имеют плохую связь друг с другом, но при этом качество связи каждой из них с точкой доступа хорошее. В таком случае передающая клиентская станция может послать на точку доступа запрос на очистку эфира. Тогда по команде с точки доступа другие клиентские станции прекращают передачу на время «общения» двух точек с плохой связью. Режим принудительной очистки эфира (протокол Request to Send/Clear to Send – RTS/CTS) реализован далеко не во всех моделях оборудования IEEE 802.11 и, если он есть, то включается лишь в крайних случаях.

В Ethernet при передаче потоковых данных используется управление доступом к каналу связи, распределенное между всеми станциями. Напротив, в IEEE 802.11 в таких случаях применяется централизованное управление с точки доступа. Клиентские станции последовательно опрашиваются на предмет передачи потоковых данных. Если какая-нибудь из станций сообщает, что она будет передавать потоковые данные, точка доступа выделяет ей промежуток времени, в который из всех станций сети будет передавать только она.

Следует отметить, что принудительная очистка эфира снижает эффективность работы беспроводной сети, поскольку связана с передачей дополнительной служебной информации и кратковременными перерывами связи. Кроме этого, в проводных сетях Ethernet при необходимости можно реализовать не только полудуплексный, но и дуплексный вариант передачи, когда коллизия обнаруживается в процессе передачи (это повышает реальную пропускную способность сети). Поэтому, увы, при про-

чих равных условиях реальная пропускная способность беспроводной сети IEEE 802.11b будет ниже, чем у проводного Ethernet. Таким образом, если сетям Ethernet 10 Мбит/с и IEEE 802.11b (максимальная скорость передачи информации 11 Мбит/с) с одинаковым числом пользователей давать одинаковую нагрузку, постепенно увеличивая ее, то, начиная с некоторого порога, сеть IEEE 802.11b начнет «тормозить», а Ethernet все еще будет функционировать нормально. Поскольку клиентские станции могут быть мобильными устройствами с автономным питанием, в стандарте IEEE 802.11 большое внимание уделено вопросам управления питанием. В частности, предусмотрен режим, когда клиентская станция через определенные промежутки времени «просыпается», чтобы принять сигнал включения, который, возможно, передает точка доступа. Если этот сигнал принят, клиентское устройство включается, в противном случае оно снова «засыпает» до следующего цикла приема информации.

5. РЕГИОНАЛЬНЫЕ БЕСПРОВОДНЫЕ СЕТИ НА ОСНОВЕ СТАНДАРТА 802.16 (WiMax)

В ближайшие годы развитие локальных беспроводных сетей пойдет по направлению массового внедрения так называемой технологии WiMAX (сокращенно от Worldwide Interoperability for Microwave Access). Сети WiMAX (стандарт IEEE 802.16a) предполагают использование частотного диапазона от 2 до 11 ГГц и обеспечивают скорость передачи данных до 70 Мбит/с на расстояние до 50 км. Новый стандарт позиционируется как средство подключения к интернету беспроводных локальных сетей WLAN и как замена DSL в качестве «последней мили». Пропускной способности одной базовой станции вполне хватит для обеспечения десятков бизнес-пользователей и сотен домашних подключений.

5.1. Архитектура, топология и основные технические характеристики беспроводных сетей на основе Стандарта 802.16

Разработанный Институтом инженеров по электротехнике и электронике (IEEE) **Стандарт 802.16** представляет собой рассчитанную на внедрение в городских беспроводных сетях технологию, задачей которой является обеспечение сетевого уровня между локальными (IEEE 802.11) и региональными сетями (WAN), где планируется применение разрабатываемого стандарта IEEE 802.20. Эти стандарты совместно со стандартом IEEE 802.15 (PAN – Personal Area Network – Bluetooth) и 802.17 (мосты уровня MAC) образуют взаимосогласованную иерархию протоколов беспроводной связи.

Краткие характеристики стандарта 802.16

- Пропускная способность до 135 Мбит/с при полосе несущей 28 МГц.
- Модуляция OFDM – 64-QAM.
- Доступ к среде адаптивный, динамический.
- Управление сетью централизованное.

Таблица 3

Название стандарта	802.16	802.16a	802.16e
Дата принятия	декабрь 2001	январь 2003	январь 2004
Частотный диапазон	10…66 ГГц	2…11 ГГц	2…6 ГГц
Быстродействие	32…135 Мбит/с для 28МГц-канала	до 75 Мбит/с для 28МГц-канала	до 15 Мбит/с для 5МГц-канала

Окончание табл. 3

Название стандарта	802.16	802.16a	802.16e
Модуляция	QPSK, 16QAM, 64QAM	OFDM 256, QPSK, 16QAM, 64QAM	OFDM 256, QPSK, 16QAM, 64QAM
Ширина канала	20, 25 и 28 МГц	Регулируемая 1,5…20 МГц	Регулируемая 1,5…20 МГц
Радиус действия	2…5 км	7…10 км макс. радиус 50 км	2…5 км
Условия работы	Прямая видимость	Работа на отражениях	Работа на отражениях

Стандарт 802.16e предназначен для мобильных систем. Безопасность в сети обеспечивается на уровне протокола 3-DES.

Характеристики стандарта 802.16a

- Дальность действия – до 50 км.
- Покрытие: расширенные возможности работы вне прямой видимости позволяют улучшить качество покрытия обслуживаемой зоны.
- Частота – от 2 до 11 ГГц.
- Спектральная эффективность – до 5 бит/сек/Гц.
- Максимальная скорость передачи данных на сектор одной базовой станции – до70 Мбит/с. Типовая базовая станция имеет до 6 секторов.

Структурная схема орханизации сети на основе стандарта 802.16 представлена на рис. 11.

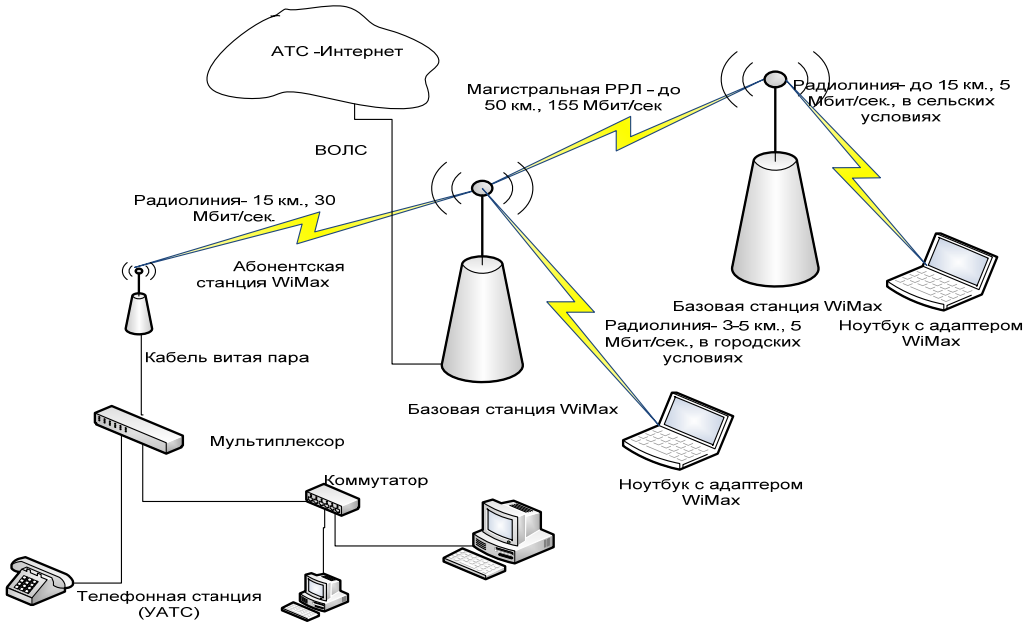


Рис. 11. Корпоративная сеть с фрагментами WiMax

Качество обслуживания контролируется на уровне управления доступом к среде, что позволяет использовать дифференцированные уровни обслуживания. Это дает возможность предоставлять коммерческим предприятиям обслуживание типа T1, а домашним пользователям – типа DSL, а также осуществлять передачу голоса и видео. Важной особенностью 802.16a является работа с отраженными радиосигналами в условиях отсутствия прямой видимости. Это достигается благодаря применению технологии OFDM для расшифровки сильно искаженного отраженного сигнала. Суть OFDM заключается в использовании большого количества узкополосных сигналов – поднесущих. Каждый из них отвечает за свой отдельный бит, а все вместе они определяют кодовое слово, в котором используются методы восстановления информации – коды Рида-Соломона вместе со сверточным кодированием. Стандарт также допускает более гибкое по сравнению с 802.11 распределение полосы частот, используемых для передач данных. Причем это можно сделать как за счет уменьшения количества поднесущих, так и с помощью их сужения. Минимальная ширина сигнала, предусмотренная стандартом, составляет 1,25 МГц, а максимальная – 20 МГц. Естественно, что с уменьшением частотного ресурса скорость передачи уменьшается, но сама эта возможность позволяет использовать частотный спектр отдельными фрагментами, а не целиком, как это было в 802.11.

Существенным отличием 802.16 от 802.11 является возможность использования протокола с разрешением конфликтов. Устройства 802.11 работают по принципам Ethernet, все они имеют равные права на доступ к радиотракту, а попытавшись одновременно установить связь, разрешают конфликты, повторяя попытки захвата среды через случайное время. В 802.16 имеется выделенное устройство – базовая станция оператора, которая раздает своим подчиненным права доступа к радиосреде. В результате протокол нового стандарта позволяет более эффективно использовать радиочастотный ресурс и обеспечить эффективную передачу данных. Причем в самом стандарте предусматриваются несколько режимов передачи – так называемых профилей. Один предназначен для пакетных данных, другой – для псевдосинхронных каналов, третий – для широковещательных передач.

Преимущества для поставщиков услуг

Решение операторского класса: данный стандарт предоставляет широкие возможности для масштабирования, необходимого для обеспечения поддержки сотен тысяч пользователей силами одной базовой станции, и позволяет дифференцировать уровни предоставляемых услуг. Один сектор одной базовой станции способен обеспечить скорость передачи данных, достаточную для одновременного обслуживания более 60 предприятий, подключенных по каналам типа T1, и сотни жилых домов, подключенных по каналам типа DSL. Типовая базовая станция имеет до 6 секторов.

Малый инвестиционный риск: этот стандарт несет в себе для поставщиков услуг меньший риск неокупаемости инвестиций по сравнению с уникальными решениями по организации широкополосного доступа, проектируемыми на заказ. Совместимость оборудования, способного работать в этом стандарте, позволяет оператору сократить затраты на конечное клиентское оборудование и одновременно использовать оборудование разных производителей. Обслуживание клиентов и управление этим обслуживанием можно осуществлять удаленно, что позволяет сократить текущие расходы.

Качество обслуживания: управление доступом к среде стандарта 802.16 рассчитано на поддержку передачи голоса и видео.

Подуровень конвергенции (Convergence Sublayer – CS)

Подуровень расположен над MAC-уровнем и предназначен для организации взаимодействия между более высокими уровнями сети и MAC-уровнем. В стандарте определены два типа уровня конвергенции: ATM и пакетный. Первый обеспечивает взаимодействие MAC-уровня 802.16 и ATM-протокола, второй – взаимодействие с пакетными протоколами.

Протокол MAC-уровня описывает порядок взаимодействия между MAC-уровнем и подуровнем CS, формат фрейма MAC (MAC Protocol Data Units – PDU), сервисы и механизмы опроса (поллинга), обеспечивающие поддержку качества обслуживания – QoS.

Unsolicited Grant Service (UGS) предназначен для поддержки потоков реального времени, генерирующих пакеты данных фиксированного размера, таких как передача потоков E1 и голоса поверх IP без подавления пауз.

Real-Time Polling Service (rtPS) предназначен для поддержки потоков реального времени, формирующих пакеты данных переменной длины, таких как MPEG видео.

Non-Real-Time Polling Service (nrtPS) предназначен для поддержки потоков, требующих пакетов переменной длины, таких как широкополосная FTP.

Best Effort (BE) Service предназначен для эффективного обслуживания трафика best effort.

В протоколе MAC-уровня предусмотрена поддержка дуплекса (частотного или временного), синхронизации, разрешение коллизий, возможных на этапе установления системы или на интервалах запроса на передачу. На этом уровне также обеспечивается измерение дальности до абонентских станций (АС), необходимое для корректной работы протокола, обновление описания канала и разделение абонентского оборудования на абонентские группы.

Уровень безопасности описывает алгоритмы шифрования на участке между базовой станцией (БС) и АС. Уровень безопасности включает два протокола:

- протокол инкапсуляции для шифрования пакетов, включающий несколько вариантов пар шифрование-аутентификация и правила их применения к пакетам MAC-уровня;
- протокол управления ключами шифрования PKM (Privacy Key Management), обеспечивающий распределение ключей от БС для АС.

5.2. 802.16 – спецификация физического уровня

Протоколы физического уровня описывают методы организации дуплекса, способы адаптации, методы множественного доступа и модуляции. Предусмотрены режимы временного и частотного дуплекса. Вид модуляции и кодирования могут изменяться адаптивно от пакета к пакету индивидуально для каждого абонента, что позволяет увеличить реальную пропускную способность примерно вдвое по сравнению с неадаптивными системами. Передача от АС к БС строится на комбинации двух методов многостанционного доступа: DAMA – доступ по запросу и TDMA – доступ с временным разделением. Структура пакетов физического уровня поддерживает переменную длину пакета MAC-уровня. Предусмотрена рандомизация, помехоустойчивое кодирование и три метода модуляции: QPSK, 16QAM и 64QAM. Два последних метода предусмотрены для АС как опциональные. Передача от БС к АС ведется в режиме временного дуплекса в едином потоке для всех АС одного сектора. Передатчик осуществляет рандомизацию, помехоустойчивое кодирование и модуляцию QPSK, 16QAM и 64QAM. Последний метод модуляции предусмотрен для БС как опциональный. Информация в системе передается фреймами, которые делятся на два субфрейма. Первый используется для передачи БС, второй – АС.

Стандартом также рекомендуются полосы частот и соответствующие скорости передачи при различных видах модуляции. Максимальная скорость передачи, предусмотренная в стандарте, – 134,4 Мбит/с при полосе 28 МГц и модуляции 64QAM. В первой версии стандарта предусматривалось использование диапазона частот 10…66 ГГц, для которого рекомендовался режим передачи на одной несущей – single-carrier (SC). Особенности распространения радиоволн этого диапазона ограничивают возможности работы условиями прямой видимости. В типичных городских условиях это позволяет подключить около 50 % абонентов, находящихся в пределах рабочей дальности от базовой станции. До остальных 50 % прямой видимости, как правило, нет. Поэтому в процессе работы над стандартом диапазон частот был расширен включением полосы 2…11 ГГц, в которой, помимо SC, предусмотрены еще и режимы ортогонального частотного мультиплексирования (Orthogonal Frequency Division Multiplexing – OFDM) и множественного доступа на основе ортогонального частотного мультиплексирования (Orthogonal Frequency Division Multiply Access – OFDMA).

В режиме **OFDM** предусмотрена одновременная передача на 256 поднесущих, что позволяет, за счет увеличения примерно в такое же число раз длительности элементарного символа, одновременно принимать прямой и отраженные от препятствий сигналы или вообще работать только по отраженным сигналам вне пределов прямой видимости. Режим OFDMA предусматривает работу на 2048 поднесущих сразу с несколькими абонентами в режиме OFDM. При стандартном количестве поднесущих – 256 обеспечивается одновременная работа с 8 абонентами.

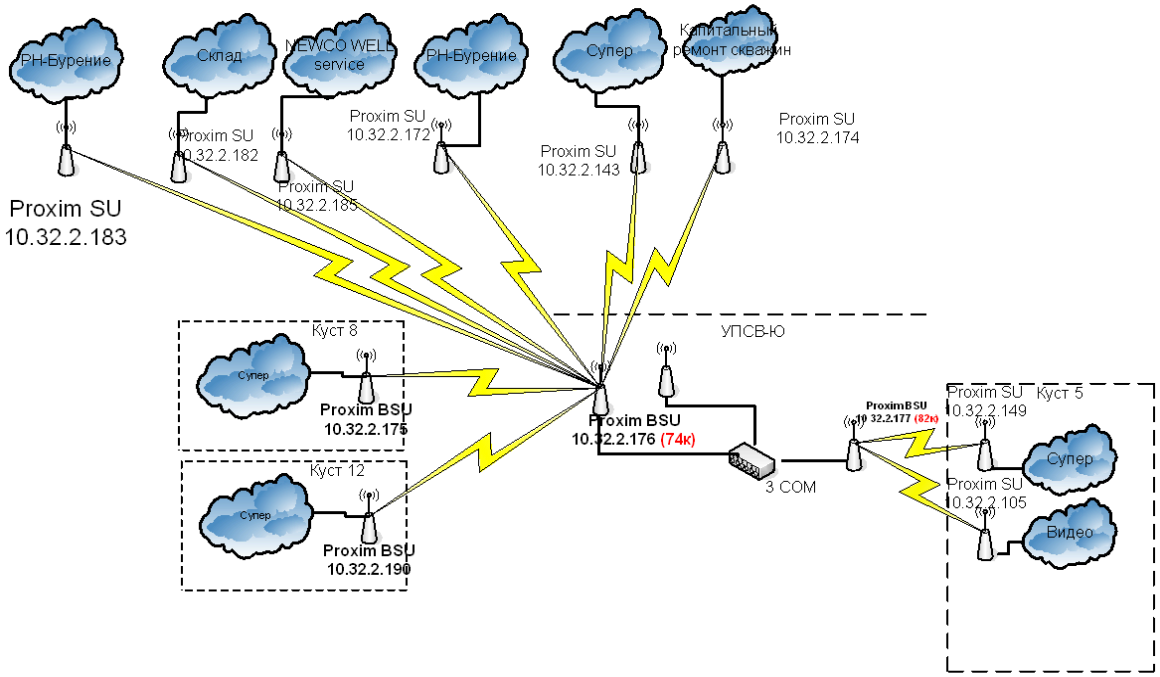


Рис. 12. Ведомственная сеть передачи данных, реализованная на базе оборудования стандарта WiMax

В стандарте также описаны модели сред распространения радиоволн и на этой основе сформулированы требования к параметрам радиооборудования. Предусмотрены возможности автоматической регулировки усиления, динамического выбора частоты в нелицензируемых диапазонах. Помимо топологии точка-многоточка стандартом опционально предусмотрена полносвязная топология – Mesh Mode, позволяющая обеспечить прямую связь между АС, преодолеть помехи, характерные для безлицензионных диапазонов, за счет выбора направления приема, свободного от них, создавать хорошо масштабируемые сети и работать вне прямой видимости даже в одночастотном режиме SC, за счет ретрансляции сигналов АС.

Пример реализации беспроводной сети стандарта 802.16 на нефтяном месторождении приведен на рис. 12.

6. БЕСПРОВОДНЫЕ СЕТИ НА ОСНОВЕ СОТОВЫХ ТЕЛЕФОНОВ

6.1. WAP-протокол. WAP-сервисы, e-port. Технология GPRS

GPRS – это доступ с мобильного телефона в Интернет. Если точнее, то мобильный доступ в Интернет с приемлемой скоростью передачи данных, быстрым соединением и тарификацией по количеству переданных/полученных данных. Сокращение GPRS расшифровывается как General Packet Radio Service, что в переводе на русский означает: Общий Пакетный Радиосервис, т. е. технология пакетной передачи данных посредством сотовой связи. Суть самого сервиса заключается не в чем ином, как в предоставлении пользователю мобильного устройства доступа в Интернет. Услуга GPRS позволяет создать постоянное подключение сети Интернет. Для работы в сети Интернет можно использовать сотовый телефон, компьютер, ноутбук или электронный органайзер. При этом Вы сможете осуществлять серфинг по сети Интернет, т. е просматривать HTML-страницы, перекачивать файлы, работать с электронной почтой и любыми другими ресурсами Интернета. Таким образом, GPRS предоставляет вам все, что нужно.

Технология GPRS работает почти так же, как и обычный компьютерный Интернет. Необходимые данные собираются в пакеты, а эти пакеты затем передаются дальше. Отличие состоит в способе передачи. В GPRS пакеты передаются по незанятым голосовым каналам, однако, из-за этого при сильной нагрузке сети оператора скорость может заметно упасть. Как и у других подобных технологий, существует много версий GPRS. И, конечно, эти версии ничем не различаются, кроме скорости. Причем в большинстве случаев более высокая скорость достигается усиленным сжатием, а также количеством тайм-слотов. Теоретически скорость GPRS составляет 180 кбит/с. К сожалению, в Мобильном Интернете, как и в обычном, есть свои опасности – наибольшую угрозу сегодня представляют мобильные вирусы, хотя и для них уже существуют антивирусы. Если до половины сотрудников компании некоторое время своего рабочего дня проводят не в офисе, для них важно оставаться в контакте с офисом путем расширения возможности использования корпоративных систем электронной почты за пределы офисных персональных компьютеров. Корпоративные системы электронной почты работают на компьютерах внутренней сети (LAN) и включают такие приложения, как Microsoft Mail, Outlook, Outlook Express, Microsoft Ex, Lotus Notes и Lotus cc:Mail.

Электронная почта через интернет. Сервисы электронной почты через интернет имеют форму шлюзовых сервисов, при котором сообщения не сохраняются, или сервисов почтового ящика, в котором сообщения сохраняются. В случае шлюзовых сервисов беспроводная платформа электронной почты просто переводит сообщение из SMTP, интернет-протокола электронной почты, в SMS и посылает его в SMS-центр. В случае сервисов электронной почты в виде почтового ящика сообщения сохраняются, а пользователь получает уведомление на свой мобильный телефон и может затем прочесть сообщение в исходном виде, переслать его и так далее. Получив новое письмо, большинство пользователей услуг электронной почты через интернет не получают на свой мобильный телефон уведомления об этом факте. Когда они находятся вне офиса, им приходится периодически присоединяться к почтовому ящику, если они ждут письма. Однако, связывая интернет-email с механизмом предупреждения, таким как SMS или GPRS, пользователи могут получать уведомление о поступлении нового письма.

Пересылка файлов. Как предполагает этот общий термин, приложения для пересылки файлов выполняют любую форму загрузки большого объема данных через мобильную сеть. Такими данными могут быть презентационные документы для менеджера турагентства, описание устройства для сервис-инженера или программное приложение, такое как Adobe Acrobat Reader, чтобы прочесть документы. Источником этой информации может быть один из методов интернет-коммуникаций, такой как FTP (File Transfer Protocol), telnet, http или Java, либо их собственная база данных или действующая платформа. Безотносительно к источнику и типу файла, который необходимо переслать, этот тип приложений требует большой пропускной способности. Поэтому высокоскоростные мобильные сервисы передачи данных, типа GPRS, EDGE или 3GSM, жизненно необходимы для того, чтобы удовлетворительно выполнять такого рода задачи.

GPRS – это стандарт ETSI (European Telecommunications Standards Institute) для пакетной коммутации в системах GSM. В настоящее время по всему миру наиболее широко распространены сети на основе GSM и их называют сетями второго поколения (2G). Технология GSM использует вариацию TDMA (time division multiple access) и является наиболее широко используемой из трех основных цифровых беспроводных технологий (TDMA, GSM и CDMA).

GSM оцифровывает и сжимает данные, затем пересылает их по каналу с двумя другими потоками пользовательских данных, каждый в своем собственном временном интервале (в тайм-слоте). Функционирует на частоте либо 900 либо 1800 МГц. С тех пор как большинство операторов

сетей GSM заключили роуминговые соглашения с иностранными операторами, клиенты продолжают пользоваться своими мобильными телефонами во время путешествий в другие страны.

GPRS является так называемой накладывающейся технологией, распространяемой на сетях GSM, CDMA и TDMA. Эта технология применяет новый метод эффективной передачи пакетных данных по радиосетям. Технология пакетной коммутации основана на методах IP и X.25, оба из которых очень популярны и широко используются во многих сетях. Пакетная коммутация GPRS работает в целом так же, как и пакетная коммутация IP, то есть данные расщепляются на пакеты и пересылаются по назначению разными путями по сети, затем снова собираются на принимающей стороне. Пакетная коммутация GPRS допускает любой существующий трафик IP или X.25 для пересылки данных через радиосеть GPRS.

GPRS использует радиополосу шириной в 200 кГц, которая делится на восемь каналов. Общая емкость каналов составляет 271 кбит/с, но каждый из этих каналов способен передавать потоки данных в 14,4 кбит/с. Теоретически возможна скорость в 115 кбит/с, но в реальных условиях она используется крайне редко или вообще не используется. Средняя скорость в 48 кбит/с является наиболее вероятной оценкой, поскольку точки доступа поделены между множественными пользователями, причем диапазон или расположение приемника будут также зависеть от имеющейся в наличии ширины полосы. Этот результат гораздо лучше, чем могут предложить существующие устройства мобильных коммуникаций, дающие всего 9,6 кбит/с. Другим важным аспектом Интернет-связи через GPRS – и это первое такого рода внедрение для широкополосной сети – является то, что соединение с Интернет непрерывно (всегда «он-лайн»), и в то же время ему не приходится подтягивать ресурсы из точек доступа в то время, когда оно не используется, потому что данные передаются только тогда, когда в этом есть необходимость. Приемник запрашивает информацию, и устройство подтягивает в этот момент радиоресурсы, а затем снова находится в нерабочем состоянии, пока не начинает принимать запрошенную информацию. Радиополосы распределяются динамическим образом, в зависимости от типа контента – одновременно несколько или даже больше, в зависимости от того, передается ли текстовое сообщение или «живое» видео. Когда пользователь включает устройство, поддерживающее GPRS, обычно оно автоматически ищет канал GPRS в данной местности. Если соответствующий канал найден, устройство будет пытаться соединиться с сетью.

Сеть GPRS – наложенная сеть, располагающаяся поверх инфраструктур GSM. Ключевые компоненты сети GPRS включают:

- PCU – блок управления пакетами, дающий возможность станциям GSM пересылать и получать пакеты при GPRS коммуникациях.
- SGSN – часть инфраструктуры GSM, ответственная за отсылку и получение пакетов от абонентов в своем районе обслуживания. Этот блок также производит авторизацию, контактируя с сервером и проверяя информацию о пользователе. Кроме того, он отслеживает маршрут перемещений абонента, чтобы иметь возможность надлежащим образом распределять ресурсы, а также собирает поступающую биллинговую информацию, пересылая ее в главный офис.
- GGSN – компонент сети GSM, ответственный за взаимодействие с Интернет и другими общественными сетями, передающими данные и голос. Компонент хранит маршрутизирующую базу данных, базу данных с адресами и фильтрующую.
- GTP – туннелирующий протокол GPRS, основанный на протоколах TCP/IP, инкапсулирующий пакеты IP и X.25, приходящие из узлов SGSN в GGSN.

Когда пользователь GPRS делает звонок, устройство GPRS контактирует со станцией GSM, которая, в свою очередь, обращается к станции SGSN, взаимодействующей с другими станциями SGSN или станциями GGSN, если ей нужно получить доступ к сети другого рода (IP или X.25). Для пользователя GPRS соединение получается «бесшовным» – нет процедуры «установления звонка». Технология GPRS, накладываемая поверх сети GSM, изначально была предназначена для того, чтобы динамически и индивидуально распределять радиоресурсы GSM «попакетно», по мере необходимости. Если к соте GSM одновременно подключается сразу много пользователей GPRS и сота GSM не способна поддерживать такой объем голосового трафика, станция GPRS воспользуется радиоресурсами соседних сот GSM. Таким образом, в реальности пользователи GPRS обслуживаются многими сотами GSM одновременно, когда в этом возникает необходимость. Итак, SGSN получает запрос на соединение, запрашивает информацию о профиле пользователя из узла HLR и производит аутентификацию пользователя. В этой точке может осуществляться шифрование. SGSN использует информацию о профиле (включая имя точки доступа, которое идентифицирует сеть и оператора) для определения, к которому узлу GGSN производить маршрутизацию. Выбранные ворота могут предоставлять сервис удаленной аутентификации пользователя (Remote Authentication Dial-In User Service, RADIUS) и назначать динамический адрес Интернет-протокола (IP) пользователю перед настройкой соединений во внешние сети. Этот процесс называется «контекстная активация пакетного профиля данных» и установки могут варь-

ироваться от оператора к оператору. Он может включать дополнительные функции, такие как менеджмент QoS (Quality of Service – качество сервиса) и менеджмент виртуальных частных сетей (virtual private network, VPN). Когда мобильное устройство выключено или находится вне зоны покрытия GPRS, его контекст дезактивируется и устройство отсоединяется от сети.

GPRS в настоящее время поддерживает средние скорости передачи данных порядка 115 кбит/с, но такие скорости достигаются только при задействовании всех восьми тайм-слотов (промежутков времени) для GPRS. Вместо этого носители и конечные устройства будут конфигурироваться типовым образом, чтобы работать с определенным количеством тайм-слотов для данных, передаваемых в обоих направлениях. Например, устройство GPRS может быть настроено для работы максимум с четырьмя слотами в прямом направлении и двумя слотами в обратном направлении. В хороших радиоусловиях это дает скорости приблизительно в 50 кбит/с в прямом направлении и 20 кбит/с в обратном направлении. Это более чем в три раза быстрее, чем в нынешних сетях GSM (14,4 кбит/с), и того же порядка, что и при хорошем модемном аналоговом соединении в кабельной линии. Совокупная ширина полосы узла сотовой связи делится между голосовым трафиком и трафиком данных. Операторы GPRS по-разному используют эту ширину полосы. Обычно они конфигурируют сети, давая приоритет голосовому трафику; некоторые из них назначают тайм-слоты для трафика данных, чтобы гарантировать минимальный уровень этого сервиса в высокозагруженные голосовым трафиком промежутки времени. Неиспользованная емкость, зарезервированная под голосовой трафик, может быть динамически переопределена под передачу данных. Имея более высокие скорости передачи данных, GPRS дает возможность реализации приложений, требующих более высокой ширины полосы и в настоящее время не осуществимых на сетях GSM.

Постоянное соединение – «всегда он-лайн» – устраняет задержки по времени, характерные для dial-up соединения, связанные с установлением нового соединения с сетью всякий раз, когда требуется отсылать и получать данные. Информация может передаваться конечному пользователю в режиме реального времени. GPRS позволяет провайдерам осуществлять биллинговый учет попакетно, а не поминутно, давая, таким образом, возможность предоставлять пользователям более эффективные по стоимости сервисы.

GPRS улучшила целостность передачи данных путем применения ряда механизмов. Во-первых, пользовательские данные кодируются с некоторой избыточностью, что улучшает их устойчивость к неблагоприят-

ным радиоусловиям. Уровень избыточности при кодировании можно варьировать, в зависимости от тех же радиоусловий. GPRS определяет четыре кодирующие схемы – с CS1 по CS4. Вначале поддерживаются только CS1 и CS2, которые обеспечивают примерно 9 и 13 кбит/с на каждый тайм-слот. Если в полученном фрейме обнаружена ошибка в BSS, этот фрейм до передачи его на центральную сеть GPRS периодически повторяется, пока не будет получен в приемлемом качестве.

Подобно сети Интернет, GPRS основан на пакетной коммутации данных. Это означает, что все собственные IP-приложения могут быть реализованы в рамках GPRS, такие как e-mail, Web-доступ, мгновенная передача сообщений и передача файлов. Кроме того, его более высокие скорости передачи данных дают возможность GPRS осуществлять работу приложений, требующих большей ширины полосы (таких как мультимедийный веб-контент), которые не идут в условиях более медленных GSM dial-up соединений. GPRS более-менее хорошо подходит для приложений, основанных на Wireless Application Protocol (WAP). WAP достиг широкого распространения в новом поколении мобильных телефонов, поддерживающих микробраузеры.

GPRS строится на проверенной на практике модели аутентификации и авторизации, используемой GSM. При инициации сессии пользователя аутентифицируют, используя секретную информацию, содержащуюся на смарт-карте, называемой «модуль идентификации абонента» (Subscriber Identity Module, SIM). Аутентификационные данные посылаются на узел сети HLR и там подтверждаются. GPRS дает возможность дополнительной аутентификации путем использования таких протоколов, как RADIUS – перед тем, как абонентам будет разрешен доступ в Интернет или корпоративную сеть данных. GPRS поддерживает шифрование пользовательских данных при передаче через беспроводный интерфейс с мобильного терминала на SGSN. Кроме того, может иметь место высокоуровневое сквозное шифрование VPN (Virtual Private Network), когда пользователь подсоединяется к частной корпоративной сети.

Под идентификацией в данном случае понимается подтверждение права человека на использование данного сотового телефона. В этом плане технология GPRS ничем не отличается от стандарта GSM. То есть в ней используются те же самые средства идентификации: PIN-коды и PUK-код. С их помощью человек подтверждает собственную личность, точнее, право на использование телефона.

Аутентификация необходима для подтверждения телефоном своего права работать в данной сети GPRS. Для этого в SIM-карте мобильного телефона и на базовой станции реализован специальный алгоритм. Суть его заключается в следующем. В начале процедуры базовая станция от-

правляет на телефон случайную последовательность цифр. SIM-карта преобразовывает его в соответствии с алгоритмом, используя при этом собственный секретный ключ, а получившееся значение (SRES, Signed RESult – подписанный результат) отправляет обратно. Точно такие же преобразования производятся и на базовой станции. Если оба значения SRES совпадают, то делается вывод о допуске данного телефона в сеть. Таким образом, идентификация пользователей и аутентификация мобильников должны предотвратить несанкционированный доступ к базовой станции, а также использование злоумышленниками чужих счетов.

Можно сказать, что в сети GPRS используется два типа каналов связи. Первый из них – радиоэфир, через который общаются между собой базовые и мобильные станции. Данный канал является наиболее уязвимым местом GPRS-сети. И действительно, перехват радиосигналов не представляет собой практически никакого труда. Для этого можно использовать как специализированные устройства (в том числе и самодельные, сделанные любителями), так и старые радиоприемники советского образца. Именно поэтому абсолютно вся информация, передающаяся по радиоканалу, предварительно зашифровывается с помощью специальных алгоритмов. В сетях GPRS для этого используются стандарты GEA1, GEA2, GEA3 – «близкие родственники» криптоалгоритмов GSM.

К сожалению, криптоалгоритмы GEA1 и GEA2 не относятся к числу самых надежных, случаи взлома зашифрованной с их помощью информации известны. Технология же GEA3 до сих пор применяется очень редко. Впрочем, большинству пользователей сетей GPRS можно об этом не беспокоиться. Ведь взлом криптоалгоритма – процедура достаточно дорогая, так что вряд ли кто-то будет использовать ее для перехвата обычной информации. Другой опасностью, которая подстерегает пользователей GPRS, является возможное отключение шифрования операторами сотовой связи по требованию спецслужб. Впрочем, это делается только во время проведения различных операций или массовых мероприятий.

Если злоумышленникам все же удастся перехватить сигналы и расшифровать (при необходимости) их, то они смогут получить всю информацию, которую отправляет и получает пользователь. С помощью такой атаки хакеры могут, например, прочитать корреспонденцию жертвы, получить ее пароли для доступа к различным сервисам, данные пластиковой карты и т. п.

Ко второму типу относятся каналы связи, использующиеся для передачи данных между внутренними узлами сети. Для обеспечения его безопасности был разработан и внедрен в GPRS специальный протокол GTP (GPRS Tunneling Protocol). Он отличается от привычных хакерам технологий. Кроме того, внутренние компьютеры сети GPRS используют для маршрутизации принцип частных IP-адресов согласно международному стан-

дарту RFC 1918. Все это позволяет говорить о действительно надежной защите внутренних каналов связи, что подтверждается и практикой. До сих пор еще не известно ни одного случая перехвата информации из них.

Под внешними угрозами понимаются вирусы или удаленные атаки. Если рассмотреть архитектуру сети GPRS, то станет ясно, что все это угрожает только одному узлу – узлу маршрутизации. Для того, чтобы выполнять свои функции, он должен быть полноценным участником обеих сетей. Так что он подвержен всем видам атак, которые на данный момент существуют в Интернете. Эта проблема отлично решается с помощью обычных средств: антивирусной программы с постоянно обновляемыми базами данных и корректно настроенного файрвола. Единственным отличием защиты данного компьютера является использование принципа трансляции адресов (network address translation). Это необходимо для предотвращения удаленного доступа злоумышленников к внутреннему сетевому оборудованию. Нерешенной остается только одна проблема. Речь идет о возможности проведения на узел маршрутизации профессиональной DDoS-атаки. От этого не застрахован ни один сервер в Интернет.

Узел маршрутизации выполняет еще одну функцию. Он отвечает за связи своей сети GPRS с другими такими же сетями. Для того чтобы защитить эти каналы, используются так называемые пограничные шлюзы (BG – border gateway). Суть действия этого программного обеспечения похожа на работу файрвола. Администратор устанавливает правила обмена трафиком, вводит доверенные сети, подключает системы роуминга и т. п. После этого вся система будет защищена от атак из других сетей GPRS.

В технологии GPRS существует ряд ограничений:

- GPRS оказывает существенное влияние на существующую емкость соты сети. Объем имеющихся радиоресурсов, которые могут быть использованы для различных целей, ограничен, причем использование ресурсов для одной цели препятствует одновременному их использованию для других. Например, и голосовые вызовы, и GPRS-сессии используют одни и те же сетевые ресурсы. Ощутимость влияния зависит от количества тайм-слотов, зарезервированных для эксклюзивного использования GPRS, если это имеет место быть. Однако в действительности GPRS динамически управляет назначением каналов и позволяет уменьшать нагрузку канала сигнала в пиковое время путем пересылки коротких сообщений по GPRS-каналам.

- Достижение теоретически максимальной скорости передачи данных через GPRS – 172,2 кбит/с потребовало бы, чтобы отдельный пользователь использовал все восемь тайм-слотов без какой-либо защиты от ошибок. Ясно, что на практике достаточно маловероятно, чтобы оператор сети позволил

использовать все тайм-слоты одному пользователю GPRS. Кроме того, «первое поколение» GPRS-терминалов жестко лимитировано на поддержку всего одного, двух или трех тайм-слотов. Поэтому ширина полосы, доступная пользователю GPRS, так же жестко лимитирована. По этой причине теоретические максимальные скорости GPRS не могут быть достигнуты в реальных сетях и на реальных терминалах. Реальность такова, что мобильные сети, вероятно, всегда будут иметь более низкие скорости передачи данных по сравнению с фиксированными сетями. Результат – относительно высокие скорости передачи данных через мобильные устройства могут не быть доступными индивидуальным пользователям мобильных сервисов, пока не появились возможности существенного повышения скоростей на сетях GSM Evolution (EDGE) или Universal Mobile Telephone System (3GSM).

• GPRS основан на технологии модуляции, известной как GMSK (Gaussian minimum-shift keying). Сети EDGE основаны на новой модуляционной схеме, допускающей гораздо более высокие скорости передачи данных через воздушный интерфейс, модуляция 8PSK (eight-phase-shift keying). Поскольку 8PSK также будет использоваться в 3GSM, сетевым операторам потребуется учесть этот момент на некоторой стадии перехода к сетям мобильной связи третьего поколения.

• Пакеты GPRS посылаются по всем направлениям, чтобы в итоге достичь одного и того же пункта назначения. Это создает опасность того, что один или несколько таких пакетов потеряются или будут повреждены во время передачи данных по радиосвязи. Стандарты GPRS учитывают это неотъемлемое свойство беспроводных пакетных технологий, закладывая в свои стратегии задачи сохранения целостности данных и ретрансмиссии. Однако в результате этой подстраховки могут происходить задержки передачи. Вследствие этого приложения, требующие высокого качества передачи видеоизображений, могут выполняться на должном уровне при использовании HSCSD (High Speed Circuit Switched Data, высокоскоростная коммутация каналов данных). HSCSD – это просто коммутация каналов данных, при которой отдельный пользователь может использовать до четырех разных каналов одновременно. Из-за принципа сквозной связи между отправителем и получателем задержки передачи менее вероятны.

6.2. Технологии EDGE и 3G

Следующим шагом развития мобильных систем передачи данных является технология EDGE (Enhanced Data Rates for GSM Evolution – «передача данных на повышенной скорости»), которая позволит осуществлять перекачку информации на скоростях до 384 кбит/с в восьми GSM-каналах (48 кбит/с на канал). Для внедрения EDGE «поверх» GPRS

операторам предстоит заменить аппаратуру базовых станций, а пользователям – приобрести поддерживающие EDGE телефонные аппараты.

Эволюцией технологии GSM является стандарт EDGE (Enhanced Data rates for Global Evolution), позволяющий повысить пропускную способность до 384 кбит/с. Радиоинтерфейс EDGE надстраивается над существующей инфраструктурой GSM и использует те же полосы частот 850/900/1800/1900 Гц, что и GSM. Полоса пропускания, необходимая для мобильных Интернет-услуг, обеспечивается в GSM за счет предварительной организации общей радиослужбы пакетной передачи (GPRS). Однако для приложений, работающих с данными в реальном времени, требуется более широкая полоса пропускания и более высокое качество обслуживания по сравнению с теми, которые обеспечивают современные системы GPRS. Эта нехватка компенсируется путем замены гауссовской манипуляции с минимальным частотным сдвигом (GMSK), которая использует только часть фазы, на восьмипозиционную фазовую манипуляцию (8PSK), которая использует все 360º. EDGE, так же как и GPRS, использует тайм-слоты (временные отрезки кадра) для передачи информации. Существует идентичная GPRS политика распределения тайм-слотов между каналами на прием и передачу. Следует отметить, что максимальная скорость потока в одном тайм-слоте составляет 48 кбит/с, она достижима при идеальных условиях приема.

В зависимости от качества связи предусмотрено 9 алгоритмов кодирования: от MCS-1 до MCS-9 (последний обладает самой малой избыточностью кодирования, соответственно – самый быстрый).

Таким образом, технология EGPRS (EDGE) способна обеспечить каждому абоненту как высокий уровень обслуживания, так и широкую полосу пропускания.

Технологии GPRS и EDGE считают лишь промежуточными этапами миграции к 3G и зачастую их называют переходными технологиями поколения 2.5G.

Главное отличие 3G от эксплуатируемых сейчас сетей второго поколения (2G) – передача большого объема информации на высоких скоростях. Возможности сетей 3G открывают новые горизонты в использовании мобильной связи, причем как частным абонентам, так и крупным корпорациям. Изменится само понятие мобильного телефона, он станет многофункциональным устройством, предназначенным для всех случаев жизни.

Одно из главнейших требований – сеть 3G должна передавать данные от абонента и обратно со скоростью до 2,048 Мбит/с при низкой мобильности (менее 3 км/ч) и локальной зоне покрытия и до 144 кбит/с при высокой мобильности (до 120 км/ч) и широкой зоне покрытия.

Сегодня в мире существуют две основные конкурирующие концепции 3G: UMTS (Universal Mobile Telecommunications Systems – универсальная мобильная телекоммуникационная система), поддерживаемая европейскими странами, и CDMA 2000 (Code Division Multiple Access – мультидоступ с кодовым разделением каналов), сторонниками которой традиционно являются азиатские страны и США.

В принципе, эти две технологии предполагают два различных подхода к организации сетей 3G: революционный (UMTS) и эволюционный (разновидности CDMA – CDMA 2000, CDMA 2000 IX, CDMA 2000 IX EvDo). Эволюционный путь подразумевает сохранение частот и постепенный переход к новым технологиям путем наращивания технических мощностей оператора. UMTS – совершенно новый стандарт, в то время как разновидности CDMA, предложенные для 3G, являются развитием уже эксплуатирующейся в мире технологии второго поколения *cdm*.

7. БЕСПРОВОДНЫЕ СЕТИ НА ОСНОВЕ СТАНДАРТА BLUETOOTH 3.0

7.1. Спецификация физического уровня, протоколы, сервисы

Что же такое Bluetooth? Так называется технология обеспечения радиосвязи между мобильными и стационарными PC, мобильными телефонами, принтерами и прочими периферийными устройствами. В настоящее время технология Bluetooth является твердо устоявшимся коммуникационным стандартом для беспроводной связи на малых расстояниях. Она заменяет целую кучу отдельных кабелей, присоединяющих одно устройство к другому посредством одной универсальной радиолинии с малым радиусом действия. Например, радиотехнология Bluetooth, встроенная и в сотовый телефон, и в ноутбук, заменяет кабель, используемый в настоящее время для присоединения ноутбука к сотовому телефону. Принтеры, персональные компьютеры, факсы, клавиатуры, джойстики и практически любые другие цифровые устройства могут быть частью системы Bluetooth. Радиотехнология Bluetooth также обеспечивает универсальный мост к существующим сетям передачи данных, интерфейсу периферийных устройств, а также обеспечивает механизм для формирования небольших частных специальных групп соединяемых устройств вне инфраструктуры фиксированной сети. Серьезной соперницей Bluetooth является технология инфракрасной связи IrDA, но она не предназначена для построения беспроводных локальных сетей и работает только по принципу точка-точка в зоне прямой видимости. При разработке спецификации во главу угла ставились экономичность (как в плане стоимости, так и в плане энергосбережения), сохранение маленького форм-фактора и предельная простота эксплуатации. Для конечного пользователя это означает быстрое и легкое подключение периферии или соединение компьютеров без каких бы то ни было кабелей. К тому же технология дает возможность связать больше двух устройств, используя единое радиосоединение. Общее число проданных во всем мире Bluetooth-совместимых устройств уже превысило 1 миллиард экземпляров. Спецификация стандарта Bluetooth приведена в табл. 4.

Таблица 4

Параметры	**Bluetooth**	**IrDA**
Тип модуляции	метод частотных скачков	амплитудная
Частотный диапазон	2,4 ГГц	излучение в оптическом диапазоне 850…900 нм

Окончание табл. 4

Параметры	Bluetooth	IrDA
Число скачков в секунду	1600	–
Мощность передатчика, мВт	100	20…80
Скорость передачи данных, Мбит/с	0,7	4
Способ модуляции	двухуровневая частотная	двухуровневая импульсная
Количество устройств в сети	не ограничено	2
Защита информации	40- и 64-битное шифрование	нет
Радиус действия, м	10…100	1

Проект являлся конкурентом стандарта IEEE 802.11 (оба стандарта используют один и тот же частотный диапазон, одни и те же 79 каналов). Главной его целью являлось удаление любых кабелей из телефонии, а если получится – и из локальных сетей. Технология Bluetooth использует нелицензируемый (практически везде кроме России) частотный диапазон 2,4…2,4835 ГГц. При этом используются широкие защитные полосы: нижняя граница частотного диапазона составляет 2 ГГц, а верхняя – 3,5 ГГц. Точность заданий частоты (положение центра спектра) устанавливается с точностью ± 75 кГц. Дрейф частоты в этот интервал не входит. Кодирование сигнала осуществляется по двухуровневой схеме **GFSK** (Gaussian Frequency Shift Keying). Логическому 0 и 1 соответствуют две разные частоты. В оговоренной частотной полосе выделяется 79 радиоканалов по 1 МГц каждый. В некоторых странах используется меньшее число каналов (например, во Франции – 23). Каждый из каналов структурируется с помощью выделения временных слотов (доменов) длительностью 625 мкс (разделение по времени). По мощности передатчики делятся на три класса: 100 мВт (для связи до 100 м; 20 дБм); 2 мВт (до 10 м; 4 дБм) и 1 мВт (~10 см; 0 дБм). Коэффициент модуляции при этом лежит в диапазоне (0,28…0,35). Чувствительность приемника должна быть не хуже 70 дБм. BER (Bit Error Rate) для приемника должна находиться на уровне <0,1 %. Желательно, чтобы приемник имел индикатор мощности входного сигнала (требование является опционным). Для первого класса предусмотрено регулирование мощности, которое осуществляется на основе анализа числа ошибок. Протокол использует

коммутацию каналов и пакетов. Передача данных выполняется с использованием алгоритма доступа **Time-Division Duplex Multiple Access**. Каждый пакет передается с использованием иного частотного канала по отношению к предыдущему. Производится 1600 переключений частоты в секунду. Последовательность переключения частот определяется BD_ADDR мастера. Скачкообразное переключение частоты отводит на переходные процессы 250…260 мкс. Длительность тика часов мастера равна 312,5 мкс, что определяет частоту часов – 3,2 кГц. Допускается временная неопределенность при приеме, равная ±20 мкс. Структура протоколов Bluetooth не следует моделям OSI, TCP/IP и даже 802 (ведутся работы по адаптации Bluetooth к модели IEEE 802). Физический уровень протокола соответствует базовым принципам моделей OSI и 802. Разработчики потратили много усилий, чтобы сделать протокол как можно дешевле для реализации. В среднем временная привязка мастерных пакетов не должна дрейфовать больше чем на $20 \cdot 10^{-6}$ относительно идеальной временной привязки слота в 625 мкс. Временной разброс при этом не должен превышать 1 мкс. В спецификации определено 5 уровней: физический, базовый (baseband), управления каналом **LMP** (Link Management Protocol) и **L2CAP** (Logical Link Control and Adaptation Protocol), сетевой и уровень приложений. На базовом уровне протокола определено 13 типов пакетов. Пакеты ID, NULL, POLL, FHS , DM1 ориентированы на каналы SCO и ACL. Пакеты DH1, AUX1, DM3, DH3, DM5 и DH5 предназначены только для каналов ACL. Кодирование данных в пакетах DM1, DM2 и DM3 осуществляется с привлечением битов четности по алгоритму FEC 2/3 (5 бит управления на 10 бит данных). Форматы пакетов HV1, HV2, HV3 и DV определены только для каналов SCO. Максимальный размер поля данных (341 байт) имеют пакеты DH5. Уровень протокола baseband специфицирует пять логических каналов: **LC** (Control Channel) и **LM** (Link Manager) используются на канальном уровне, а **UA** (User Asynchronous), **UI** (User Isosynchronous) и **US** (User Synchronous) служат для асинхронной, изосинхронной и синхронной транспортировки пользовательских данных. Предусмотрено семь субсостояний, которые используются для добавления клиента или подключения к пикосети: **page, page scan, inquiry, inquiry scan, master response, slave response** и **inquiry response**. Состояние Standby по умолчанию является режимом с пониженным энергопотреблением, при этом работает только внутренний задающий генератор. В состоянии соединения главный узел (master) и клиент (slave) могут обмениваться пакетами, используя код доступа к каналу.

В протоколе baseband предусмотрено три типа схем коррекции ошибок: 1/3 FEC, 2/3 FEC и ARQ.

- В 1/3 FEC каждый бит повторяется три раза.

- В 2/3 FEC используется полиномиальный генератор для получения 15-битовых кодов для исходных 10 бит.
- В схеме ARQ пакеты DM, DH и поле данных пакета DV передаются повторно до тех пор, пока не будет получено подтверждение или не произойдет тайм-аут. При тайм-ауте возможно продолжение со следующего пакета.

Протоколом baseband рекомендуется использование буферов типа FIFO. Если данные не могут быть приняты, контроллер приема (Link Controller) вставляет в заголовок отклика индикатор **stop**. Когда передачик получает индикатор stop, он блокирует очереди в FIFO. Получатель может возобновить процесс передачи, послав отправителю индикатор **go**. Взаимодействие протоколов в рамках Bluetooth показано на рис. 13.

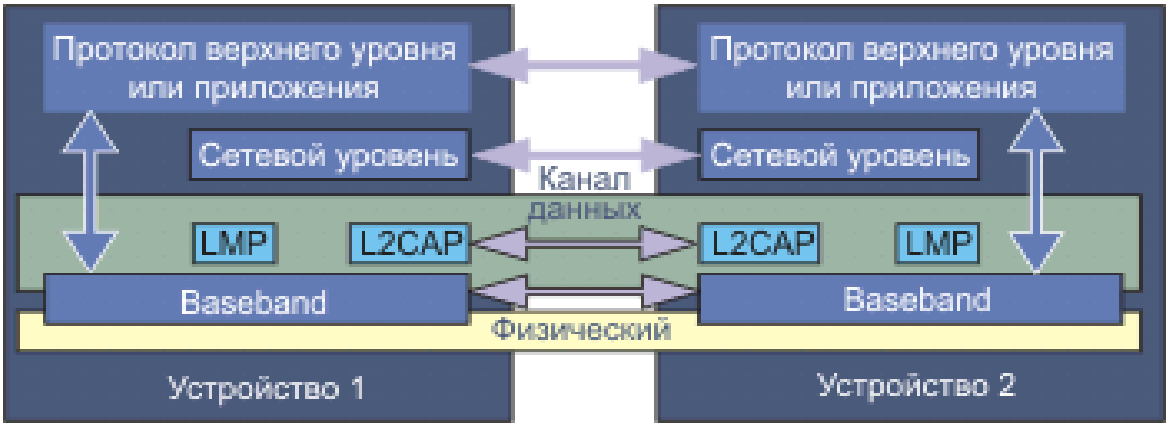


Рис. 13. Взаимодействие сетевых субуровней в протоколе Bluetooth

Соединение между устройствами присходит следующим образом: если ничего не известно об удаленном устройстве, используются процедуры **inquiry** и **page**. Если некоторая информация о партнере имеется, то достаточно процедуры **page**.

Этап 1

Процедура **inquiry** позволяет устройству определить, какие приборы доступны, выяснить адреса и осуществить синхронизацию.

1. Посылаются пакеты inquiry и получаются отклики.
2. Будем считать, что блок (адресат), получивший пакет inquiry, находится в состоянии inquiry scan (тогда он способен принимать такие пакеты).
3. Получатель переходит в состояние inquiry response и посылает отправителю пакет-отклик.

После того как процедура inquiry завершена, соединение может быть установлено с помощью процедуры paging.

Этап 2

Процедура **paging** реализует соединение. Для осуществления этой процедуры необходим адрес. Устройство, выполняющее процедуру paging, атоматически становится хозяином этого соединения.

1. Посылается пакет paging.
2. Адресат получает этот пакет (находится в состоянии page Scan).
3. Получатель посылает отправителю пакет-отклик (находится в состоянии Slave Response).
4. Инициатор посылает адресату пакет FHS (находится в состоянии Master Response).
5. Получатель посылает отправителю второй пакет-отклик (находится в состоянии Slave Response).
6. Получатель и отправитель устанавливают параметры канала, заданные инициатором (находятся в состоянии Master Response & Slave Response).

После установления соединения главный узел (master) посылает пакет POLL, чтобы проверить, синхронизовал ли клиент свои часы и настроился ли на коммутацию частот. Клиент при этом может откликнуться любым пакетом.

Устройство Bluetooth при установлении соединения может работать в четырех режимах: **Active, Hold, Sniff** и **Park** (активный, удержание, прослушивание и пассивный соответственно), табл. 5.

Таблица 5

Режимы работы Bluetooth

Название режима	Описание
Active	В активном режиме устройство Bluetooth участвует в работе канала. Главный узел (master) диспетчеризует обмены на основе запросов трафика, поступающих от участников. Кроме того, этот режим предусматривает регулярные обмены с целью синхронизации клиентов. Активные клиенты прослушивают домены master-to-slave пакетов. Если к активному клиенту нет обращений, он может пребывать в пассивном состоянии (sleep) до очередной передачи со стороны главного узла
Sniff	Устройства, синхронизованные в рамках пикосети, могут перейти в режим экономного расходования энергии, когда их активность понижается. В режиме **SNIFF** устройство-клиент прослушивает пикосеть с пониженной частотой. Этот режим имеет наивысшую скважность рабочего цикла (наименьшая экономия энергии) из 3 экономичных режимов (**sniff, hold** и **park**)

Окончание табл. 5

Название режима	Описание
Hold	Главный узел пикосети может перевести клиента в режим HOLD, когда работает только внутренний таймер. Устройство-клиент может запросить перевода в режим **HOLD**. Передача данных возобновляется мгновенно, когда устройство выходит из режима **HOLD**. Клиент имеет промежуточную скважность (промежуточный уровень экономии энергии)
Park	В режиме **PARK** устройство еще синхронизовано в рамках пикосети, но не принимает участия в обменах. Пассивные устройства отказываются от своих MAC-адресов (AM_ADDR), прослушивают трафик главного модуля, с целью ресинхронизации, и отслеживают широковещательные сообщения. Данный режим имеет минимально возможную скважность (максимальная экономия энергии) из указанных 3-х режимов (sniff, hold и park). Устройства, находящиеся в режиме **PARK**, должны посылать пакеты широковещательно, так как лишены собственного активного адреса

Протокол L2CAP отвечает за формирование пакетов, деление на кадры и сборку пакетов (вспомним, что нижележащий протокол baseband позволяет иметь пакеты не длиннее 341 байта), которые в данном стандарте могут достигать размера 64 кБ. L2CAP производит мультиплексирование и демультиплексирование для отправителей пакетов. Кроме того, протокол ответственен за качество обслуживания как при передаче, так и во время ожидания. На фазе установления соединения L2CAP согласует максимальный размер поля данных, так как не все узлы могут работать с 64-килобайтными пакетами. Этот протокол не используется в случае синхронных коммуникаций. В стандарте Bluetooth предусмотрены обмены как с установлением соединения, так и без. Последний режим называется **ASL** (Asynchronous Connectionless). Трафик ASL доставляется с использованием принципа максимально возможного сервиса. Никаких гарантий при этом не предоставляется. У подчиненного узла может быть только одно ASL-соединение с главным. Обмен с установлением соединения называется **SCO** (Synchronous Connection Oriented). Этот вид коммуникаций используется, например, при телефонных переговорах. Здесь для каждого из направлений передачи выделяется фиксированный временной интервал. Повторных передач не производится, вместо этого для случая ошибок применяется их коррекция. У подчиненного узла может быть до 3 соединений типа SCO с главным узлом, каждое из которых

представляет собой PCM-канал с пропускной способностью 64 кбит/с. Протокол должен поддерживать протокольное мультиплексирование, так как уровень basband не имеет тип поля, позволяющего идентифицировать протокол более высокого уровня. Протокол L2CAP присваивает виртуальным каналам (точка-точка) идентификаторы CID (Channel Identifier). Для целей управления трафиком он целиком полагается на уровень LM (Link Manager) протокола baseband.

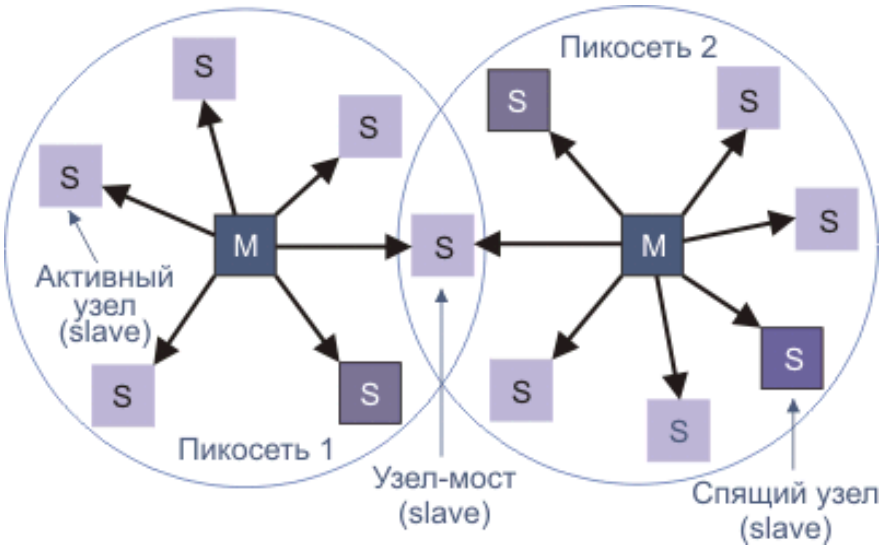


Рис. 14. Две пикосети, образующие рассеянную сеть (Э. Таненбаум «Компьютерные сети»)

Основу сети Bluetooth составляют *пикосети* (piconet), состоящие из одного главного узла и до семи клиентских узлов, размещенных в радиусе 10 м (рис. 14). Все узлы такой сети работают на одной частоте и разделяют общий канал. В одной достаточно большой комнате могут располагаться несколько пикосетей. Эти сети могут связываться друг с другом через мосты. Пикосети, объединененные вместе, составляют рассеянную (**scatternet**) сеть. Поскольку в каждой пикосети имеется свой master, последовательность и фазы переключения их частот не будут совпадать. Если пикосети взаимодействуют друг с другом, это приводит к понижению пропускной способности. Устройство Bluetooth может выступать в качестве клиента в нескольких пикосетях, но главным узлом (master) может быть только в одной пикосети. Кроме 7 активных клиентских узлов, главный узел может поддерживать до 255 пассивных (спящих) узлов (переведенных управляющим узлом в режим пониженного энергопотребления).

Иногда мастер и клиент могут захотеть поменяться ролями. Это может быть выполнено в два этапа:

1. Происходит отключение обоих участников процесса от пикосети и осуществляется переключение TDD (Time Division Duplex) трансиверов.
2. Если требуется, узлы старой пикосети образуют новую пикосеть.

Когда узел получил подтверждение на свой FHS-пакет, он будет использовать параметры новой пикосети, заданные новым мастером. На этом переключение мастер-клиент завершается.

Самым низким уровнем протокола является уровень *радиосвязи*. На этом уровне данные передаются от главного узла к подчиненному бит за битом. Все узлы пикосети перестраивают частоту одновременно, последовательность частот определяется главным узлом (M на рис. 14). Главный узел (master) является источником синхронизации для всех клиентов пикосети.

Выше уровня радиосвязи размещен уровень *немодулированной передачи*. Он преобразует поток бит в кадры и определяет базовые форматы. Передача со стороны главного узла производится в четные такты, а со стороны подчиненных узлов – в нечетные. Кадры могут иметь длину 1, 3 или 5 тактов. Все кадры передаются между главным и подчиненным узлами по логическому каналу, называемому соединением.

Одним из активных состояний узла является **paging state**. В этом состоянии возможно установление или возобновление соединения. Главный узел в этом состоянии непрерывно посылает в эфир короткие ID-пакеты, содержащие только код доступа устройства (*device access code*). В рамках одного временного домена посылается два пакета на двух разных частотах. Узел-клиент в состоянии paging прослушивает за время 625 мкс две частоты, проверяя наличие своего кода (ID). Для установления соединения посылается запрос. Отправитель запроса не сообщает ничего, кроме своего типа. Узел, который хочет, чтобы о его существовании знали окружающие, периодически (раз в 2,56 с) прослушивает запросы (состояние inquiry state). Когда пассивное устройство обнаружено главным узлом пикосети (откликнулось пакетом **FHS**, сообщающем о состоянии внутренних часов, об адресе и т. д.), главный узел формирует и посылает пакет POLL, с целью проверки правильности конфигурационных параметров и готовности к приему данных. Клиент может ответить любым пакетом, но если мастер не получил никакого отклика, он переходит в состояние paging или inquiry. Клиент может подключиться и к другой пикосети, для чего в текущей сети он может сделать запрос перехода в режим park или hold. В режиме sniff клиент имеет несколько свободных временных слотов, чтобы участвовать в обменах с соседними сетями. Терминал, находящийся вне зоны связи, должен пребывать в состоянии page mode. Шлюз-сервер должен выделять достаточно ресурсов для запросов page scanning.

Спецификация Bluetooth v1.1 определяет 13 типов поддерживаемых приложений, которые называются **профилями**. Существует также 12 дополнительных профилей. Профили работают на самом верху иерархии слоев протокола (табл. 6). По существу профили являются регламентациями прикладного уровня.

Таблица 6

Основные и дополнительные профили Bluetooth

N	Название	Описание
Основные профили		
1	GAP (Generic Access Profile)	Процедура управления связью
2	SDAP (Service Discovery Application Profile)	Протокол определения предлагаемых сервисов
3	CTP (Cordless Telephony Profile)	Профиль беспроводной телефонии
4	GOEP (Generic Object Exchange Profile)	Протокол операций клиент-сервер при работе с объектами (обмен данными). Клиентская станция инициирует обмен, но она может выполнять и роль сервера
5	LAP (LAN Access Profile)	Протокол связи мобильной ЭВМ со стационарной LAN
6	DNP (Dial-up Networking Profile)	Протокол связи ЭВМ с сетью посредством мобильного телефона
7	FP (Fax Profile)	Протокол связи мобильного факса с мобильным телефоном
8	SPP (Serial Port Profile)	Профиль для работы с последовательным портом
9	IP (Intercom Profile)	Мобильные телефоны могут работать как переносные цифровые рации
10	HS (Headset Profile)	Протокол связи устройства hands-free с мобильным телефоном
11	OPP (Object Push Profile)	Протокол пересылки простых объектов
12	FTP (File Transfer Profile)	Протокол пересылки файлов
13	SP (Synchronization Profile)	Протокол синхронизации PDA с другой ЭВМ

Окончание табл. 6

N	Название	Описание
Дополнительные профили		
1	ESDP (Extended Service Discovery Profile)	Профиль для реализации процедур Plug and Play
2	A2DR (Advanced Audio Distribution Profile)	Продвинутый профиль рассылки аудиоданных
3	AVRCD (Audio Video Remote Control Profile)	Аудиовидеопрофиль удаленного управления
4	BIP (Basic Imaging Profile)	Базовый профиль работы с изображением
5	BPP (Basic Printing Profile)	Базовый профиль для печати
6	CIP (Common ISDN Access Profile)	Общий профиль доступа к ISDN
7	GAVDP (Generic Audio Video Distribution Profile)	Общий профиль рассылки аудио- и видеоданных
8	HFR (Hands-Free Profile)	Профиль для освобождения рук (hands-free)
9	HCRP (Hardcopy Cable Replacement Profile)	Протокол замены приборного связного кабеля
10	HID (Human Interface Device Profile)	Профиль для реализации интерфейса с человеком
11	PAN (Personal Area Networking)	Протокол формирования персональной сети
12	SAP (SIM Access Profile)	Протокол доступа к SIM

Профили 5–7 конкурируют с протоколом IEEE 802.11. Профиль удаленного доступа служит для подключения ЭВМ к мобильному телефону, снабженному модемом, без использования проводов. Профайл факс позволяет беспроводным факс-устройствам отсылать и получать факсы посредством мобильного телефона. Профили 8–10 имеют отношение к телефонии, в перспективе мобильный телефон и беспроводная трубка домашнего телефона станут взаимозаменяемыми. Профиль 10 представляет собой приложение, позволяющее устройствам hands-free держать связь с базой, что удобно, например, при езде в автомобиле. Профили 11–13 служат для пересылки объектов между беспроводными устройствами. Объектами могут быть изображения, информационные файлы и т. д.

Во главе семейства протоколов находится **SDP** (Service Description Protocol), предназначенный для определения услуг, оказываемых удаленным устройствам. С помощью команд данного протокола можно считать данные из локальной БД и определить характеристики удаленного устройства и на основе этой информации выяснить параметры оказываемых услуг. SDP использует модель запрос/отклик, где каждая транзакция включает в себя один запрос и один отклик. С помощью посылки одиночного SDP-пакета можно осуществлять простое управление информационным потоком. Такой пакет может не сопровождаться откликом.

Поле данных пакета SDP имеет заголовок, содержащий три поля:

- **PDU ID** – идентификатор типа поля данных (1 байт);
- **TransactionID** – идентификатор транзакции (2 байта);
- **ParameterLength** – длина (в байтах) всех параметров в поле данных (2 байта).

Параметры могут содержать атрибут состояния продолжения (**continuation state**). Некоторые запросы могут потребовать такого большого отклика, который не поместится в одно поле данных. Тогда SDP-сервер генерирует частичный отклик с параметром состояния продолжения. Аналогичный атрибут должен присутствовать в очередном запросе клиента, требующего следующую порцию данных отклика. Такой запрос имеет только два поля: *InfoLength* (1 байт) и *Continuation Information* (InfoLength байт).

Сервис (service) является единственной сущностью (entity), которая предоставляет информацию для выполнения каких-либо действий. Сервис может реализоваваться аппаратно или программно. Информация о сервисах содержится в записях, которые представляют собой списки атрибутов.

Некоторые атрибуты являются общими для всех записей сервиса, но сервис-провайдеры могут определить свои собственные атрибуты услуг в зарезервированных полях.

Атрибут содержит два компонента: идентификатор (ID) и значение атрибута.

- ID атрибута представляет собой 16-битовое число без знака, которое должно быть уникальным для данной сервисной записи. Идентификатор определяет и семантику значения атрибута;
- значение атрибута представляет собой поле переменной длины, чей смысл определяется идентификатором и ассоциированным с ним классом записи услуг.

Различные виды сервиса группируются в классы. Все атрибуты, содержащиеся в записи сервиса, относятся к одному классу. Каждому классу

присвоен уникальный идентификатор UUID, который представляет собой 128-битовый код, но возможны и псевдонимы (16- и 32-битовой длины).

Клиент может, зная значение UUID, получить указатель на соответствующую запись сервиса. Можно провести поиск и по идентификатору класса.

Значение атрибута имеет вид информационного элемента, который содержит два поля: *заголовок* и *данные*. Заголовок включает в себя две части: *дескриптор типа* и *дескриптор размера* (табл. 7).

Таблица 7

Type Descriptor	5-битовый код, составляющий старшие разряды информационного элемента заголовка
Size Descriptor	3-битовый код индекса, за которым следует 0, 8, 16 или 32 бита. Индекс содержит младшие 3 бита информационного элемента заголовка

Взаимодействующие приборы в Bluetooth могут выполнять роль локального устройства (**LocDev**) или удаленного устройства (**RemDev**). LocDev – прибор, который может инициировать процедуру выявления доступной услуги. RemDev может быть любым прибором, который участвует в процессе выявления доступных услуг, посылая отклик на запрос LocDev. Кроме того, RemDev имеет базу данных сервисных записей.

Прежде чем два устройства Bluetooth начнут взаимодействовать, каждый из них должен:

- быть включенным и инициализированным. При инициализации может потребоваться PIN для формирования ключа соединения (link key);
- должно быть сформировано Bluetooth-соединение, которое может потребовать BD_ADDR других устройств;

Выявление услуг (Service Discovery) поддерживает следующие прикладные примитивы для взаимодействия с другими устройствами:

- serviceSearch;
- serviceBrowse;
- enumerateRemDev;
- terminatePrimitive.

Менеджер канала служит для аутентификации, установления и конфигурации соединения, а также шифрования. Данные управления укладываются в однослотовые кадры. Для транспортировки протокольных данных используются пакеты DM1 (в случае SCO – пакеты PM1). Заголовки этих пакетов содержат всегда 1 байт. Менеджер канала (LM) обнаруживает другие LM и взаимодействует с ними через протокол

LMP. Чтобы выполнить роль провайдера, LM использует ниже расположенный контроллер канала (LC). LMP-протокол регламентирует структуру управляющих данных (PDU). Приложение должно поддерживать часть типов PDU, остальные являются опционными.

Таблица 8

Обязательные типы PDU протокола LMP

Функция	Тип PDU	Описание
Изменение ключа канала	LMP_comb_key	Ключ канала получается из комбинационных ключей. Содержимое LMP_comb_key защищается с помощью операции XOR с привлечением текущего ключа канала
Изменение текущего ключа канала	LMP_temp_rand, LMP_temp_key, LMP_use_semi_permanent_key	Текущий ключ канала может быть полупостоянным или временным; может быть изменен временно, но изменение действует только на время сессии. Изменение временного ключа канала нужно, если пикосеть поддерживает шифрованные бродкасты
Запрос сдвига часов	LMP_clkoffset_req, LMP_clkoffset_res	Когда клиент получает FHS-пакет, вычисляется разность между показанием его часов и часов мастера, записанным в поле данных пакета. Мастер может запросить значение сдвига часов в любое время
Версия LMP	LMP_version_req, LMP_version_res	Уровень LMP поддерживает запросы версии LMP. Запрашиваемое устройство должно прислать отклик с тремя параметрами: VersNr (номер версии протокола), CompId (служит для отслеживания проблем на нижних протокольных уровнях) и Sub-VersNr (рекомендуется, чтобы фирма имела уникальное значение Sub-VersNr для каждого RF/BB/LM)

Продолжение табл. 8

Поддерживаемые возможности	LMP_feature_req, LMP_feature_res	Контроллер радио и канала может поддерживать только субнабор типов пакетов и возможностей. Устройство может не посылать никаких пакетов кроме ID, FHS, NULL, POLL, BM1 или DH1, прежде чем озаботится возможностями других устройств. После выполнения запроса возможностей может быть передана область перекрытия возможностей взаимодействующих устройств
Запрос имени	LMP_name_req, LMP_name_res	LMP поддерживает запрос имени другого устройства. Имя состоит максимум из 248 байтов (UTF-8)
Запрос разрыва	LMP_detach	Соединение может быть разорвано в любое время по запросу мастера или клиента. В сообщение включаются данные, поясняющие причину разрыва
Качество обслуживания	LMP_quality_of_service, LMP_quality_of_service_req	LM предоставляет возможности качества обслуживания. Интервал, который определяет максимальное время между последовательными передачами мастера и заданным клиентом, используется для обеспечения определенной полосы пропускания и RTT
Управление мультислотовыми пакетами	LMP_max_slot, LMP_max_slot_req	Число слотов, используемых устройством может быть ограничено. Устройство позволяет удаленному устройству использовать максимальное число слотов, послав ему значение LMP_max_slot
Управление каналом	LMP_supervision_timeout	Каждый канал имеет таймер, который используется для управления каналом. Этот таймер служит для детектирования потери связи при уходе устройства из зоны достигаемости, отказа источника питания или другой поломки. Процедура определяет значение таймаута

Окончание табл. 8

Установление соединения	LMP_host_connection_req, LMP_setup_complete	Если устройство желает установить соединение, включающее уровни выше LM, оно посылает LMP_host_connection_req. Когда партнер получает такое сообщение, он может принять или отвергнуть предлагаемое соединение, послав LMP_accepted или LMP_not_accepted
Режим проверки	LMP_test_activate, LMP_test_control	LMP имеет PDU для поддержки различных методов тестирования, которые используются на уровне radio и baseband
Обработка ошибок	LMP_not_accepted	Если LM получает PDU с нераспознанным кодом, он реагирует посылкой сообщения LMP_not_accepted

В протоколе Bluetooth определены 4 типа адресов: BD_ADDR, AM_ADDR, PM_ADDR и AR_ADDR (табл. 9)

Таблица 9

BD_ADDR	Каждому трансиверу Bluetooth присваивается уникальный 48-битовый адрес прибора. Он содержит 24-битовое поле **LAP**, 16-битовое поле **NAP** и 8-битовое поле **UAP**
AM_ADDR	3-битовый код определяет какой адрес будет рабочим, если клиентский узел пикосети является активным, иногда называется MAC-адресом модуля Bluetooth
PM_ADDR	8-битовый код, идентифицирующий пассивный узел пикосети. PM_ADDR является рабочим, пока подчиненный узел пикосети пассивен (parked)
AR_ADDR	Используется пассивным узлом пикосети (parked), чтобы определить полудомен slave-to-master в окне доступа, которое ему предназначено для отправки сообщений запросов доступа. Адрес является рабочим, пока подчиненный узел пассивен, и не обязательно является уникальным

В рамках протокола определена структура интерфейса HCI (Host Controller Interface). Этот интерфейс осуществляет интеграцию низкоуровневых интерфейсов baseband и программного обеспечения клиента. Спецификация поддерживает работу с интерфейсами RS232, UART и USB. HCI предлагает командный метод доступа к аппаратным воз-

можностям Bluetooth. Канальные команды HCI позволяют управлять канальным уровнем соединения с другими устройствами. В перечень входят команды менеджера канала (LM – Link Manager), предназначенные для обмена LMP-командами с удаленными устройствами. Данные для канала LM транспортируются кадрами DM. Команды HCI Policy используются для воздействия на локальный и удаленный LM. Команды Host Controller, Baseband, Informational и Status предоставляют доступ к различным регистрам интерфейса.

Эмуляция последовательных портов (в частности RS-232) посредством L2CAP осуществляется транспортным протоколом RFCOMM. Протокол базируется на стандарте ETSI TS 07.10. RFCOMM поддерживает до 60 одновременных соединений между приборами. Это могут быть модемы, принтеры или ЭВМ.

Транспортный уровень контроллера устройства обеспечивает обмен специфической HCI-информацией. Спецификация HCI определяет формат команд, событий и данных в рамках обмена между устройством и контроллером. Протокол HCI специфицирует 32 различного рода события (Inquiry Complete Event, Page Scan Repetition Mode Change Event и т. д.).

На рис. 15 показан формат заголовка кадра протокола Bluetooth. Структура заголовка регламентируется уровнем baseband.

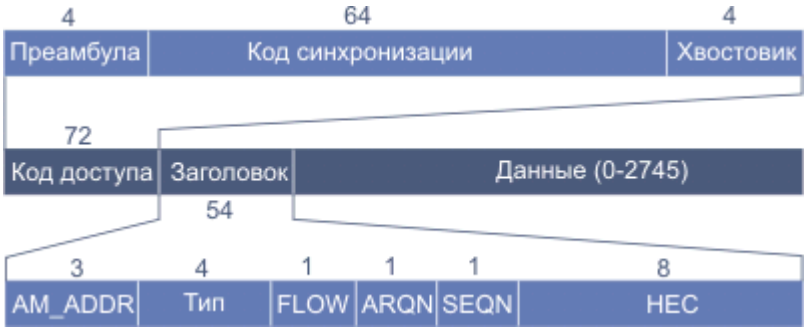


Рис. 15. Формат кадров Bluetooth

Предусмотрено три типа кодов доступа: **CAC** (Channel Access Code – код доступа к каналу), **DAC** (Device Access Code) и **IAC** (Inquiry Access Code). Код доступа к каналу CAC идентифицирует пикосеть, в то время как DAC используется для запросов соединения и для их откликов (paging). IAC служит для информационных запросов. Поле *код синхронизации* (64 бита) состоит из 24-битового адреса узла – инициатора соединения (paging). Алгоритм его вычисления обеспечивает достаточно большое расстояние Хэмминга между разными синхрокодами, что гарантирует невозможность перепутывния идентификаторов разных устройств даже в случае приема их с ошибками. Поле *хвостовик* служит для обеспечения балансировки сигнала по постоянному току и синхронизации. 8-битовый заголовок кадра повторяется

трижды (18 × 3 = 54 бита), содержит в себе флаги подтверждения и нумерации, а также средства управления потоком. Поле *адрес* (AM_ADDR – 3 бита) задает один из восьми узлов, которому предназначен кадр. Поле *тип* (4 бита) характеризует тип передаваемого кадра (ACL, SCO, опрос или пустой кадр), метод коррекции ошибок и число временных интервалов, из которых состоит кадр. Бит FLOW (поток) устанавливается подчиненным узлом и уведомляет о том, что его буфер заполнен. Бит ACK (подтверждение) указывает на подтверждение, посылаемое вместе с кадром. Если этот бит равен 1, предыдущий пакет успешно доставлен. Бит SEQN (последовательность) служит для нумерации кадров, что помогает обнаруживать повторные передачи. Для каждого очередного пакета этот бит инвертируется. Данный протокол предполагает ожидание, поэтому одного бита оказывается достаточно. Поле HEC представляет собой 8-битовую контрольную сумму. Принимающая сторона анализирует все три копии заголовка бит за битом. Значение бита определяется мажоритарной схемой (2 или 3 совпадающие бита из трех определяют истинное значение).

В кадрах ACL используются разные форматы данных. Возможны три варианта: 80, 160 и 240 бит. Оставшееся место используется для коррекции ошибок. По этой причине вариант с 80 битами самый надежный. При этом данные повторяются три раза (80 × 3 = 240). Фактически применяется тот же прием, что и в случае заголовка. Поле данных кадра SCO всегда имеет 240 бит. Так как подчиненные узлы могут использовать только нечетные временные домены, им достается 800 доменов в секунду, столько же получает и главный узел. При 80 битах данных в кадре подчиненный узел может передать 64 кбит/с. Этого вполне достаточно для для голосового обмена. При самом ненадежном варианте (240 бит данных на кадр) можно иметь три полнодуплексных голосовой связи. Это и ограничивает максимальное число SCO-соединений.

Существует 4 категории пакетов Bluetooth. К первой категории относятся пакеты, общие для всех видов соединений (NULL, POLL, FHS, DM1). Большинство типов пока не определены. ID-кадры имеют длину 64 бита и используются для пейджинга и запросов. NULL-кадры содержат поля лишь кода доступа и заголовка и используются для передачи подтверждений. Кадры POLL похожи на NULL, но требуют от получателя отклика. Пакеты рассматриваются как широковещательные в пикосети, если поле адреса имеет нулевое значение. Прием широковещательных кадров никогда не подтверждается, а для надежности они передаются несколько раз.

Кадры FHS содержат информацию об адресе, классе устройства и о тактовой частоте передатчика. Эти кадры используются при инициализации новой пикосети или при смене схемы переключения несущей частоты. К этой категории следует отнести и кадры DM1, транспортирующие

управляющую информацию. Для синхронных соединений определены несколько кадров, различающихся длиной, HV1, HV2 и HV3 с длинами поля данных 10, 20 и 30 байт соответственно. Тип кадров HV (High quality Voice) предназначен для трансляции голосовых потоков. Тип кадра DV предназначен для передачи как голоса, так и данных, и содержит 80 бит для голоса и 150 бит для данных. Блок данных защищается посредством CRC и в случае ошибки может пересылаться повторно.

Как и для всех радиосредств коммуникации, для Bluetooth проблема безопасности крайне актуальна. Безопасность протокола обеспечивается с помощью механизма аутентификации и шифрования передаваемых данных. Ключ авторизации имеет 128 бит. Длина ключа шифрования может лежать в пределах 8…128 бит. Кроме того, целям безопасности служат ключи соединения (link key), которые могут быть полупостоянными и временными. Первые хранятся в энергонезависимой памяти, вторые обновляются при каждом соединении. Устройство может генерировать свой ключ (unit key). Возможно формирование совместного ключа (combination key), при его вычислении используется информация от обоих участников будущего обмена. Особое место занимает мастер-ключ (master key), используемый для рассылки данных нескольким узлам одновременно, вместо текущего ключа соединения (current link key). Для выполнения аутентификации устройству нужно получить от партнера случайное число, сформировать на основе него и своего BD_ADDR некоторый код и отослать его партнеру, который проверяет его корректность. Если общий ключ не сгенерирован, формируется инициализационный ключ. Инициатор процедуры посылает партнеру случайное число, которое в сочетании с идентификатором BD_ADDR последнего образует инициализационный ключ.

8. СТАНДАРТ ZigBee

8.1. Спецификация стандарта IEEE 802.15.4 (ZigBee)

Стандарт ZigBee предназначен для объединения различных устройств в единую сеть для беспроводной передачи с них телеметрической информации и отправки к ним управляющих сигналов. Для этих целей можно пытаться использовать и стандарт Bluetooth, однако он не подходит для применения в широком масштабе. У ZigBee есть ряд преимуществ, прежде всего низкое энергопотребление, а также поддержка сложной ячеистой топологии самоорганизующейся сети, позволяющая передавать данные от узла к узлу разными маршрутами. К тому же в этой технологии повышенная дальность действия – сотни метров в условиях прямой видимости и десятки метров при нахождении в здании. Правда, высокая дальность «компенсируется» меньшей скоростью – 256 кбит/с, что делает эти сети пригодными только для передачи небольших объемов информации, например текстов или управляющих команд. Основная особенность технологии ZigBee™ заключается в том, что она поддерживает не только простые топологии беспроводной связи («точка-точка» и «звезда»), но и сложные беспроводные сети с ретрансляцией и маршрутизацией сообщений с ячеистой топологией при относительно невысоком энергопотреблении.

Что такое ZigBee?

ZigBee – технология, которая в настоящее время находит применение в беспроводных сенсорных сетях. Подобная сеть представляет собой инфраструктуру, состоящую из датчиков, вычислительных и коммуникационных элементов, которые позволяют осуществлять измерение параметров, наблюдать за ними и реагировать на происходящие события и явления в конкретной среде. Средой наблюдения могут быть физические объекты, биологические системы или ИТ-инфраструктуры. Сенсорные сети относятся к числу развивающихся технологий, которые уже в ближайшие годы могут получить широкое распространение. Аналитики считают, что количество поддерживающих технологию ZigBee сетевых узлов может увеличиться до 100 млн в 2008 году.

В течение нескольких лет производители применяли собственные «фирменные» технологии для сбора данных датчиков. После 2000 года они начали искать способы стандартизации решений. Разработчики вскоре отказались от использования с данной целью технологий WiFi из-за слишком большой сложности и дороговизны систем на их основе.

Технология Bluetooth также рассматривалась как возможный вариант, но и она оказалась довольно сложной.

Все это привело к появлению нового стандарта, IEEE 802.15.4, который рассчитан на работу в частотном диапазоне 2,4 ГГц, выделенном для промышленных, научных и медицинских приложений, и предусматривает передачу данных со скоростью до 256 кбит/с на расстояние около 60 м. Предполагается, что ZigBee станет международной спецификацией, регламентирующей создание надежных, недорогих, низкоэнергоемких беспроводных приложений, обеспечивая совместимость и требуемые характеристики радиочастотной производительности.

Сенсорные сети, которые действуют за пределами зданий, а также в протяженных географических зонах, могут использовать другие технологии беспроводной связи, например стандарт WiMAX (IEEE 802.16) в сетях масштаба города и сотовые технологии третьего поколения.

Области применения новой технологии – это беспроводные сети датчиков, системы автоматизации зданий, устройства автоматического считывания показаний счетчиков, охранные системы, системы управления в промышленности. Стандарт ZigBee будет незаменим для систем телеметрии, систем противопожарной безопасности, охранных систем автомобилей и недвижимости, для дистанционной диагностики и сбора информации, организации передачи данных, линий обмена информацией автоматизированных систем управления, а также для дистанционного управления. Модули, работающие в стандарте ZigBee, имеют две модификации: Xbee и XBee-PRO. Последние отличаются большей выходной мощностью и, соответственно, большим радиусом действия, превышающим 1200 м при распространении на открытом пространстве. Обе модели поддерживают топологии сети типа «точка-точка», «звезда», «кластерное дерево» и «многоячейковая сеть». Количество каналов на частоте 2,4 ГГц – 16. Модули являются полностью взаимозаменяемыми. Технология ZigBee находит применение также в таких областях, как:

- «умный дом»;
- медицинское, спортивное оборудование;
- активные RFID-метки;
- технология M2M.

Особенности сетей ZigBee

Сети ZigBee называют самоорганизующимися и самовосстанавливающимися сетями, т. к. ZigBee-устройства при включении питания, благодаря встроенному программному обеспечению, умеют сами находить

друг друга и формировать сеть, а в случае выхода из строя какого-либо из узлов умеют устанавливать новые маршруты для передачи сообщений.

Технология ZigBee имеет частотные каналы в диапазонах 868, 915 МГц и 2,4 ГГц. Наибольшие скорости передачи данных и наивысшая помехоустойчивость достигаются в диапазоне 2,4 ГГц, поэтому большинство производителей микросхем выпускают приемопередатчики именно для этого диапазона, в котором предусмотрено 16 частотных каналов с шагом 5 МГц. Скорость передачи данных вместе со служебной информацией в сетях ZigBee составляет 250 кбит/с. Радиус охвата приемопередатчиков ZigBee зависит от очень многих параметров, но в первую очередь – от чувствительности приемника и мощности передатчика. На открытом пространстве расстояние между узлами в сети ZigBee измеряется сотнями метров, а в помещении – десятками метров. При этом следует помнить, что зона покрытия сети ZigBee значительно больше, чем расстояние между узлами, т. к. за счет ретрансляции сообщений осуществляется наращивание сети.

Таблица 10

Спецификация стандарта IEEE 802.15.4

Стандарт	802.15.4 ZigBee™		
Частота	868 МГц	915 МГц	2,4 ГГц
Число каналов/шаг	1/–	10/2 МГц	16/5 МГц
География распространения	Европа	Америка	Весь мир
Макс. скорость, модуляция	20 кбит/с, BPSK	40 кбит/с, BPSK	250 кбит/с, O-QPSK
Выходная мощность, номинальная	0 dBm (1 мВт)	0 dBm (1 мВт)	0 dBm (1 мВт)
Дальность	10…100м		
Чувствительность (спецификация)	–92 dBm	–92 dBm	–85 dBm
Размер стека	4…32 кбайт		
Срок службы батареи	От 100 до 1000 и более дней		
Размер сети	65 536 (16-битные адреса), 264 (64-битные адреса)		

Стек протоколов ZigBee

Спецификация ZigBee™ регламентирует стек протоколов (рис. 16) сети, в котором протоколы верхних уровней используют сервисы, предоставляемые протоколами нижележащих уровней. В качестве двух нижних уровней (физического и уровня доступа к среде MAC) используется стандарт IEEE 802.15.4. MAC-уровень в сети ZigBee™ реализует механизм CSMA (прослушивания несущей и устранения коллизий), сетевой уровень

NWK отвечает за маршрутизацию сообщений, а уровень поддержки приложений APS обеспечивает интерфейс с уровнем приложения.

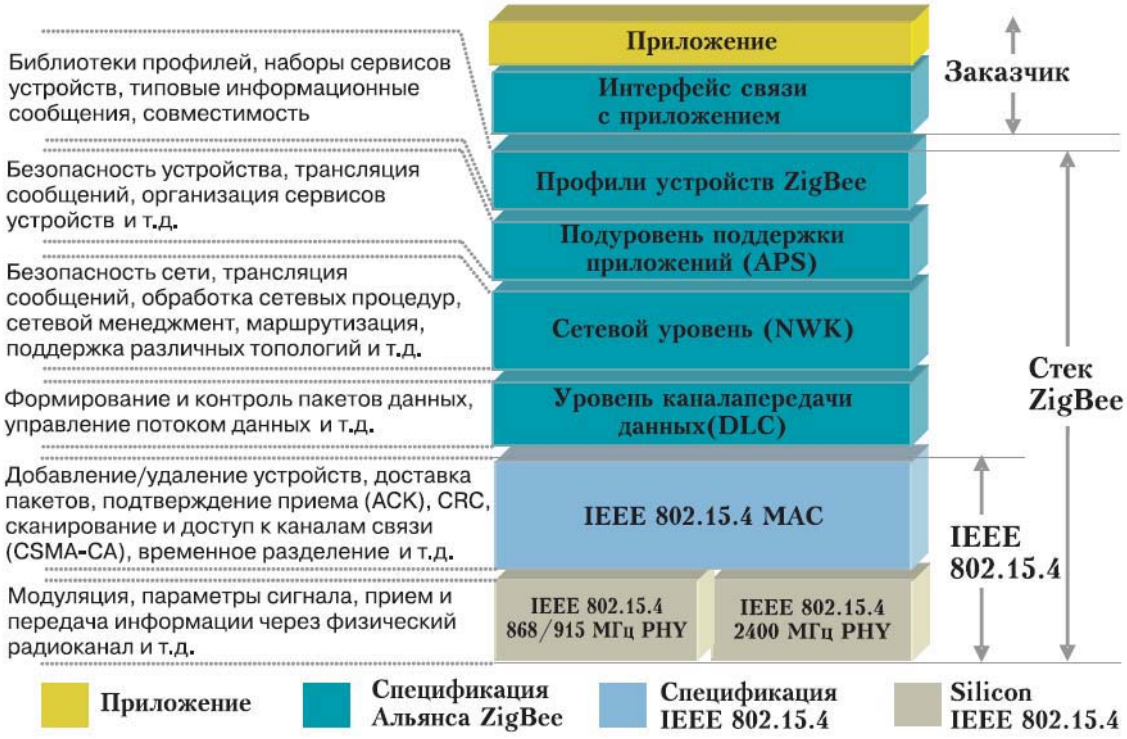


Рис. 16. Конфигурация стека протокола ZigBee

Совместимость устройств, профили, кластеры

Совокупность настроек программного обеспечения узлов сети, обеспечивающая их совместную работу, называется профилем. Различают профили стека и профили приложения. Если устройства совместимы на уровне стека, то они могут образовать единую сеть, обмениваться сообщениями, ретранслировать сообщения друг друга, но понимать смысл передаваемых сообщений могут только устройства, для которых эти сообщения предназначены. Например, лампочка может адекватно отреагировать на сообщение «включить/выключить» или «установить заданный уровень яркости», но не может понять команду «переключить номер канала», которую без проблем выполнит, например, интеллектуальный приемник или телевизионное устройство. Поэтому специалисты альянса ZigBee вводят классификацию типов устройств и для заданных групп устройств разрабатывают стандартные наборы сообщений – кластеры. Библиотека ZigBee-кластеров (ZigBee Cluster Library) группирует кластеры по функциональному признаку. Каждый профиль приложения включает кластеры из разных функциональных групп. На базе последней спецификации «ZigBee PRO Feature Set» в настоящее время опубликован стандартный профиль приложения «Home Automation», который рег-

ламентирует информационный обмен в сети ZigBee между такими устройствами, как осветительное оборудование, жалюзи, вентиляционные устройства, пульты дистанционного управления, устройства климат-контроля. Технология ZigBee/802.15.4 предоставляет разработчику несколько классов устройств: FFD-устройства-маршрутизаторы (Full Function Device – устройство с полным набором функций), устройства-координаторы (Coordinators – FFD с дополнительными системными ресурсами в зависимости от сложности сети) и RFD-оконечные устройства (Reduced Function Device – устройство с ограниченным набором функций). В каждой локальной сети ZigBee имеется только одно устройство-координатор. Основная задача координатора заключается в установке параметров и создании сети, выборе основного радиочастотного канала, в задании уникального сетевого идентификатора. При этом координатор является наиболее сложным из трех типов устройств, обладает наибольшим объемом памяти и повышенным энергопотреблением (питание от сети). Маршрутизаторы используются для расширения радиуса действия сети, поскольку способны выполнять функции ретрансляторов между устройствами, расположенными далеко друг от друга. Устройства поддерживают любую сетевую топологию ZigBee, могут выполнять функции координатора и обращаться ко всем узлам сети (FFD и RFD). Устройства с ограниченным набором функций не участвуют в маршрутизации, не могут выполнять функции координатора, обращаются только к координатору локальной сети (FFD-устройству), поддерживают соединения типа «точка–точка» и «звезда», играют роль оконечных сетевых узлов. На практике большинство узлов сети являются RFD-устройствами, а применение FFD-устройств и координаторов необходимо для образования мостов связи и соответствующей сетевой топологии. Как только маршрутизаторы и другие устройства подключаются к сети, они получают информацию о ней от координатора или любого уже задействованного в сети маршрутизатора и на основе этой информации устанавливают свои операционные параметры в соответствии с характеристиками сети. Маршрутизатор ZigBee получает таблицу сетевых адресов, которые он распределяет между подключившимися к сети оконечными устройствами. Устройство FFD использует древовидную адресацию при принятии решений о маршрутизации. Для повышения эффективности маршрутизации алгоритм ZigBee позволяет FFD-устройствам использовать сокращенную адресацию. Каждый маршрутизатор, на котором предполагается использовать сокращения, должен поддерживать таблицу, содержащую пары вида DN, где D – это адрес цели, а N – адрес следующего устройства на пути к этой цели. Сочетание маршрутизации по древовидному принципу и на основе таблицы обеспечивает гибкость работы и предоставляет разработчикам выбор оптимального соотношения цена/производительность. В зависимости от типа каждое устройство имеет определенные сетевые функции:

- координатор сканирует сеть и определяет свободные каналы для организации сети;
- маршрутизатор (FFD) сканирует сеть, находит активные каналы и пытается войти в состав существующей сети либо создает собственную персональную сеть на правах координатора, если нет активных каналов или не произошло объединение с активной сетью. Если произошло объединение, согласно правилам уже существующей сети, координатор примыкающей локальной сети переводится в ранг маршрутизатора и передает всю информацию о локальной сети координатору существующей сети. Из сигнального пакета синхронизации от координатора новообразованный маршрутизатор получает необходимую информацию о временных параметрах сети для обнаружения последующих сигнальных пакетов (см. рис. 16);
- оконченое RFD-устройство всегда пытается войти в существующую сеть.

На рис. 17 представлены различные варианты топологии сетей ZigBee. Соединения типа «точка–точка» и «звезда» подходят для самых простых приложений, обладают минимальной стоимостью, максимально низким энергопотреблением и позволяют использовать стратегию стандартного множественного доступа. В каждой сети с топологией «звезда» имеется один координатор сети, но при этом могут быть и другие полнофункциональные оконечные устройства (FFD), которые являются подчиненными по отношению к координатору.

Топология «кластерное дерево» обеспечивает масштабируемость сети и расширение зоны покрытия, не требуя дополнительных затрат на инфраструктуру. На рис. 17 показана такая топология, включающая в себя только основу дерева. Сеть типа «кластерное дерево» может включать в себя несколько подсетей с топологией «звезда» и устройствами с ограниченными функциями (RFD). Помимо топологий типа «звезда» и «кластерное дерево» технология ZigBee поддерживает многоячейковый принцип построения сетей. При такой топологии любой сетевой узел может выполнять также функции маршрутизатора для других устройств в сети. Если возникло препятствие на пути сигнала от одного узла к другому (бетонная или металлическая преграда и т. п.), выбирается альтернативный маршрут для передачи данных адресату. Более плотная концентрация сетевых узлов приводит к более защищенной, надежной системе. Если один из узлов вышел из строя, маршрут автоматически определяется через другие узлы сети и в результате сеть становится самовосстанавливающейся. Однако в многоячейковой сети срок службы автономных источников питания уменьшается за счет применения метода синхронизованного доступа, увеличивается сложность определения каналов передачи и происходит задержка (десятки миллисекунд) при каждой пересылке сообщения сетевым узлам.

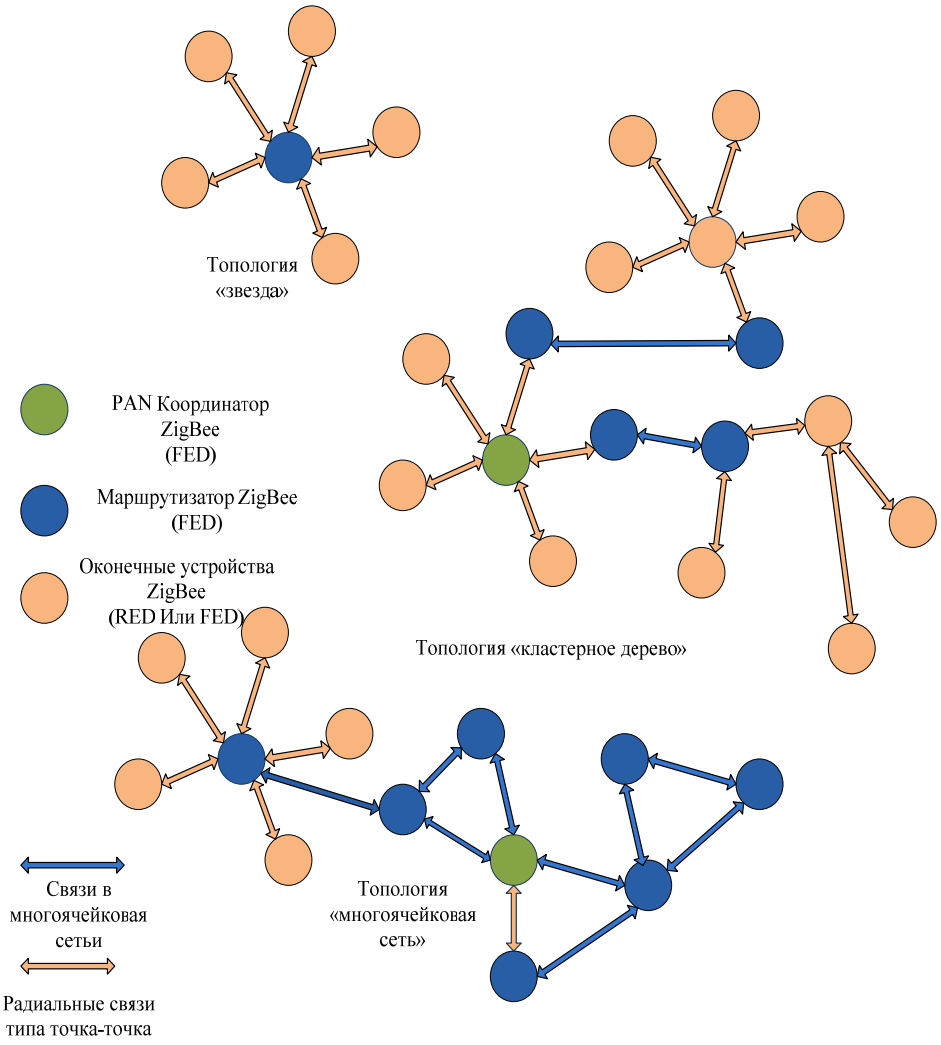


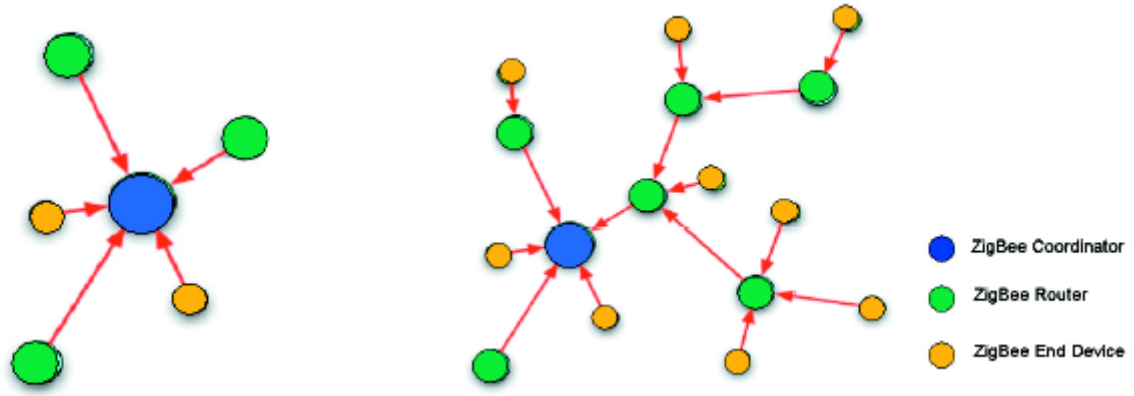
Рис. 17. Варианты топологии сетей ZigBee

Все узлы многоячейковой сети способны обнаруживать другие узлы и, распознав друг друга, вычислять оптимальный путь передачи пакетов, максимальную скорость обмена, частоту возникновения ошибок и время ожидания. Рассчитанные значения передаются соседним узлам, а оптимальный путь передачи трафика выбирается исходя из мощности принимаемых сигналов. Процессы обнаружения узлов и выбора пути идут постоянно, поэтому каждый узел поддерживает текущий 802.15.4.

Создание и расширение сетей

В разработанных версиях протоколов ZigBee закреплены механизмы создания и расширения одной PAN и не рассматриваются механизмы создания сетей путем объединения разных PAN. Этот факт отмечен термином intraPAN. На рис.18 приведена сложная топология сети из устройств ZigBee, иллюстрирующая их свойства. Сеть ZigBee включает три типа ло-

гических устройств: координатор ZigBee, маршрутизатор ZigBee и оконечное устройство ZigBee. Координатор ZigBee (ZigBeeCoordinator, ZC) является координатором PAN. Функции, выполняемые ZC, зависят от топологии сети. Маршрутизатор ZigBee (ZigBeeRouter) – полнофункциональное устройство стандарта IEEE 802.15.4, которое не является координатором ZigBee, однако может быть координатором стандарта 802.15.4 и маршрутизатором сообщений между устройствами ZigBee и устройством, присоединяющим новые устройства к сети. Оконечное устройство (ZigBeeEnd Device, ZED) – любое устройство стандарта IEEE 802.15.4 (RFD иFFD), не являющееся ни координатором ZigBee, ни маршрутизатором ZigBee. Пример присоединения сетевых устройств ZigBee к сети приведен на рис. 18. Присоединение производится по принципу: родительское устройство присоединяет (на что указывает входящая стрелка) дочернее. На рис. 18, *а* родительским устройством является координатор ZigBee. На рис. 18, *б* присоединенные к сети маршрутизаторы ZigBee присоединяют новые сетевые устройства. В результате образуется адресная иерархия из родителей и детей. Эта иерархия в дальнейшем может быть использована маршрутизаторами ZigBee при доставке данных по сети. Этот алгоритм в протоколах ZigBee реализован процедурами языка XML.



а *б*

Рис. 18. Присоединение новых сетевых узлов к маршрутизатору ZigBee

Терминология сетей ZigBee

ZigBee Coordinator *– координатор PAN стандарта IEEE 802.15.4.*

ZigBee Router *– полнофункциональное устройство стандарта IEEE 802.15.4, которое не является координатором ZigBee, однако может быть координатором стандарта IEEE 802.15.4 внутри своей области радиодоступа и маршрутизатором сообщений между устройствами в сети ZigBee.*

Zig Bee End Device *– любое устройство стандарта IEEE 802.15.4, не являющееся ни координатором ZigBee, ни маршрутизатором ZigBee.*

9. УПРАВЛЕНИЕ БЕСПРОВОДНЫМИ СЕТЯМИ

Управление беспроводными сетями включает в себя следующее:

- радиочастотное планирование;
- установления политик безопасности;
- оптимизация сети;
- устранение неполадок;
- отслеживание пользователей;
- конфигурирование и управление беспроводными сетями.

Существует ряд программных продуктов для управления корпоративными беспроводными сетями, включая описание способов базового управления такими сетями – CiscoWorks Wireless LAN Solutions Engine (WLSE) и расширенного управления с использованием Cisco Wireless Control System (WCS).

Существует ряд программных продуктов других фирм, но основными являются данные.

Система управления беспроводными сетями Cisco Wireless Control System

Cisco Wireless Control System (WCS) является лидером в области планирования, конфигурирования и управления беспроводными сетями, а также предоставляет мощные средства, позволяющие проектировать и централизованно осуществлять мониторинг, что существенно снижает показатель общей стоимости владения. Cisco WCS, вообще говоря, является опциональным сетевым компонентом, который работает с беспроводными точками Cisco Aironet 1000 и контроллерами беспроводного доступа. Cisco WCS предоставляет администраторам единое решение для радиочастотного планирования, установления политик безопасности, оптимизации сети, устранения неполадок, отслеживания пользователей и управления беспроводной сетью. Графический интерфейс упрощает и ускоряет процесс настройки, а детальные коментарии и автоматические отчеты делают использование Cisco WCS еще более удобным. Кроме всего вышеперечисленного, Cisco WCS содержит дополнительные инструменты по определению местоположения активных радиообъектов, а также интегрированную систему предотвращения атак. Это самостоятельные продукты серии CiscoWorks.

CiscoWorks – это полномасштабное программное средство сетевого управления, в котором предусмотрены все возможности, необходимые для управления сетью малого предприятия, предприятия средних размеров или рабочей группы предприятия большого размера.

Серия программных продуктов CiscoWorks делится на два типа:

1. Решения CiscoWorks, представляющие собой набор полномасштабных решений для средних и больших сетей (enterprise).

Эти решения фокусируются на трех основных областях: управление глобальными сетями (WAN), управление локальными сетями (LAN) и управление на уровне предоставления услуг. Для предоставления законченных (end-to-end) решений в этих областях Cisco предлагает следующие наборы программных продуктов:

- CiscoWorks LAN Management Solution (LMS) – решение для управления локальными коммутируемыми сетями;
- CiscoWorks Routed WAN Management Solution (RWAN) – решение для управления маршрутизируемыми территориальными сетями;
- CiscoWorks Small Network Management Solution (SNMS) – решение для управления локальными сетями небольшого размера;
- CiscoWorks VPN / Security Management Solution (VMS) – решение для управления системой сетевой безопасности;
- CiscoWorks IP Telephony Environment Monitor (ITEM) – решение для управления мультисервисными сетями, поддерживающее Cisco IP Telephony и приложения IP-телефонии.

2. Самостоятельные продукты серии CiscoWorks (WLSE, WCS и т. д.).

Средства управления сетями

Процесс управления сетью требует наличия соответствующих инструментов и возможностей. В данном пособии мы будем в основном рассматривать средства управления беспроводных сетей фирмы Cisco – безусловного лидера на рынке сетевых устройств и средств управления ими. Операционная система Cisco IOS, являющаяся встроенным компонентом маршрутизаторов, коммутаторов и точек доступа, включает в себя функциональность, необходимую для эффективного управления сетью, в том числе:

Инструменты удаленной настройки, отладки и мониторинга:

- интерфейс командной строки Cisco IOS обеспечивает доступ ко всем инструментам управления;
- поддержка протоколов Telnet, SSH, HTTP и HTTPS;
- удобные встроенные инструменты удаленного web-управления SDM, CRWS, CMS;
- поддержка протокола SNMP версий 1, 2 и 3;
- поддержка функциональности RMON;
- поддержка протокола NTP (Network Time Protocol).

Cisco IOS хранится, как правило, в ПЗУ (постоянном запоминающем устройстве), расположенном на системной плате устройства.

Интерфейс командной строки Cisco IOS до недавнего времени был единственным и остается основным инструментом настройки точек доступа, маршрутизаторов и коммутаторов фирмы Cisco. Для работы с интерфейсом командной строки Cisco IOS используется специальный порт «Console» на корпусе точки доступа и программа Hyper Terminal, входящая в состав любой операционной системы Windows. Но работа с интерфейсом командной строки Cisco IOS требует специальных знаний и опыта, поэтому мы остановимся на более современном, Web-инструменте Cisco Router and Security Device Manager (SDM).

Cisco Router and Security Device Manager

Менеджер маршрутизаторов и устройств безопасности Cisco (SDM) – это Web-инструмент управления устройствами для маршрутизаторов и точек доступа Cisco, который способствует производительной работе администраторов сетей, упрощает развертывание точек доступа и помогает устранять проблемы в работе сетей и в установлении VPN-соединений. Cisco SDM поддерживает широкий спектр программного обеспечения Cisco IOS и доступен бесплатно на маршрутизаторах Cisco, от серии Cisco 830 до 7301. Cisco SDM инсталлируется на предприятии-изготовителе на всех новых маршрутизаторах с интегрированными сервисами серии Cisco 850, 870, 1800, 2800 и 3800 и точке доступа Cisco 1310. Администраторы сетей и систем безопасности, бизнес-партнеры Cisco могут использовать Cisco SDM с целью более простого и быстрого развертывания маршрутизаторов и точек доступа Cisco для использования интегрированных сервисов, в частности динамической маршрутизации, доступа к WAN, WLAN, межсетевых экранов, VPN, SSL VPN, IPS и QoS. Типичный фрагмент беспроводной сети на основе точек доступа фирмы Cisco представлен на рис. 19.

На рис. 20 представлен пример домашней страницы точки доступа Cisco Aironet 1300, слева – основное меню параметров настройки:

- EXPRESS SET-UP – быстрая настройка основных параметров точки доступа.
- EXPRESS SECURITY – быстрая настройка основных параметров безопасности точки доступа.
- NETWORK INTERFACES – состояние сетевых интерфейсов и их тип.

На поле слева выведены основные параметры точки доступа:

- IP-адрес, MAK-адрес, активные интерфейсы и т. д.

Существует ряд прогаммных продуктов позволяющих осуществлять мониторинг беспроводных систем, их планирование и проектирование. К ним относится, например, набор программных продуктов – AIRMAGNET Laptop анализатор, AirMagnet Laptop архитектура.

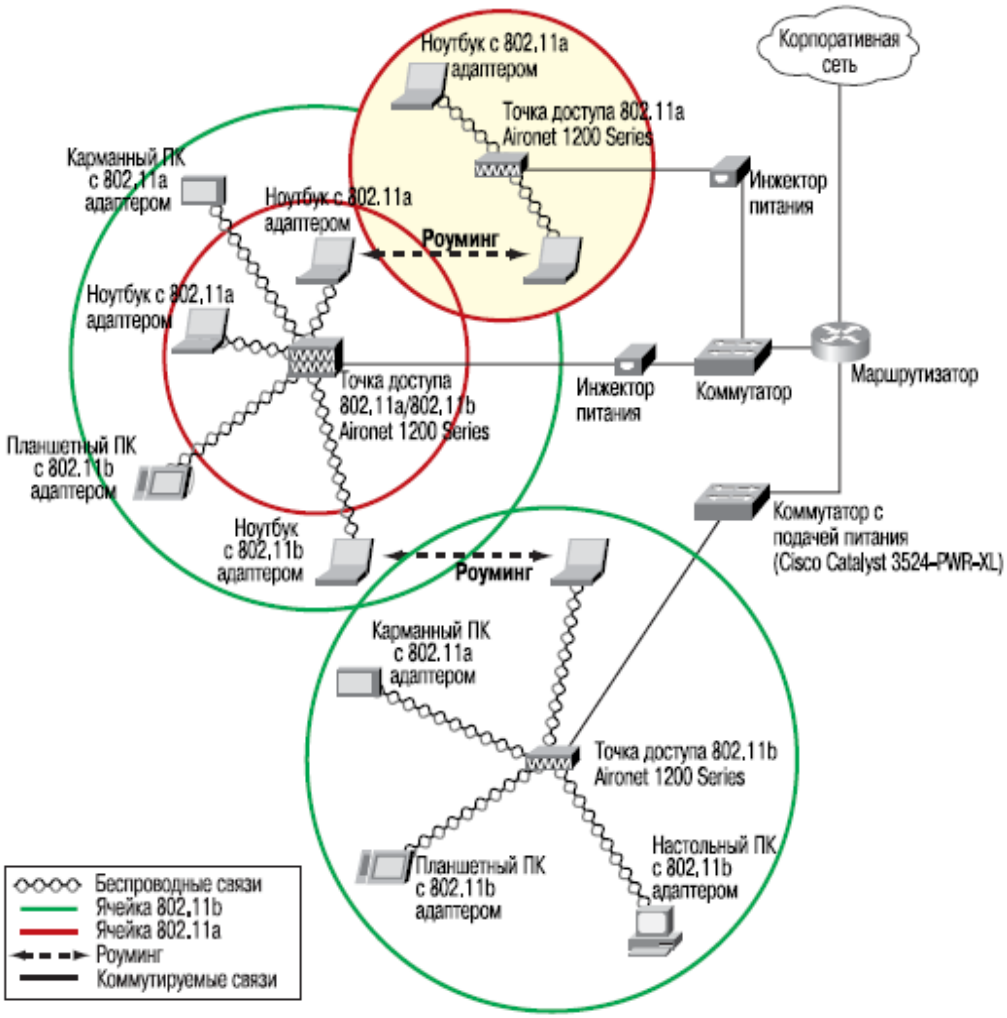


Рис. 19. Роуминг в беспроводной сети

AirMagnet Laptop product включает административные инструменты в следующих областях:

- надежность управления;
- производительность управления;
- обзор инсталляции;
- поиск неисправностей;
- администрирование беспроводного доступа.

AirMagnet Laptop архитектура

Аналитическое приложение. Анализатор снабжен AirWise, запатентованной компанией аналитической машиной, которая помогает профессионалам быть в курсе всех событий на сети. AirWise работает постоянно, собирая статистику на сети, идентифицируя и отслеживая отличительные характеристики беспроводного оборудования, осуществляя мониторинг и анализ WLAN-проблем и предлагая потенциальные решения.

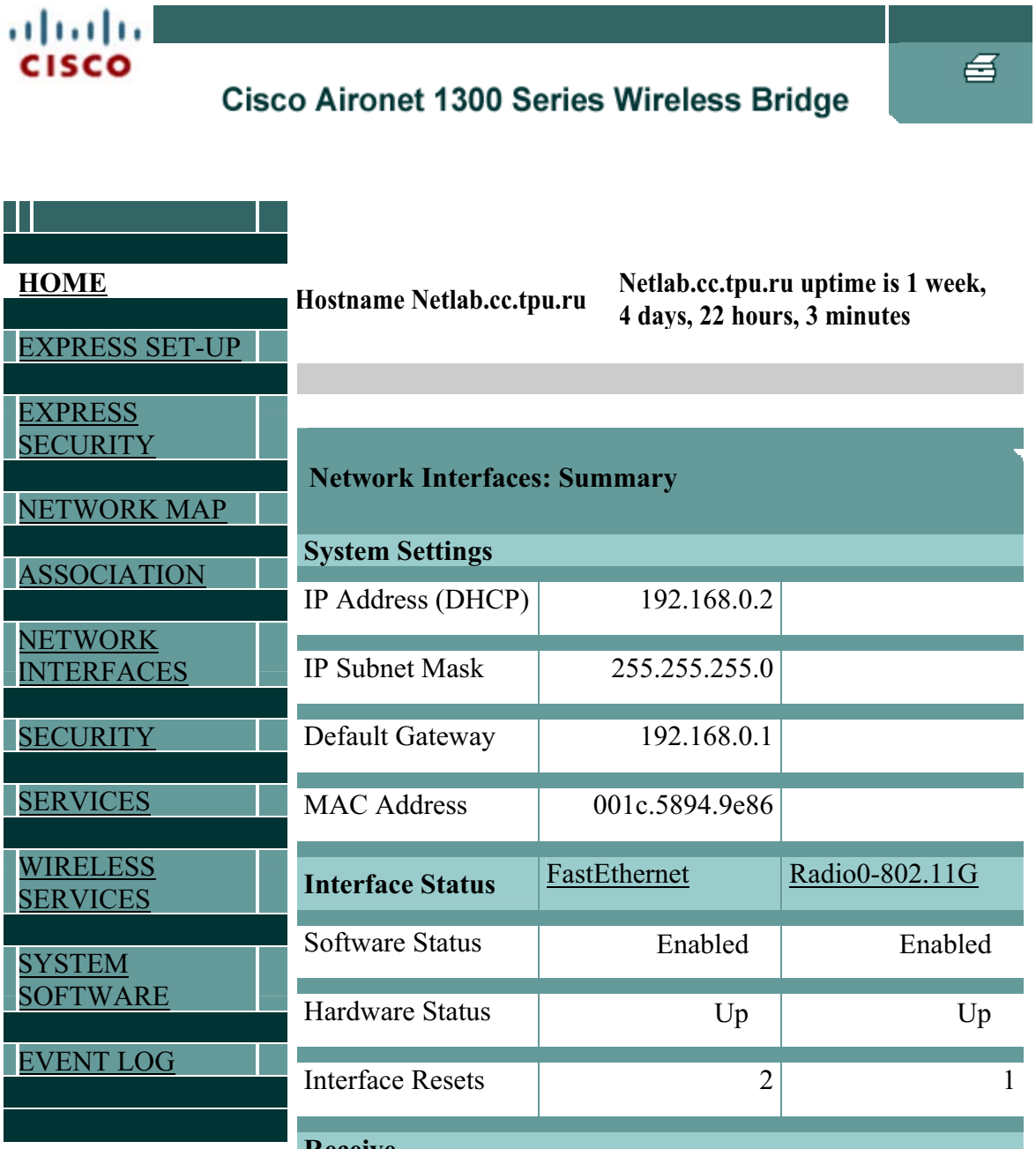


Рис. 20. Домашняя страница точки доступа Cisco Aironet 1300

10. БЕЗОПАСНОСТЬ В БЕСПРОВОДНЫХ СЕТЯХ

Проблема обеспечения безопасности – одна из основных при построении беспроводных сетей.

Стандарт 802.11 предусматривает три средства защиты беспроводных сетей:

- контроль доступа по имени сети (ESSID). Используется уникальный код ESSID, который идентифицирует сеть. Клиентские устройства должны использовать корректный ESSID для доступа к своей беспроводной сети;
- контроль доступа по MAC-адресам в беспроводной сети. На точке доступа задается список MAC-адресов, которым разрешена или запрещена авторизация;
- шифрование трафика по протоколу WEP. Шифрование использует алгоритм RC4 с длиной ключа 64 и 128 bit (в нынешних моделях беспроводных устройств также 152 bit).

Эти средства нельзя считать очень надежными, исследования выявили уязвимости протокола WEP. В случаях, когда требуется обеспечить надежную защиту передаваемых по радиоканалу данных, следует применять оборудование, которое поддерживает протоколы IEEE 802.1x и WPA.

Протокол VPA (WiFi Protected Access)

Протокол WPA (WiFi Protected Access) реализует преимущества шифрования при помощи протокола целостности временных ключей (Temporal Key Integrity Protocol – TKIP). Аутентификация пользователей производится при помощи 802.1x и EAP. WPA предусматривает совместимость с будущим протоколом безопасности беспроводных сетей 802.11i. При использовании WPA в малых сетях имеется возможность обойтись без настройки сервера RADIUS – режим Pre-Shared Key (PSK), позволяющий задавать ключи вручную. Протоколы 802.1x и WPA являются весьма надежными, сообщений об их взломах не поступало.

Серверы RADIUS

Серверы RADIUS получили широкое распространение в системах безопасности стандарта IEEE 802.1x, поскольку многие крупные предприятия применяют их для контроля коммутируемого доступа к своим сетям. Этот сервер избавляет от необходимости хранить информацию о пользователях в каждой точке доступа или в каждом сетевом коммута-

торе. Кроме того, чтобы повысить надежность работы системы сетевой безопасности, можно установить резервный сервер RADIUS, который будет аутентифицировать пользователей в случае отказа основного сервера. Сервер RADIUS поддерживает большинство используемых с протоколом EAP алгоритмов аутентификации, в том числе TLS, TTLS, LEAP, MD5 и PEAP, сервер также может быть встроенным в точку доступа и доступен с помощью SDM.

Для защиты небольшой беспроводной сети, где не имеет смысла устанавливать сервер RADIUS, администратор может использовать разделяемый ключ, информация о котором вводится в клиентское беспроводное устройство и точку доступа вручную – SSID Manager. Последняя создает WEP-ключ и отсылает его клиентскому устройству, предварительно зашифровав с помощью разделяемого ключа.

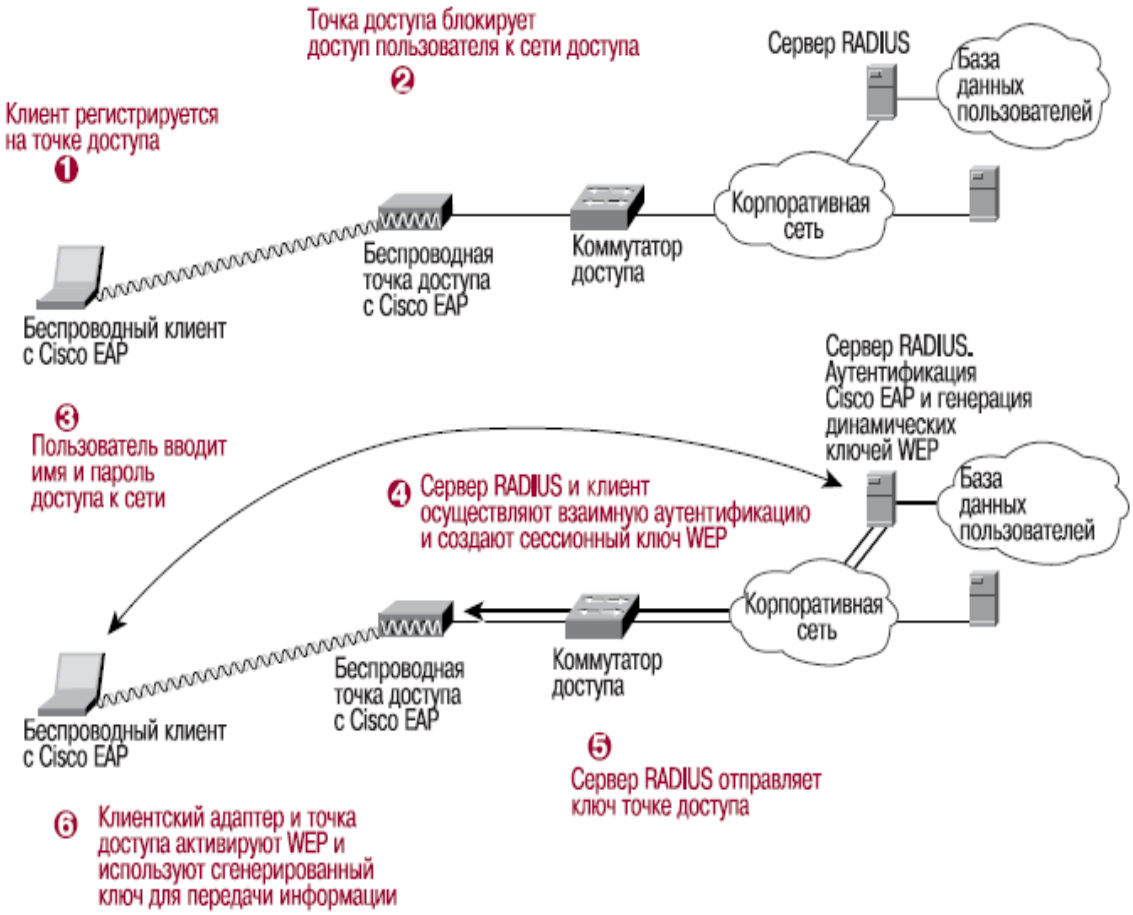


Рис. 21. Реализация архитектуры Cisco 802.1 для WiFi-сетей

Заключение

Дальнейшие развитие беспроводных сетей пойдет по трем основным направлениям:

- развитие на основе стандарта 802.16, в том числе оснащение адаптерами для подключения к данным сетям мобильных платформ – ноутбуков и КПК;
- повсеместное внедрение стандартов 3G и 4G;
- стандарт ZigBee, возможно, станет одним из основных компонентов домашних сетей.

Но говорить о полном переходе на беспроводные сети, пожалуй, преждевременно. Базовыми технологиями в обозримом будущем останутся сети на основе витой пары и оптоволокна. Исключением, пожалуй, будет технология 4G.

Список условных сокращений и обозначений

ACL	(access control list) – список контроля доступа.
ATM	(asynchronous transfer mode) – асинхронный режим передачи.
DHCP	(Dynamic Host Configuration Protocol) – протокол динамической конфигурации хоста.
DSCP	(differentiated services code point) – код предоставляемых дифференцированных услуг.
DSP	(digital signal processing) – цифровая обработка сигналов.
EIGRP	(Enhanced Interior Gateway Routing Protocol) – расширенный протокол внутренней маршрутизации.
IGMP	(Internet Group Management Protocol) – межсетевой протокол управления группами.
IPsec	протокол IP-Security.
ISDN	(integrated services digital network) – цифровая сеть с интеграцией служб.
OSPF	(Open Shortest Path First) – протокол предпочтения кратчайших маршрутов.
PBX	(private branch exchange) – телефонная система для частного использования.
PoE	(power over Ethernet) – технология питания сетевых устройств по кабелю Ethernet.
PRI	(primary rate interface) – первичный интерфейс обмена.
PSTN	(public switched telephone network) – коммутируемая сеть общего пользования.
QoS	(Quality of Service) – качество обслуживания.
RADIUS	(Remote Authentication Dial In User Service) – протокол аутентификации удаленных пользователей.
RIP	(Routing Information Protocol) – протокол маршрутной информации.
SIP	(Session Initiation Protocol) – протокол установки соединения.
SSID	(service set identifier) – идентификатор сети.
TDM	(time – division multiplexing) – мультиплексная передача с разделением каналов по времени.
VoIP	(Voice over Internet Protocol) – передача голоса по интернет-протоколу, IP-телефония.
VPN	(virtual private network) – виртуальная частная сеть.
WLAN	(wireless LAN) – беспроводная локальная вычислительная сеть.
WiFi	(wireless fidelity) – стандарт WiFi (беспроводная точность).

Список литературы

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб: Питер, 2006.
2. Семенов Ю.А. Сети IEEE 802.11. – М: Издательство ГНЦ ИТЭФ, 2007.
3. Олифер В.Г., Олифер Н.А. Основы сетей передачи данных: Курс лекций. М.: ИНТУИТ.РУ «Интернет-университет Информационных технологий», 2004.
4. Таненбаум Э. Компьютерные сети – СПб.: Питер, 2003
5. Варгаузин В. Сетевая технология ZigBee // Интернет-журнал по широкополосным сетям и мультимедийным технологиям, 2008. – Режим доступа: http://www.rphf.spbstu.ru/dsp/dsp.html
6. Compliance information for 2,4GHz Cisco Systems, Inc… 2004.
7. Cisco Aironet 1300 Series Wireless Bridge. Cisco Systems, Inc… 2004.

Учебное издание

МАРЧУКОВ Артур Викторович

БЕСПРОВОДНЫЕ ИНФОРМАЦИОННЫЕ СЕТИ

Учебное пособие

Научный редактор
доктор технических наук,
профессор В.А. Силич

Редактор *Д.В. Заремба*

Компьютерная верстка *Д.В. Сотникова*

Дизайн обложки *О.Ю. Аршинова*

Подписано к печати 28.12.2009. Формат 60×84/16. Бумага «Снегурочка».
Печать XEROX. Усл.печ.л. 4,88. Уч.-изд.л. 4,41.
Заказ 186-10. Тираж 200 экз.

Томский политехнический университет
Система менеджмента качества
Томского политехнического университета сертифицирована
NATIONAL QUALITY ASSURANCE по стандарту ISO 9001:2008

ИЗДАТЕЛЬСТВО ТПУ. 634050, г. Томск, пр. Ленина, 30.
Тел/факс: +7 (3822) 56-35-35, www.tpu.ru