СОДЕРЖАНИЕ

ВВЕДЕНИЕ

История беспроводных технологий передачи информации началась в конце XIX века с передачей первого радиосигнала и появлением в 20-х годах XX века первых радиоприемников с амплитудной модуляцией. В 30-е годы появилось радио с частотной модуляцией и телевидение. В 70-е годы созданы первые беспроводные телефонные системы как естественный итог удовлетворения потребности в мобильной передаче голоса. Сначала это были аналоговые сети, а начале 80-х был разработан стандарт GSM, ознаменовавший начало перехода на цифровые стандарты, как обеспечивающие лучшее распределение спектра, лучшее качество сигнала, лучшую безопасность. С 90-х годов XX века происходит укрепление позиций беспроводных сетей. Беспроводные технологии прочно входят в нашу жизнь. Развиваясь с огромной скоростью, они создают новые устройства и услуги.

Обилие новых беспроводных технологий таких, как CDMA (Code Division Multiple Access, технология с кодовым разделением каналов), GSM (Global for Mobile Communications, глобальная система для мобильных коммуникаций), TDMA (Time Division Multiple Access, множественный доступ с разделением во времени), 802.11, WAP (Wireless Application Protocol, протокол беспроводных технологий), 3G (третье поколение), GPRS (General Packet Radio Service, услуга пакетной передачи данных), Bluetooth (голубой зуб, по имени Харальда Голубого Зуба – предводителя викингов, жившего в X веке), EDGE (Enhanced Data Rates for GSM Evolution, увеличенная скорость передачи даны для GSM), i-mode и т.д. говорит о том, что начинается революция в этой области.

Весьма перспективно и развитие беспроводных локальных сетей (WLAN), Bluetooth (сети средних и коротких расстояний). Беспроводные сети развертываются в аэропортах, университетах, отелях, ресторанах, предприятиях. История разработки стандартов беспроводных сетей началась в 1990 году, когда был образован комитет 802.11 всемирной организацией IEEE (Институт инженеров по электричеству и электронике). Значительный импульс развитию беспроводных технологий дала Всемирная паутина и идея работы в Сети при помощи беспроводных устройств. В конце 90-х годов пользователям была предложена WAP-услуга, сначала не вызвавшая у населения большого интереса. Это были основные информационные услуги – новости, погода, всевозможные расписания и т.п. Также весьма низким спросом пользовались вначале и Bluetooth, и WLAN в основном из-за высокой стоимости этих средств связи. Однако по мере снижения цен рос и интерес населения. К середине первого десятилетия XXI века счет пользователей беспроводного Интернет – сервиса пошел на десятки миллионов. С появлением беспроводной Интернет - связи на первый план вышли вопросы обеспечения безопасности. Основные проблемы при использовании беспроводных сетей это перехват сообщений спецслужб, коммерческих предприятий и частных лиц, перехват номеров кредитных карточек, кража оплаченного времени соединения, вмешательство в работу коммуникационных центров. Эти проблемы решаются усовершенствованием стандартов связи.

Существенным для развития беспроводных технологий является и возможность их использования домашними пользователями. С ростом числа устройств в домашней сети все более актуальной становится проблема множества проводов, соединяющих эти устройства между собой. А это - уже повод для перехода на беспроводные технологии. Повышение степени комфортности современного дома, объединение в единое целое всех его структур и объектов (компьютеров, телевизоров, цифровых фотокамер, домашнего развлекательного центра, систем охраны, климатических систем, кухонных устройств и т.д.) - основа идеи создания интеллектуального цифрового дома – также реализуется с помощью беспроводных устройств.

Хотя насчитывается огромное число единичных пользователей наиболее быстрорастущим сегментом потребителей беспроводных технологий является

корпоративный. Беспроводная передача данных является важным стратегическим средством и обеспечивает рост производительности (сотрудники получают постоянный и быстрый доступ к корпоративной информации, они быстрее узнают новости), повышает качество обслуживания клиентов (можно мгновенно принимать жалобы и пожелания и мгновенно реагировать на них), создает конкурентные преимущества (повышение скорости обмена информацией и, следовательно, скорости принятия решения).

Ну а в будущем нас ждет беспроводной мир.

В нашей книге мы постарались рассмотреть теоретические и практические вопросы, связанные с созданием беспроводных сетей и устройствами, их реализующими.

ГЛАВА 1. ОРГАНИЗАЦИЯ БЕСПРОВОДНЫХ СЕТЕЙ

1.1 ЧТО ТАКОЕ WI-FI?

Это современная беспроводная технология соединения компьютеров в локальную сеть и подключения их к Интернету. Именно с помощью этой технологии Интернет становится мобильным и дает пользователю свободу перемещения как в пределах одной комнаты, так и по всему миру.

Представьте себе картину будущего. Вы пользуетесь вашим компьютером так же, как сейчас своим мобильным телефоном. Вам не нужны провода, вы можете взять свой ноутбук в любую точку Москвы и войти в Интернет практически отовсюду. Это – ближайшее будущее.

Под аббревиатурой Wi-Fi (от английского словосочетания Wireless Fidelity, которое можно дословно перевести как «высокая точность беспроводной передачи данных») в настоящее время развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам.

С увеличением числа мобильных пользователей возникает острая необходимость в оперативном осуществлении коммуникаций между ними, в обмене данными, в быстром получении информации. Поэтому естественным образом происходит интенсивное развитие технологий беспроводных коммуникаций, рынок которых на данный момент развивается быстрыми темпами. Особенно это актуально в отношении беспроводных сетей. Или так называемых WLAN-сетей (Wireless Local Area Network). Сети Wireless LAN – это беспроводные сети (вместо обычных проводов в них используются радиоволны). Установка таких сетей рекомендуется там, где развертывание кабельной системы невозможно или экономически нецелесообразно.

Беспроводные сети особенно целесообразны на предприятиях, где сотрудники активно перемещаются по территории во время рабочего дня с целью обслуживания клиентов или сбора информации (крупные склады, агентства, офисы продаж, учреждения здравоохранения и др.).

Благодаря функции роуминга между точками доступа пользователи могут перемещаться по территории покрытия сети Wi-Fi без разрыва соединения.

WLAN-сети имеют ряд преимуществ перед обычными кабельными сетями:

- 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 108 Мб/с), что позволяет их использовать для решения очень широкого спектра задач;
- WLAN-сеть может оказаться единственным выходом, если невозможна прокладка кабеля для обычной сети.

Вместе с тем необходимо помнить об ограничениях беспроводных сетей. Это, как правило, всё-таки меньшая скорость, подверженность влиянию помех и более сложная схема обеспечения безопасности передаваемой информации.

Сегмент Wi-Fi сети может использоваться как самостоятельная сеть, либо в составе более сложной сети, содержащей как беспроводные, так и обычные проводные сегменты. Wi-Fi сеть может использоваться:

- для беспроводного подключения пользователей к сети;
- для объединения пространственно разнесенных подсетей в одну общую сеть там, где кабельное соединение подсетей невозможно или нежелательно;
- для подключения к сетям провайдера интернет-услуги вместо использования выделенной проводной линии или обычного модемного соединения.

1.2 ОСНОВНЫЕ ЭЛЕМЕНТЫ СЕТИ

Для построения беспроводной сети используются Wi-Fi – адаптеры и точки доступа.

Адаптер (рис. 1.1) представляет собой устройство, подключающееся через слот расширения PCI, PCMCI, CompactFlash. Существуют также адаптеры с подключением через порт USB 2.0. Wi-Fi–адаптер выполняет ту же функцию, что и сетевая карта в проводной сети. Он служит для подключения компьютера пользователя к беспроводной сети. Благодаря платформе Centrino все современные ноутбуки имеют встроенные адаптеры Wi-Fi, которые совместимы со многими современными стандартами. Wi-Fi-адаптерами, как правило, снабжены и КПК (карманные персональные компьютеры), что также позволяет подключать их к беспроводным сетям.

Рис. 1.1 Адаптеры

Для доступа к беспроводной сети адаптер может устанавливать связь непосредственно с другими адаптерам. Такая сеть называется *беспроводной одноранговой сетью* или *Ad Hoc* (в переводе «к случаю»). Адаптер может также устанавливать связь через специальное устройство – *точку доступа*. Такой режим называется *инфраструктурой*.

Для выбора способа подключения адаптер должен быть настроен либо на использование Ad Hoc, либо инфраструктурного режима.

Точка доступа (рис. 1.2) представляет собой автономный модуль со встроенным микрокомпьютером и приемно-передающим устройством. Через точку доступа осуществляется взаимодействие и обмен информацией между беспроводными адаптерами, а также связь с проводным сегментом сети. Таким образом, точка доступа играет роль коммутатора.

Рис. 1.2 Точка доступа

Точка доступа имеет сетевой интерфейс (uplink port), при помощи которого эта точка может быть подключена к обычной проводной сети. Через этот же интерфейс может осуществляться и настройка точки.

Описание беспроводного оборудования можно найти в Приложении А.

Точка доступа может использоваться как для подключения к ней клиентов (базовый режим точки доступа), так и для взаимодействия с другими точками доступа для построения распределенной сети (Wireless Distributed System, WDS). Это режимы беспроводного моста «точка-точка» и «точка-много точек», беспроводный клиент и повторитель.

Доступ к сети обеспечивается путем передачи широковещательных сигналов через эфир. Принимающая станция может получать сигналы в диапазоне работы нескольких передающих станций. Станция-приемник использует идентификатор зоны обслуживания (service set indentifier, SSID) для фильтрации получаемых сигналов и выделения того, который ей нужен.

Зоной обслуживания (service set, SS) называются логически сгруппированные устройства, обеспечивающие подключение к беспроводной сети.

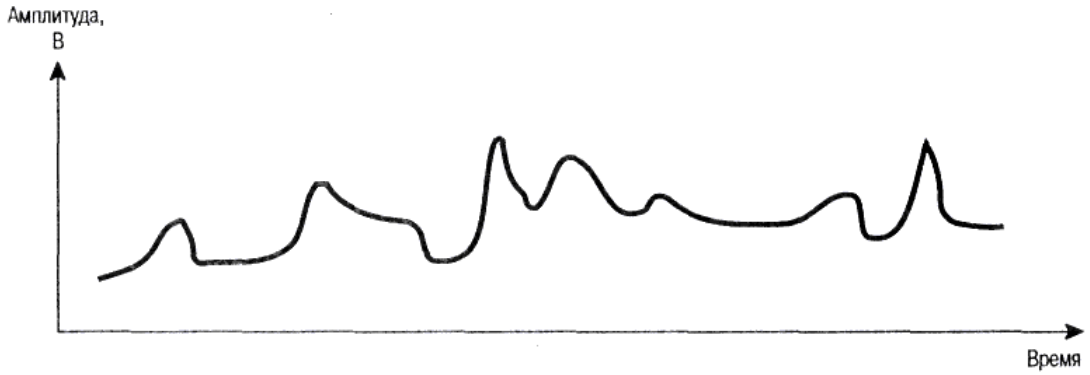
Базовая зона обслуживания (basic service set, BSS) – это группа станций, связывающихся одна с другой по беспроводной связи. Технология BSS предполагает наличие особой станции, которая называется *точкой доступа* (access point).

Для более подробного понимания работы беспроводных устройств обратимся к следующему разделу.

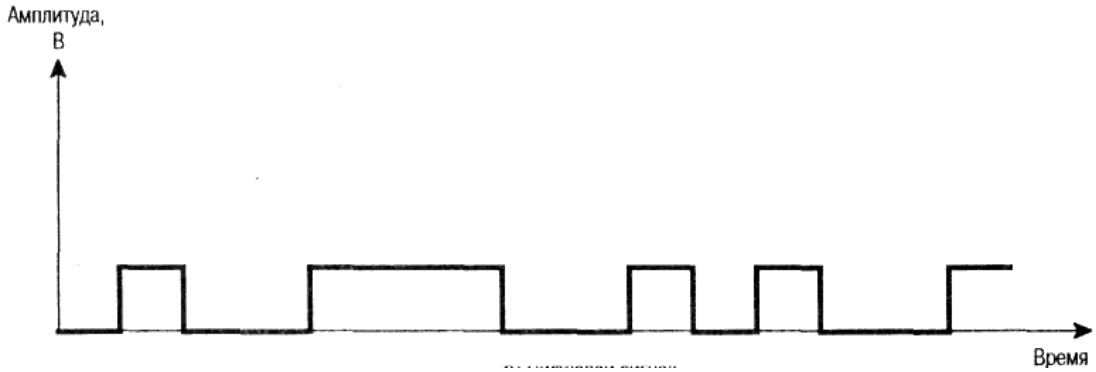
1.3 ОСНОВЫ ПЕРЕДАЧИ ДАННЫХ В БЕСПРОВОДНЫХ СЕТЯХ

1.3.1 СИГНАЛЫ ДЛЯ ПЕРЕДАЧИ ИНФОРМАЦИИ

Если рассматривать сигнал как функцию времени, то он может быть, либо аналоговым, либо цифровым. *Аналоговым* называется сигнал, интенсивность которого во времени изменяется постепенно. Другими словами, в сигнале не имеется пауз или разрывов. *Цифровым* называется сигнал, интенсивность которого в течение некоторого периода поддерживается на постоянном уровне, а затем изменяется также на постоянную величину (это определение идеализировано). На рис. 1.3 приведены примеры сигналов обоих типов. Аналоговый сигнал может представлять речь, а цифровой – набор двоичных единиц и нулей.



а) Аналоговый сигнал



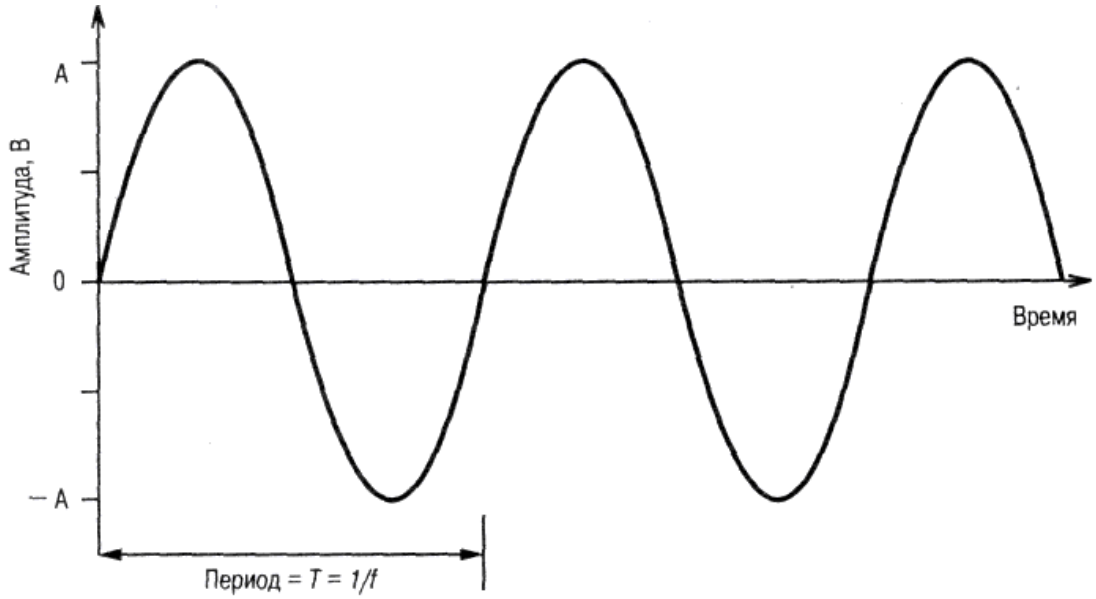
б) Цифровой сигнал

Рис. 1.3 Аналоговый и цифровой сигналы

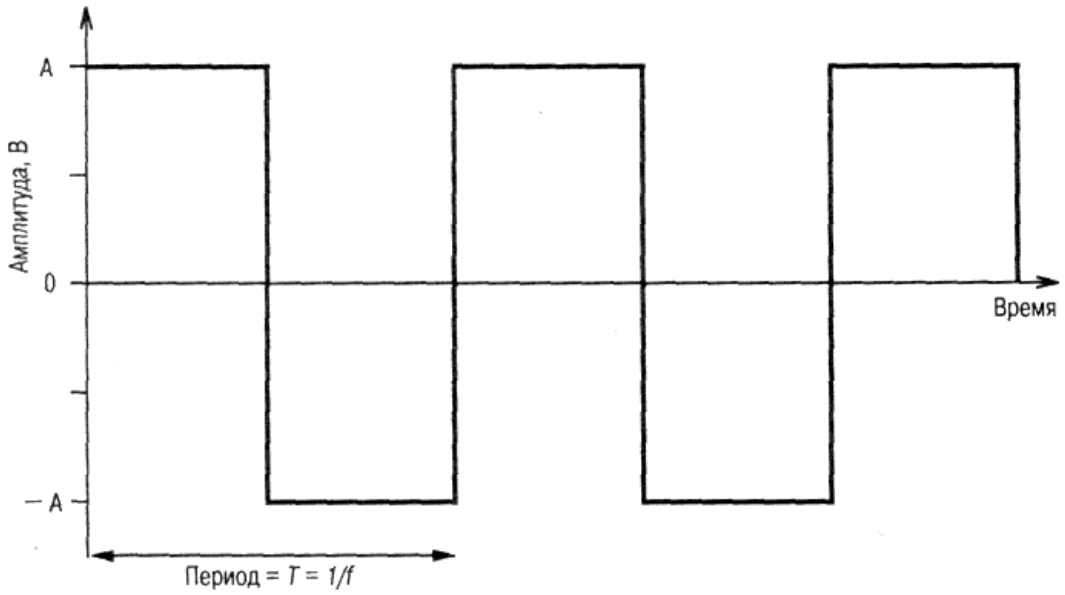
Простейшим типом сигнала является *периодический* сигнал, в котором некоторая структура периодически повторяется во времени. На рис. 1.4 приведен пример периодического аналогового сигнала (синусоида) и периодического цифрового сигнала (прямоугольный сигнал, или меандр). Математическое определение: сигнал s(t) является периодическим тогда и только тогда, когда

$$s(t + T) = s(t), \text{ при } -\infty < t < +\infty ,$$

где постоянная T является периодом сигнала (T – наименьшая величина, удовлетворяющая этому уравнению).



а) Синусоидальный сигнал



б) Прямоугольный сигнал

Рис. 1.4 Периодические сигналы

Фундаментальным аналоговым сигналом является синусоида. В общем случае такой сигнал можно определить тремя параметрами: максимальной амплитудой A, частотой f и фазой ϕ. Максимальной амплитудой называется максимальное значение или интенсивность сигнала во времени; измеряется максимальная амплитуда, как правило, в вольтах. Частотой называется темп повторения сигналов (в периодах за секунду, или герцах). Эквивалентным параметром является период сигнала T, представляющий собой время, за которое происходит повторение сигнала; следовательно, $T = 1/f$. Фаза является мерой относительного сдвига по времени в пределах отдельного периода сигнала (данный термин будет проиллюстрирован несколько ниже).

В общем случае синусоидальный сигнал можно представить в следующем виде:

$$s(t) = Asin(2\pi ft + \varphi).$$

Существует соотношение между двумя синусоидальными сигналами, один из которых изменяется во времени, а другой – в пространстве. Определим длину волны сигнала λ как расстояние, занимаемое одним периодом или, иными словами, как расстояние между двумя точками равных фаз двух последовательных циклов. Предположим, что сигнал распространяется со скоростью v. Тогда длина волны связана с периодом следующим соотношением: $\lambda = vT$, что равносильно $\lambda f = v$. Особое значение для нашего изложения имеет случай $v=c$, где c–скорость света в вакууме, приблизительно равная $3 \cdot 10^8$ м/с.

Применив анализ Фурье, т.е. сложив вместе достаточное количество синусоидальных сигналов с соответствующими амплитудами, частотами и фазами, можно получить электромагнитный сигнал любой формы. Аналогично, любой электромагнитный сигнал рассматривается как совокупность периодических аналоговых (синусоидальных) сигналов с разными амплитудами, частотами и фазами.

Спектром сигнала называется область частот, составляющих данный сигнал.

Цифровой сигнал можно выразить следующим образом:

$$s(t) = A \times \frac{4}{\pi} \sum_{k=1,3,5...}^{\infty} \frac{\sin(2\pi kft)}{k}.$$

Этот сигнал содержит бесконечное число частотных составляющих и, следовательно, имеет бесконечную ширину полосы.

Из приведенного выше изложения можем сделать следующие выводы. В общем случае любой цифровой сигнал имеет бесконечную ширину полосы. Если мы попытаемся передать этот сигнал через какую-то среду, передающая система наложит ограничения на ширину полосы, которую можно передать. Более того, для каждой конкретной среды справедливо следующее: чем больше передаваемая полоса, тем больше стоимость передачи. Поэтому, с одной стороны, по экономическим и практическим соображениям следует аппроксимировать цифровую информацию сигналом с ограниченной шириной полосы. С другой стороны, при ограничении ширины полосы возникают искажения, затрудняющие интерпретацию принимаемого сигнала. Чем больше ограничена полоса, тем больше искажение сигнала и тем больше потенциальная возможность возникновения ошибок при приеме.

1.3.2 ПЕРЕДАЧА ДАННЫХ

Определим *данные* как объекты, передающие смысл, или информацию. *Сигналы* – это электромагнитное представление данных. *Передача* – процесс перемещения данных путем распространения сигналов по передающей среде и их обработки.

Аналоговые и цифровые данные

Понятия аналоговые и цифровые данные достаточно просты. Аналоговые данные принимают непрерывные значения из некоторого диапазона. Например, звуковые сигналы и видеосигналы представляют собой непрерывно изменяющиеся величины. Цифровые данные, напротив, принимают только дискретные значения; примеры – текст и целые числа.

Аналоговые и цифровые сигналы

В системе связи информация распространяется от одной точки к другой посредством электрических сигналов. Аналоговый сигнал представляет собой непрерывно изменяющуюся электромагнитную волну, которая может распространяться через множество сред, в зависимости от частоты; в качестве примеров таких сред можно назвать проводные линии, такие, как витая пара и коаксиальный кабель, оптоволокно; этот сигнал может также распространяться через атмосферу или космическое пространство. Цифровой сигнал представляет собой последовательность импульсов напряжения, которые могут передаваться по проводной линии; при этом постоянный положительный уровень напряжения может использоваться для представления двоичного нуля, а постоянный отрицательный уровень — для представления двоичной единицы.

В беспроводной технологии используются цифровые данные и аналоговые сигналы, так как цифровые сигналы сильнее затухают, чем аналоговые.

Пример 1.1:

Речь, представляя собой звуковые волны, содержит частотные составляющие в области 20 Гц – 20 кГц. Однако большая часть энергии речи находится в намного более узком диапазоне. Стандартный спектр речевых сигналов – 300-3400 Гц, и этого диапазона вполне хватает для разборчивой и четкой передачи речи. Именно такой диапазон обрабатывает телефонный аппарат. Все поступающие звуковые колебания в диапазоне 300-3400 Гц преобразуются в электромагнитный сигнал с подобными амплитудами и частотами. В другом аппарате выполняется обратный процесс: электромагнитная энергия преобразуется в звук.

Цифровые данные можно представить аналоговыми сигналами, применив с этой целью модем (модулятор/демодулятор). Модем или беспроводный адаптер преобразует

последовательность двоичных (принимающих два значения) импульсов напряжения в аналоговый сигнал, модулируя их несущей частотой. Получившийся в результате сигнал занимает определенный спектр частот с центром на несущей частоте и может распространяться в окружающую среду. На другом конце линии другой модем или беспроводный адаптер демодулирует сигнал и восстанавливает исходные данные.

1.3.3 МОДУЛЯЦИЯ СИГНАЛОВ

Исторически модуляция начала применяться для аналоговой информации и только потом для дискретной.

Необходимость в модуляции аналоговой информации возникает, когда нужно передать низкочастотный (например, голосовой) аналоговый сигнал через канал, находящийся в высокочастотной области спектра.

Для решения этой проблемы амплитуду высокочастотного несущего сигнала изменяют (модулируют) в соответствии с изменением низкочастотного сигнала.

В беспроводной технологии в процессе модулирования задействованы одна или несколько характеристик несущего сигнала: амплитуда, частота и фаза. Соответственно, существуют три основные технологии кодирования или модуляции, выполняющие преобразование цифровых данных в аналоговый сигнал (рис. 1.5):

- амплитудная модуляция (Amplitude-Shift Keying, ASK);
- частотная модуляция (Frequency-Shift Keying, FSK);
- фазовая модуляция (Phase-Shift Keying, PSK).

Отметим, что во всех перечисленных случаях результирующий сигнал центрирован на несущей частоте.

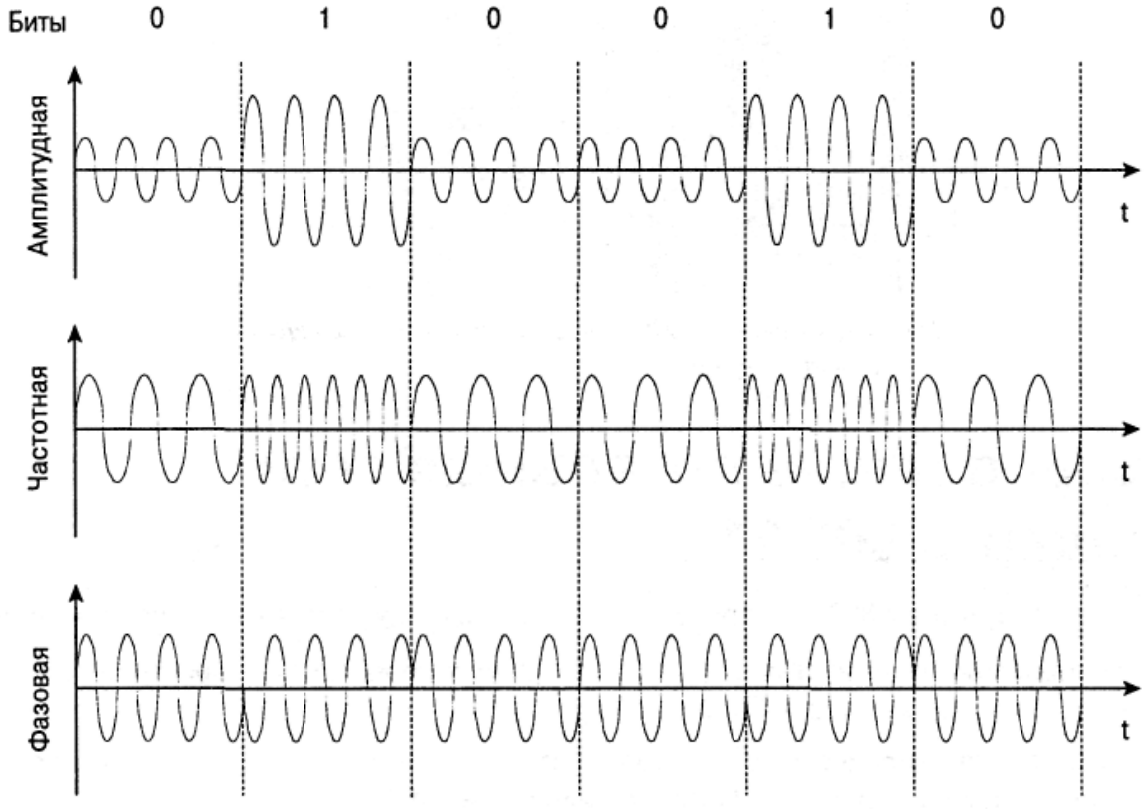


Рис. 1.5 Модуляция цифровых данных аналоговыми сигналами

Амплитудная модуляция

При амплитудной модуляции два двоичных значения представляются сигналами несущей частоты с двумя различными амплитудами. Одна из амплитуд, как правило, выбирается равной нулю; т.е. одно двоичное число представляется наличием несущей частоты при постоянной амплитуде, а другое – ее отсутствием (рис. 1.5, а).

При амплитудной модуляции результирующий сигнал равен:

$$s(t) = \begin{cases} A\cos(2\pi f_c t) \text{ - двоичная 1} \\ 0 \text{ - двоичный 0} \end{cases}. \quad (1.1)$$

Здесь $A\cos(2\pi f_c t)$ — несущий сигнал.

Частотная модуляция

Наиболее распространенной формой частотной модуляции является *бинарная* (Binary FSK, BFSK), в которой два двоичных числа представляются сигналами двух различных частот, расположенных около несущей (рис. 1.5, б). Результирующий сигнал равен

$$s(t) = \begin{cases} A\cos(2\pi f_1 t) \text{ - двоичная 1} \\ A\cos(2\pi f_2 t) \text{ - двоичный 0} \end{cases}, \quad (1.2)$$

где f_1 и f_2 — частоты, смещенные от несущей частоты f_c на величины, равные по модулю, но противоположные по знаку.

Бинарная частотная модуляция менее восприимчива к ошибкам, чем амплитудная модуляция.

Более эффективной, но и более подверженной ошибкам, является схема *многочастотной* модуляции (Multiple FSK, MFSK), в которой используются более двух частот. В этом случае каждая сигнальная посылка представляет более одного бита. Переданный сигнал MFSK (для одного периода передачи сигнальной посылки) можно определить следующим образом:

$$s_i = A\cos(2\pi f_i t), \;\; 1 \ll i \ll M \quad (1.3)$$

Здесь

$f_i = f_c + (2i - 1 - M) f_d$

f_c – несущая частота;

f_d – разностная частота;

M – число различных сигнальных посылок = 2^L;

L – количество битов на одну сигнальную посылку.

На рис. 1.6 представлен пример схемы MFSK с M = 4. Входной поток битов кодируется по два бита, после чего передается одна из четырех возможных 2-битовых комбинаций.

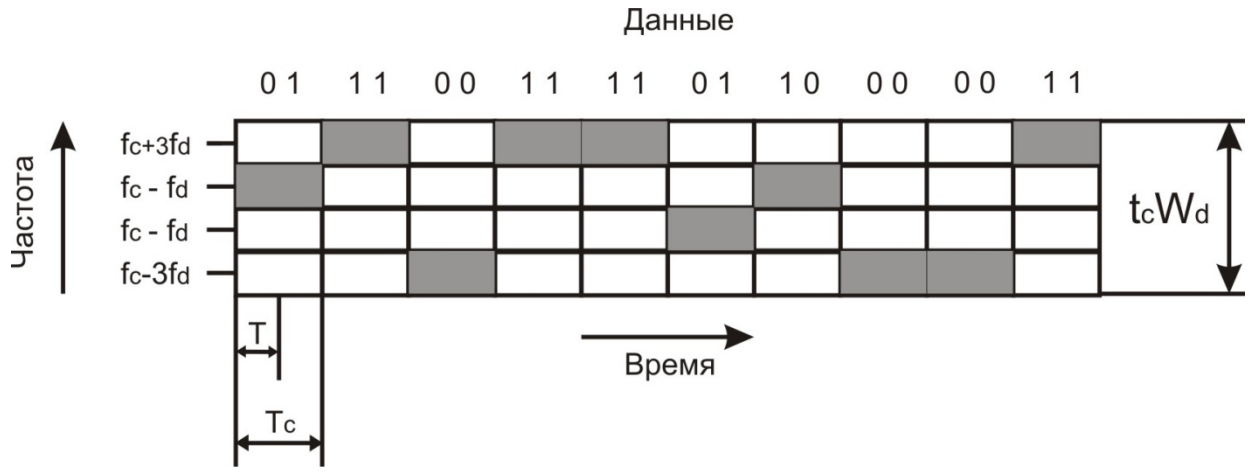


Рис. 1.6 Использование частоты схемой MFSK (M = 4)

Для уменьшения занимаемой полосы частот в модуляторах сигналов с фазовой модуляцией применяют сглаживающие фильтры. Применение сглаживающих фильтров приводит к увеличению эффективности использования полосы, но в тоже время из-за сглаживания уменьшается расстояние между соседними сигналами, что приводит к снижению помехоустойчивости.

Фазовая модуляция

При фазовой модуляции для представления данных выполняется смещение несущего сигнала.

Самой простой фазовой модуляцией является *двухуровневая* модуляция (Binary PSK, BPSK), где для представления двух двоичных цифр используются две фазы (рис. 1.5, в). Получающийся сигнал имеет следующий вид (для одного периода передачи бита):

$$s(t) = \begin{cases} A\cos(2\pi f_c t) \\ A\cos(2\pi f_c t + \pi) \end{cases} = \begin{cases} A\cos(2\pi f_c t) \text{- двоичная 1} \\ -A\cos(2\pi f_c t) \text{- двоичный 0} \end{cases} \quad (1.4)$$

Альтернативной формой двухуровневой PSK является *дифференциальная* PSK (DPSK), пример которой приведен на рис. 1.7. В данной системе двоичный 0 представляется сигнальным пакетом, фаза которого совпадает с фазой предыдущего посланного пакета, а двоичная 1 представляется сигнальным пакетом с фазой, противоположной фазе предыдущего пакета. Такая схема называется дифференциальной, поскольку сдвиг фаз выполняется относительно предыдущего переданного бита, а не относительно какого-то эталонного сигнала. При дифференциальном кодировании передаваемая информация представляется не сигнальными посылками, а изменениями между последовательными сигнальными посылками. Схема DPSK делает излишним строгое согласование фазы местного гетеродина приемника и передатчика. До тех пор пока предыдущая полученная фаза точна, точен и фазовый эталон.

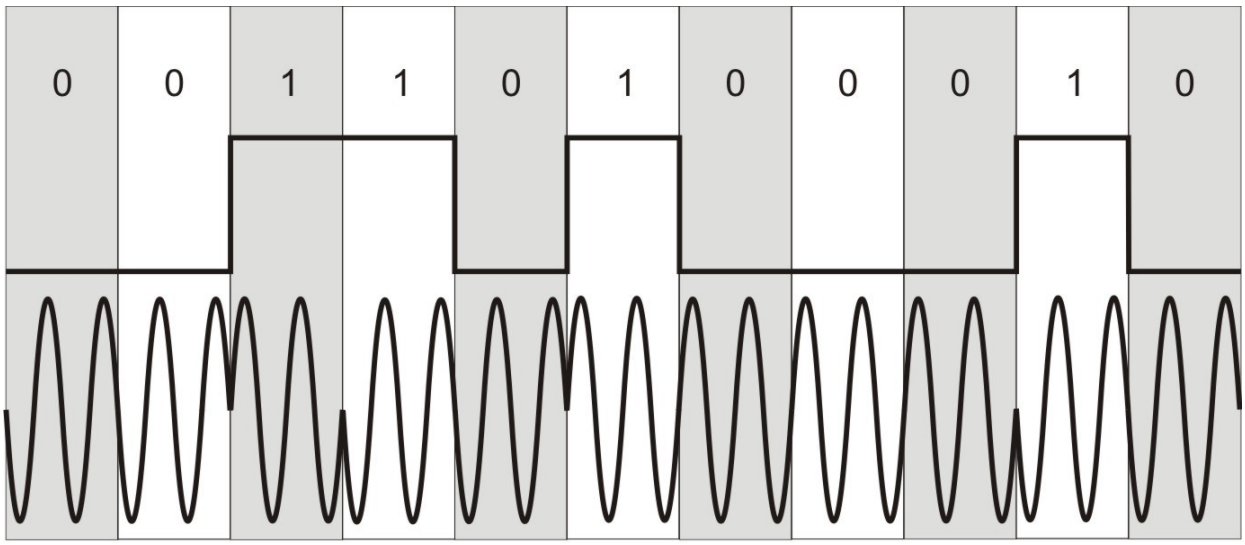


Рис. 1.7 Дифференциальная фазовая модуляция (DPSK)

Если каждой сигнальной посылкой представить более одного бита, то это позволит эффективнее использовать полосу сигнала. Например, в распространенной кодировке, известной как *квадратурная* фазовая модуляция (Quadrature phase-shift keying, QPSK), вместо сдвига фазы на 180°, как в кодировке BPSK, используются сдвиги фаз, кратные $\pi/2$ (90°).

При квадратурной фазовой модуляции:

$$s(t) = \begin{cases} A\cos(2\pi f_c t + \frac{\pi}{4}) - 11 \\ A\cos(2\pi f_c t + \frac{3\pi}{4}) - 10 \\ A\cos(2\pi f_c t + \frac{5\pi}{4}) - 00 \\ A\cos(2\pi f_c t + \frac{7\pi}{4}) - 01 \end{cases} \quad (1.5)$$

Таким образом, каждая сигнальная посылка представляет не один бит, а два.

Описанную схему можно расширить: передавать, например, по три бита в каждый момент времени, используя для этого восемь различных углов сдвига фаз. Более того, при каждом угле можно использовать несколько амплитуд. Такая модуляция называется *многоуровневой* фазовой модуляцией (Multiple FSK, MFSK).

Квадратурная амплитудная модуляция

Квадратурная амплитудная модуляция (Quadrature amplitude modulation, QAM) является популярным методом аналоговой передачи сигналов, используемым в некоторых беспроводных стандартах.

Данная схема модуляции совмещает в себе амплитудную и фазовую модуляции. В методе QAM использованы преимущества одновременной передачи двух различных сигналов на одной несущей частоте, но при этом задействованы две копии несущей частоты, сдвинутые относительно друг друга на 90°. При квадратурной амплитудной модуляции обе несущие являются амплитудно-модулированными. Итак, два независимых сигнала одновременно передаются через одну среду. В приемнике эти сигналы демодулируются, а результаты объединяются с целью восстановления исходного двоичного сигнала.

При использовании двухуровневой амплитудной модуляции (2QAM) каждый из двух потоков может находиться в одном из двух состояний, а объединенный поток – в одном из 2·2 = 4 состояний. При использовании четырехуровневой модуляции (т.е. четырех различных уровней амплитуды, 4QAM) объединенный поток будет находиться в одном из 4·4 = 16 состояний. Уже реализованы системы, имеющие 64 или даже 256 состояний. Чем больше число состояний, тем выше скорость передачи данных, возможная при определенной ширине полосы. Разумеется, как указывалось ранее, чем больше число состояний, тем выше потенциальная частота возникновения ошибок вследствие помех или поглощения.

1.3.4 ПРОПУСКНАЯ СПОСОБНОСТЬ КАНАЛА

Существует множество факторов, способных исказить или повредить сигнал. Наиболее распространенные из них – помехи или шумы, представляющие собой любой нежелательный сигнал, который смешивается с сигналом, предназначенным для передачи или приема, и искажает его. Для цифровых данных возникает вопрос: насколько эти искажения ограничивают возможную скорость передачи данных. Максимально возможная при определенных условиях скорость, при которой информация может передаваться по конкретному тракту связи, или каналу, называется *пропускной способностью* канала.

Существуют четыре понятия, которые мы попытаемся связать воедино.

- Скорость передачи данных – скорость в битах в секунду (бит/с), с которой могут передаваться данные;
- Ширина полосы – ширина полосы передаваемого сигнала, ограничиваемая передатчиком и природой передающей среды. Выражается в периодах в секунду, или герцах (Гц).
- Шум. Средний уровень шума в канале связи.
- Уровень ошибок – частота появления ошибок. Ошибкой считается прием 1 при переданном 0 и наоборот.

Проблема, заключается в следующем: средства связи недешевы и, в общем случае, чем шире их полоса, тем дороже они стоят. Более того, все каналы передачи, представляющие практический интерес, имеют ограниченную ширину полосы. Ограничения обусловлены физическими свойствами передающей среды или преднамеренными ограничениями ширины полосы в самом передатчике, сделанными для предотвращения интерференции с другими источниками. Естественно, нам хотелось бы максимально эффективно использовать имеющуюся полосу. Для цифровых данных это означает, что для определенной полосы желательно получить максимально возможную при существующем уровне ошибок скорость передачи данных. Главным ограничением при достижении такой эффективности являются помехи.

1.3.5 МЕТОДЫ ДОСТУПА К СРЕДЕ В БЕСПРОВОДНЫХ СЕТЯХ

Одна из основных проблем построения беспроводных систем – это решение задачи доступа многих пользователей к ограниченному ресурсу среды передачи. Существует несколько базовых методов доступа (их еще называют методами уплотнения или мультиплексирования), основанных на разделении между станциями таких параметров, как пространство, время, частота и код. Задача уплотнения – выделить каждому каналу связи пространство, время, частоту и/или код с минимумом взаимных помех и максимальным использованием характеристик передающей среды.

Уплотнение с пространственным разделением

Основано на разделении сигналов в пространстве, когда передатчик посылает сигнал, используя код c, время t и частоту f в области s_i. То есть каждое беспроводное устройство может вести передачу данных только в границах одной определенной территории, на которой любому другому устройству запрещено передавать свои сообщения.

К примеру, если радиостанция вещает на строго определенной частоте на закрепленной за ней территории, а какая-либо другая станция в этой же местности также начнет вещать на той же частоте, то слушатели радиопередач не смогут получить «чистый» сигнал ни от одной из этих станций. Другое дело, если радиостанции работают на одной частоте в разных городах. Искажений сигналов каждой радиостанции не будет в связи с ограниченной дальностью распространения сигналов этих станций, что исключает их наложение друг на друга.

Характерный пример – системы сотовой телефонной связи.

Уплотнение с частотным разделением (Frequency Division Multiplexing, FDM)

Каждое устройство работает на строго определенной частоте, благодаря чему несколько устройств могут вести передачу данных на одной территории (рис. 1.8). Это один из наиболее известных методов, так или иначе используемый в самых современных системах беспроводной связи.

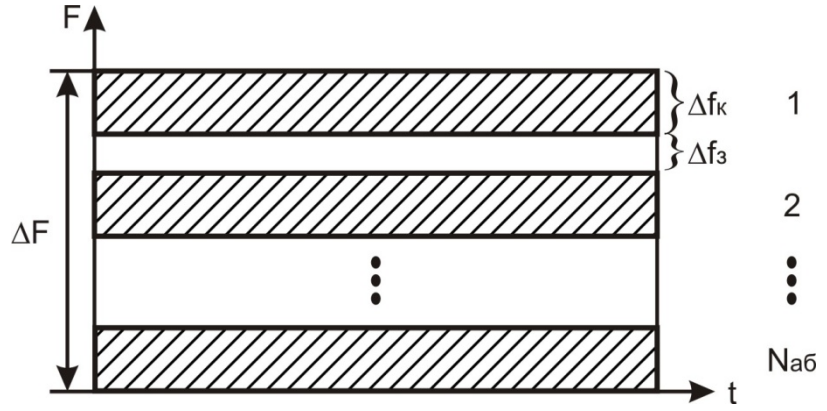


Рис. 1.8 Принцип частотного разделения каналов

Наглядная иллюстрация схемы частотного уплотнения — функционирование в одном городе нескольких радиостанций, работающих на разных частотах. Для надежной отстройки друг от друга их рабочие частоты должны быть разделены защитным частотным интервалом, позволяющим исключить взаимные помехи.

Эта схема, хотя и позволяет использовать множество устройств на определенной территории, сама по себе приводит к неоправданному расточительству обычно скудных частотных ресурсов, поскольку требует выделения отдельной частоты для каждого беспроводного устройства.

Уплотнение с временным разделением (Time Division Multiplexing, TDM)

В данной схеме распределение каналов идет по времени, т. е. каждый передатчик транслирует сигнал на одной и той же частоте f в области s, но в различные промежутки времени t_i (как правило, циклически повторяющиеся) при строгих требованиях к синхронизации процесса передачи (рис 1.9).

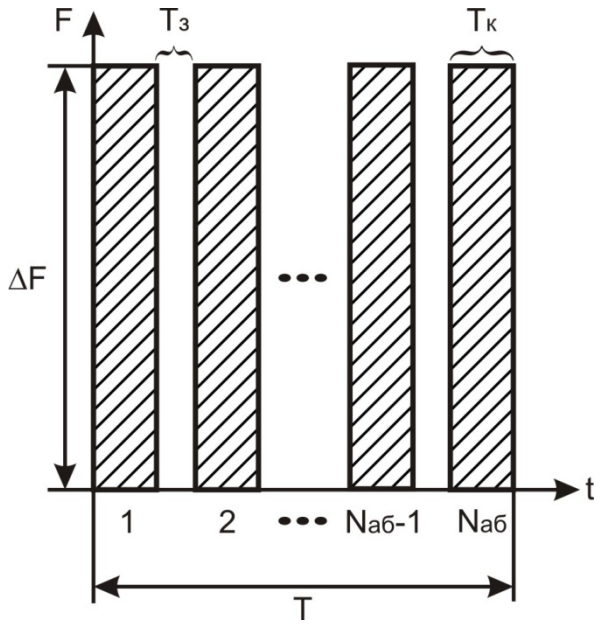


Рис. 1.9 Принцип временного разделения каналов

Подобная схема достаточно удобна, так как временные интервалы могут динамично перераспределяться между устройствами сети. Устройствам с большим трафиком назначаются более длительные интервалы, чем устройствам с меньшим объемом трафика.

Основной недостаток систем с временным уплотнением – это мгновенная потеря информации при срыве синхронизации в канале, например, из-за сильных помех, случайных или преднамеренных. Однако успешный опыт эксплуатации таких знаменитых TDM-систем, как сотовые телефонные сети стандарта GSM, свидетельствует о достаточной надежности механизма временного уплотнения.

Уплотнение с кодовым разделением (Code Division Multiplexing, CDM)

В данной схеме все передатчики передают сигналы на одной и той же частоте f, в области s и во время t, но с разными кодами c_i.

Именем основанного на CDM механизма разделения каналов (CDMA, CDM Access) даже назван стандарт сотовой телефонной связи IS-95a, а также ряд стандартов третьего поколения сотовых систем связи (cdma2000, WCDMA и др.).

В схеме CDM каждый передатчик заменяет каждый бит исходного потока данных на CDM-символ — кодовую последовательность длиной в 11, 16, 32, 64 и т.п. бит (их называют чипами). Кодовая последовательность уникальна для каждого передатчика. Как правило, если для замены «1» в исходном потоке данных используют некий CDM-код, то для замены «0» применяют тот же код, но инвертированный.

Приемник знает CDM-код передатчика, сигналы которого должен воспринимать. Он постоянно принимает все сигналы, оцифровывает их. Затем в специальном устройстве (коррелляторе) производит операцию свертки (умножения с накоплением) входного оцифрованного сигнал с известным ему CDM-кодом и его инверсией. В несколько упрощенном виде это выглядит как операция скалярного произведения вектора входного сигнала и вектора с CDM-кодом. Если сигнал на выходе коррелятора превышает некий установленный пороговый уровень, приемник считает, что принял 1 или 0. Для увеличения вероятности приема передатчик может повторять посылку каждого бита несколько раз. При этом сигналы других передатчиков с другими CDM-кодами приемник воспринимает как аддитивный шум. Более того, благодаря большой избыточности (каждый бит заменяется десятками чипов), мощность принимаемого сигнала может быть

сопоставима с интегральной мощностью шума. Похожести CDM-сигналов на случайный (гауссов) шум добиваются, используя CDM-коды, порожденные генератором псевдослучайных последовательностей. Поэтому данный метод еще называют методом расширения спектра сигнала посредством прямой последовательности (DSSS — Direct Sequence Spread Spectrum), о расширении спектра будет рассказано ниже.

Наиболее сильная сторона данного уплотнения заключается в повышенной защищенности и скрытности передачи данных: не зная кода, невозможно получить сигнал, а в ряде случаев — и обнаружить его присутствие. Кроме того, кодовое пространство несравненно более значительно по сравнению с частотной схемой уплотнения, что позволяет без особых проблем присваивать каждому передатчику свой индивидуальный код. Основной же проблемой кодового уплотнения до недавнего времени являлась сложность технической реализации приемников и необходимость обеспечения точной синхронизации передатчика и приемника для гарантированного получения пакета.

Механизм мультиплексирования посредством ортогональных несущих частот (Orthogonal Frequency Division Multiplexing, OFDM)

Его суть: весь доступный частотный диапазон разбивается на достаточно много поднесущих (от нескольких сот до тысяч). Одному каналу связи (приемнику и передатчику) назначают для передачи несколько таких несущих, выбранных из всего множества по определенному закону. Передача ведется одновременно по всем поднесущим, т. е. в каждом передатчике исходящий поток данных разбивается на N субпотоков, где N – число поднесущих, назначенных данному передатчику.

Распределение поднесущих в ходе работы может динамически изменяться, что делает данный механизм не менее гибким, чем метод временного уплотнения.

Схема OFDM имеет несколько преимуществ. Во-первых, селективному замиранию будут подвержены только некоторые подканалы, а не весь сигнал. Если поток данных защищен кодом прямого исправления ошибок, то с этим замиранием легко бороться. Но что более важно, OFDM позволяет подавить межсимвольную интерференцию. Межсимвольная интерференция оказывает значительное влияние при высоких скоростях передачи данных, так как расстояние между битами (или символами) является малым. В схеме OFDM скорость передачи данных уменьшается в N раз, что позволяет увеличить время передачи символа в N раз. Таким образом, если время передачи символа для исходного потока составляет T_s, то период сигнала OFDM будет равен NT_s. Это позволяет существенно снизить влияние межсимвольных помех. При проектировании системы N выбирается таким образом, чтобы величина NT_s значительно превышала среднеквадратичный разброс задержек канала.

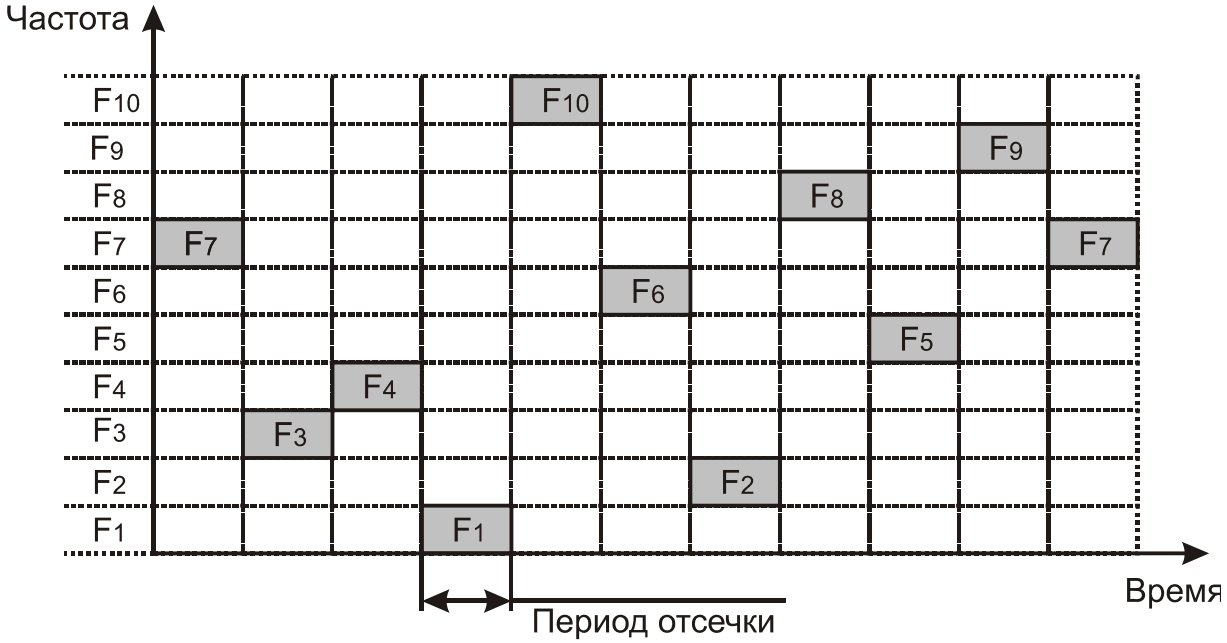
1.3.6 ТЕХНОЛОГИЯ РАСШИРЕННОГО СПЕКТРА

Изначально метод расширенного спектра создавался для разведывательных и военных целей. Основная идея метода состоит в том, чтобы распределить информационный сигнал по широкой полосе радиодиапазона, что в итоге позволит значительно усложнить подавление или перехват сигнала. Первая разработанная схема расширенного спектра известна как метод перестройки частоты. Более современной схемой расширенного спектра является метод прямого последовательного расширения. Оба метода используются в различных стандартах и продуктах беспроводной связи.

Расширение спектра скачкообразной перестройкой частоты (Frequency Hopping Spread Spectrum, FHSS)

Для того чтобы радиообмен нельзя было перехватить или подавить узкополосным шумом, было предложено вести передачу с постоянной сменой несущей в пределах широкого диапазона частот. В результате мощность сигнала распределялась по всему диапазону, и прослушивание какой-то определенной частоты давало только небольшой шум. Последовательность несущих частот выбиралась псевдослучайной, известной только передатчику и приемнику. Попытка подавления сигнала в каком-то узком диапазоне также не слишком ухудшала сигнал, так как подавлялась только небольшая часть информации.

Идею этого метода иллюстрирует рис. 1.10.

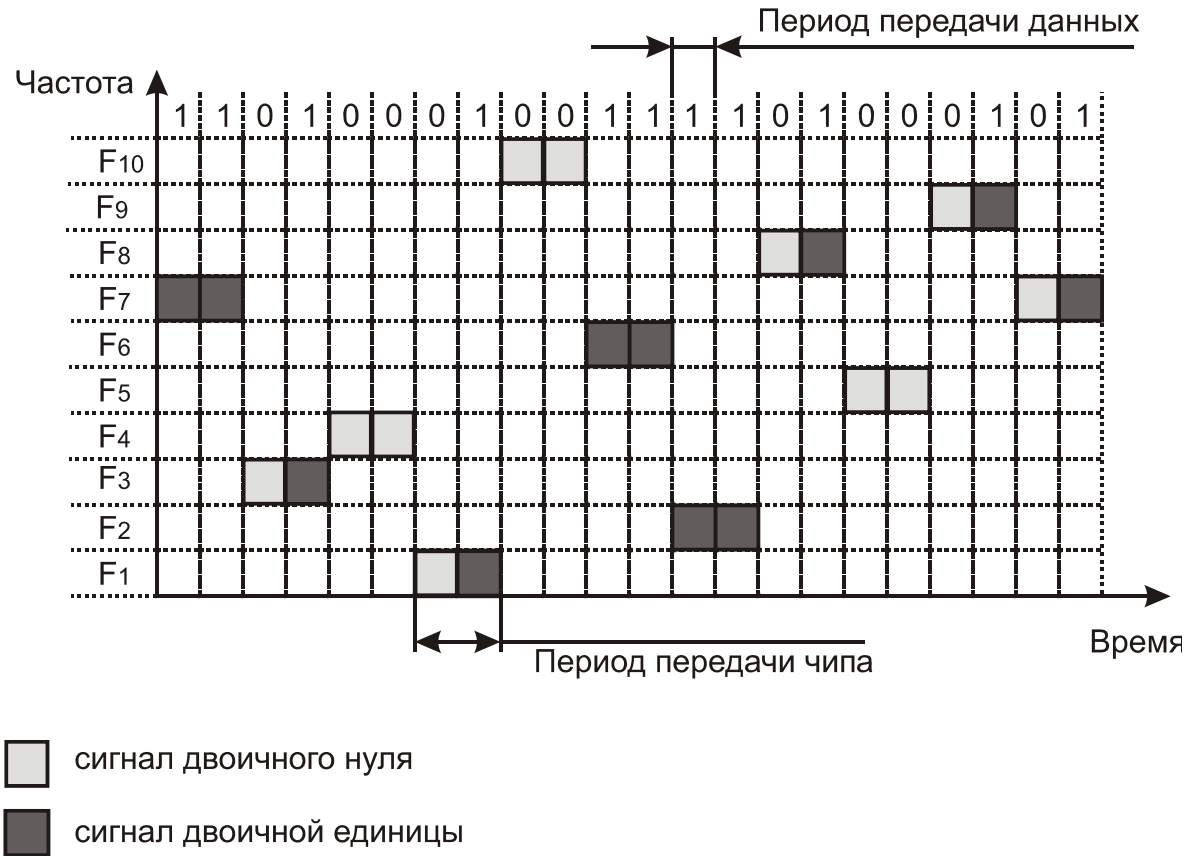


Последовательность перестройки частот: F7-F3-F4-F1-F10-F6-F2-F8-F5-F9-F7

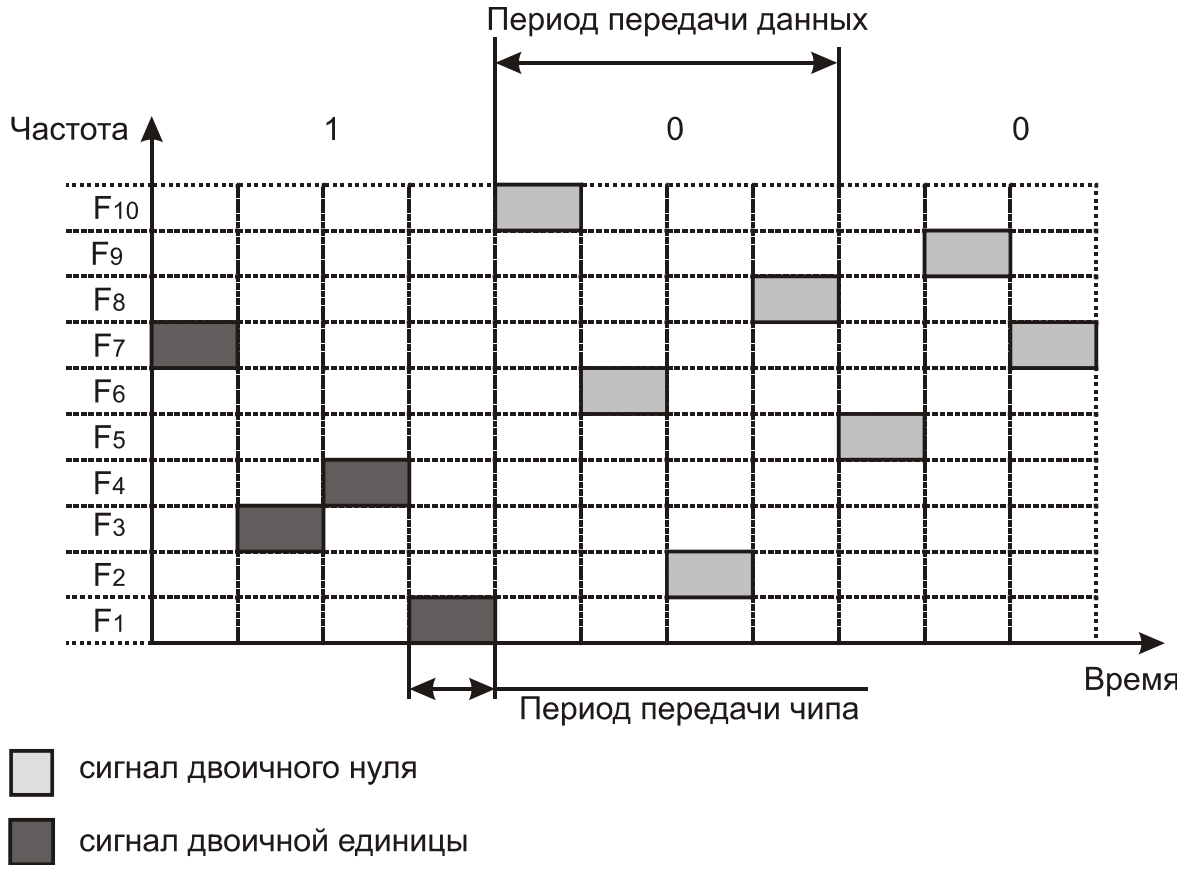
Рис. 1.10 Расширение спектра скачкообразной перестройкой частоты

В течение определенного фиксированного интервала времени передача ведется на неизменной несущей частоте. На каждой несущей частоте для передачи дискретной информации применяются стандартные методы модуляции, такие как FSK или PSK. Для того чтобы приемник синхронизировался с передатчиком, для обозначения начала каждого периода передачи в течение некоторого времени передаются синхробиты. Так что полезная скорость этого метода кодирования оказывается меньше из-за постоянных накладных расходов на синхронизацию.

Несущая частота меняется в соответствии с номерами частотных подканалов, вырабатываемых алгоритмом псевдослучайных чисел. Псевдослучайная последовательность зависит от некоторого параметра, который называют *начальным* числом. Если приемнику и передатчику известны алгоритм и значение начального числа, то они меняют частоты в одинаковой последовательности, называемой последовательностью псевдослучайной перестройки частоты.



а) Скорость передачи данных выше чиповой скорости



б) Скорость передачи данных ниже чиповой скорости

Рис. 1.11 Соотношение между скоростью передачи данных и частотой смены подканалов

Если частота смены подканалов ниже, чем скорость передачи данных в канале, то такой режим называют *медленным расширением спектра* (рис. 1.11, а); в противном случае мы имеем дело с *быстрым расширением спектра* (рис. 1.11, б).

Метод быстрого расширения спектра более устойчив к помехам, поскольку узкополосная помеха, которая подавляет сигнал в определенном подканале, не приводит к потере бита, так как его значение повторяется несколько раз в различных частотных подканалах. В этом режиме не проявляется эффект межсимвольной интерференции, потому что ко времени прихода задержанного вдоль одного из путей сигнала система успевает перейти на другую частоту.

Метод медленного расширения спектра таким свойством не обладает, но зато он проще в реализации и имеет меньшие накладные расходы.

Методы FHSS используются в беспроводных технологиях IEEE 802.11 и Bluetooth.

В методах FHSS подход к использованию частотного диапазона не такой, как в других методах кодирования — вместо экономного расходования узкой полосы делается попытка занять весь доступный диапазон. На первый взгляд это кажется не очень эффективным — ведь в каждый момент времени в диапазоне работает только один канал. Однако последнее утверждение не всегда справедливо — коды расширенного спектра можно использовать также и для мультиплексирования нескольких каналов в широком диапазоне. В частности, методы FHSS позволяют организовать одновременную работу нескольких каналов путем выбора для каждого канала таких псевдослучайных последовательностей, чтобы в каждый момент времени каждый канал работал на своей частоте (конечно, это можно сделать, только если число каналов не превышает числа частотных подканалов).

Прямое последовательное расширение спектра (Direct Sequence Spread Spectrum, DSSS)

В методе прямого последовательного расширения спектра также используется весь частотный диапазон, выделенный для одной беспроводной линии связи. В отличие от метода FHSS весь частотный диапазон занимается не за счет постоянных переключений с частоты на частоту, а за счет того, что каждый бит информации заменяется N битами, так что тактовая скорость передачи сигналов увеличивается в N раз. А это, в свою очередь, означает, что спектр сигнала также расширяется в N раз. Достаточно соответствующим образом выбрать скорость передачи данных и значение N, чтобы спектр сигнала заполнил весь диапазон.

Цель кодирования методом DSSS та же, что методом FHSS — повышение устойчивости к помехам. Узкополосная помеха будет искажать только определенные частоты спектра сигнала, так что приемник с большой степенью вероятности сможет правильно распознать передаваемую информацию.

Код, которым заменяется двоичная единица исходной информации, называется *расширяющей последовательностью*, а каждый бит такой последовательности — чипом.

Соответственно, скорость передачи результирующего кода называют *чиповой скоростью*. Двоичный нуль кодируется инверсным значением расширяющей последовательности. Приемники должны знать расширяющую последовательность, которую использует передатчик, чтобы понять передаваемую информацию.

Количество битов в расширяющей последовательности определяет коэффициент расширения исходного кода. Как и в случае FHSS, для кодирования битов результирующего кода может использоваться любой вид модуляции, например BFSK.

Чем больше коэффициент расширения, тем шире спектр результирующего сигнала и тем больше степень подавления помех. Но при этом растет занимаемый каналом диапазон спектра. Обычно коэффициент расширения имеет значения от 10 до 100.

Пример 1.2:

Очень часто в качестве значения расширяющей последовательности берут последовательность Баркера (Barker), которая состоит из 11 бит: 10110111000. Если передатчик использует эту последовательность, то передача трех битов 110 ведет к передаче следующих битов:
10110111000 10110111000 01001000111.

Последовательность Баркера позволяет приемнику быстро синхронизироваться с передатчиком, то есть надежно выявлять начало последовательности. Приемник определяет такое событие, поочередно сравнивая получаемые биты с образцом последовательности. Действительно, если сравнить последовательность Баркера с такой же последовательностью, но сдвинутой на один бит влево или вправо, то мы получим меньше половины совпадений значений битов. Значит, даже при искажении нескольких битов с большой долей вероятности приемник правильно определит начало последовательности, а значит, сможет правильно интерпретировать получаемую информацию.

Метод DSSS в меньшей степени защищен от помех, чем метод быстрого расширения спектра, так как мощная узкополосная помеха влияет на часть спектра, а значит, и на результат распознавания единиц или нулей.

Беспроводные локальные сети DSSS используют каналы шириной 22 МГц, благодаря чему многие WLAN могут работать в одной и той же зоне покрытия. В Северной Америке и большей части Европы, в том числе и в России, каналы шириной 22 МГц позволяют создать в диапазоне 2,4–2,483 ГГц три неперекрывающихся канала передачи. Эти каналы показаны на рис. 1.12.

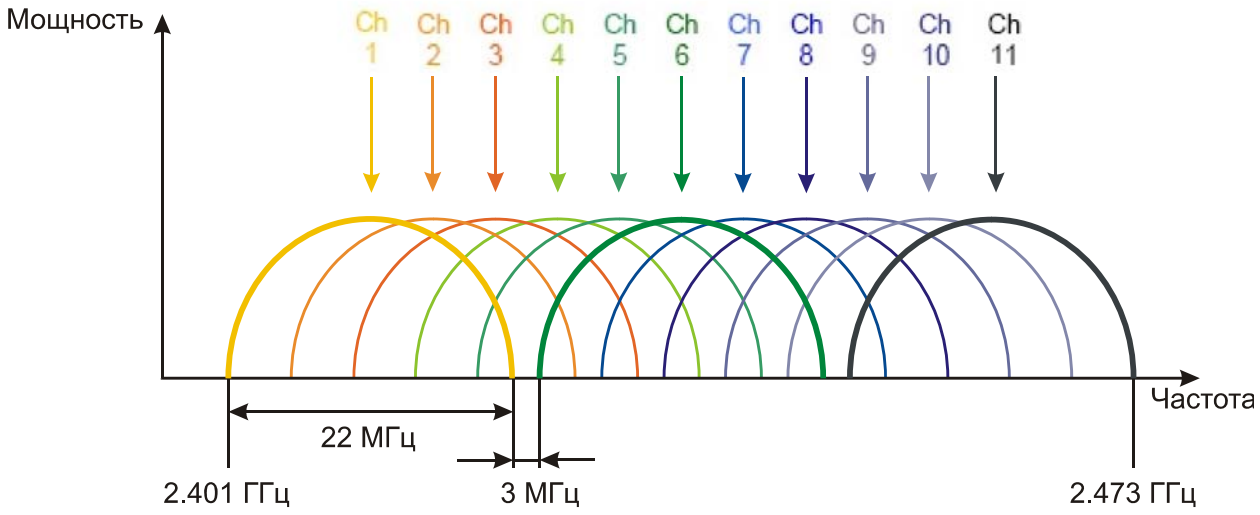


Рис. 1.12 Каналы, используемые в технологии DSSS

1.3.7 КОДИРОВАНИЕ И ЗАЩИТА ОТ ОШИБОК

Существуют три наиболее распространенных орудия борьбы с ошибками в процессе передачи данных:

- коды обнаружения ошибок;
- коды с коррекцией ошибок, называемые также схемами прямой коррекции ошибок (Forward Error Correction, FEC);

– протоколы с автоматическим запросом повторной передачи (Automatic Repeat Request, ARQ).

Код обнаружения ошибок позволяет довольно легко установить наличие ошибки. Как правило, подобные коды используются совместно с определенными протоколами канального или транспортного уровня имеющими схему ARQ. В схеме ARQ приемник попросту отклоняет блок данных, в котором была обнаружена ошибка, после чего передатчик передает этот блок повторно. Коды с прямой коррекцией ошибок позволяют не только обнаружить ошибки, но и исправить их, не прибегая к повторной передаче. Схемы FEC часто используются в беспроводной передаче, где повторная передача крайне неэффективна, а уровень ошибок довольно высок.

1) Методы обнаружения ошибок

Методы обнаружения ошибок основаны на передаче в составе блока данных избыточной служебной информации, по которой можно судить с некоторой степенью вероятности о достоверности принятых данных.

Избыточную служебную информацию принято называть контрольной суммой, или контрольной последовательностью кадра (Frame Check Sequence, FCS). Контрольная сумма вычисляется как функция от основной информации, причем не обязательно путем суммирования. Принимающая сторона повторно вычисляет контрольную сумму кадра по известному алгоритму и в случае ее совпадения с контрольной суммой, вычисленной передающей стороной, делает вывод о том, что данные были переданы через сеть корректно. Рассмотрим несколько распространенных алгоритмов вычисления контрольной суммы, отличающихся вычислительной сложностью и способностью обнаруживать ошибки в данных.

Контроль по паритету представляет собой наиболее простой метод контроля данных. В то же время это наименее мощный алгоритм контроля, так как с его помощью можно обнаружить только одиночные ошибки в проверяемых данных. Метод заключается в суммировании по модулю 2 всех битов контролируемой информации. Нетрудно заметить, что для информации, состоящей из нечетного числа единиц, контрольная сумма всегда равна 1, а при четном числе единиц - 0. Например, для данных 100101011 результатом контрольного суммирования будет значение 1. Результат суммирования также представляет собой один дополнительный бит данных, который пересылается вместе с контролируемой информацией. При искажении в процессе пересылки любого одного бита исходных данных (или контрольного разряда) результат суммирования будет отличаться от принятого контрольного разряда, что говорит об ошибке. Однако двойная ошибка, например 110101010, будет неверно принята за корректные данные. Поэтому контроль по паритету применяется к небольшим порциям данных, как правило, к каждому байту, что дает коэффициент избыточности для этого метода 1/8. Метод редко применяется в компьютерных сетях из-за значительной избыточности и невысоких диагностических способностей.

Вертикальный и горизонтальный контроль по паритету представляет собой модификацию описанного выше метода. Его отличие состоит в том, что исходные данные рассматриваются в виде матрицы, строки которой составляют байты данных. Контрольный разряд подсчитывается отдельно для каждой строки и для каждого столбца матрицы. Этот метод обнаруживает большую часть двойных ошибок, однако обладает еще большей избыточностью. На практике этот метод сейчас также почти не применяется при передаче информации по сети.

Циклический избыточный контроль (Cyclic Redundancy Check, CRC) является в настоящее время наиболее популярным методом контроля в вычислительных сетях (и не только в сетях, например, этот метод широко применяется при записи данных на гибкие и жесткие диски). Метод основан на рассмотрении исходных данных в виде одного многоразрядного двоичного числа. Например, кадр стандарта Ethernet, состоящий из 1024

байт, будет рассматриваться как одно число, состоящее из 8192 бит. Контрольной информацией считается остаток от деления этого числа на известный делитель R. Обычно в качестве делителя выбирается семнадцати- или тридцатитрехразрядное число, чтобы остаток от деления имел длину 16 разрядов (2 байт) или 32 разряда (4 байт). При получении кадра данных снова вычисляется остаток от деления на тот же делитель R, но при этом к данным кадра добавляется и содержащаяся в нем контрольная сумма. Если остаток от деления на R равен нулю, то делается вывод об отсутствии ошибок в полученном кадре, в противном случае кадр считается искаженным.

Этот метод обладает более высокой вычислительной сложностью, но его диагностические возможности гораздо выше, чем у методов контроля по паритету. Метод CRC обнаруживает все одиночные ошибки, двойные ошибки и ошибки в нечетном числе битов. Метод обладает также невысокой степенью избыточности. Например, для кадра Ethernet размером 1024 байт контрольная информация длиной 4 байт составляет только 0,4 %.

2) Методы коррекции ошибок

Техника кодирования, которая позволяет приемнику не только понять, что присланные данные содержат ошибки, но и исправить их, называется прямой коррекцией ошибок (Forward Error Correction, FEC). Коды, которые обеспечивают прямую коррекцию ошибок, требуют введения большей избыточности в передаваемые данные, чем коды, которые только обнаруживают ошибки.

При применении любого избыточного кода не все комбинации кодов являются разрешенными. Например, контроль по паритету делает разрешенными только половину кодов. Если мы контролируем три информационных бита, то разрешенными 4-битными кодами с дополнением до нечетного количества единиц будут:

000 1, 001 0, 010 0, 011 1, 100 0, 101 1, 110 1, 111 0, то есть всего 8 кодов из 16 возможных.

Для того чтобы оценить количество дополнительных битов, требуемых для исправления ошибок, нужно знать так называемое расстояние Хемминга между разрешенными комбинациями кода. Расстоянием Хемминга называется минимальное число битовых разрядов, в которых отличается любая пара разрешенных кодов. Для схем контроля по паритету расстояние Хемминга равно 2.

Можно доказать, что если мы сконструировали избыточный код с расстоянием Хемминга, равным n, то такой код будет в состоянии распознавать (n- 1)-кратные ошибки и исправлять (n-1)/2-кратные ошибки. Так как коды с контролем по паритету имеют расстояние Хемминга, равное 2, то они могут только обнаруживать однократные ошибки и не могут исправлять ошибки.

Коды Хемминга эффективно обнаруживают и исправляют изолированные ошибки, то есть отдельные искаженные биты, которые разделены большим количеством корректных битов. Однако при появлении длинной последовательности искаженных битов (пульсации ошибок) коды Хемминга не работают.

Наиболее часто в современных системах связи применяется тип кодирования, реализуемый сверточным кодирующим устройством (Convolutional coder), потому что такое кодирование может быть довольно просто реализовано аппаратно с использованием линий задержки (delay) и сумматоров. В отличие от рассмотренного выше кода, который относится к блочным кодам без памяти, сверточпый код относится к кодам с конечной памятью (Finite memory code); это означает, что выходная последовательность кодера является функцией не только текущего входного сигнала, но также нескольких из числа последних предшествующих битов. Длина кодового ограничения (Constraint length of a code) показывает, как много выходных элементов выходит из системы в пересчете на один входной. Коды часто характеризуются их эффективной степенью (или коэффициентом) кодирования (Code rate). Вам может встретиться сверточный код с коэффициентом

кодирования 1/2. Этот коэффициент указывает, что на каждый входной бит приходятся два выходных. При сравнении кодов обращайте внимание на то, что, хотя коды с более высокой эффективной степенью кодирования позволяют передавать данные с более высокой скоростью, они соответственно более чувствительны к шуму.

В беспроводных системах с блочными кодами широко используется метод чередования блоков. Преимущество чередования состоит в том, что приемник распределяет пакет ошибок, исказивший некоторую последовательность битов, по большому числу блоков, благодаря чему становится возможным исправление ошибок. Чередование выполняется с помощью чтения и записи данных в различном порядке. Если во время передачи пакет помех воздействует на некоторую последовательность битов, то все эти биты оказываются разнесенными по различным блокам. Следовательно, от любой контрольной последовательности требуется возможность исправления лишь небольшой части от общего количества инвертированных битов.

3) Методы автоматического запроса повторной передачи

В простейшем случае защита от ошибок заключается только в их обнаружении. Система должна предупредить передатчик об обнаружении ошибки и необходимости повторной передачи. Такие процедуры защиты от ошибок известны как методы автоматического запроса повторной передачи (Automatic Repeat Request, ARQ). В беспроводных локальных сетях применяется процедура запрос ARQ с остановками (stop-and-wait ARQ). В этом случае источник, пославший кадр ожидает получения подтверждения (Acknowledgement, ACK), или как еще его называют квитанции, от приемника и только после этого посылает следующий кадр. Если же подтверждение не приходит в течение тайм-аута, то кадр (или подтверждение) считается утерянным и его передача повторяется. На рисунке 1.13 видно, что в этом случае производительность обмена данными ниже потенциально возможной, хотя передатчик и мог бы послать следующий кадр сразу же после отправки предыдущего, он обязан ждать прихода подтверждения.

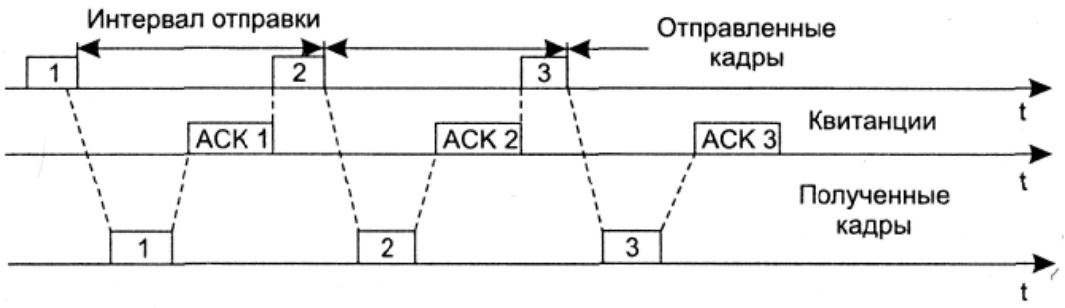


Рис. 1.13 Процедура запрос ARQ с остановками

1.4 АРХИТЕКТУРА IEEE 802.11

Институт инженеров по электротехнике и электронике IEEE (Institute of Electrical and Electronics Engineers) сформировал рабочую группу по стандартам для беспроводных локальных сетей 802.11 в 1990 году. Эта группа занялась разработкой всеобщего стандарта для радиооборудования и сетей, работающих на частоте 2,4 ГГц, со скоростями доступа 1 и 2 Мбит/с. Работы по созданию стандарта были завершены через 7 лет, и в июне 1997 года была ратифицирована первая спецификация 802.11. Стандарт IEEE 802.11 являлся первым стандартом для продуктов WLAN от независимой международной организации, разрабатывающей большинство стандартов для проводных сетей.

В этом подразделе будет рассмотрена архитектура самого популярного стандарта беспроводных локальных сетей — IEEE 802.11, а в следующем подразделе рассмотрим наиболее популярные стандарты: IEEE 802.11a, IEEE 802.11b и IEEE 802.11g.

1.4.1 СТЕК ПРОТОКОЛОВ IEEE 802.11

Естественно, что стек протоколов стандарта IEEE 802.11 соответствует общей структуре стандартов комитета 802, то есть состоит из физического уровня и канального уровня с подуровнями управления доступом к среде MAC (Media Access Control) и логической передачи данных LLC (Logical Link Control). Как и у всех технологий семейства 802, технология 802.11 определяется нижними двумя уровнями, то есть физическим уровнем и уровнем MAC, а уровень LLC выполняет свои стандартные общие для всех технологий LAN функции (рис. 1.14).

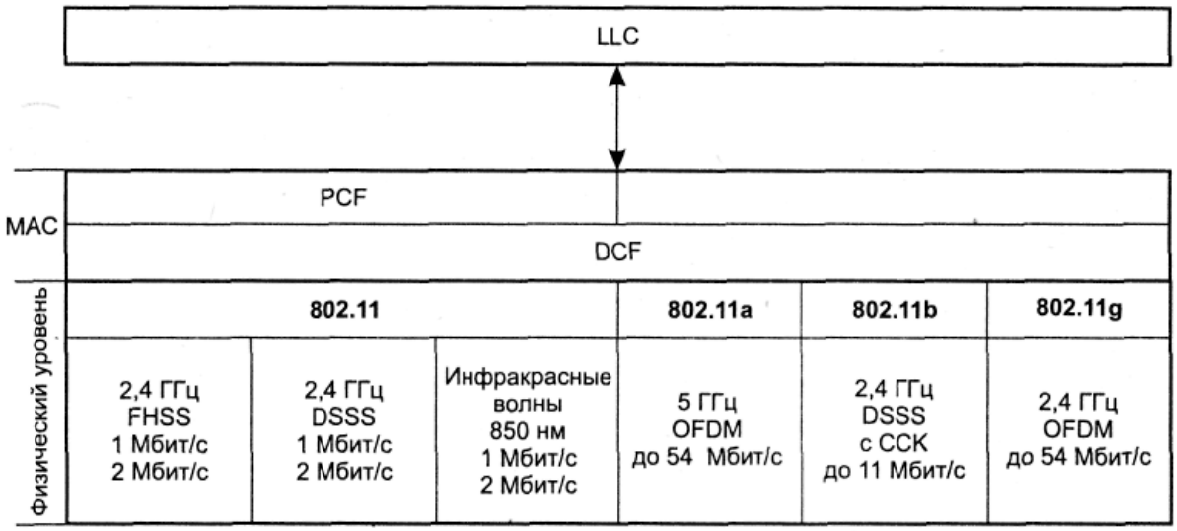


Рис. 1.14 Стек протоколов IEEE 802.11

На физическом уровне существует несколько вариантов спецификаций, которые отличаются используемым частотным диапазоном, методом кодирования и как следствие — скоростью передачи данных. Все варианты физического уровня работают с одним и тем же алгоритмом уровня MAC, но некоторые временные параметры уровня MAC зависят от используемого физического уровня.

1.4.2 УРОВЕНЬ ДОСТУПА К СРЕДЕ СТАНДАРТА 802.11

В сетях 802.11 уровень MAC обеспечивает два режима доступа к разделяемой среде (рис. 1.14):

- распределенный режим DCF (Distributed Coordination Function);
- централизованный режим PCF (Point Coordination Function).

1) Распределенный режим доступа DCF

Рассмотрим сначала, как обеспечивается доступ в распределенном режиме DCF. В этом режиме реализуется метод *множественного доступа с контролем несущей и предотвращением коллизий* (Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA). Вместо неэффективного в беспроводных сетях прямого распознавания коллизий по методу CSMA/CD, здесь используется их косвенное выявление. Для этого

каждый переданный кадр должен подтверждаться кадром положительной квитанции, посылаемым станцией назначения. Если же по истечении оговоренного тайм-аута квитанция не поступает, станция-отправитель считает, что произошла коллизия.

Режим доступа DCF требует синхронизации станций. В спецификации 802.11 эта проблема решается достаточно элегантно — временные интервалы начинают отсчитываться от момента окончания передачи очередного кадра (рис. 1.15). Это не требует передачи каких-либо специальных синхронизирующих сигналов и не ограничивает размер пакета размером слота, так как слоты принимаются во внимание только при принятии решения о начале передачи кадра.

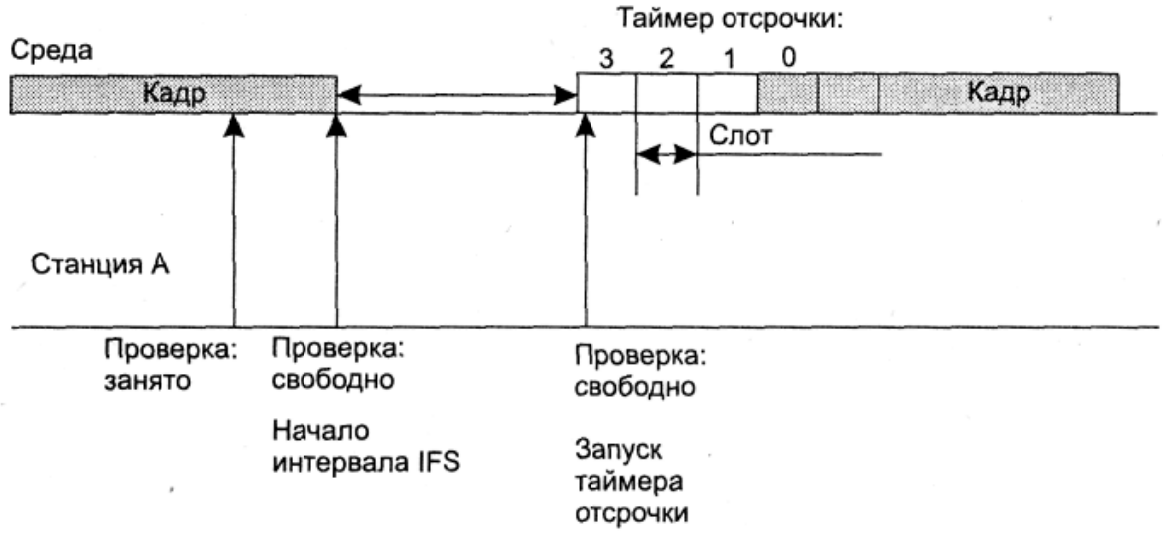


Рис. 1.15 Режим доступа DCF

Станция, которая хочет передать кадр, обязана предварительно прослушать среду. Стандарт IEEE 802.11 предусматривает два механизма контроля за активностью в канале (обнаружения несущей): *физический* и *виртуальный*. Первый механизм реализован на физическом уровне и сводится к определению уровня сигнала в антенне и сравнению его с пороговой величиной. Виртуальный механизм обнаружения несущей основан на том, что в передаваемых кадрах данных, а также в управляющих кадрах ACK и RTS/CTS содержится информация о времени, необходимом для передачи пакета (или группы пакетов) и получения подтверждения. Все устройства сети получают информацию о текущей передаче и могут определить, сколько времени канал будет занят, т.е. устройство при установлении связи всем сообщает, на какое время оно резервирует канал. Как только станция фиксирует окончание передачи кадра, она обязана отсчитать интервал времени, равный межкадровому интервалу (IFS). Если после истечения IFS среда все еще свободна, то начинается отсчет слотов фиксированной длительности. Кадр можно начать передавать только в начале какого-либо из слотов при условии, что среда свободна. Станция выбирает для передачи слот на основании усеченного экспоненциального двоичного алгоритма отсрочки, аналогичного используемому в методе CSMA/CD. Номер слота выбирается как случайное целое число, равномерно распределенное в интервале [0, CW], где CW означает Contention Window (конкурентное окно).

Рассмотрим этот довольно непростой метод доступа на примере рисунка 1.15. Пусть станция А выбрала для передачи на основании усеченного экспоненциального двоичного алгоритма отсрочки слот 3. При этом она присваивает таймеру отсрочки (назначение которого будет ясно из дальнейшего описания) значение 3 и начинает проверять

состояние среды в начале каждого слота. Если среда свободна, то из значения таймера отсрочки вычитается 1, и если результат равен нулю, то начинается передача кадра.

Таким образом, обеспечивается условие незанятости всех слотов, включая выбранный. Это условие является необходимым для начала передачи.

Если же в начале какого-нибудь слота среда оказывается занятой, то вычитания единицы не происходит, и таймер «замораживается». В этом случае станция начинает новый цикл доступа к среде, изменяя только алгоритм выбора слота для передачи. Как и в предыдущем цикле, станция следит за средой и при ее освобождении делает паузу в течение межкадрового интервала. Если среда осталась свободной, то станция использует значение «замороженного» таймера в качестве номера слота и выполняет описанную выше процедуру проверки свободных слотов с вычитанием единиц, начиная с замороженного значения таймера отсрочки.

Размер слота зависит от способа кодирования сигнала; так, для метода FHSS размер слота равен 28 мкс, а для метода DSSS — 1 мкс. Размер слота выбирается таким образом, чтобы он превосходил время распространения сигнала между любыми двумя станциями сети плюс время, затрачиваемое станцией на распознавание занятости среды. Если такое условие соблюдается, то каждая станция сети сумеет правильно распознать начало передачи кадра при прослушивании слотов, предшествующих выбранному ею для передачи слоту. Это, в свою очередь, означает следующее.

Коллизия может случиться только в том случае, когда несколько станций выбирают один и тот же слот для передачи.

В этом случае кадры искажаются, и квитанции от станций назначения не приходят. Не получив в течение определенного времени квитанцию, отправители фиксируют факт коллизии и пытаются передать свои кадры снова. При каждой повторной неудачной попытке передачи кадра интервал [0, CW], из которого выбирается номер слота, удваивается. Если, например, начальный размер окна выбран равным 8 (то есть CW = 7), то после первой коллизии размер окна должен быть равен 16 (CW = 15), после второй последовательной коллизии — 32 и т. д. Начальное значение CW в соответствии со стандартом 802.11 должно выбираться в зависимости от типа физического уровня, используемого в беспроводной локальной сети.

Как и в методе CSMA/CD, в данном методе количество неудачных попыток передачи одного кадра ограничено, но стандарт 802.11 не дает точного значения этого верхнего предела. Когда верхний предел в N попыток достигнут, то кадр отбрасывается, а счетчик последовательных коллизий устанавливается в нуль. Этот счетчик также устанавливается в нуль, если кадр после некоторого количества неудачных попыток все же передается успешно.

В беспроводных сетях возможна ситуация, когда два устройства (A и B) удалены и не слышат друг друга, однако оба попадают в зону охвата третьего устройства C (рис. 1.16) — так называемая проблема скрытого терминала. Если оба устройства A и B начнут передачу, то они принципиально не смогут обнаружить конфликтную ситуацию и определить, почему пакеты не проходят.

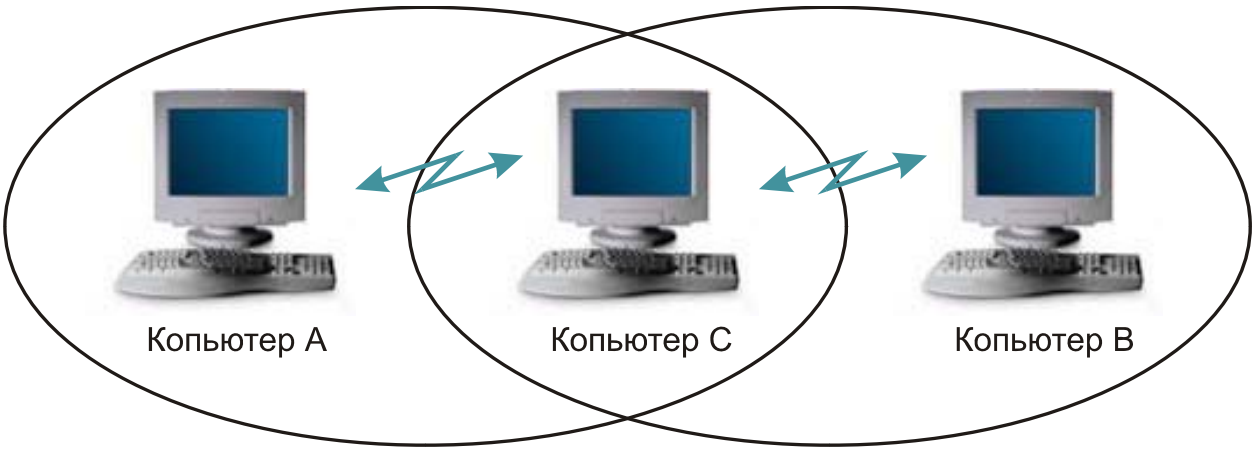


Рис. 1.16 Проблема скрытого терминала

В режиме доступа DCF применяются меры для устранения эффекта скрытого терминала. Для этого станция, которая хочет захватить среду и в соответствии с описанным алгоритмом начинает передачу кадра в определенном слоте, вместо кадра данных сначала посылает станции назначения короткий служебный кадр RTS (Request To Send, запрос на передачу). На этот запрос станция назначения должна ответить служебным кадром CTS (Clear To Send, свободна для передачи), после чего станция-отправитель посылает кадр данных. Кадр CTS должен оповестить о захвате среды те станции, которые находятся вне зоны сигнала станции-отправителя, но в зоне досягаемости станции-получателя, то есть являются скрытыми терминалами для станции-отправителя.

Максимальная длина кадра данных 802.11 равна 2346 байт, длина RTS-кадра — 20 байт, CTS-кадра — 14 байт. Так как RTS- и CTS-кадры гораздо короче, чем кадр данных, то потери данных в результате коллизии RTS- или CTS-кадров гораздо меньше, чем при коллизии кадров данных. Процедура обмена RTS- и CTS-кадрами не обязательна. От нее можно отказаться при небольшой нагрузке сети, поскольку в такой ситуации коллизии случаются редко, а значит, не стоит тратить дополнительное время на выполнение процедуры обмена RTS- и CTS-кадрами.

При помехах иногда случается, что теряются большие фреймы данных, поэтому можно уменьшить длину этих фреймов, путём *фрагментации*. Фрагментация фрейма - это выполняемая на уровне MAC функция, назначение которой - повысить надежность передачи фреймов через беспроводную среду. Под фрагментацией понимается дробление фрейма на меньшие фрагменты и передача каждого из них отдельно (рис. 1.17). Предполагается, что вероятность успешной передачи меньшего фрагмента через зашумленную беспроводную среду выше. Получение каждого фрагмента фрейма подтверждается отдельно; следовательно, если какой-нибудь фрагмент фрейма будет передан с ошибкой или вступит в коллизию, только его придется передавать повторно, а не весь фрейм. Это увеличивает пропускную способность среды.

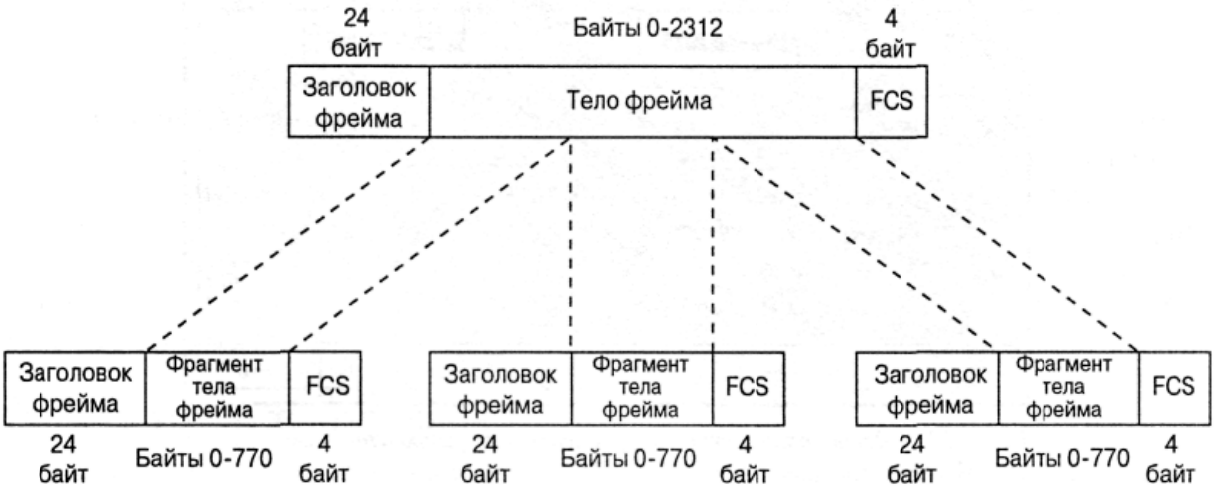


Рис. 1.17 Фрагментация фрейма

Размер фрагмента может задавать администратор сети. Фрагментации подвергаются только одноадресные фреймы. Широковещательные, или многоадресные, фреймы передаются целиком. Кроме того, фрагменты фрейма передаются пакетом, с использованием только одной итерации механизма доступа к среде DCF.

Хотя за счет фрагментации можно повысить надежность передачи фреймов в беспроводных локальных сетях, она приводит к увеличению «накладных расходов» MAC-протокола стандарта 802.11. Каждый фрагмент фрейма включает информацию, содержащуюся в заголовке 802.11 MAC, а также требует передачи соответствующего фрейма подтверждения. Это увеличивает число служебных сигналов MAC-протокола и снижает реальную производительность беспроводной станции. Фрагментация — это баланс между надежностью и непроизводительной загрузкой среды.

2) Централизованный режим доступа PCF

В том случае, когда в сети имеется станция, выполняющая функции точки доступа, может применяться также централизованный режим доступа PCF, обеспечивающий приоритетное обслуживание трафика. В этом случае говорят, что точка доступа играет роль арбитра среды.

Режим доступа PCF в сетях 802.11 сосуществует с режимом DCF. Оба режима координируются с помощью трех типов межкадровых интервалов (рис. 1.18).

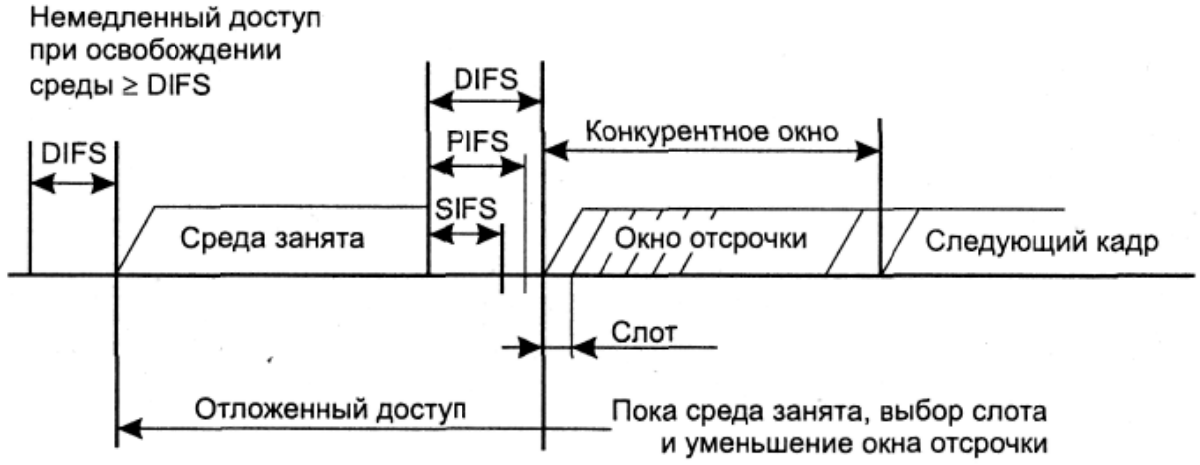


Рис. 1.18 Сосуществование режимов PCF и DCF

После освобождения среды каждая станция отсчитывает время простоя среды, сравнивая его с тремя значениями:

- короткий межкадровый интервал (Short IFS, SIFS);
- межкадровый интервал режима PCF (PIFS);
- межкадровый интервал режима DCF (DIFS).

Захват среды с помощью распределенной процедуры DCF возможен только в том случае, когда среда свободна в течение времени, равного или большего, чем DIFS. То есть в качестве IFS в режиме DCF нужно использовать интервал DIFS — самый длительный период из трех возможных, что дает этому режиму самый низкий приоритет.

Межкадровый интервал SIFS имеет наименьшее значение, он служит для первоочередного захвата среды ответными CTS-кадрами или квитанциями, которые продолжают или завершают уже начавшуюся передачу кадра.

Значение межкадрового интервала PIFS больше, чем SIFS, но меньше, чем DIFS. Промежутком времени между завершением PIFS и DIFS пользуется арбитр среды. В этом промежутке он может передать специальный кадр, который говорит всем станциям, что начинается контролируемый период. Получив этот кадр, станции, которые хотели бы воспользоваться алгоритмом DCF для захвата среды, уже не могут этого сделать, они должны дожидаться окончания контролируемого периода. Длительность этого периода объявляется в специальном кадре, но этот период может закончиться и раньше, если у станций нет чувствительного к задержкам трафика. В этом случае арбитр передает служебный кадр, после которого по истечении интервала DIFS начинает работать режим DCF.

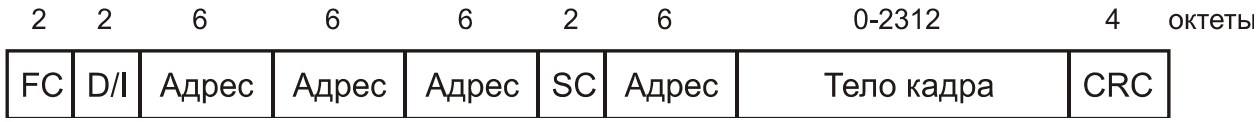
На управляемом интервале реализуется централизованный метод доступа PCF. Арбитр выполняет процедуру опроса, чтобы по очереди предоставить каждой такой станции право на использование среды, направляя ей специальный кадр. Станция, получив такой кадр, может ответить другим кадром, который подтверждает прием специального кадра и одновременно передает данные (либо по адресу арбитра для транзитной передачи, либо непосредственно станции).

Для того чтобы какая-то доля среды всегда доставалась асинхронному трафику, длительность контролируемого периода ограничена. После его окончания арбитр передает соответствующий кадр и начинается неконтролируемый период.

Каждая станция может работать в режиме PCF, для этого она должна подписаться на эту услугу при присоединении к сети.

1.4.3 КАДР MAC-ПОДУРОВНЯ

На рисунке 1.19 изображен формат кадра 802.11. Приведенная общая структура используется для всех информационных и управляющих кадров, хотя не все поля используются во всех случаях.



FC — управление кадром
D/I — идентификатор длительности/соединения
SC — управление очередностью

Рис. 1.19 Формат кадра MAC IEEE 802.11

Перечислим поля общего кадра:

- Управление кадром. Указывается тип кадра и предоставляется управляющая информация (объясняется ниже).
- Идентификатор длительности/соединения. Если используется поле длительности, указывается время (в микросекундах), на которое требуется выделить канал для успешной передачи кадра MAC. В некоторых кадрах управления в этом поле указывается идентификатор ассоциации, или соединения.
- Адреса. Число и значение полей адреса зависит от контекста. Возможны следующие типы адреса: источника, назначения, передающей станции, принимающей станции.
- Управление очередностью. Содержит 4-битовое подполе номера фрагмента, используемое для фрагментации и повторной сборки, и 12-битовый порядковый номер, используемый для нумерации кадров, передаваемых между данными приемником и передатчиком.
- Тело кадра. Содержит модуль данных протокола LLC или управляющая информация MAC.
- Контрольная последовательность кадра. 32-битовая проверка четности с избыточностью.

Поле управления кадром, показанное на рисунке 1.20 состоит из следующих полей:

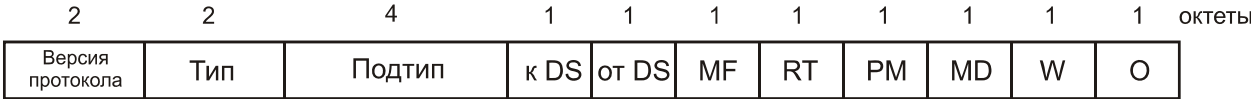
- Версия протокола. Версия 802.11, текущая версия - 0.
- Тип. Определим тип кадра: контроль, управление или данные.
- Подтип. Дальнейшая идентификация функций кадра. Разрешенные сочетания типов и подтипов перечислены в табл. 1.1.

Таблица 1.1. Разрешенные комбинации типа и подтипа

Значение типа	Описание типа	Значение подтипа	Описание подтипа
00	Управление	0000	Запрос ассоциации
00	Управление	0001	Ответ на запрос ассоциации
00	Управление	0010	Запрос повторной ассоциации
00	Управление	0011	Ответ на запрос повторной ассоциации
00	Управление	0100	Пробный запрос
00	Управление	0101	Ответ на пробный запрос
00	Управление	1000	Сигнальный кадр
00	Управление	1001	Объявление наличия трафика
00	Управление	1010	Разрыв ассоциации
00	Управление	1011	Аутентификация
00	Управление	1100	Отмена аутентификации
01	Контроль	1010	PS-опрос
01	Контроль	1011	Запрос передачи
01	Контроль	1100	«Готов к передаче»
01	Контроль	1101	Подтверждение
01	Контроль	1110	Без состязания (CF)-конец
01	Контроль	1111	CF-конец + CF-подтверждение
10	Данные	0000	Данные
10	Данные	0001	Данные + CF-подтверждение
10	Данные	0010	Данные + CF-опрос

10	Данные	0011	Данные + CF-подтверждение + CF-опрос .
10	Данные	0100	Нулевая функция (без данных)
10	Данные	0101	Данные + CF-подтверждение
10	Данные	0110	Данные + CF-опрос
10	Данные	0111	Данные + CF-подтверждение + CF-опрос

- К DS. Координационная функция MAC присваивает этому биту значение 1, если кадр предназначен распределительной системе.
- От DS. Координационная функция MAC присваивает этому биту значение 0, если кадр исходит от распределительной системы.
- Больше фрагментов. 1, если за данным фрагментом следует еще несколько.
- Повтор. 1, если данный кадр является повторной передачей предыдущего.
- Управление мощностью. 1, если передающая станция находится в режиме ожидания.
- Больше данных. Указывает, что станция передала не все данные. Каждый блок данных может передаваться как один кадр или как группа фрагментов в нескольких кадрах.
- WEP. 1, если реализован алгоритм конфиденциальности проводного эквивалента (Wired Equivalent Privacy, WEP). Протокол WEP используется для обмена ключами шифрования при безопасном обмене данными.
- Порядок. 1, если используется услуга строгого упорядочения, указывающая адресату, что кадры должны обрабатываться строго по порядку.



DS — система распределения
MF — больше фрагментов
RT — повтор
PM — управление мощностью
MD — больше данных
W—бит защиты проводного эквивалента
0 — порядок

Рис. 1.20 Поле управления кадром

Рассмотрим теперь различные типы кадров MAC.

Контрольные кадры

Контрольные кадры способствуют надежной доставке информационных кадров. Существует шесть подтипов контрольных кадров:

- Опрос после выхода из экономичного режима (PS-опрос). Данный кадр передается любой станцией станции, включающей точку доступа. В кадре запрашивается передача кадра, прибывшего, когда станция находилась в режиме энергосбережения, и в данный момент размещенного в буфере точки доступа.
- Запрос передачи (RTS). Данный кадр является первым из четверки, используемой для обеспечения надежной передачи данных. Станция, пославшая это сообщение, предупреждает адресата и остальные станции, способные принять данное сообщение, о своей попытке передать адресату информационный кадр.

- «Готов к передаче» (CTS). Второй кадр четырехкадровой схемы. Передается станцией-адресатом станции-источнику и предоставляет право отправки информационного кадра.
- Подтверждение (АСК). Подтверждение успешного приема предыдущих данных, кадра управления или кадра PS-опрос.
- Без состязания (CF)-конец. Объявляет конец периода без состязания; часть стратегии использования распределенного режима доступа.
- CF-конец + CF-подтверждение. Подтверждает кадр CF-конец. Данный кадр завершает период без состязания и освобождает станции от ограничений, связанных с этим периодом.

Информационные кадры

Существует восемь подтипов информационных кадров, собранных в две группы. Первые четыре подтипа определяют кадры, переносящие данные высших уровней от исходной станции к станции-адресату. Перечислим эти кадры:

- Данные. Просто информационный кадр. Может использоваться как в период состязания, так и в период без состязания.
- Данные + CF-подтверждение. Может передаваться только в период без состязания. Помимо данных в этом кадре имеется подтверждение полученной ранее информации.
- Данные + CF-опрос. Используется точечным координатором для доставки данных к мобильной станции и для запроса у мобильной станции информационного кадра, который находится в ее буфере.
- Данные + CF-подтверждение + CF-опрос. Объединяет в одном кадре функции двух описанных выше кадров.

Остальные четыре подтипа информационных кадров фактически не переносят данных пользователя. Информационный кадр «нулевая функция» не переносит ни данных, ни запросов, ни подтверждений. Он используется только для передачи точке доступа бита управления питанием в поле управления кадром, указывая, что станция перешла в режим работы с пониженным энергопотреблением. Оставшиеся три кадра (CF-подтверждение, CF-опрос, CF-подтверждение + CF-опрос) имеют те же функции, что и описанные выше подтипы кадров (данные + CF-подтверждение, данные + CF-опрос, данные + CF-подтверждение + CF-опрос), но не несут пользовательских данных.

Кадры управления

Кадры управления используются для управления связью станций и точек доступа. Возможны следующие подтипы:

- Запрос ассоциации. Посылается станцией к точке доступа с целью запроса ассоциации с данной сетью с базовым набором услуг (Basic Service Set, BSS). Кадр включает информацию о возможностях, например, будет ли использоваться шифрование, или способна ли станция отвечать при опросе.
- Ответ на запрос ассоциации. Возвращается точкой доступа и указывает, что запрос ассоциации принят.
- Запрос повторной ассоциации. Посылается станцией при переходе между BSS, когда требуется установить ассоциацию с точкой доступа в новом BSS. Использование повторной ассоциации, а не просто ассоциации позволяет новой точке доступа договариваться со старой о передаче информационных кадров по новому адресу.

- Ответ на запрос повторной ассоциации. Возвращается точкой доступа и указывает, что запрос повторной ассоциации принят.
- Пробный запрос. Используется станцией для получения информации от другой станции или точки доступа. Кадр используется для локализации BSS стандарта IEEE 802.11.
- Ответ на пробный запрос. Отклик на пробный запрос.
- Сигнальный кадр. Передается периодически, позволяет мобильным станциям локализировать и идентифицировать BSS.
- Объявление наличия трафика. Посылается мобильной станцией с целью уведомления других (которые могут находиться в режиме пониженного энергопотребления), что в буфере данной станции находятся кадры, адресованные другим.
- Разрыв ассоциации. Используется станцией для аннуляции ассоциации.
- Аутентификация. Для аутентификации станций используются множественные кадры.
- Отмена аутентификации. Передается для прекращения безопасного соединения.

1.5 СТАНДАРТЫ IEEE 802.11

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

В стандарте IEEE 802.11b благодаря высокой скорости передачи данных (до 11 Мбит/с), практически эквивалентной пропускной способности обычных проводных локальных сетей Ethernet, а также ориентации на диапазон 2,4 ГГц, этот стандарт завоевал наибольшую популярность у производителей оборудования для беспроводных сетей.

Поскольку оборудование, 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.

Стандарт IEEE 802.11a имеет большую ширину полосы из семейства стандартов 802.11, предусматривая скорость передачи данных до 54 Мбит/с.

В отличие от базового стандарта, ориентированного на область частот 2,4 ГГц, спецификациями 802.11a предусмотрена работа в диапазоне 5 ГГц. В качестве метода модуляции сигнала выбрано ортогональное частотное мультиплексирование (OFDM).

К недостаткам 802.11a относятся более высокая потребляемая мощность радиопередатчиков для частот 5 ГГц, а так же меньший радиус действия.

Стандарт IEEE 802.11g является логическим развитием 802.11b и предполагает передачу данных в том же частотном диапазоне. Кроме того, стандарт 802.11g полностью совместим с 802.11b, то есть любое устройство 802.11g должно поддерживать работу с устройствами 802.11b. Максимальная скорость передачи в стандарте 802.11g составляет 54 Мбит/с, поэтому на сегодняшний день это наиболее перспективный стандарт беспроводной связи.

При разработке стандарта 802.11g рассматривались две несколько конкурирующие технологии: метод ортогонального частотного разделения OFDM и метод двоичного пакетного сверочного кодирования PBCC, опционально реализованный в стандарте 802.11b. В результате стандарт 802.11g содержит компромиссное решение: в качестве базовых применяются технологии OFDM и CCK, а опционально предусмотрено использование технологии PBCC. О технологиях CCK и OFDM расскажем чуть позже.

Набор стандартов 802.11 определяет целый ряд технологий реализации физического уровня (Physical Layer Protocol, PHY), которые могут быть использованы подуровнем 802.11 MAC. В этой главе рассматривается каждый из уровней PHY:

- Уровень PHY стандарта 802.11 со скачкообразной перестройкой частоты (FHSS) в диапазоне 2,4 ГГц.
- Уровень PHY стандарта 802.11 с расширением спектра методом прямой последовательности (DSSS) в диапазоне 2,4 ГГц.
- Уровень PHYстандарта 802.l1b с комплиментарным кодированием в диапазоне 2,4 ГГц.
- Уровень PHY стандарта 802.11a с ортогональным частотным мультиплексированием (OFDM) в диапазоне 5 ГГц.
- Расширенный физический уровень (Extended Rate Physical Layer, ERP) стандарта 802.11g в диапазоне 2,4 ГГц.

Основное назначение физических уровней стандарта 802.11 - обеспечить механизмы беспроводной передачи для подуровня MAC, а также поддерживать выполнение вторичных функций, таких как оценка состояния беспроводной среды и сообщение о нем подуровню MAC. Уровни MAC и PHY разрабатывались так, чтобы они были независимыми. Именно независимость между MAC и подуровнем PHY и позволила использовать дополнительные высокоскоростные физические уровни, описанные в стандартах 802.l1b, 802.11a и 802.11g.

Каждый из физических уровней стандарта 802.11 имеет два подуровня.

- Physical Layer Convergence Procedure (PLCP). Процедура определения состояния физического уровня.
- Physical Medium Dependent (PMD). Подуровень физического уровня, зависящий от среды передачи.

На рисунке 1.21 показано, как эти подуровни соотносятся между собой и с вышестоящими уровнями в модели взаимодействия открытых систем (Open System Interconnection, OSI).

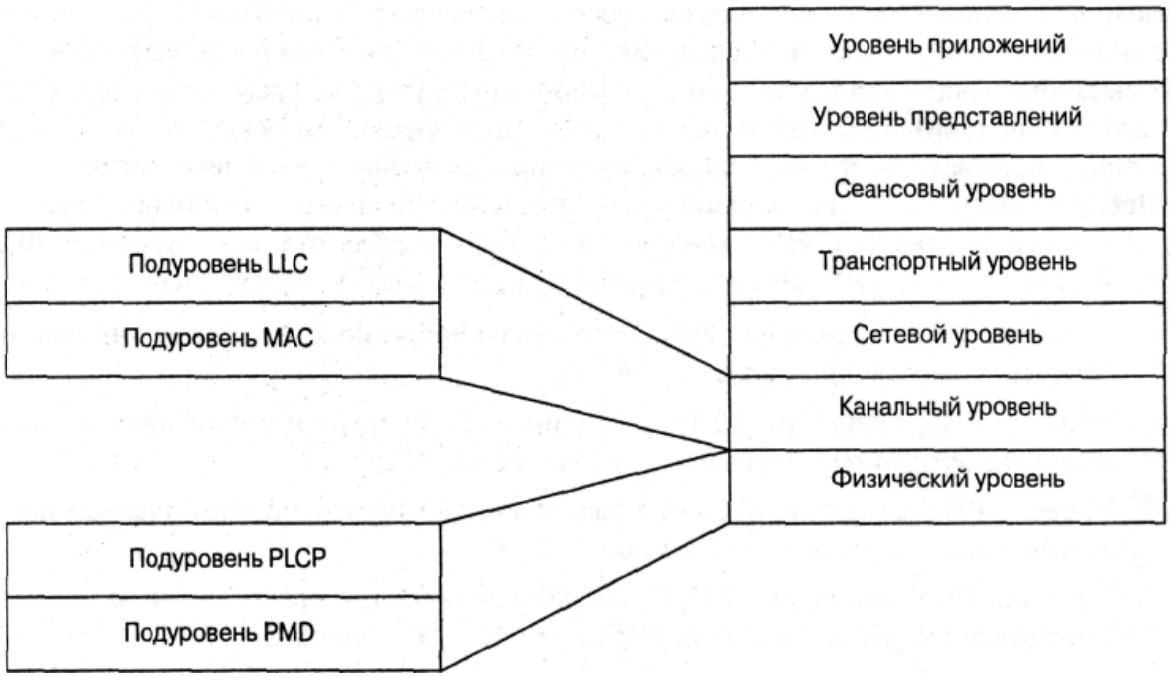


Рис. 1.21 Подуровни уровня PHY

Подуровень PLCP по существу является уровнем обеспечения взаимодействия, на котором осуществляется перемещение элементов данных протокола MAC (MAC Protocol Data Units, MPDU) между MAC-станциями с использованием подуровня PMD, на котором

реализуется тот или иной метод передачи и приема данных через беспроводную среду. Подуровни PLCP и PMD отличаются для разных вариантов стандарта 802.11.

Перед тем как приступить к рассмотрению физических уровней рассмотрим одну из составляющих физического уровня, до сих пор не упомянутую, а именно скремблирование.

Одна из особенностей, лежащих в основе современных передатчиков, благодаря которой данные можно передавать с высокой скоростью, — это предположение о том, что данные, которые предлагаются для передачи, поступают, с точки зрения передатчика, случайным образом. Без этого предположения многие преимущества, получаемые за счет применения остальных составляющих физического уровня, остались бы нереализованными.

Однако вполне вероятно и часто происходит на практике, что принимаемые данные не вполне случайны и на самом деле могут содержать повторяющиеся наборы и длинные последовательности нулей и единиц.

Скремблирование (перестановка элементов) — это метод, посредством которого принимаемые данные делаются более похожими на случайные; достигается это путем перестановки битов последовательности таким образом, чтобы превратить ее из структурированной в похожую на случайную. Эту процедуру иногда называют отбеливание потока данных. Дескремблер приемника затем выполняет обратное преобразование этой случайной последовательности с целью получения исходной структурированной последовательности. Большинство из способов скремблирования относится к числу самосинхронизирующихся; это означает, что дескремблер способен самостоятельно синхронизироваться со скремблером.

1.5.1 IEEE 802.11

Исходный стандарт 802.11 определяет три метода передачи на физическом уровне:

- Передача в диапазоне инфракрасных волн.
- Технология расширения спектра путем скачкообразной перестройки частоты (FHSS) в диапазоне 2,4 ГГц.
- Технология широкополосной модуляции с расширением спектра методом прямой последовательности (DSSS) в диапазоне 2,4 ГГц.

1) Передача в диапазоне инфракрасных волн

Средой передачи являются инфракрасные волны диапазона 850 нм, которые генерируются либо полупроводниковым лазерным диодом, либо светодиодом (LED). Так как инфракрасные волны не проникают через стены, область покрытия LAN ограничивается зоной прямой видимости. Стандарт предусматривает три варианта распространения излучения: ненаправленную антенну, отражение от потолка и фокусное направленное излучение. В первом случае узкий луч рассеивается с помощью системы линз. Фокусное направленное излучение предназначено для организации двухточечной связи, например, между двумя зданиями

2) Беспроводные локальные сети со скачкообразной перестройкой частоты (FHSS)

Беспроводные локальные сети FHSS поддерживают скорости передачи 1 и 2 Мбит/с. Устройства FHSS делят предназначенную для их работы полосу частот от 2,402 до 2,480 ГГц на 79 неперекрывающихся каналов (это справедливо для Северной Америки и большей части Европы). Ширина каждого из 79 каналов составляет 1 МГц, поэтому беспроводные локальные сети FHSS используют относительно высокую скорость передачи символов, 1 МГц, и намного меньшую скорость перестройки с канала на канал.

Последовательность перестройки частоты должна иметь следующие параметры: частота перескоков не менее 2,5 раз в секунду как минимум между 6-ю (6 МГц) каналами.

Чтобы минимизировать число коллизий между перекрывающимися зонами покрытия, возможные последовательности перескоков должны быть разбиты на три набора последовательностей, длина которых для Северной Америки и большей части Европы составляет 26. В табл. 1.2 представлены схемы скачкообразной перестройки частоты, обеспечивающие минимальное перекрытие.

Таблица 1.2 Схема FHSS для Северной Америки и Европы

Набор	Схема скачкообразной перестройки частоты
1	{0,3,6,9,12,15,18,21,24,27,30,33,36,39,42,45,48,51,54,57,60,63,66,69,72,75}
2	{1,4,7,10,13,16,19,22,25,28,31,34,37,40,43,46,49,52,55,58,61,64,67,70,73,76}
3	{2,5,8,11,14,17,20,23,26,29,32,35,38,41,44,47,50,53,56,59,62,65,68,71,72,77}

По сути, схема скачкообразной перестройки частоты обеспечивает неторопливый переход с одного возможного канала на другой таким образом, что после каждого скачка покрывается полоса частот, равная как минимум 6 МГц, благодаря чему в многосотовых сетях минимизируется возможность возникновения коллизий.

После того как уровень MAC пропускает MAC-фрейм, который в локальных беспроводных сетях FHSS называется также служебный элемент данных PLCP, или PSDU (PLCP Service Data Unit), подуровень PLCP добавляет два поля в начало фрейма, чтобы сформировать таким образом фрейм PPDU (PPDU — элемент данных протокола PLCP). На рисунке 1.22 представлен формат фрейма FHSS подуровня PLCP.

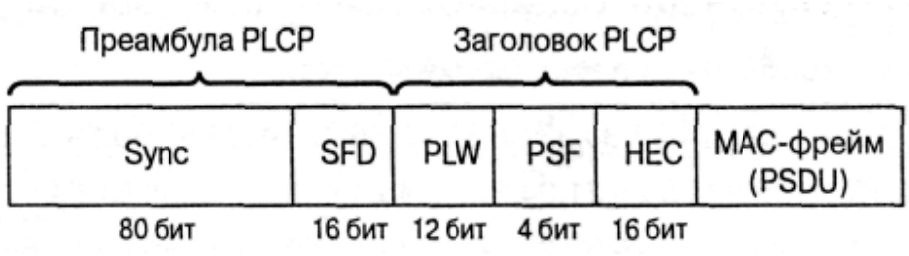


Рис. 1.22. Формат фрейма FHSS подуровня PLCP

Преамбула PLCP состоит из двух подполей:

- Подполе Sync размером 80 бит. Строка, состоящая из чередующихся 0 и 1, начинается с 0. Приемная станция использует это поле, чтобы принять решение о выборе антенны при наличии такой возможности, откорректировать уход частоты (frequency offset) и синхронизировать распределение пакетов (packet timing).
- Подполе флага начала фрейма (start of frame delimiter, SFD) размером 16 бит. Состоит из специфической строки (0000 1100 1011 1101, крайний слева бит первый) в обеспечение синхронизации фреймов (frame timing) для приемной станции.

Заголовок фрейма PLCP состоит из трех подполей:

- Слово длины служебного элемента данных PLCP (PSDU), PSDU Length Word (PLW) размером 12 бит. Указывает размер фрейма MAC (PSDU) в октетах.
- Сигнальное поле PLCP (Signaling Field PLCP, PSF) размером 4 бит. Указывает скорость передачи данных конкретного фрейма.
- HEC (Header Error Check) – контрольная сумма фрейма.

Служебный элемент данных PLCP (PSDU) проходит через операцию скремблирования с целью отбеливания (рандомизации) последовательности входных битов. Получившийся в результате PSDU представлен на рисунке 1.23. Заполняющие символы вставляются между всеми 32-символьными блоками. Эти заполняющие символы устраняют любые систематические отклонения в данных, например, когда единиц больше,

чем нулей, или наоборот, которые могли бы привести к нежелательным эффектам при дальнейшей обработке.

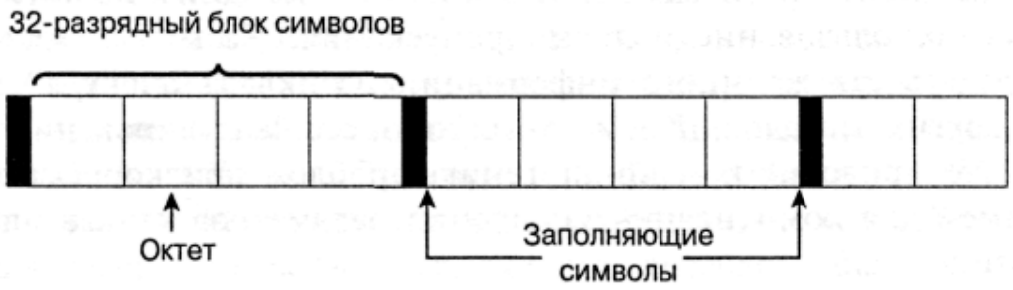


Рис. 1.23 Скремблированный PSDU в технологии FHSS

Подуровень PLCP преобразует фрейм в поток битов и передает его на подуровень PMD. Подуровень PMD технологии FHSS модулирует поток данных с использованием модуляции, основанной на гауссовой частотной модуляции (Gaussian Frequency Shift Keying, GFSK).

3) Беспроводные локальные сети, использующие широкополосную модуляцию DSSS с расширением спектра методом прямой последовательности

В спецификации стандарта 802.11 оговорено использование и другого физического уровня — на основе технологии широкополосной модуляции с расширением спектра методом прямой последовательности (DSSS). Как было указано в стандарте 802.11 разработки 1997 года, технология DSSS поддерживает скорости передачи 1 и 2 Мбит/с.

Аналогично подуровню PLCP, используемому в технологии FHSS, подуровень PLCP технологии DSSS стандарта 802.11 добавляет два поля во фрейм MAC, чтобы сформировать PPDU: преамбулу PLCP и заголовок PLCP. Формат фрейма представлен на рисунке 1.24.

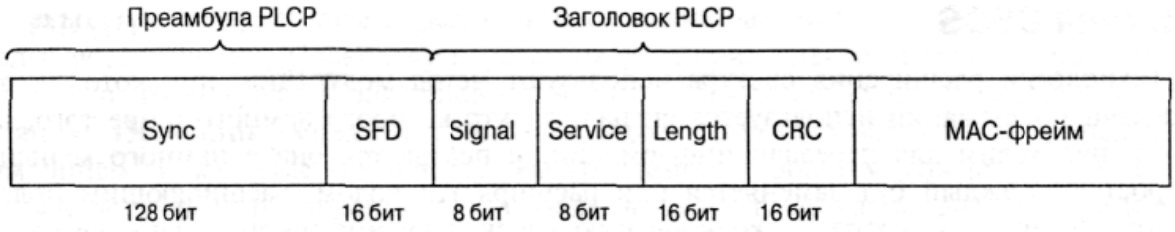


Рис. 1.24. Формат фрейма DSSS подуровня PLCP

Преамбула PLCP состоит из двух подполей:

- Подполе Sync шириной 128 бит, представляющее собой строку, состоящую из единиц. Задача этого подполя — обеспечить синхронизацию для приемной станции.
- Подполе SFD шириной 16 бит; в нем содержится специфичная строка OxF3A0; его задача - обеспечить тайминг (timing) для приемной станции.

Заголовок PLCP состоит из четырех подполей:

- Подполе Signal шириной 8 бит, указывающее тип модуляции и скорость передачи для данного фрейма.

- Подполе Service шириной 8 бит, зарезервировано. Это означает, что во время разработки спецификации стандарта оно осталось неопределенным; предполагается, что оно пригодится в будущих модификациях стандарта.
- Подполе Length шириной 16 бит, указывающее количество микросекунд (из диапазона 16—216 - 1), необходимое для передачи части MAC фрейма.
- Подполе CRC 16-битная контрольная сумма.

Подуровень PLCP преобразует фрейм в поток битов и передает данные на подуровень PMD. Весь PPDU проходит через процесс скремблирования с целью рандомизации данных.

Скремблированная преамбула PLCP всегда передается со скоростью 1 Мбит/с, в то время как скремблированный фрейм MPDU передается со скоростью, указанной в подполе Signal. Подуровень PMD модулирует отбеленный поток битов, используя следующие методы модуляции:

- Двоичная относительная фазовая модуляция (Differential Binary Phase Shift Keying, DBPSK) для скорости передачи 1 Мбит/с.
- Квадратурная относительная фазовая модуляция (Differential Quadrature Phase Shift Key, DQPSK) для скорости передачи 2 Мбит/с.

1.5.2 IEEE 802.11B

На физическом уровне к MAC-кадрам (MPDU) добавляется заголовок физического уровня, состоящий из преамбулы и собственно PLCP-заголовка (рис. 1.25).

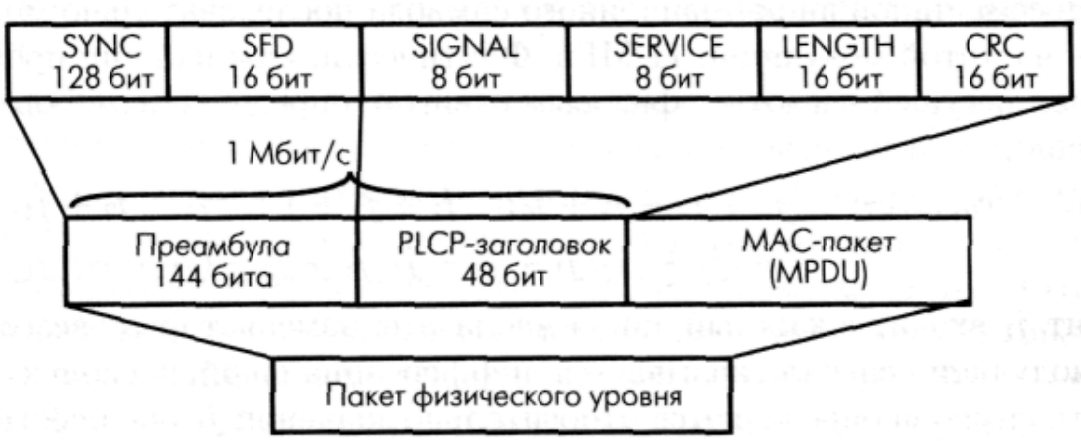


Рис. 1.25 Структура кадров сети IEEE 802.11b физического уровня

Преамбула содержит стартовую синхропоследовательность (SYNC) для настройки приемника и 16-битный код начала кадра (SFD) — число $F3A0_{16}$. PLCP-заголовок включает поля SIGNAL (информация о скорости и типе модуляции), SERVICE (дополнительная информация, в том числе о применении высокоскоростных расширений и PBSS-модуляции) и LENGTH (время в микросекундах, необходимое для передачи следующей за заголовком части кадра). Все три поля заголовка защищены 16-битной контрольной суммой CRC.

В стандарте IEEE 802.11b предусмотрено два типа заголовков: длинный и короткий (рис. 1.26).

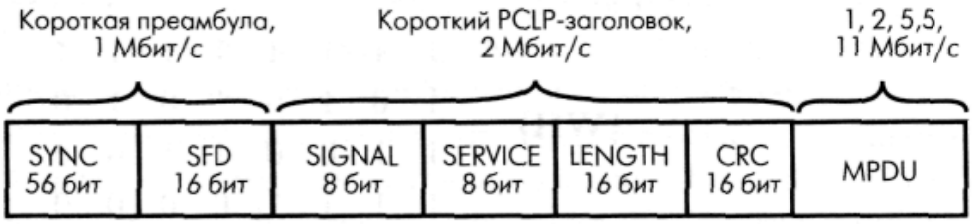


Рис. 1.26. Короткий заголовок кадров сети 802.11b

Они отличаются длиной синхропоследовательности (128 и 56 бит), способом ее генерации, а также тем, что символ начала кадра в коротком заголовке передается в обратном порядке. Кроме того, если все поля длинного заголовка передаются со скоростью 1 Мбит/с, то при коротком заголовке преамбула транслируется на скорости 1 Мбит/с, другие поля заголовка — со скоростью 2 Мбит/с. Остальную часть кадра можно передавать на любой из допустимых стандартом скоростей передачи, указанных в полях SIGNAL и SERVICE. Короткие заголовки физического уровня предусмотрены спецификацией IEEE 802.11b для увеличения пропускной способности сети.

Из описания процедур связи сети IEEE 802.11 видно, что «накладные расходы» в этом стандарте выше, чем в проводной сети Ethernet. Поэтому крайне важно обеспечить высокую скорость передачи данных в канале. Повысить пропускную способность канала с заданной шириной полосы частот можно, разрабатывая и применяя более совершенные методы модуляции. По этому пути пошла группа разработчиков IEEE 802.11b.

Напомним, что изначально стандарт IEEE 802.11 предусматривал работу в режиме DSSS с использованием так называемой Баркеровской последовательности (Barker) длиной 11 бит: B1 = (10110111000). Каждый информационный бит замещается своим произведением по модулю 2 (операция «исключающее ИЛИ») с данной последовательностью, т. е. каждая информационная единица заменяется на B1, каждый ноль — на инверсию B1. В результате бит заменяется последовательностью 11 чипов. Далее сигнал кодируется посредством дифференциальной двух- или четырехпозиционной фазовой модуляции (DBPSK или DQPSK, один или два чипа на символ соответственно). При частоте модуляции несущей 11 МГц общая скорость составляет в зависимости от типа модуляции 1 и 2 Мбит/с.

Стандарт IEEE 802.11b дополнительно предусматривает скорости передачи 11 и 5,5 Мбит/с. Для этого используется так называемая CCK-модуляция (Complementary Code Keying — кодирование комплементарным кодом).

Хотя механизм расширения спектра, используемый для получения скоростей 5,5 и 11 Мбит/с с применением CCK, относится к методам, которые применяются для скоростей 1 и 2 Мбит/с, он по-своему уникален. В обоих случаях применяется метод расширения, но при использовании модуляции CCK расширяющий код представляет собой код из 8 комплексных чипов, в то время как при работе со скоростями 1 и 2 Мбит/с применяется 11-разрядный код. 8-чиповый код определяется или 4, или 8 битами — в зависимости от скорости передачи данных. Скорость передачи чипов составляет 11 Мчип/с, т.е. при 8 комплексных чипах на символ и 4 или 8 битов на символ можно достигнуть скорости передачи данных 5,5 и 11 Мбит/с.

Для того чтобы передавать данные со скоростью 5,5 Мбит/с, нужно сгруппировать скремблированный поток битов в символы по 4 бита (b0, b1, b2 и b3). Последние два бита (b2 и b3) используются для определения 8 последовательностей комплексных чипов, как показано в табл. 1.3, где {cl, c2, c3, c4, c5, c6, c7, c8} представляют чипы последовательности. В табл. 1.3 j представляет мнимое число, корень квадратный из -1, и откладывается по мнимой, или квадратурной оси комплексной плоскости.

Таблица 1.3 Последовательность чипов ССК

(b2, b3)	C1	C2	C3	C4	C5	C6	C7	C8
00	j	1	j	-1	j	1	-1	1
01	-j	-1	-j	1	j	1	-j	1
10	-j	1	-j	-1	-j	1	j	1
11	j	-1	j	1	-j	1	j	1

Теперь, имея последовательность чипов, определенную битами (b2, b3), можно использовать первые два бита (b0, b1) для определения поворота фазы, осуществляемого при модуляции по методу DQPSK, который будет применен к последовательности (табл. 1.4). Вы должны также пронумеровать каждый 4-битовый символ PSDU, начиная с 0, чтобы можно было определить, преобразуете вы четный либо нечетный символ в соответствии с этой таблицей. Следует помнить, что речь идет об использовании DQPSK, а не QPSK, и поэтому представленные в таблице изменения фазы отсчитываются по отношению к предыдущему символу или, в случае первого символа PSDU, по отношению к последнему символу предыдущего DQPSK символа, передаваемого со скоростью 2 Мбит/с.

Таблица 1.4. Поворот фазы при модуляции ССК

(b0,b1)	Изменение фазы четных символов	Изменение фазы нечетных символов
00	0	π
01	$\pi/2$	$-\pi/2$
11	π	0
10	$-\pi/2$	$\pi/2$

Это вращение фазы применяется по отношению к 8 комплексным чипам символа, затем осуществляется модуляция на подходящей несущей частоте.

Чтобы передавать данные со скоростью 11 Мбит/с, скремблированная последовательность битов PSDU разбивается на группы по 8 символов. Последние 6 битов выбирают одну последовательность, состоящую из 8 комплексных чипов, из числа 64 возможных последовательностей, почти так же, как использовались биты (b2, b3) для выбора одной из четырех возможных последовательностей. Биты (b0,b1) используются таким же образом, как при модуляции ССК на скорости 5,5 Мбит/с для вращения фазы последовательности и дальнейшей модуляции на подходящей несущей частоте.

В чем достоинство ССК-модуляции? Дело в том, что чипы символа определяются на основе последовательностей Уолша-Адамара. Последовательности Уолша-Адамара хорошо изучены, обладают отличными автокорреляционными свойствами. Что немаловажно, каждая такая последовательность мало коррелирует сама с собой при фазовом сдвиге - очень полезное свойство при борьбе с переотраженными сигналами. Нетрудно заметить, что теоретическое операционное усиление ССК-модуляции - 3 дБ (в два раза), поскольку без кодирования QPSK-модулированный с частотой 11 Мбит/с сигнал может транслировать 22 Мбит/с. Как видно, ССК-модуляция представляет собой вид блочного кода, а потому достаточно проста при аппаратной реализации. Совокупность этих свойств и обеспечила ССК место в стандарте IEEE 802.11b в качестве обязательного вида модуляции.

На практике важно не только операционное усиление. Существенную роль играет и равномерность распределения символов в фазовом пространстве — они должны как можно дальше отстоять друг от друга, чтобы минимизировать ошибки их детектирования. И с этой точки зрения ССК-модуляция не выглядит оптимальной, ее реальное операционное усиление не превышает 2 дБ. Поэтому изначально прорабатывался другой

способ модуляции — пакетное бинарное сверточное кодирование PBCC (Packet Binary Convolutional Coding). Этот метод вошел в стандарт IEEE 802.11b как дополнительная (необязательная) опция. Механизм PBCC (рис. 1.27) позволяет добиваться в сетях IEEE 802.11b пропускной способности 5,5; 11 и 22 Мбит/с.

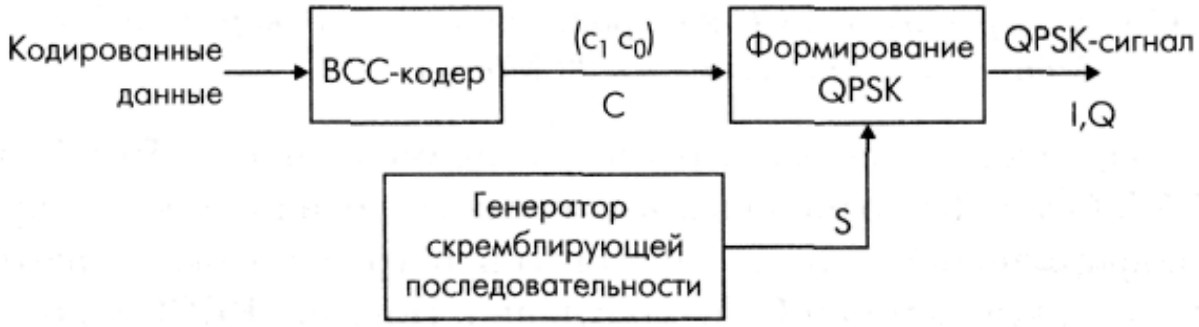


Рис. 1.27 Общая схема PBCC-модуляции

Как следует из названия, метод основан на сверточном кодировании. Для скоростей 5,5 и 11 Мбит/с поток информационных битов поступает в шестиразрядный сдвиговый регистр с сумматорами (рис. 1.28). В начальный момент времени все триггеры сдвигового регистра инициализируют нулем. В результате каждый исходный бит d заменяется двумя битами кодовой последовательности (c0, c1). При скорости 11 Мбит/с c0 и c1 задают один символ четырехпозиционной QPSK-модуляции. Для скорости 5,5 Мбит/с используют двухпозиционную BPSK-модуляцию, последовательно передавая кодовые биты c0 и c1. Если же нужна скорость 22 Мбит/с, схема кодирования усложняется (рис. 1.29): три кодовых бита (c0-c2) определяют один символ в 8-позиционной 8-PSK-модуляции.

После формирования PSK-символов происходит скремблирование. В зависимости от сигнала s (рис. 1.23) символ остается без изменений (s = 0), либо его фаза увеличивается на (s = 1). Значение s определяет 256-битовая циклически повторяющаяся последовательность S. Она формируется на основе начального вектора U = 338Bh, в котором равное число нулей и единиц.

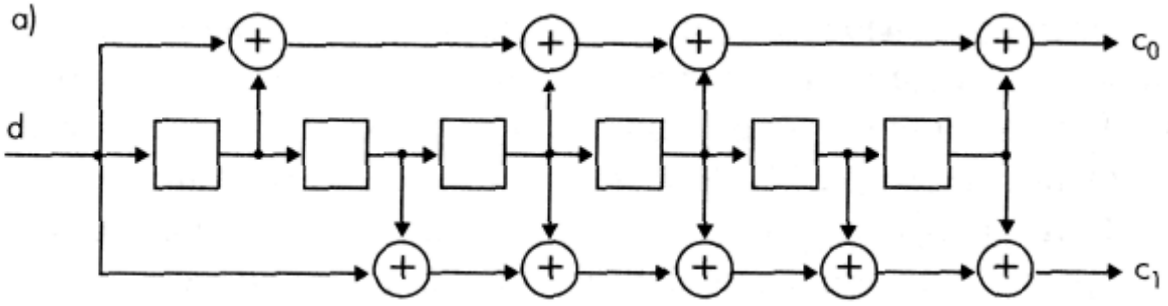


Рис. 1.28 Свёрточное кодирование с двумя битами кодовой последовательности

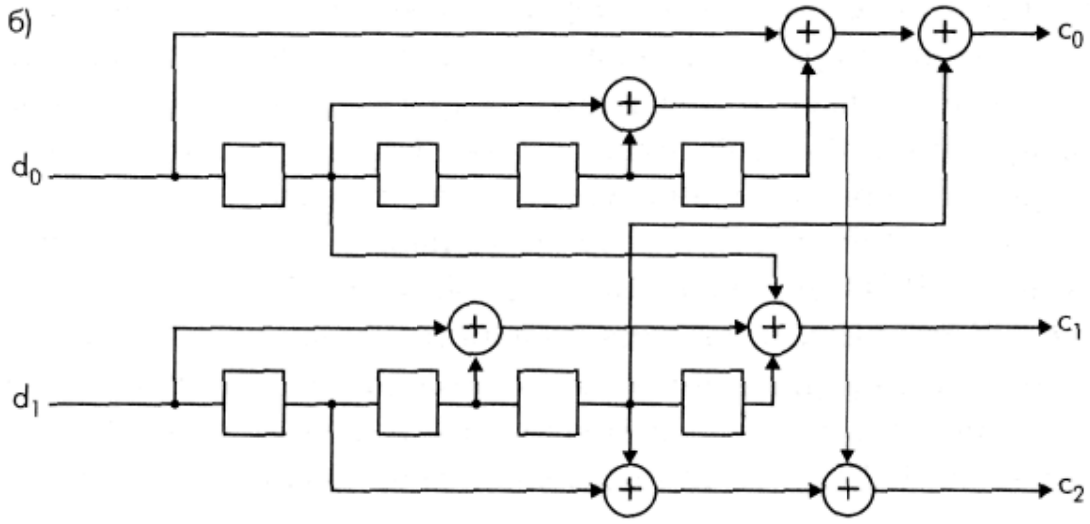


Рис. 1.29 Свёрточное кодирование с тремя битами кодовой последовательности

У шестиразрядного сдвигового регистра, применяемого в PBCC для скоростей 11 и 5,5 Мбит/с, 64 возможных выходных состояния. Так что при модуляции PBCC информационные биты в фазовом пространстве оказываются гораздо дальше друг от друга, чем при CCK-модуляции. Поэтому PBCC и позволяет при одних и тех же соотношении сигнал/шум и уровне ошибок вести передачу с большей скоростью, чем в случае CKK. Однако плата за более эффективное кодирование - сложность аппаратной реализации данного алгоритма.

1.5.3 IEEE 802.11A

Стандарт IEEE 802.11a появился практически одновременно с IEEE 802.11b, в сентябре 1999 года. Эта спецификация была ориентирована на работу в диапазоне 5 ГГц и основана на принципиально ином, чем описано выше, механизме кодирования данных — на частотном мультиплексировании посредством ортогональных несущих (OFDM).

Стандарт 802.11a определяет характеристики оборудования, применяемого в офисных или городских условиях, когда распространение сигнала происходит по многолучевым каналам из-за множества отражений.

В IEEE 802.11a каждый кадр передается посредством 52 ортогональных несущих, каждая с шириной полосы порядка 300 кГц (20 МГц/64). Ширина одного канала — 20 МГц. Несущие модулируют посредством BPSK, QPSK, а также 16- и 64-позиционной квадратурной амплитудной модуляции (QAM). В совокупности с различными скоростями кодирования r (1/2 и 3/4, для 64-QAM — 2/3 и 3/4) образуется набор скоростей передачи 6, 9, 12, 18, 24, 36, 48 и 54 Мбит/с. В табл. 1.5 показано, как необходимая скорость передачи данных преобразуется в соответствующие параметры узлов передатчика OFDM.

Таблица 1.5 Параметры передатчика стандарта 802.11a

Скорость передачи данных (Мбит/с)	Модуляция	Скорость сверточного кодирования	Число канальных битов на поднесущую	Число канальных битов на символ	Число битов данных на символ OFDM
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36

12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

Из 52 несущих 48 предназначены для передачи информационных символов, остальные 4 — служебные. Структура заголовков физического уровня отличается от принятого в спецификации IEEE 802.11b, но не существенно (рис. 1.30).

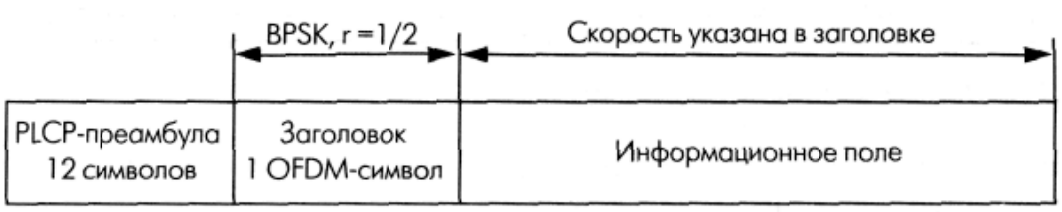


Рис. 1.30 Структура заголовка физического уровня стандарта IEEE 802.11a

Кадр включает преамбулу (12 символов синхропоследовательности), заголовок физического уровня (PLCP-заголовок) и собственно информационное поле, сформированное на MAC-уровне. В заголовке передается информация о скорости кодирования, типе модуляции и длине кадра. Преамбула и заголовок транслируются с минимально возможной скоростью (BPSK, скорость кодирования r = 1/2), а информационное поле — с указанной в заголовке, как правило максимальной, скоростью, в зависимости от условий обмена. OFDM-символы передаются через каждые 4 мкс, причем каждому символу длительностью 3,2 мкс предшествует защитный интервал 0,8 мкс (повторяющаяся часть символа). Последний необходим для борьбы с многолучевым распространением сигнала — отраженный и пришедший с задержкой символ попадет в защитный интервал и не повредит следующий символ.

Естественно, формирование/декодирование OFDM-символов происходит посредством быстрого преобразования Фурье (обратного/прямого, ОБПФ/БПФ). Функциональная схема трактов приема/передачи (рис. 1.31) достаточно стандартна для данного метода и включает сверточный кодер, механизм перемежения /перераспределения (защита от пакетных ошибок) и процессор ОБПФ. Фурье-процессор, собственно, и формирует суммарный сигнал, после чего к символу добавляется защитный интервал, окончательно формируется OFDM-символ и посредством квадратурного модулятора/конвертера переносится в заданную частотную область. При приеме все происходит в обратном порядке.

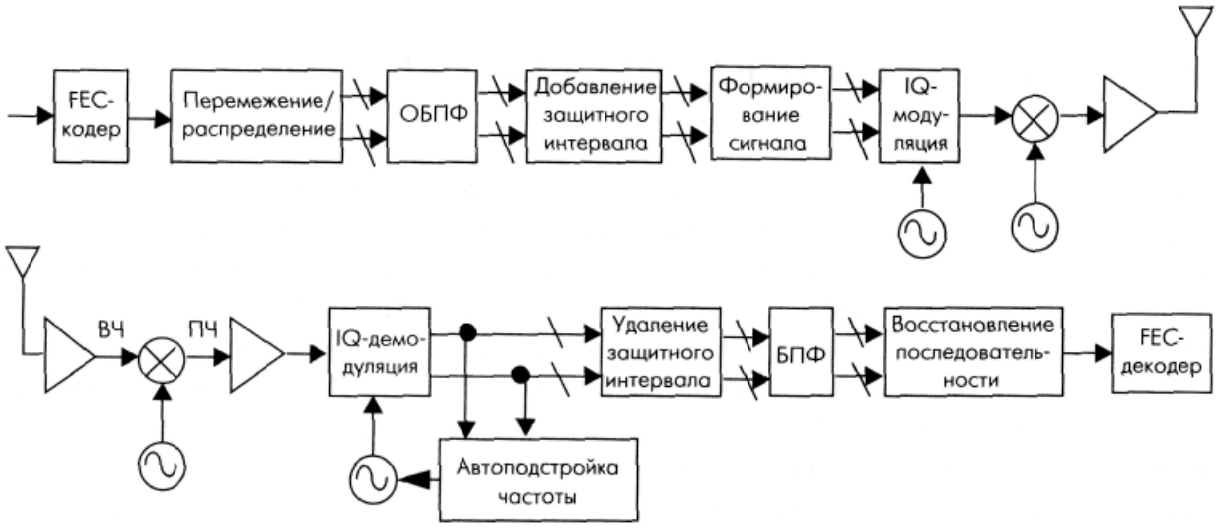


Рис. 1.31 Функциональная схема трактов приема/передачи стандарта IEEE 802.11a

1.5.4 IEEE 802.11G

Стандарт IEEE 802.11g по сути представляет собой перенесение схемы модуляции OFDM, прекрасно зарекомендовавшей себя в 802.11a, из диапазона 5 ГГц в область 2,4 ГГц при сохранении функциональности устройств стандарта 802.11b. Это возможно, поскольку в стандартах 802.11 ширина одного канала в диапазонах 2,4 и 5 ГГц схожа — 22 МГц.

Одним из основных требований к спецификации 802.11g была обратная совместимость с устройствами 802.11b. Действительно, в стандарте 802.11b в качестве основного способа модуляции принята схема CCK (Complementary Code Keying), а в качестве дополнительной возможности допускается модуляция PBSS.

Разработчики 802.11g предусмотрели CCK-модуляцию для скоростей до 11 Мбит/с и OFDM для более высоких скоростей. Но сети стандарта 802.11 при работе используют принцип CSMA/CA — множественный доступ к каналу связи с контролем несущей и предотвращением коллизий. Ни одно устройство 802.11 не должно начинать передачу, пока не убедится, что эфир в его диапазоне свободен от других устройств. Если в зоне слышимости окажутся устройства 802.11b и 802.11g, причем обмен будет происходить между устройствами 802.11g посредством OFDM, то оборудование 802.11b просто не поймет, что другие устройства сети ведут передачу, и попытается начать трансляцию. Последствия очевидны.

Чтобы подобную ситуацию не допустить, предусмотрена возможность работы в смешанном режиме — CCK-OFDM. Информация в сетях 802.11 передается кадрами. Каждый информационный кадр включает два основных поля: преамбулу с заголовком и информационное поле (рис. 1.32).

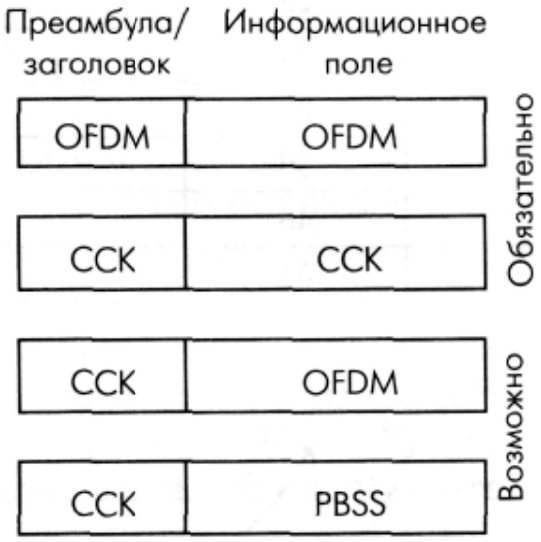


Рис. 1.32 Кадры IEEE 802.11g в различных режимах модуляции

Преамбула содержит синхропоследовательность и код начала кадра, заголовок - служебную информацию, в том числе о типе модуляции, скорости и продолжительности передачи кадра. В режиме CCK-OFDM преамбула и заголовок модулируются методом CCK (реально - путем прямого расширения спектра DSSS посредством последовательности Баркера, поэтому в стандарте 802.11g этот режим именуется DSSS-OFDM), а информационное поле — методом OFDM. Таким образом, все устройства 802.11b, постоянно «прослушивающие» эфир, принимают заголовки кадров и узнают, сколько времени будет транслироваться кадр 802.11g. В этот период они «молчат». Естественно, пропускная способность сети падает, поскольку скорость передачи преамбулы и заголовка — 1 Мбит/с.

Видимо, данный подход не устраивал лагерь сторонников технологии PBSS, и для достижения компромисса в стандарт 802.11g в качестве дополнительной возможности ввели, так же как и в 802.11b, необязательный режим — PBSS, в котором заголовок и преамбула передаются так же, как и при CCK, а информационное поле модулируется по схеме PBSS и передается на скорости 22 или 33 Мбит/с. В результате устройства стандарта 802.11g должны оказаться совместимыми со всеми модификациями оборудования 802.11b и не создавать взаимных помех. Диапазон поддерживаемых им скоростей отражен в табл. 1.6, зависимость скорости от типа модуляции — на рис. 1.33.

Таблица 1.6 Возможные скорости и тип модуляции в спецификации IEEE 802. 11g

Скорость, Мбит/с	Тип модуляции	
	Обязательно	Допустимо
1	Последовательность Баркера	
2	Последовательность Баркера	
5,5	CCK	PBCC
6	OFDM	CCK-OFDM
9		OFDM, CCK-OFDM
11	CCK	PBCC
12	OFDM	CCK-OFDM

18		OFDM, CCK-OFDM
22		PBCC
24	OFDM	CCK-OFDM
33		PBCC
36		OFDM, CCK-OFDM
48		OFDM, CCK-OFDM
54		OFDM, CCK-OFDM

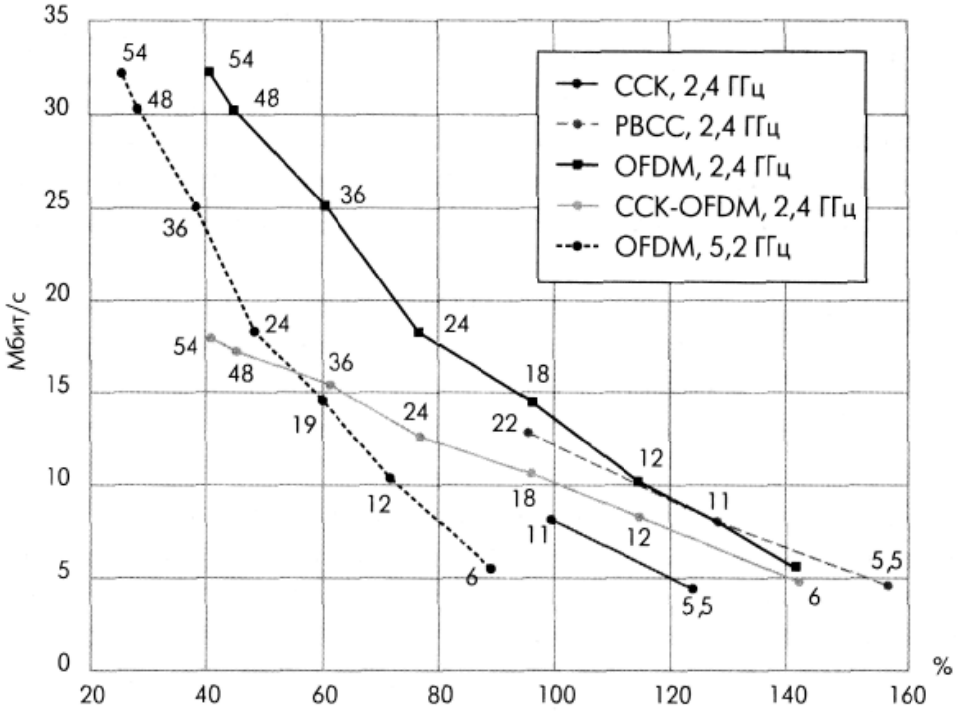


Рис. 1.33 Зависимость скорости передачи от расстояния для различных технологий передачи. Расстояние приведено в процентах, 100% — дальность передачи с модуляцией ССК на скорости 11 Мбит/с

Очевидно, что устройствам стандарта IEEE 802.11g достаточно долго придется работать в одних сетях с оборудованием 802.11b. Также очевидно, что производители в массе своей не будут поддерживать режимы CCK-OFDM и PBSS в силу их необязательности, ведь почти все решает цена устройства. Поэтому одна из основных проблем данного стандарта — как обеспечить бесконфликтную работу смешанных сетей 802.11b/g.

Основной принцип работы в сетях 802.11 — «слушать, прежде чем вещать». Но устройства 802.11b не способны услышать устройства 802.11g в OFDM-режиме. Ситуация аналогична проблеме скрытых станций: два устройства удалены настолько, что не слышат друг друга и пытаются обратиться к третьему, которое находится в зоне слышимости обоих. Для предотвращения конфликтов в подобной ситуации в 802.11 введен защитный механизм, предусматривающий перед началом информационного обмена передачу короткого кадра «запрос на передачу» (RTS) и получение кадра подтверждения «можно передавать» (CTS). Механизм RTS/CTS применим и к смешанным сетям 802.11b/g. Естественно, эти кадры должны транслироваться в режиме ССК, который обязаны понимать все устройства. Однако защитный механизм существенно снижает пропускную способность сети.

В табл. 1.7 представлена сводная информация по параметрам физических уровней.

Таблица 1.7 Стандарты физического уровня

Параметр	802.11 DSSS	802.11 FHSS	802.11b	802.11a	802.11g
Частотный диапазон (ГГц)	2,4	2,4	2,4	5	2,4
Максимальная скорость передачи данных (Мбит/с)	2	2	11	54	54
Технология	DSSS	FHSS	CCK	OFDM	OFDM
Тип модуляции (для максимальной скорости передачи)	QPSK	GFSK	QPSK	64-QAM	64-QAM
Число неперекрывающихся каналов	3	3	3	15	3

1.6 РЕЖИМЫ И ОСОБЕННОСТИ ИХ ОРГАНИЗАЦИИ

1.6.1 РЕЖИМ AD HOC

В режиме *Ad Hoc* (рис. 1.34) клиенты устанавливают связь непосредственно друг с другом. Устанавливается одноранговое взаимодействие по типу «точка-точка», и компьютеры взаимодействуют напрямую без применения точек доступа. При этом создается только одна зона обслуживания, не имеющая интерфейса для подключения к проводной локальной сети.

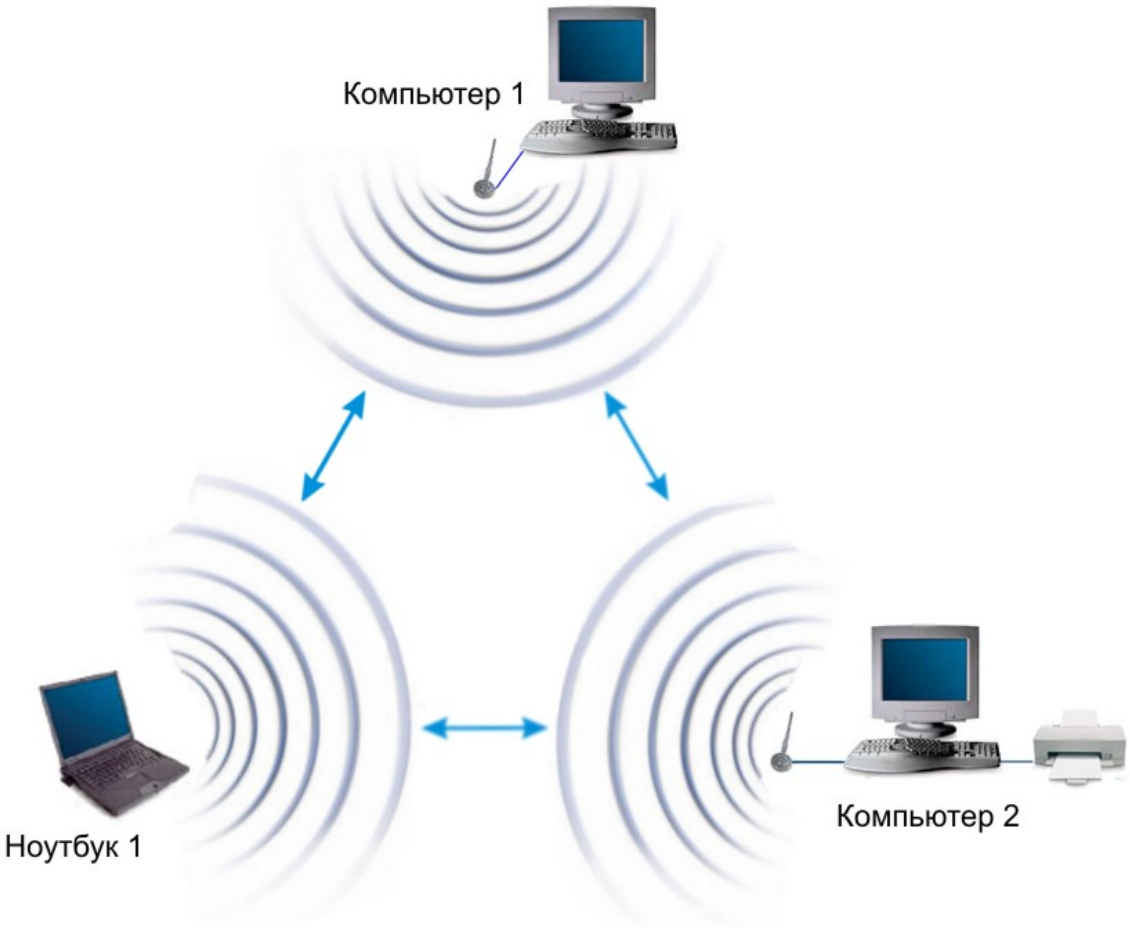


Рис. 1.34 Ad Hoc

Основное достоинство данного режима – простота организации: он не требует дополнительного оборудования (точки доступа). Режим может применяться для создания временных сетей для передачи данных.

Однако необходимо иметь в виду, что режим Ad Hoc позволяет устанавливать соединение на скорости не более 11 Мбит/с, независимо от используемого оборудования. Реальная скорость обмена данных будет ниже, и составит не более 11/N Мбит/с, где N – число устройств в сети. Дальность связи составляет не более ста метров, а скорость передачи данных быстро падает с увеличением расстояния.

Для организации долговременных беспроводных сетей следует использовать инфраструктурный режим.

Пример 1.3:

На клиентской стороне будем использовать беспроводный USB-адаптер. Все настройки для других типов адаптеров (PCI, PCMCI, ExpressCard и т.д.) проводятся аналогичным образом.

При подключении адаптера необходимо установить драйвер, который идёт в комплекте со всем беспроводным оборудованием. В окне *Сетевые подключения* должен появиться значок *Беспроводное сетевое соединения* (рис. 1.35)

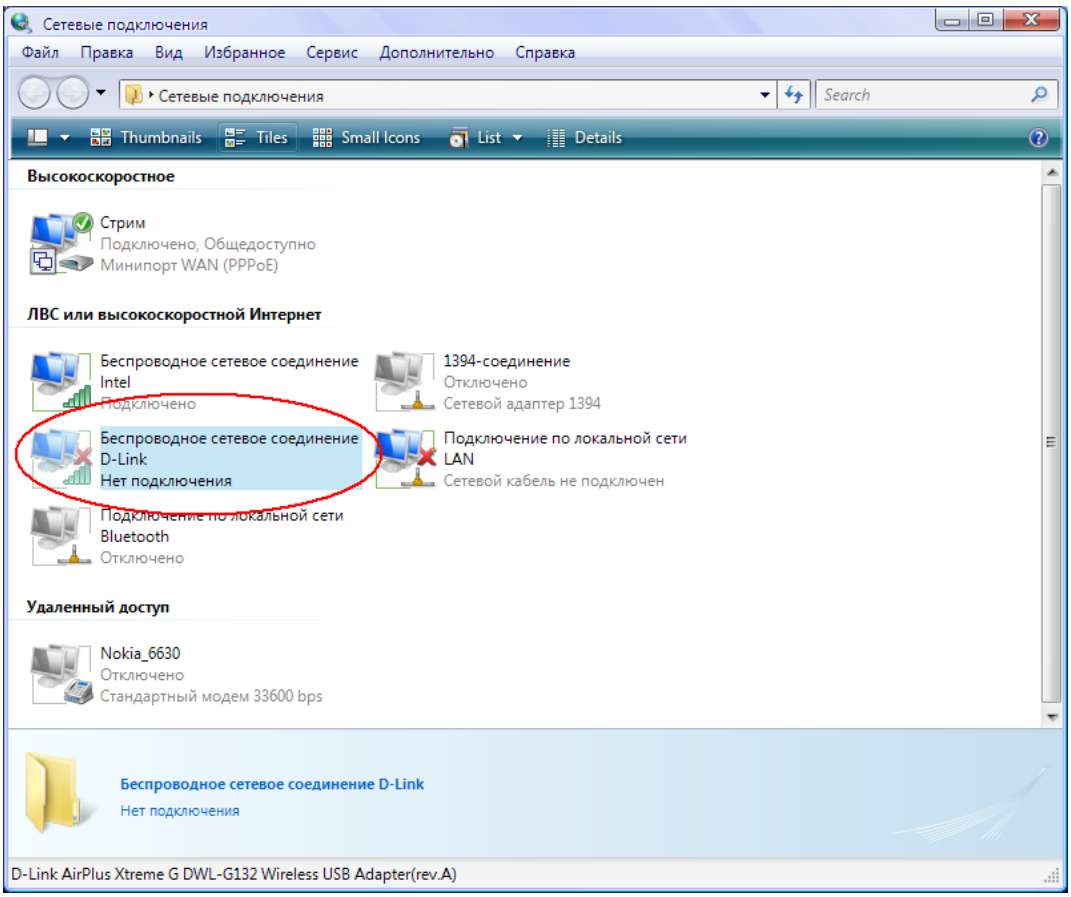


Рис. 1.35

Беспроводную сеть в режиме Ad Hoc сначала будем строить из компьютера1 и ноутбука1 (рис.1.34), а затем можно будет подключить и остальные компьютеры. Это можно сделать двумя способами: с помощью встроенной службы Windows XP или Windows Vista и программой D-Link AirPlus XtremeG Wireless Utility, которая идёт в комплекте с оборудованием D-Link.

1) Настройка подключения с помощью встроенной службы Windows.

При установке интерфейса, при помощи встроенной утилиты Windows, дополнительные программы не требуются. Но для этого требуется установить галочку *Использовать Windows для настройки сети* на вкладке *Беспроводные сети* в свойствах беспроводного соединения (рис. 1.36)

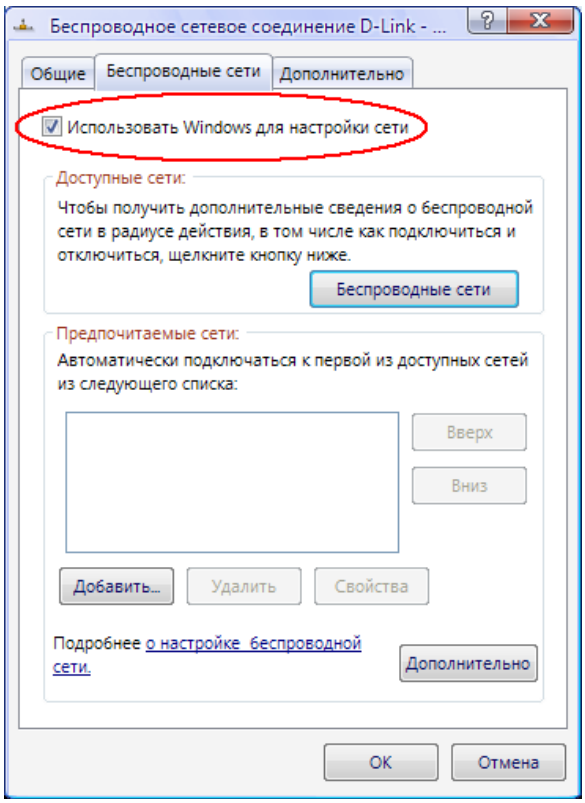


Рис. 1.36

Перед установкой соединения необходимо настроить статические IP-адреса. Они настраиваются в свойствах беспроводного соединения, на вкладке *Общие*, в свойствах *Протокол Интернета (TCP/IP)* (рис. 1.37)

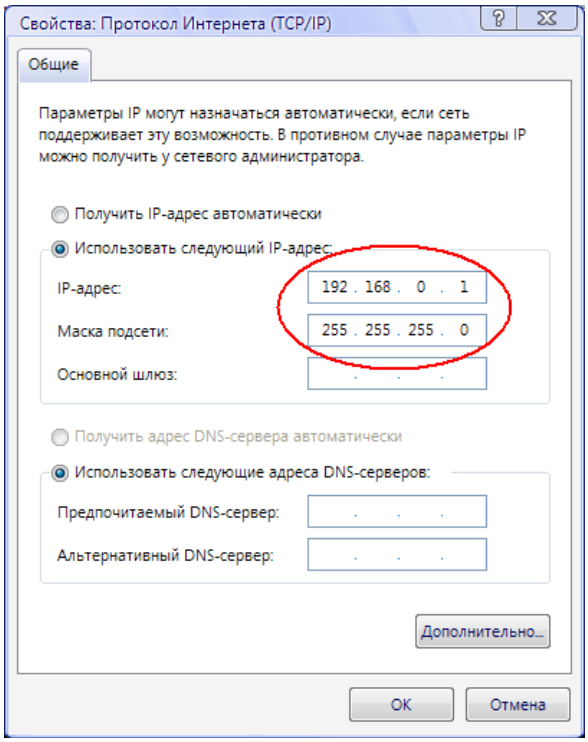


Рис. 1.37

Первый компьютер (*Компьютер1*) пусть будет иметь IP-адрес: 192.168.0.1, а второй (*Ноутбук1*): 192.168.0.2, а маска подсети: 255.255.255.0.

Теперь для организации сети в режиме Ad Hoc, двойным щелчком левой кнопки мыши по беспроводному интерфейсу (рис. 1.35) запустим службу Windows. Здесь, на одном из компьютеров, запустим *Установить беспроводную сеть* (рис. 1.38). В появившемся мастере надо ввести SSID (например, AdHocNet) и ввести ключ доступа. На этом конфигурирование одного компьютера заканчивается.

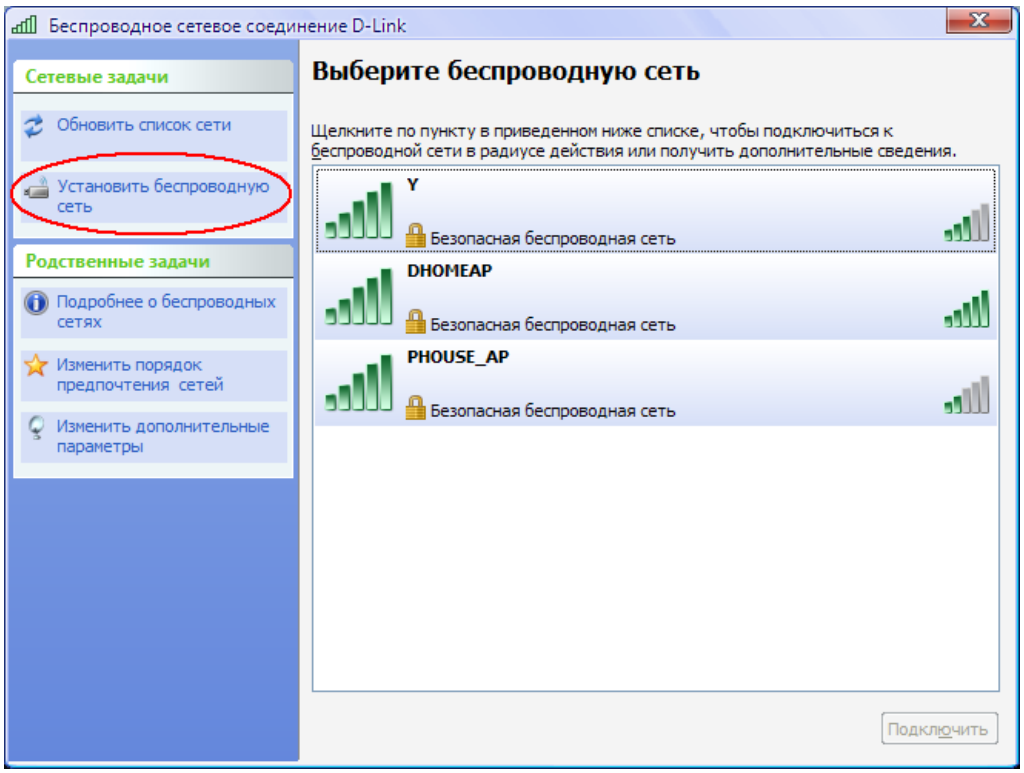


Рис. 1.38

На другом компьютере тоже запускаем службу Windows (рис. 1.38), и в основном окне выбираем появившуюся сеть (AdHocNet). При совпадении ключей доступа этот компьютер подключается к первому и таким образом, создаётся беспроводная сеть Ad Hoc.

Если нужно подключить ещё компьютеры, то проводятся все те же действия, что и со вторым. В этом случае сеть уже будет состоять из нескольких компьютеров.

2) Настройка подключения с помощью программы D-Link AirPlus XtremeG Wireless Utility.

В этом случае надо установить эту программу и убрать галочку *Использовать Windows для настройки сети*, показанную на рисунке 1.36.

Чтобы организовать беспроводную связь Ad Hoc запустите эту программу на первом компьютере и перейдите на вкладку *Настройка* (рис. 1.39).

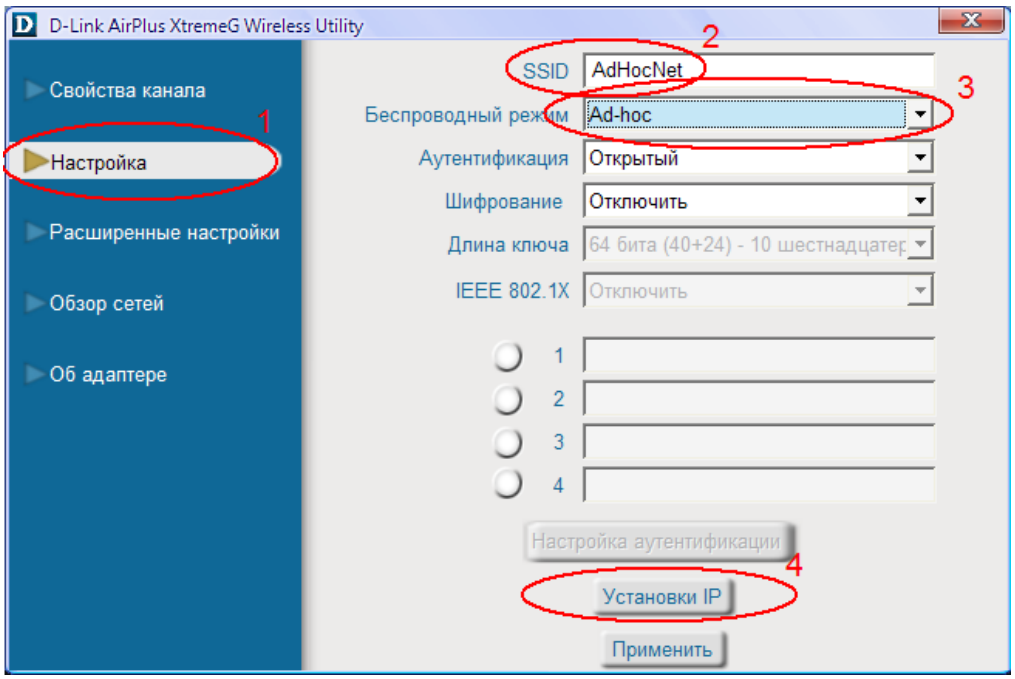


Рис. 1.39

Затем введите SSID создаваемой сети (например, AdHocNet), выберете режим Ad Hoc и установите IP-адрес с маской беспроводного интерфейса. Аутентификацию и шифрование пока оставим открытыми. Если нужно сделать дополнительные настройки, то их можно произвести на вкладке *Расширенные настройки*.

На других компьютерах также запускаем эту программу и открываем вкладку *Обзор сетей* (рис. 1.40)

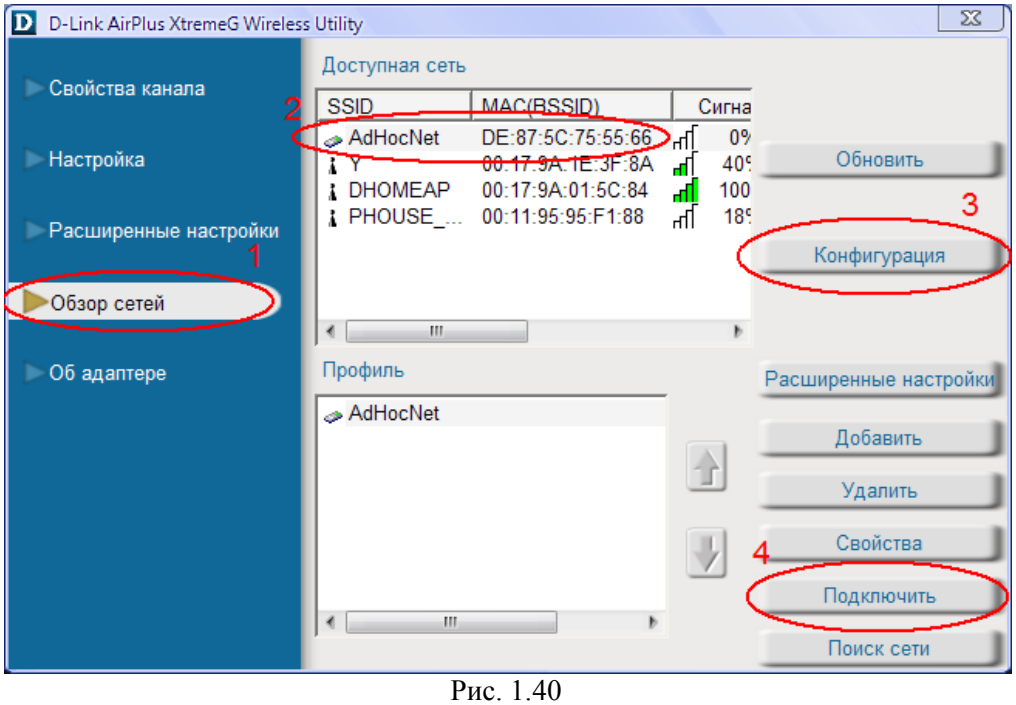


Рис. 1.40

В появившемся окне выбрать сеть, и для настройки IP-адреса второго компьютера нажать кнопку *Конфигурация*. Затем нажать кнопку *Подключить*, и при совпадении ключей доступа беспроводный адаптер подключится к первому компьютеру. Остальные компьютеры подключаются аналогичным образом. Обновление доступных сетей производится кнопкой *Обновить*.

1.6.2 ИНФРАСТРУКТУРНЫЙ РЕЖИМ

В этом режиме точки доступа обеспечивают связь клиентских компьютеров (рис. 1.41). Точку доступа можно рассматривать как беспроводный коммутатор. Клиентские станции не связываются непосредственно одна с другой, а связываются с точкой доступа, и она уже направляет пакеты адресатам.

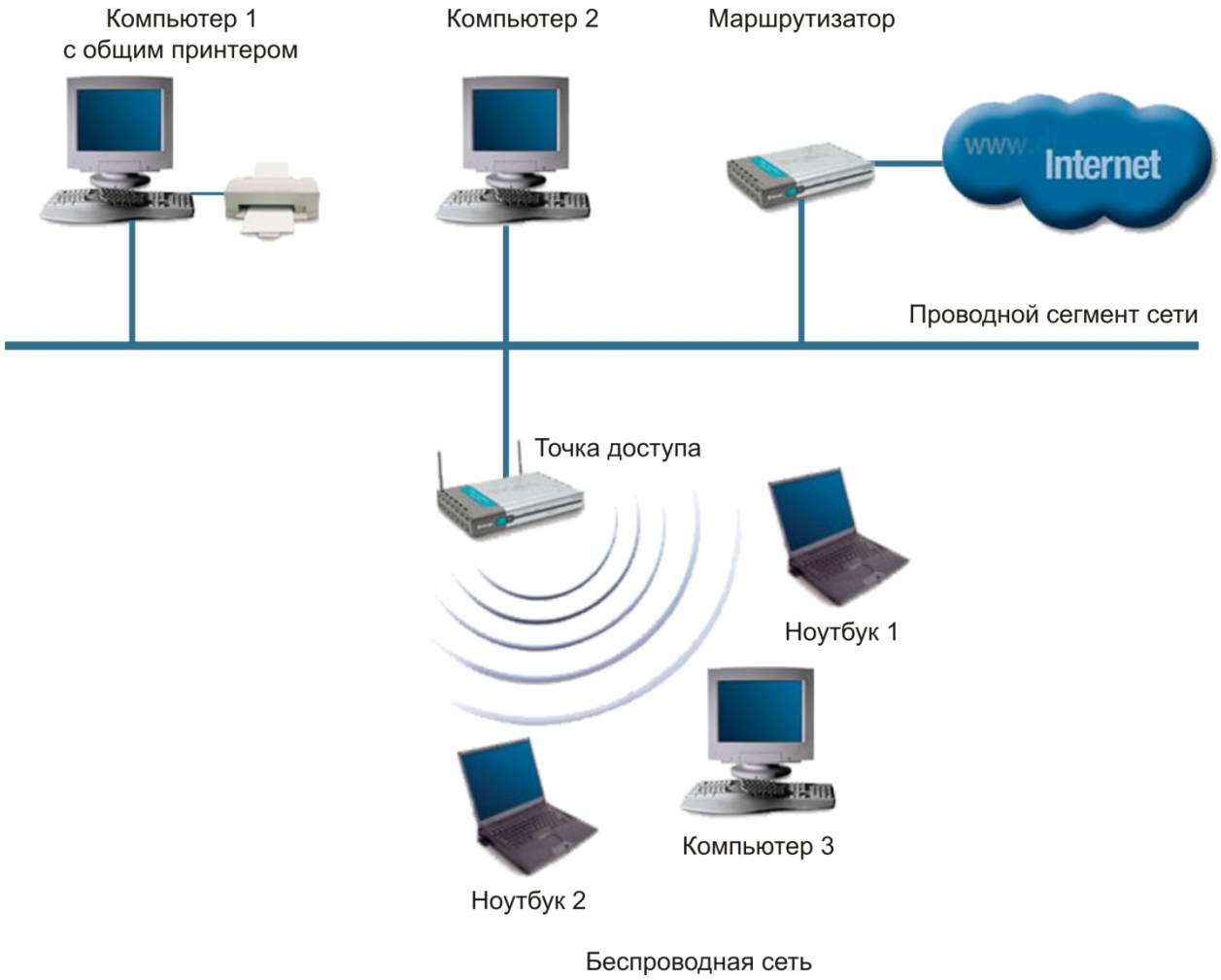


Рис. 1.41 Инфраструктурный режим

Точка доступа имеет порт Ethernet, через который базовая зона обслуживания подключается к проводной или смешанной сети – к сетевой *инфраструктуре*.

Пример 1.4:

Настроим беспроводную точку доступа в инфраструктурном режиме.

Настройка производиться через проводной интерфейс, т.е. используя Ethernet-соединение. Хотя можно это делать и через беспроводный интерфейс, но мы не рекомендуем, т.к. при достаточно большом количестве точек доступа может возникнуть путаница в настройках.

1. В окне *Сетевые подключения* отключите сетевые и бессетевые адаптеры (рис. 1.35). В контекстном меню выбрать «Отключить» для каждого адаптера.

В результате все компьютеры изолированы друг от друга, сетевых подключений нет.

2. Настраиваем сетевые адаптеры для связи с точкой доступа.

Подключения по локальной сети->Свойства->Протокол TCP/IP->Свойства

-Использовать следующий IP-адрес

-Укажите адрес 192.168.0.xxx, где xxx – номер вашего компьютера (1, 2, 3 и т.д).

-Укажите маску 255.255.255.0

-Включите кабельное соединение

3.Подключаемся к точке доступа.

Соединяем точку доступа сетевым кабелем с сетевым адаптером, подаем питание.

Сбрасываем настройки точки. Для этого в течение пяти секунд нажимаем и держим кнопку reset. Не отключайте питание при нажатой reset!

Время загрузки точки – около 20 секунд.

По окончании загрузки на точке загораются индикаторы Power и LAN.

В браузере Internet Explorer наберите http://192.168.0.50 ,

Появится приглашение на ввод имени и пароля (рис. 1.42).

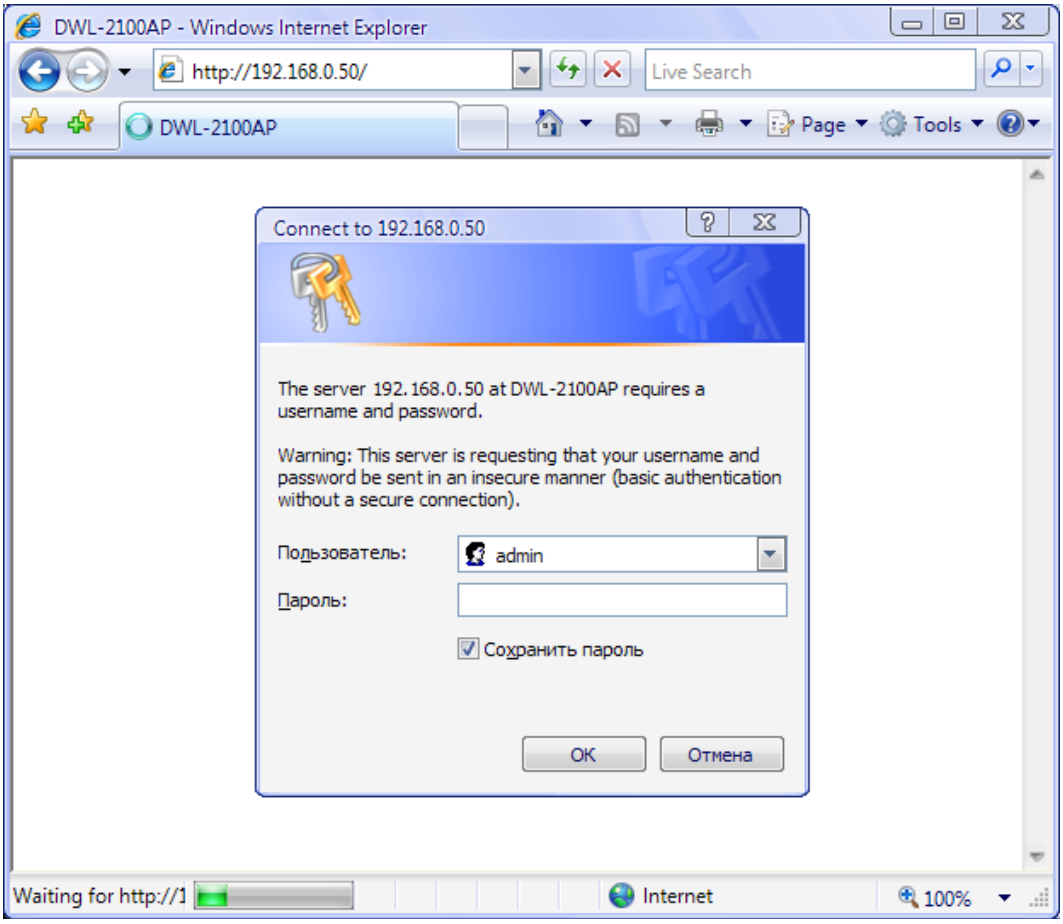


Рис. 1.42

4.Начинаем настройку.

Введите в качестве имени пользователя «admin» с пустым паролем.

Настроим сначала IP-адрес точки. Это нужно лишь в том случае, когда у вас много точек доступа. На вкладке *Home* жмем кнопку *Lan* (слева).

-Выставляем адрес 192.168.0.xxx, где xxx – уникальный номер точки.

-Маска 255.255.255.0

-Default Gateway 192.168.0.50

По завершении настройки нажать «Apply», чтобы перезагрузить точку с новыми настройками.

5. Включение режима точки доступа.

Дождитесь загрузки точки, и введите в браузере новый адрес http://192.168.0.xxx

На вкладке *Home* нажмите кнопку *Wireless* (слева)

Устанавливаем (рис. 1.43):
Mode (режим): Access Point
SSID: Network
SSID Broadcast: Enable
Channel: 6
Authentication: Open System
Encryption: Disable

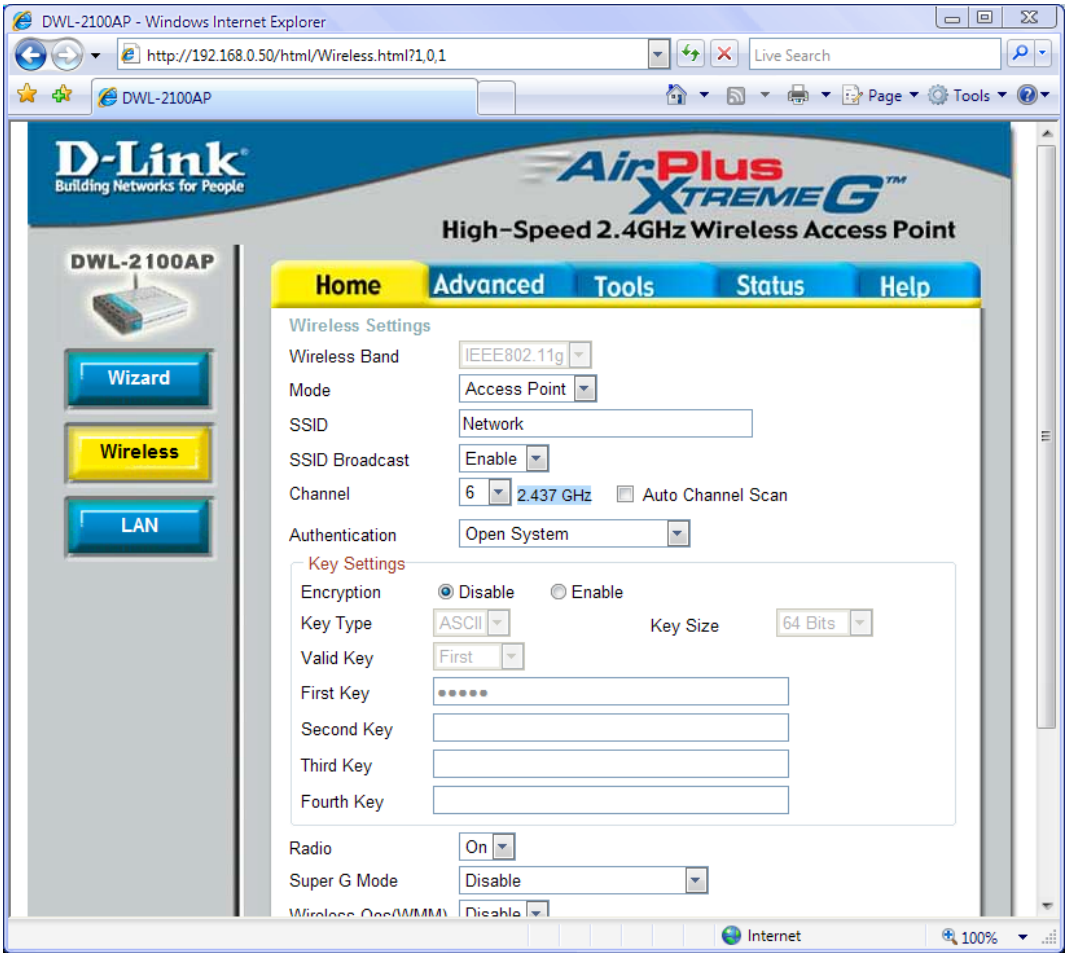


Рис. 1.43

Заметьте, что выбранные нами установки не обеспечивают безопасность беспроводного подключения, и используются только с целью обучения.

Если нужно сделать более тонкие настройки, перейдите на вкладку *Advanced*. Настоятельно рекомендуем перед настройкой вашей точки доступа прочитать документацию по настройке, краткое описание всех параметров есть на вкладке *Help*.

По завершении настройки нажать «Apply», чтобы перезагрузить точку с новыми настройками.

Отключите точку от сетевого интерфейса. Теперь ваша точка настроена на подключение беспроводных клиентов. В простейшем случае, чтобы предоставить клиентам Интернет, нужно к точке подключить широкополосный канал или ADSL-модем.

Клиентские компьютеры подключаются аналогичным образом, как это было описано в предыдущем примере (рис. 1.40).

1.6.3 РЕЖИМЫ WDS И WDS WITH AP

Термин *WDS* (Wireless Distribution System) расшифровывается как «распределённая беспроводная система». В этом режиме точки доступа соединяются только между собой, образуя мостовое соединение. При этом каждая точка может соединяться с несколькими другими точками. Все точки в этом режиме должны использовать одинаковый канал, поэтому количество точек, участвующих в образовании моста, не должно быть чрезмерно большим. Подключение клиентов осуществляется только по проводной сети через uplink-порты точек (рис. 1.44).

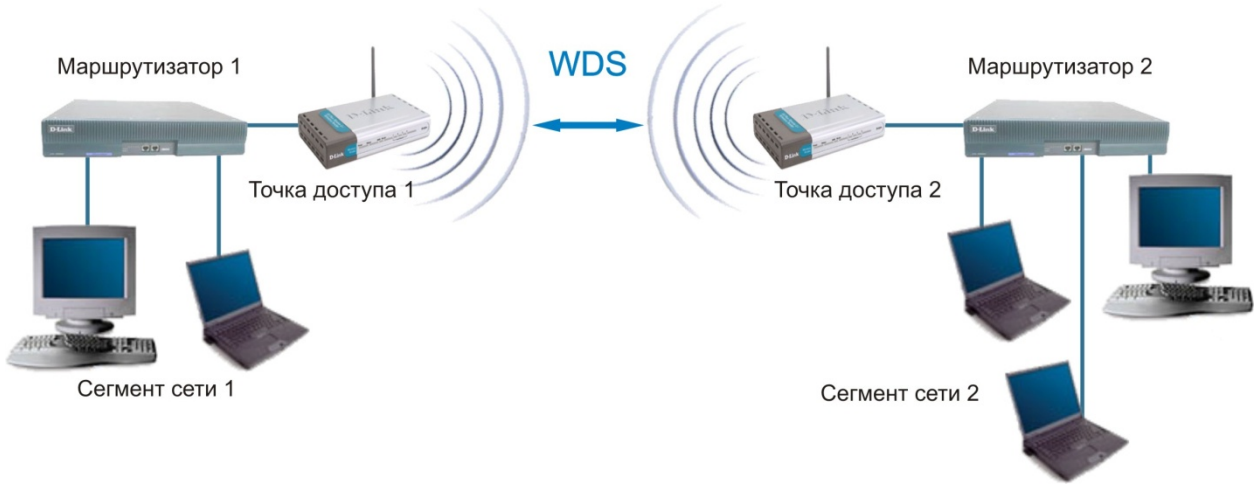


Рис. 1.44 Мостовой режим

Режим беспроводного моста, аналогично проводным мостам, служит для объединения подсетей в общую сеть. С помощью беспроводных мостов можно объединять проводные LAN, находящиеся как на небольшом расстоянии в соседних зданиях, так и на расстояниях до нескольких километров. Это позволяет объединить в сеть филиалы и центральный офис, а также подключать клиентов к сети провайдера Интернет (рис. 1.45).

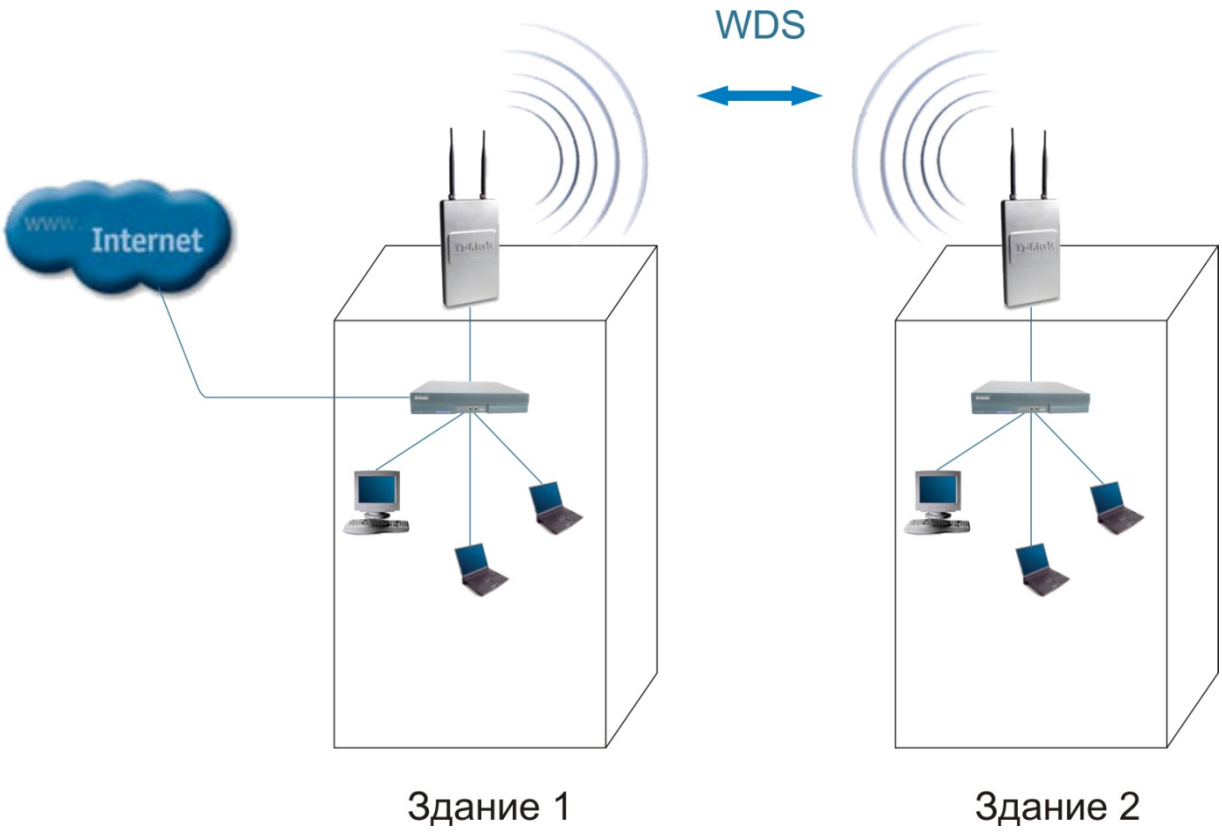


Рис. 1.45 Мостовой режим между зданиями

Беспроводный мост может использоваться там, где прокладка кабеля между зданиями нежелательна или невозможна. Данное решение позволяет достичь значительной экономии средств и обеспечивает простоту настройки и гибкость конфигурации при перемещении офисов.

К точке доступа, работающей в режиме моста, подключение беспроводных клиентов невозможно. Беспроводная связь осуществляется только между парой точек, реализующих мост.

Термин *WDS with AP* (WDS with Access Point) обозначает «распределённая беспроводная система, включая точку доступа», т.е. с помощью этого режима можно организовать не только мостовую связь между точками доступа, но и одновременно подключить клиентские компьютеры (рис. 1.46). Это позволяет достичь существенной экономии оборудования и упростить топологию сети. Данная технология поддерживается большинством современных точек доступа.

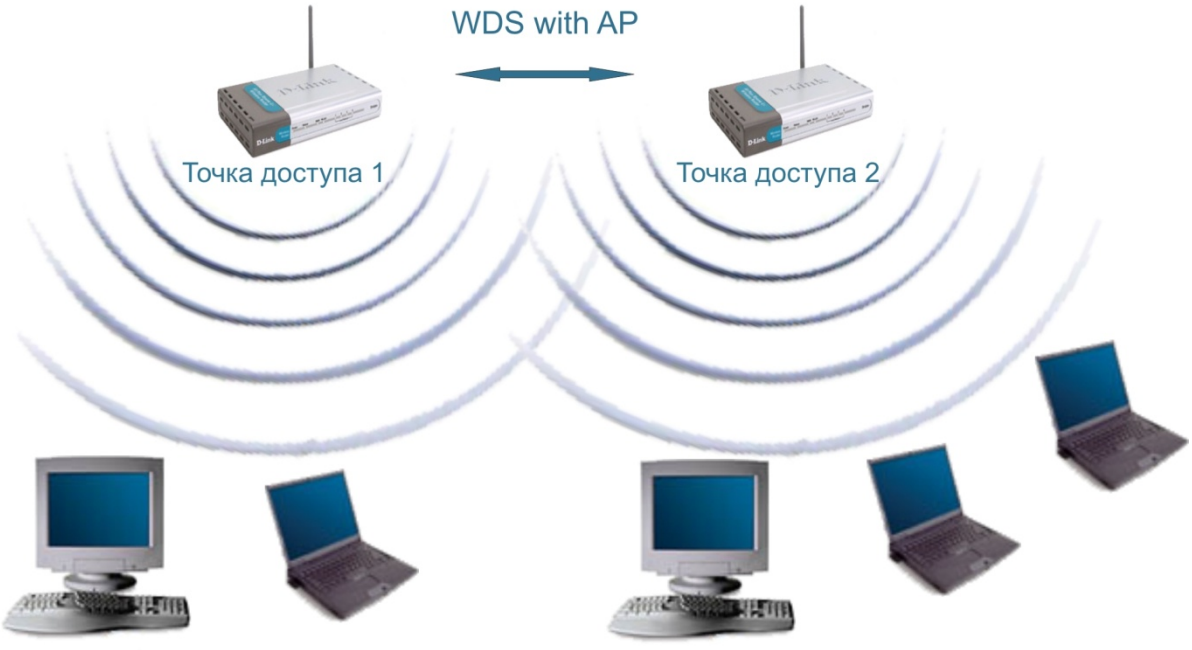


Рис. 1.46 Режим WDS with AP

Тем не менее, необходимо помнить, что все устройства в составе одной WDS with AP работают на одной частоте и создают взаимные помехи, что ограничивает количество клиентов до 15-20 узлов. Для увеличения количества подключаемых клиентов можно использовать несколько WDS-сетей, настроенных на разные неперекрывающиеся каналы и соединенные проводами через uplink-порты.

Топология организации беспроводных сетей в режиме WDS аналогична обычным проводным топологиям.

Топология типа «шина»

Топология типа «шины» самой своей структурой предполагает идентичность сетевого оборудования компьютеров, а также равноправие всех абонентов (рис. 1.47).

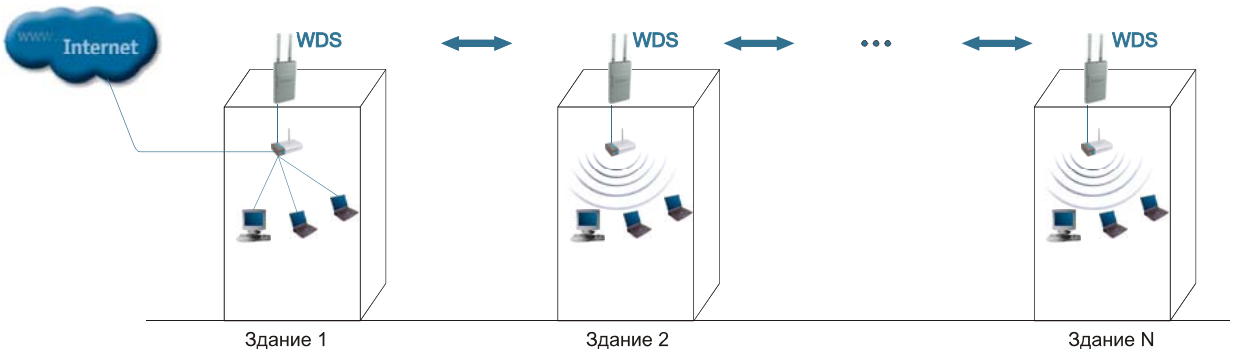


Рис. 1.47 Топология типа «шина»

Здесь отсутствует центральный абонент, через которого передается вся информация, что увеличивает ее надежность (ведь при отказе любого центра перестает

функционировать вся управляемая этим центром система). Добавление новых абонентов в шину довольно просто. Надо ввести параметры новой точки доступа в последнюю, что приведёт только кратковременную перезарузку последней точки.

Шине не страшны отказы отдельных точек, так как все остальные компьютеры сети могут нормально продолжать обмен между собой, но при этом оставшаяся часть компьютеров не смогут получить доступ в Интернет.

Топология типа «кольцо»

«Кольцо» — это топология, в которой каждая точка доступа соединена только с двумя другими (рис. 1.48). Четко выделенного центра в данном случае нет, все точки могут быть одинаковыми.

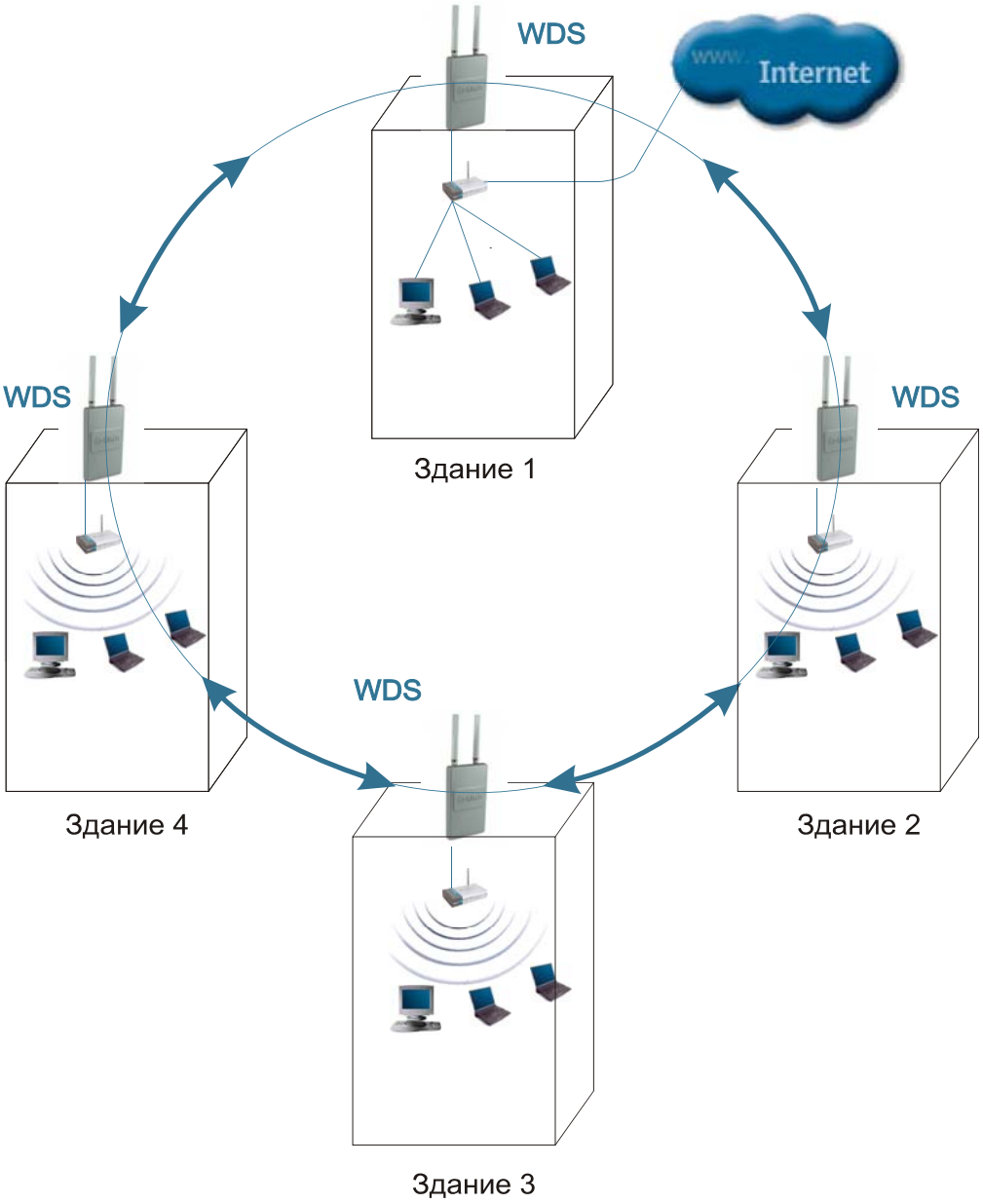


Рис. 1.48 Топология тип «кольцо»

Подключение новых абонентов в «кольцо» обычно совершенно безболезненно, хотя и требует обязательной остановки работы двух крайних точек от новой точки доступа.

В то же время основное преимущество кольца состоит в том, что ретрансляция сигналов каждым абонентом позволяет существенно увеличить размеры всей сети в целом (порой до нескольких десятков километров). Кольцо в этом отношении существенно превосходит любые другие топологии.

Топология связей между точками в этом режиме представляет собой ациклический граф типа дерево, то есть данные из Интернета от точки 4 к точке 2 может проходят по двум направлениям – через точку 1 и 3 (рис. 1.48). Для устранения лишних связей, способных приводить к появлению циклов в графе, реализуется алгоритм *Spanning tree*. Его работа приводит к выявлению и блокированию лишних связей. При изменении топологии сети, например – из-за отключения некоторых точек или невозможности работы каналов – алгоритм *Spanning tree* запускается заново, и прежде заблокированные лишние связи могут использоваться взамен вышедших из строя.

Топология типа «звезда»

«Звезда» – это топология с явно выделенным центром, к которому подключаются все остальные абоненты (рис. 1.49). Весь обмен информацией идет исключительно через центральную точку доступа, на которую таким образом ложится очень большая нагрузка.

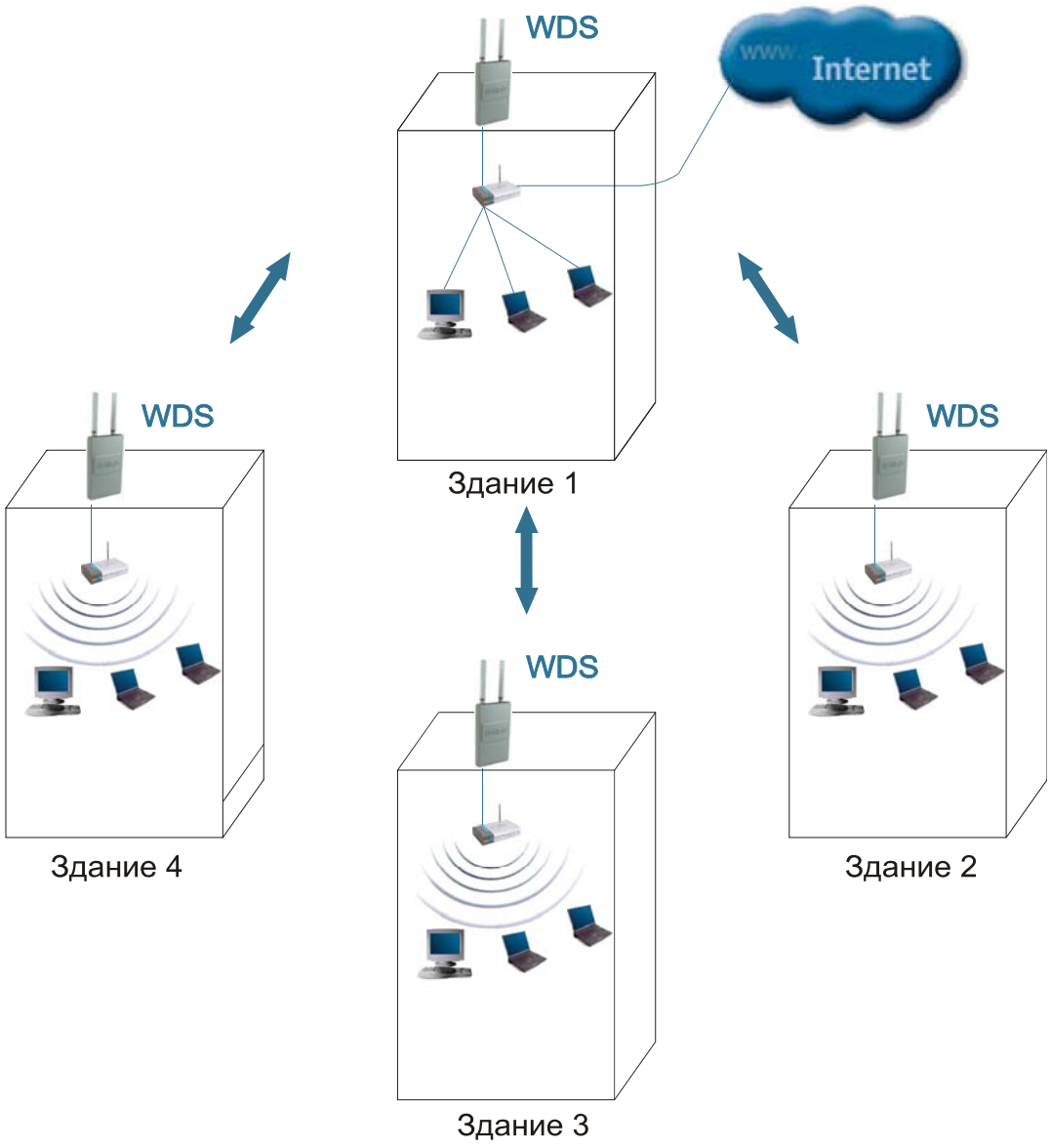


Рис. 1.49 Топология типа «звезда»

Если говорить об устойчивости звезды к отказам точек, то выход из строя обычной точки доступа никак не отражается на функционировании оставшейся части сети, зато любой отказ центральной точки делает сеть полностью неработоспособной.

Серьезный недостаток топологии «звезда» состоит в жестком ограничении количества абонентов. Так как все точки работают на одном канале, то обычно центральный абонент может обслуживать не более 10 периферийных абонентов из-за большого падения скорости.

В большинстве случаев, например для объединения нескольких районов в городе, используют комбинированные топологии.

Пример 1.5:

Создадим мост типа «точка-точка». Для этого понадобиться две точки доступа.

1. Настраиваем IP-адрес проводным интерфейсам точек доступа:

-Отключаем беспроводные интерфейсы и запускаем браузер Internet Explorer, в адресной строке вводим 192.168.0.50, по умолчанию логин: admin, пароль пустой.

-Заходим на вкладку Home->LAN и в поле IP address вводим: 192.168.0.5X, где X – номер точки доступа (например, 1, 2, 3 и т.д.).

2. Настраиваем мостовое соединение, показанное на рис. 1.50

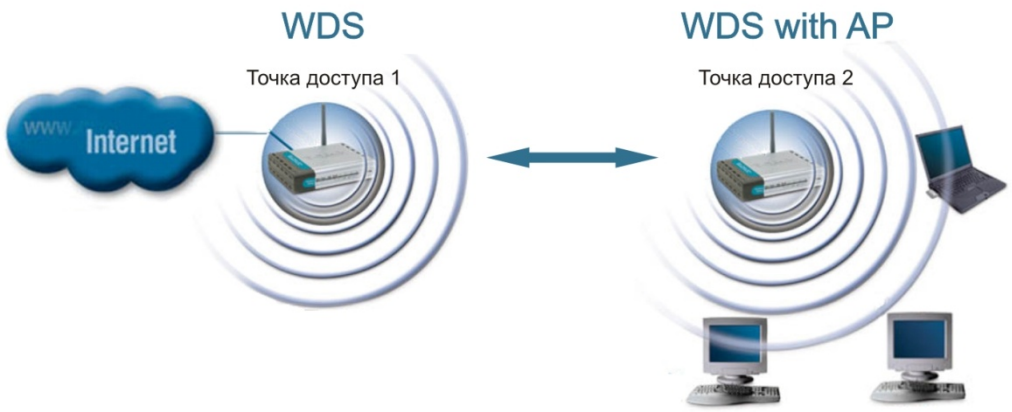


Рис. 1.50

-Заходим на вкладку Home->Wireless в первой точке доступа делаем режим (Mode): WDS (рис. 1.51), во второй – WDS with AP (рис. 1.52).

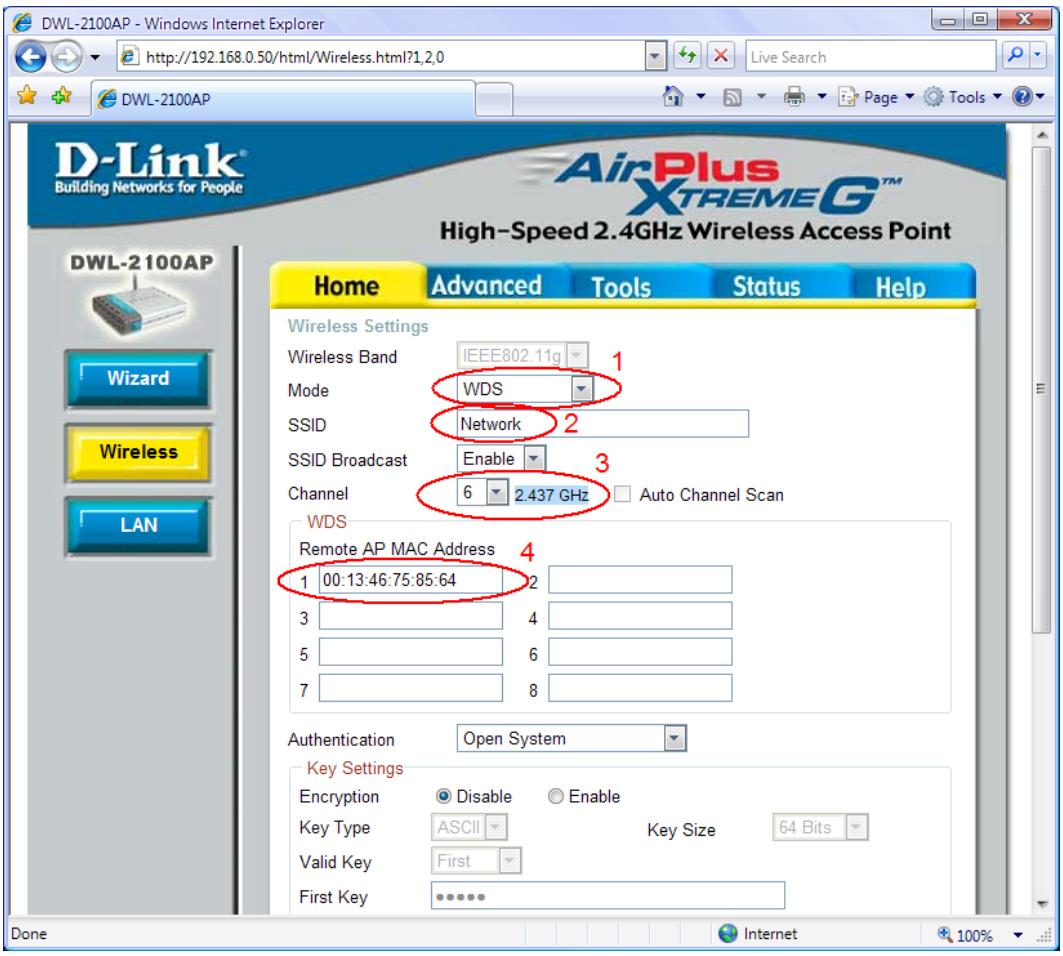


Рис. 1.51

-Во второй точке указываем SSID: Network (в первой точке доступа можно указать любой SSID, т.к. к ней всё равно нельзя будет подключиться беспроводным клиентам).

-В двух точках доступа указываем один и тот же канал: 6.

-В первой точке доступа в поле Remote AP MAC Address указываем MAC-адрес второй точки (например, 00:13:46:75:85:64), во второй точке доступа указываем MAC-адрес первой точки (например, 00:17:9A:01:5C:84).

-При желании можно настроить шифрование данных.

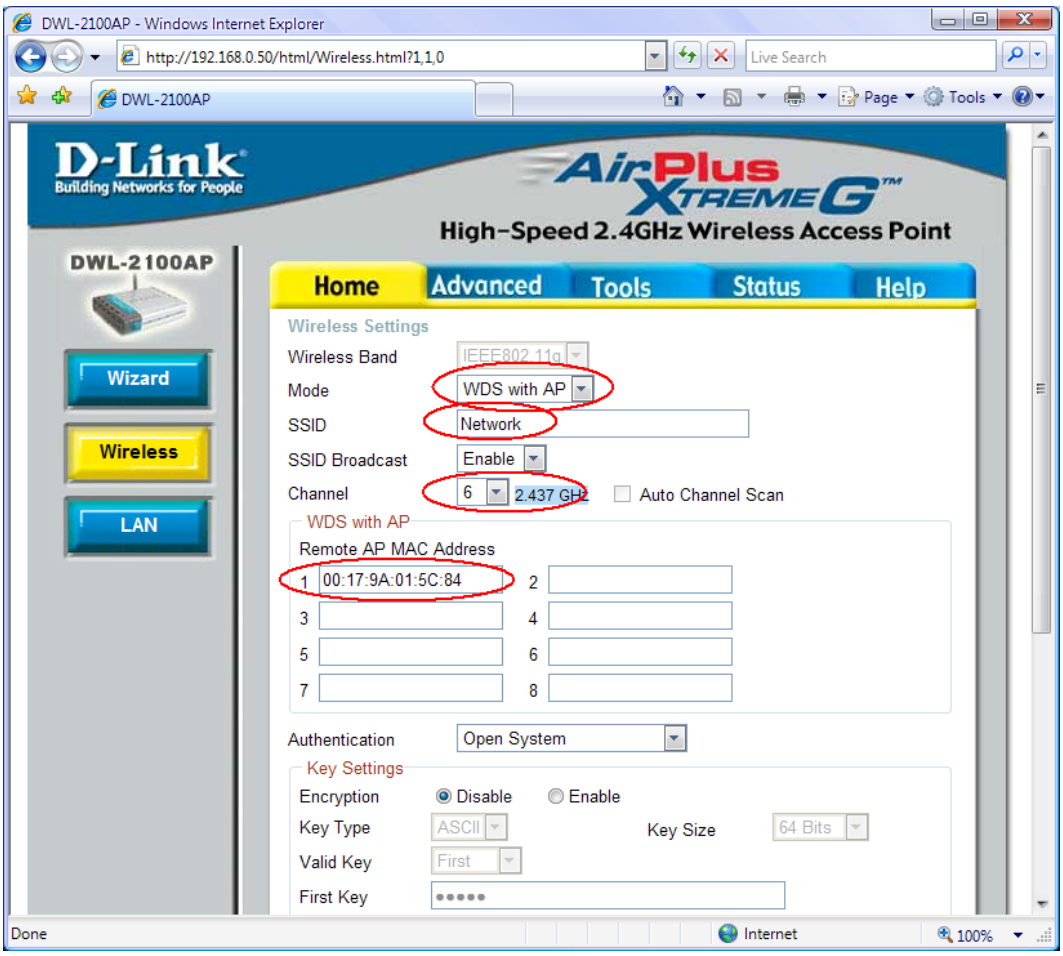


Рис. 1.52

-Применяем настройки, и после перезагрузки точки доступа войдут в режим моста.

3. Проверяем соединение:

-Подключаемся беспроводными адаптерами ко второй точке доступа.

-Командой ping последовательно проверяем вторую точку, первую и, если первая точка подключена к Интернету, сайт: ping 192.168.0.5X, где X – номер точки доступа, ping www.dlink.ru

Пример 1.6:

Теперь создадим мост точка-много точек (рис. 1.53). Для этого нам понадобиться не менее трёх точек доступа.

1.Одна точка доступа переводиться в режим WDS (рис. 1.51):

-Заходим на вкладку Home->Wireless в первой точке доступа делаем режим (Mode): WDS.

-Указываем канал (например, 1, 6 или 11).

-В полях Remote AP MAC Address указываем MAC-адреса остальных точек доступа.

-При желании можно настроить шифрование данных.

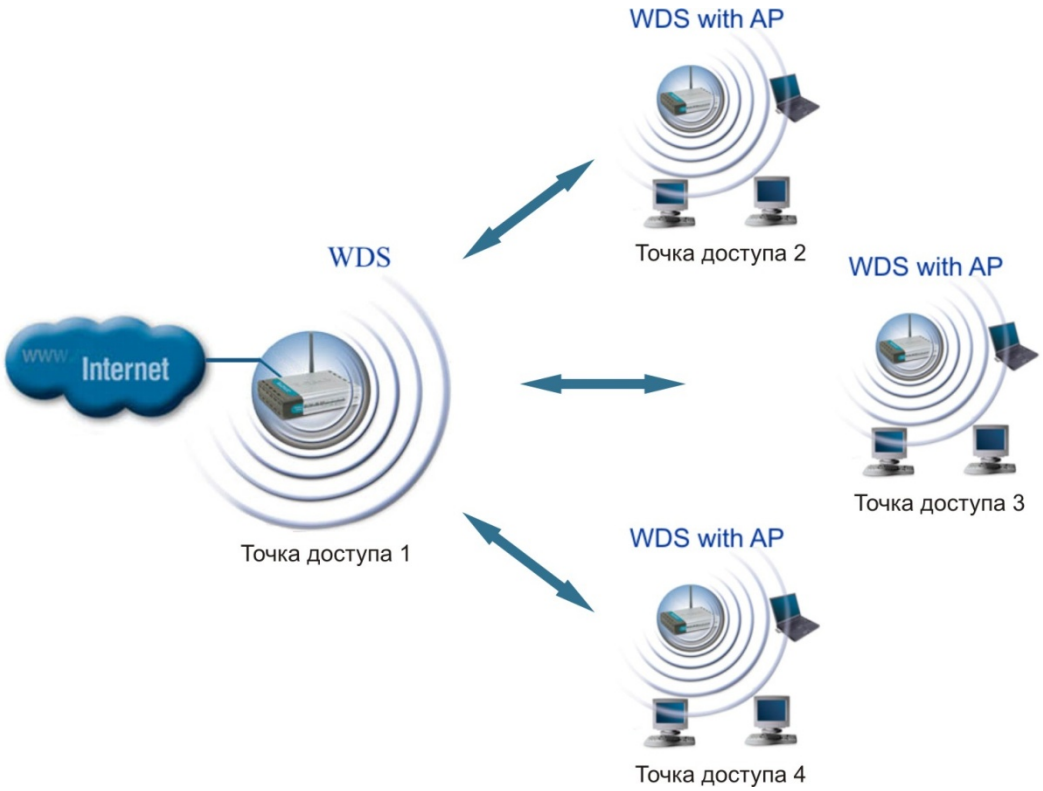


Рис. 1.53

2. Другие точки доступа переводятся в режим WDS with AP (рис. 1.52):

-Заходим на вкладку Home->Wireless и делаем режим (Mode): WDS with AP.

-Указываем SSID: NetworkX, где X – номер подсети.

-Указываем такой же канал, как и у первой точки доступа.

-Во всех точках доступа в поле Remote AP MAC Address указываем MAC-адрес первой точки.

-Если в первой точке настроено шифрование данных, то здесь тоже надо настроить точно такое же шифрование.

-Применяем настройки, и после перезагрузки точки доступа войдут в режим моста.

3. Проверяем соединение:

-Подключаемся беспроводными адаптерами к любой точке доступа.

-Командой ping последовательно проверяем вторую (третью или четвёртую) точку, первую и сайт в Интернете: ping 192.168.0.5X, где X – номер точки доступа, ping www.dlink.ru

1.6.4 РЕЖИМ ПОВТОРИТЕЛЯ

Может возникнуть ситуация, когда оказывается невозможно, или неудобно, соединить точку доступа с проводной инфраструктурой, или какое-либо препятствие затруднит осуществление связи точки доступа с местом расположения беспроводных станций клиентов напрямую. В такой ситуации можно использовать точку в режиме *повторителя (Repeater)* (рис. 1.54).

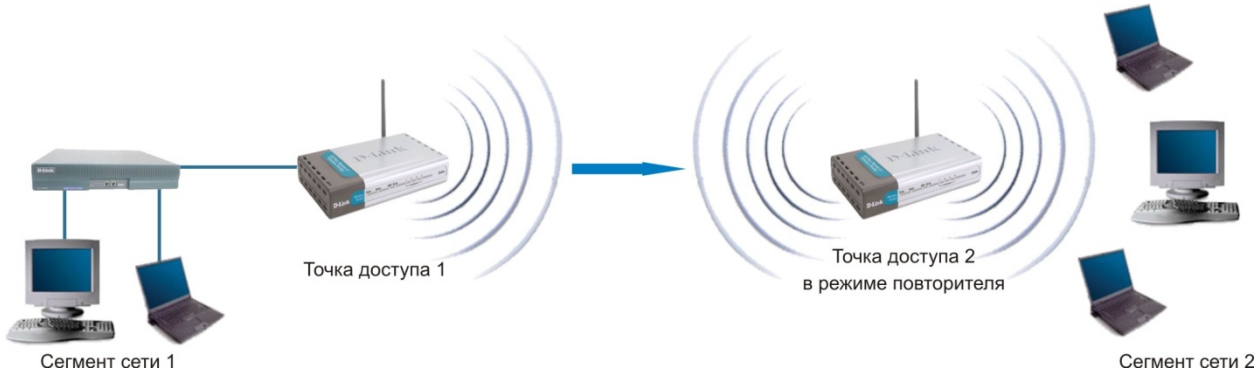


Рис. 1.54 Режим повторителя

Аналогично проводному повторителю, беспроводный повторитель просто ретранслирует все пакеты, поступившие на его беспроводный интерфейс. Эта ретрансляция осуществляется через тот же канал, через который они были получены.

При применении точки доступа-повторителя следует помнить, что наложение широковещательных доменов может привести к сокращению пропускной способности канала вдвое, потому что начальная точка доступа также «слышит» ретранслированный сигнал.

Режим повторителя не включен в стандарт 802.11, поэтому для его реализации рекомендуется использовать однотипное оборудование (вплоть до версии прошивки) и от одного производителя. С появлением WDS данный режим потерял свою актуальность, потому что функционал WDS заменяет его. Однако его можно встретить в старых версиях прошивок и в устаревшем оборудовании.

1.6.5 РЕЖИМ КЛИЕНТА

При переходе от проводной архитектуры к беспроводной иногда можно обнаружить, что имеющиеся сетевые устройства поддерживают проводную сеть Ethernet, но не имеют интерфейсных разъемов для беспроводных сетевых адаптеров. Для подключения таких устройств к беспроводной сети можно использовать точку доступа – клиент (рис. 1.55)

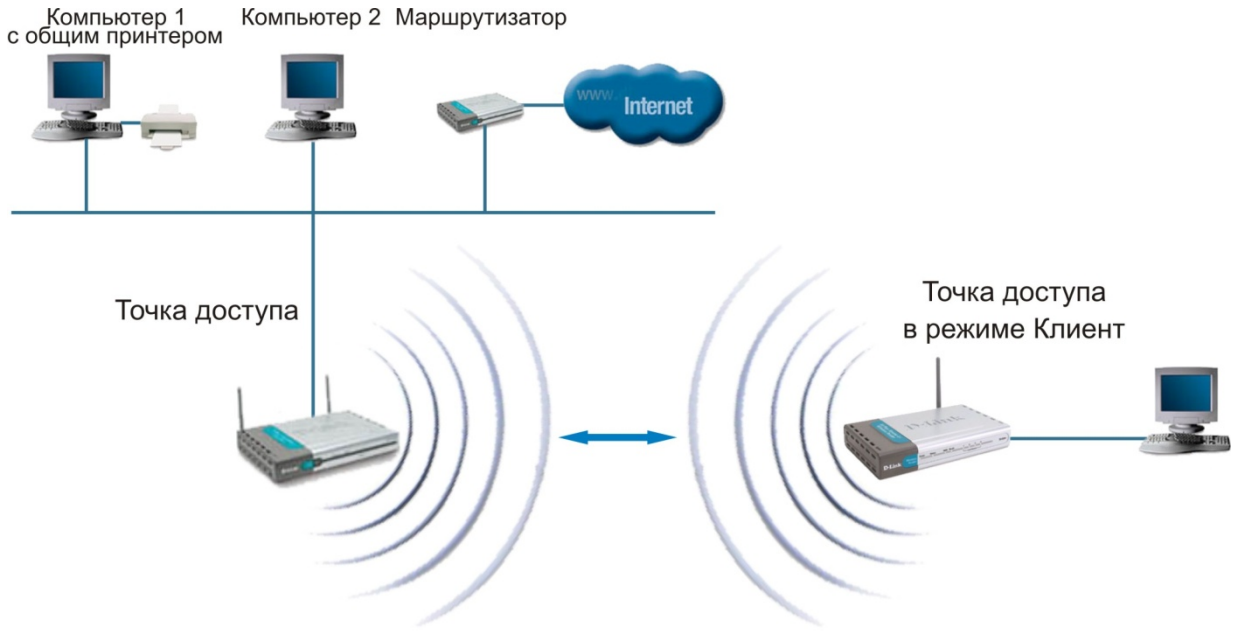


Рис. 1.55 Режим клиента

При помощи точки доступа-клиента к беспроводной сети подключается только одно устройство. Этот режим не включен в стандарт 802.11, и поддерживаются не всеми производителями.

1.7 ОРГАНИЗАЦИЯ И ПЛАНИРОВАНИЕ БЕСПРОВОДНЫХ СЕТЕЙ

При организации беспроводной локальной сети необходимо учитывать некоторые особенности окружающей среды. На качество и дальность работы связи влияет множество физических факторов: число стен, перекрытий и других объектов через которые должен пройти сигнал. Обычно расстояние зависит от типа материалов и радиочастотного шума от других электроприборов в вашем помещении. Для увеличения проникаемости надо следовать базовым принципам:

1. Сократить число стен и перекрытий между абонентами беспроводной сети - каждая стена и перекрытие отнимает от максимального радиуса от 1м до 25м. Расположить точки доступа и абонентов сети так чтобы количество преград между ними было минимально.
2. Проверить угол между точками доступа и абонентами сети. Стена толщиной 0,5 м, при угле в 45 градусов, для радиоволны становиться как 1 м стена. При угле в 2 градуса стена становиться преградой толщиной в 12 м! Надо стараться расположить абонентов сети так, чтобы сигнал проходил под углом в 90 градусов к перекрытиям или стенам.
3. Строительные материалы влияют на прохождение сигнала по-разному – целиком металлические двери или алюминиевая облицовка негативно сказываются на прохождении радиоволн. Желательно, чтобы между абонентами сети не находились металлические или железобетонные препятствия.
4. С помощью программного обеспечения проверки мощности сигнала надо позиционировать антенну на лучший прием.
5. Удалить от абонентов беспроводных сетей, по крайней мере, на 1-2 метра электроприборы, генерирующие радиопомехи, микроволновые печи, мониторы, электромоторы, ИБП. Для уменьшения помех эти приборы должны быть надежно заземлены.
6. Если используются беспроводные телефоны стандарта 2.4 ГГц или оборудование X-10 (например, системы сигнализации), качество беспроводной связи может заметно ухудшиться или прерваться.

Для типичного жилья расстояние связи не представляет особой проблемы. Если обнаружена неуверенная связь в пределах дома, то надо расположить точку доступа между комнатами, которые надо связать беспроводной связью.

Для обнаружения точек доступа, попадающих в зону действия беспроводной сети и определения каналов, на которых они работают, можно использовать программу Network Stumbler (http://www.stumbler.net/). С ее помощью можно также оценить соотношение сигнал/шум на выбранных каналах.

1.7.1 ОФИСНАЯ СЕТЬ

Простая беспроводная сеть для небольшого офиса или домашнего использования (Small Office / Home Office – SOHO) может быть построена на основе одной точки доступа (рис. 1.56).

Рис. 1.56 Офисная сеть

Для организации сети адаптеры переводятся в режим инфраструктуры, а точка доступа – в режим точки доступа. При этом создается одна зона обслуживания, в которой находятся все пользователи сети.

При размещении точки доступа при организации малой сети следует обеспечить достаточное качество связи на всех рабочих местах, а также удобство в размещении самой точки. Типовое решение – закрепить точку доступа непосредственно на фальш-потолке, при этом провода электропитания и проводной сети будут проходить над фальш-потолком либо в коробах.

Необходимо иметь в виду, что при расширении сети и при увеличении количества пользователей скорость связи будет падать (пропорционально числу пользователей). Наибольшее разумное количество пользователей обычно составляет 16-20. Помимо этого, скорость и качество связи зависят и от расстояния между клиентом и точкой. Эти соображения могут потребовать расширения базовой сети.

Для расширения сети можно использовать uplink-порт точки доступа. Он может использоваться как для объединения базовых зон обслуживания в сеть, так и для интеграции в имеющуюся проводную или беспроводную инфраструктуру, например, для обеспечения пользователей доступом к разделяемым ресурсам других подразделений или для подключения к сети Интернет.

При расширении сети необходимо следить, чтобы частоты соседних точек доступа не перекрывались во избежание взаимных помех и снижения скорости передачи. Это

достигается настройкой соседних точек на неперекрывающиеся по частоте каналы 1, 6 и 11. Чередуя каналы таким образом, что соседние точки с каналами 1, 6 и 11 окажутся в вершинах равностороннего треугольника, можно охватить беспроводной связью сколь угодно большую площадь без перекрытия частот (рис. 1.57).

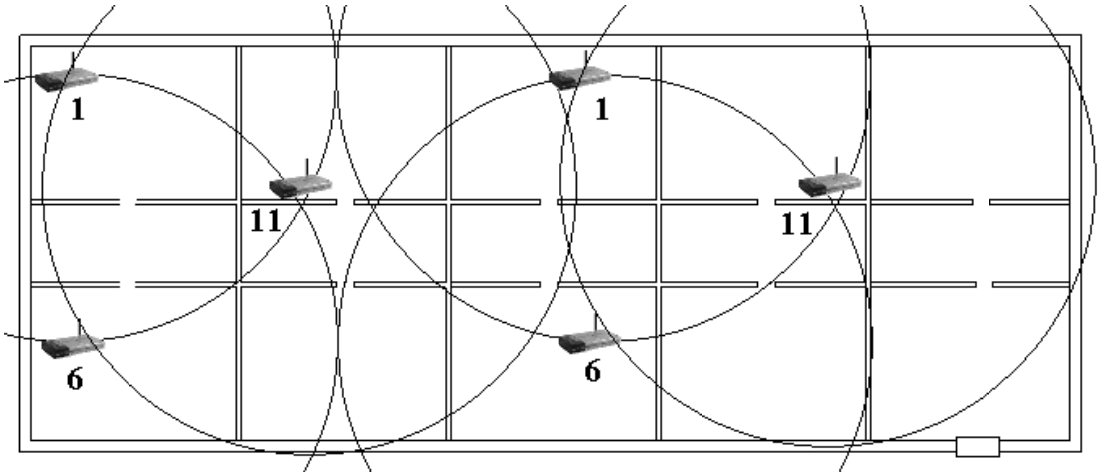


Рис. 1.57 Расширение беспроводной сети

На развертывание беспроводных сетей используемые приложения оказывают влияние по-разному. Наиболее важные факторы – это:

- Расчетная скорость в пересчете на одного клиента;
- Типы используемых приложений;
- Задержки в передаче данных.

Расчетная скорость каждого клиента уменьшается с вводом в зону обслуживания новых клиентов. Следовательно, если дома или в офисе используются требовательные к скорости приложения (например, программа интернет-телефонии Skype), то необходимо увеличить количество точек доступа на единицу площади (рис. 1.58)

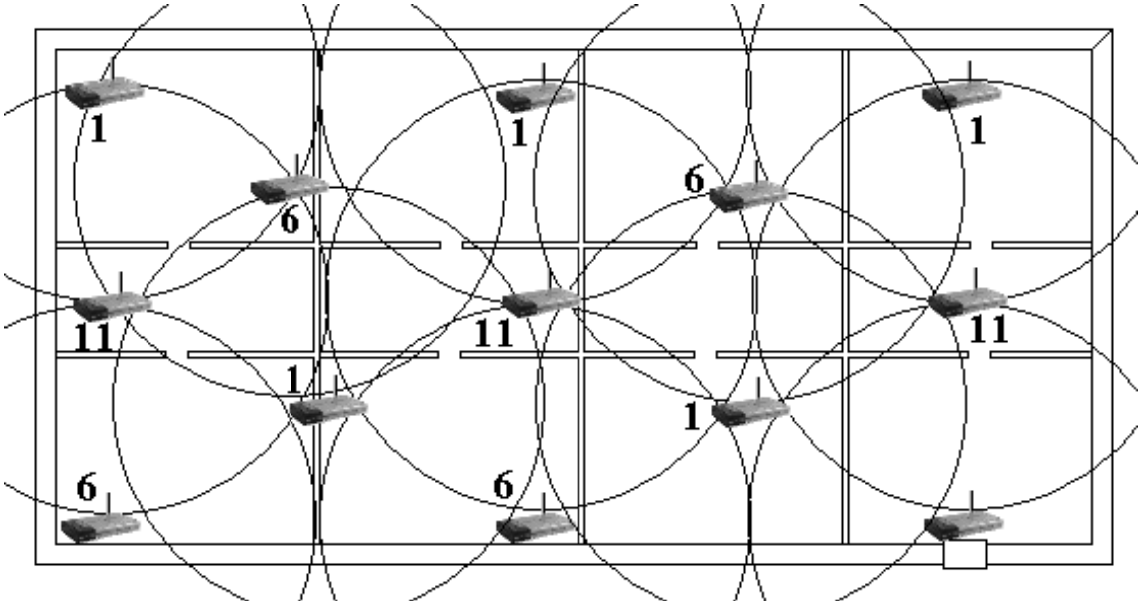


Рис. 1.58 Расширение беспроводной сети с максимальной скоростью

Для определения границы действия точек доступа используется ноутбук с установленной программой Network Stumbler. Она показывает, на какой скорости будет

работать адаптер в зависимости от удаления от точки доступа. По мере удаления скорость автоматически падает, и при достижении порогового уровня необходимо ставить новую точку.

Объединение всех точек доступа в офисе в локальную сеть можно осуществить несколькими способами. Самым простым и распространённым способом организации является объединение через проводную инфраструктуру (рис. 1.59)

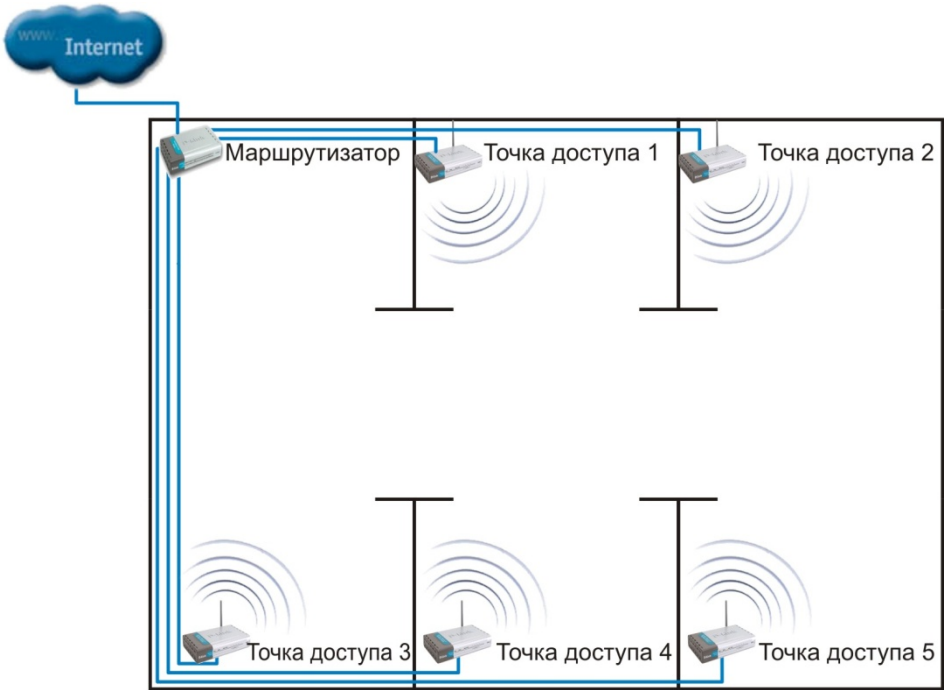


Рис. 1.59 Объединение точек доступа через проводную инфраструктуру

В таком случае ставиться коммутатор, к которому подключаются точки доступа посредством витой пары через uplink-порт. Также к этому коммутатору можно подвести широкополосный Интернет. Преимуществом такого подключения является простота настройки зоны действия точек доступа на разные каналы, недостатком – прокладка проводов от точек доступа к коммутатору.

Вторым способом подключения является подключение с использованием расширенного режима WDS (рис. 1.60).

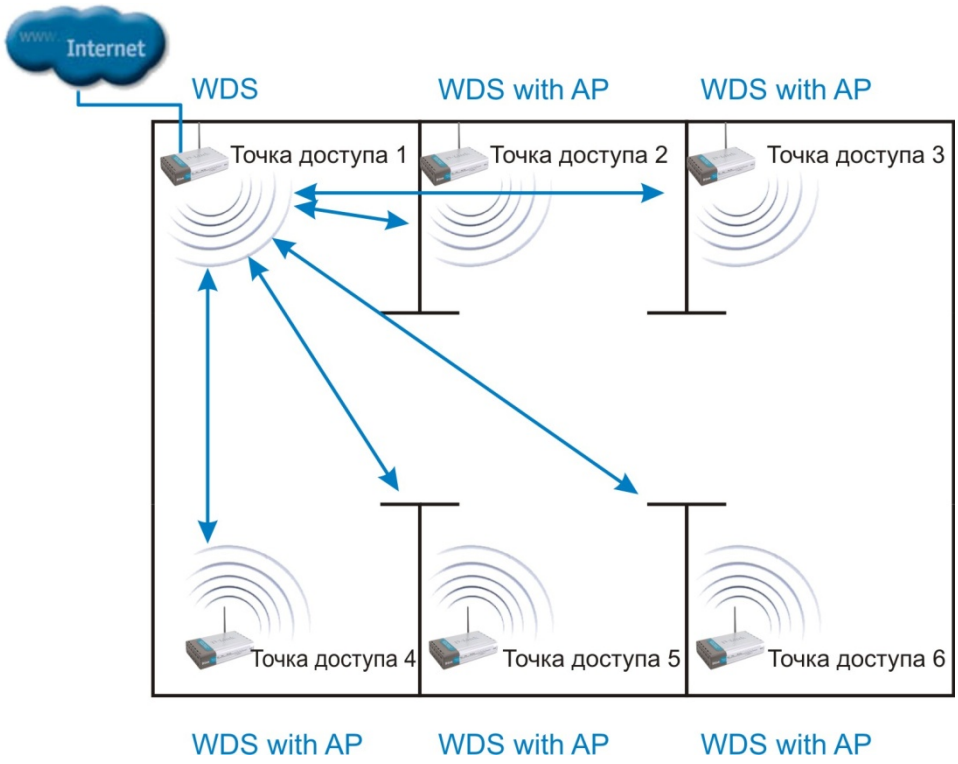


Рис. 1.60 Объединение точек доступа с использованием расширенного режима WDS

Одна точка доступа, которая имеет подключение к Интернету переводиться в мостовой режим WDS, остальные точки настраиваются на тот же канал, что и первая, и устанавливается режим WDS with AP. Использование такого способа нежелательно, т.к. все точки работают на одном канале, и при достаточно большом их количестве резко уменьшается скорость. Рекомендуется устанавливать не более 2-3 точек.

Третий способ подключения аналогичен предыдущему, но дополнительно к каждой точке доступа через проводной интерфейс подключена ещё одна точка, работающая на другом канале, для организации связи в одной комнате (рис. 1.61)

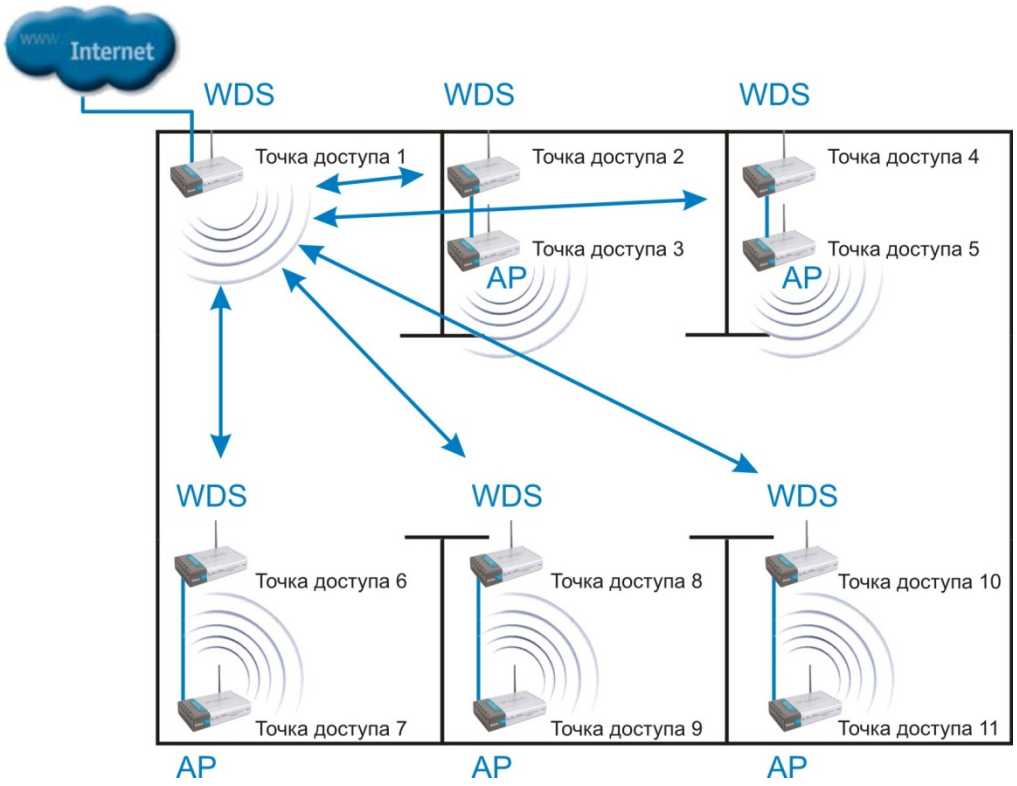


Рис. 1.61 Объединение точек доступа с дополнительными точками

Здесь переводятся те точки доступа в режим WDS, которые будут связаны с первой, а остальные – через проводные интерфейсы подключаются к ним. Они должны работать в режиме точки доступа и на других каналах, чтобы не было коллизий. Преимуществом такого способа подключения является полной отсутствие проводной инфраструктуры (за исключением связи между соседними точками), недостатком – большая стоимость, в связи с большим количеством точек доступа и использование одного канала для связи с базовой точкой.

Чтобы пользователь мог передвигаться от одной точки доступа к другой без потери доступа к сетевым службам и разрыва соединения во всем оборудовании компании D-Link есть функция роуминга.

Роуминг – это возможность радиоустройства перемещаться за пределы действия базовой станции и, находясь в зоне действия «гостевой» станции, иметь доступ к «домашней» сети (рис. 1.62).

Рис. 1.62 Роуминг

При его организации все точки доступа, обеспечивающие роуминг, конфигурируются на использование одинакового идентификатора зоны обслуживания (SSID). Все точки доступа относятся к одному широковещательному домену, или одному *домену роуминга*.

Механизм определения момента времени, когда необходимо начать процесс роуминга, не определен в стандарте 802.11, и, таким образом, оставлен на усмотрение поставщиков оборудования. Наиболее простой широко распространенный алгоритм переключения заключается в том, что адаптер взаимодействует с одной точкой вплоть до момента, когда уровень сигнала не упадет ниже допустимого уровня. После этого осуществляется поиск точки доступа с одинаковым SSID и максимальным уровнем сигнала, и переподключение к ней.

Роуминг включает значительно больше процессов, чем необходимо для поиска точки доступа, с которой можно связаться. Опишем некоторые из задач, которые должны решаться в ходе роуминга на канальном уровне:

- Предыдущая точка доступа должна определить, что клиент уходит из ее области действия.
- Предыдущая точка доступа должна буферизовать данные, предназначенные для клиента, осуществляющего роуминг.
- Новая точка доступа должна показать предыдущей, что клиент успешно переместился в ее зону.
- Предыдущая точка доступа должна послать буферизованные данные новой точке доступа.
- Предыдущая точка доступа должна определить, что клиент покинул ее зону действия.
- Точка доступа должна обновить таблицы MAC-адресов на коммутаторах инфраструктуры, чтобы избежать потери данных перемещающегося клиента.

1.7.2 СЕТЬ МЕЖДУ НЕСКОЛЬКИМИ ОФИСАМИ

Беспроводная связь может использоваться для объединения подсетей отдельных зданий, например – центрального офиса и филиалов, там, где прокладка кабеля между зданиями нежелательна или невозможна (рис. 1.63).

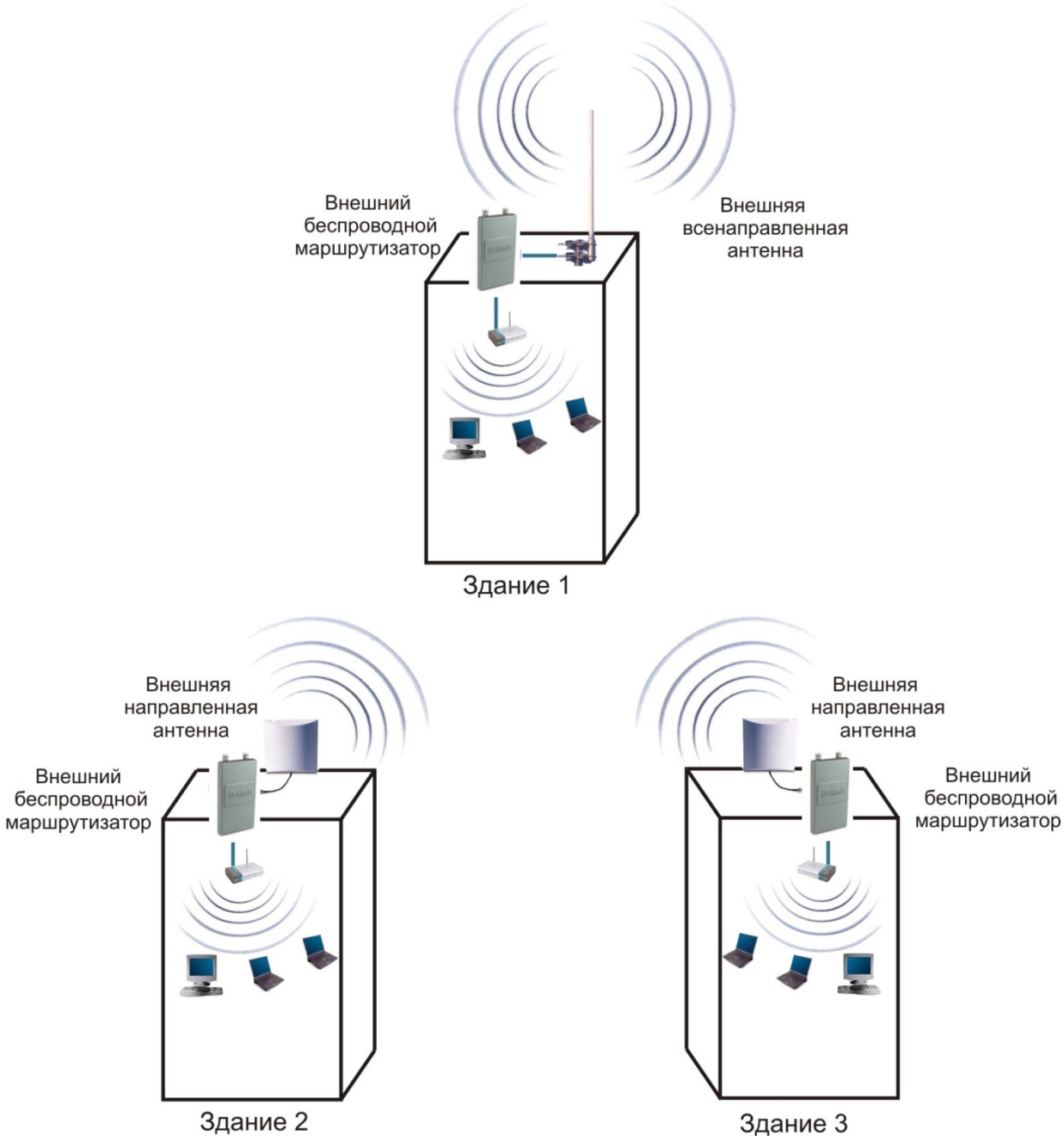


Рис. 1.63 Сеть между несколькими офисами

Для организации связи между зданиями могут использоваться внешние беспроводные точки, работающие в режиме моста. Через uplink-порт внешняя точка подключается к обычному коммутатору, и через него обеспечивает связь со всеми компьютерами подсети.

Внешние беспроводные точки имеют водонепроницаемый термостатированный корпус, систему грозовой защиты, систему питания Power-over-Ethernet. Благодаря сменной антенне, можно обеспечивать устойчивую радиосвязь на расстоянии до нескольких километров на специализированные узконаправленные антенны.

При организации внешней беспроводной связи особое внимание следует обратить обеспечению безопасности передачи данных, в связи с ее большей уязвимостью как к прослушиванию, так и к прямому физическому воздействию. Поэтому рекомендуется использовать точки доступа, специально предназначенные для наружного применения, и

позволяющие использовать аутентификацию, контроль доступа и шифрование передаваемых данных.

Необходимо также обратить внимание, что для внешних точек предусмотрена более сложная процедура получения разрешений на использование частот. Правила использования радиочастотного спектра в России приведены в Приложении Б.

1.8 БЕСПРОВОДНАЯ ТЕХНОЛОГИЯ WIMAX

1.8.1 ЦЕЛИ И ЗАДАЧИ WIMAX

При всем богатстве выбора сетевых подключений сложно одновременно соблюсти три основных требования к сетевым соединениям: высокая пропускная способность, надёжность и мобильность. Решить подобную задачу может следующее поколение беспроводных технологий WiMAX (Worldwide Interoperability for Microwave Access), стандарт IEEE 802.16.

Для продвижения и развития технологии WiMAX был сформирован WiMAX-форум: http://www.wimaxforum.org на базе рабочей группы IEEE 802.16, созданной в 1999 году. В форум вошли такие фирмы, как Nokia, Harris Corporation, Ensemble, Crosspan и Aperto. К маю 2005 года форум объединял уже более 230 участников. В том же году Всемирный съезд по вопросам информационного сообщества (World Summit on Information Society, WSIS) сформулировал следующие задачи, которые были возложены на технологию WiMAX:

1) Обеспечить при помощи WiMAX доступ к услугам информационных и коммуникационных технологий для небольших поселений, удалённых регионов, изолированных объектов, учитывая при этом, что в развивающихся странах 1,5 миллиона поселений с числом жителей более 100 человек не подключены к телефонным сетям и не имеют кабельного сообщения с крупными городами.
2) Обеспечить при помощи WiMAX доступ к услугам информационных и коммуникационных технологий более половины населения планеты в пределах своей досягаемости, учитывая при этом, что общее число пользователей Интернета в 2005 году составляло приблизительно 960 млн. человек, или около 14,5 процента всего населения Земли.

Цель технологии WiMAX заключается в том, чтобы предоставить универсальный беспроводный доступ для широкого спектра устройств (рабочих станций, бытовой техники «умного дома», портативных устройств и мобильных телефонов) и их логического объединения - локальных сетей. Надо отметить, что технология имеет ряд преимуществ:

1) По сравнению с проводными (xDSL или широкополосным), беспроводными или спутниковыми системами сети WiMAX должны позволить операторам и сервис-провайдерам экономически эффективно охватить не только новых потенциальных пользователей, но и расширить спектр информационных и коммуникационных технологий для пользователей, уже имеющих фиксированный (стационарный) доступ.
2) Стандарт объединяет в себя технологии уровня оператора связи (для объединения многих подсетей и предоставления им доступа к Интернет), а также технологии «последней мили» (конечного отрезка от точки входа в сеть провайдера до компьютера пользователя), что создает универсальность и, как следствие, повышает надёжность системы.
3) Беспроводные технологии более гибки и, как следствие, более просты в развёртывании, так как по мере необходимости могут масштабироваться.
4) Простота установки как фактор уменьшения затрат на развертывание сетей в развивающихся странах, малонаселённых или удалённых районах.

5) Дальность охвата является существенным показателем системы радиосвязи. На данный момент большинство беспроводных технологий широкополосной передачи данных требуют наличия прямой видимости между объектами сети. WiMAX благодаря использованию технологии OFDM создает зоны покрытия в условиях отсутствия прямой видимости от клиентского оборудования до базовой станции, при этом расстояния исчисляются километрами.
6) Технология WiMAX изначально содержит в себе протокол IP, что позволяет легко и прозрачно интегрировать её в локальные сети.
7) Технология WiMAX подходит для фиксированных, перемещаемых и подвижных объектов сетей на единой инфраструктуре.

1.8.2 ПРИНЦИПЫ РАБОТЫ

Система WiMAX состоит из двух основных частей:

1) Базовая станция WiMAX, может размещаться на высотном объекте: здании или вышке.
2) Приёмник WiMAX: антенна с приёмником (рис. 1.64).

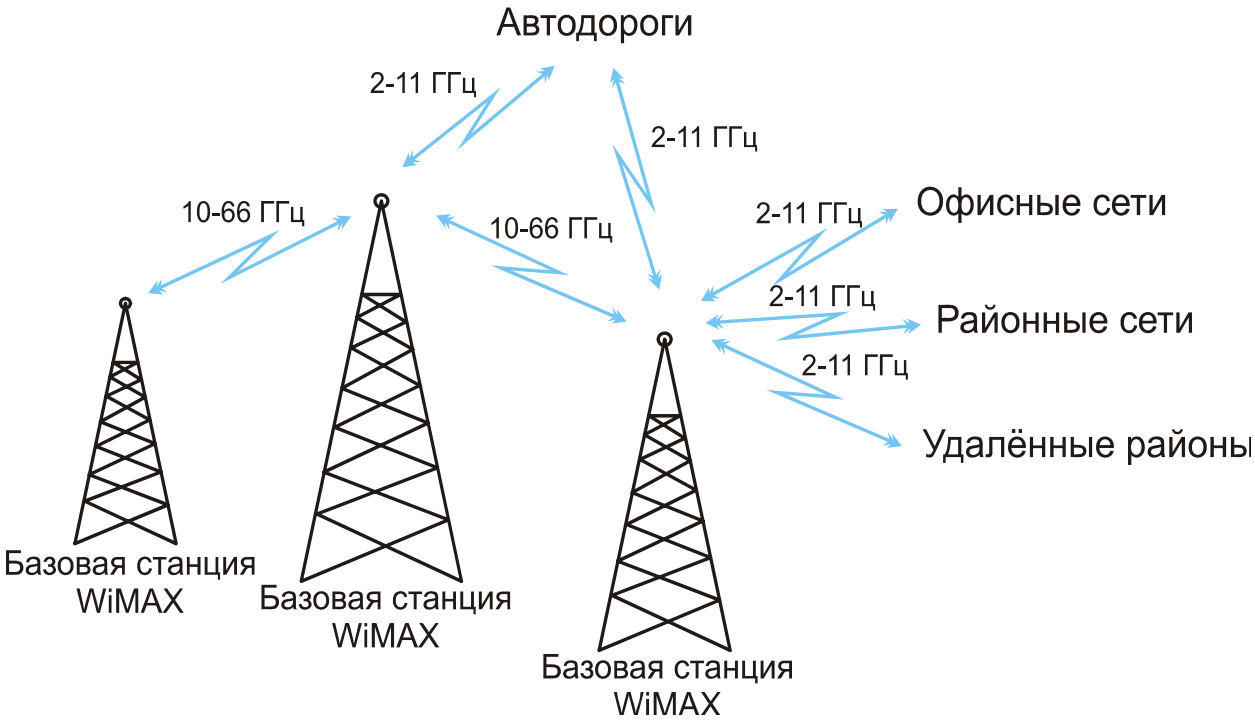


Рис. 1.64 Архитектура WiMAX

Соединение между базовой станцией и клиентским приёмником производится в низкочастотном диапазоне 2-11 ГГц. Данное соединение в идеальных условиях позволяет передавать данные со скоростью до 20 Мбит/с и не требует наличия прямой видимости между станцией и пользователем. Этот режим работы базовой станции WiMAX близок широко используемому стандарту 802.11 (Wi-Fi), что допускает совместимость уже выпущенных клиентских устройств и WiMAX.

Следует помнить, что технология WiMAX применяется как на «последней миле» - конечном участке между провайдером и пользователем, так и для предоставления доступа региональным сетям: офисным, районным.

Между соседними базовыми станциями устанавливается постоянное соединение с использованием сверхвысокой частоты 10-66 ГГц радиосвязи прямой видимости. Данное соединение в идеальных условиях позволяет передавать данные со скоростью до

120 Мбит/с. Ограничение по условию прямой видимости, разумеется, не является плюсом, однако оно накладывается только на базовые станции, участвующие в цельном покрытии района, что вполне возможно реализовать при размещении оборудования.

Как минимум, одна из базовых станций может быть постоянно связана с сетью провайдера через широкополосное скоростное соединение. Фактически, чем больше станций имеют доступ к сети провайдера, тем выше скорость и надёжность передачи данных. Однако даже при небольшом количестве точек система способна корректно распределить нагрузку за счёт сотовой топологии.

На базе сотового принципа разрабатываются также пути построения оптимальной сети, огибающей крупные объекты (например, горные массивы), когда серия последовательных станций передаёт данные по эстафетному принципу. Подобные разработки планируется включить в следующую версию стандарта. Ожидается, что эти изменения позволят существенно поднять скорость (рис. 1.65).

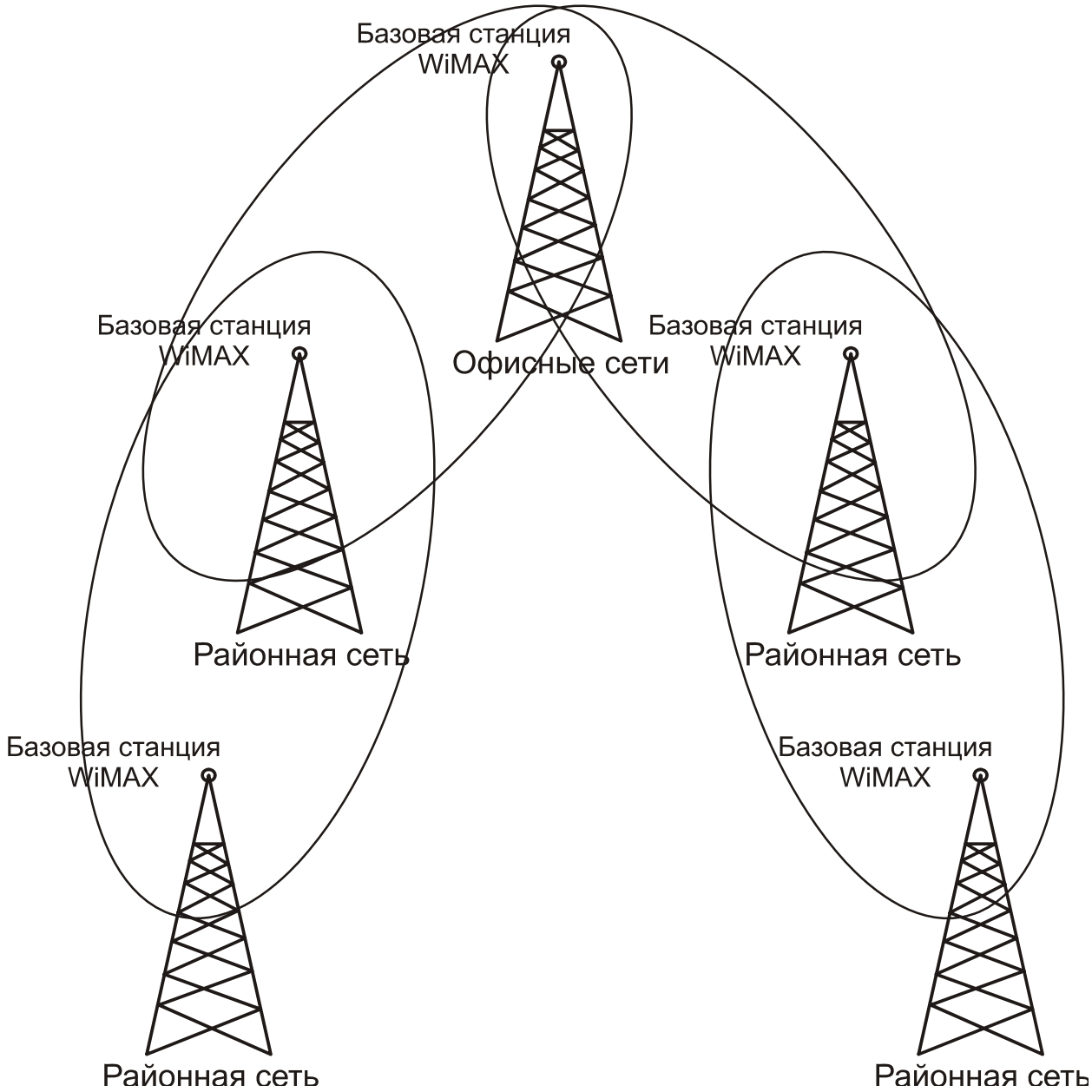


Рис. 1.65 Покрытие WiMAX

По структуре сети стандарта IEEE 802.16 очень похожи на традиционные сети мобильной связи: здесь тоже имеются базовые станции, которые действуют в радиусе до 50 км, при этом их также не обязательно устанавливать на вышках. Для них вполне подходят крыши домов, требуется лишь соблюдение условия прямой видимости между станциями. Для соединения базовой станции с пользователем необходимо наличие абонентского оборудования. Далее сигнал может поступать по стандартному Ethernet-кабелю, как непосредственно на конкретный компьютер, так и на точку доступа стандарта 802.11 Wi-Fi или в локальную проводную сеть стандарта Ethernet.

Это позволяет сохранить существующую инфраструктуру районных или офисных локальных сетей при переходе с кабельного доступа на WiMAX. Это позволяет также максимально упростить развёртывание сетей, позволяя использовать знакомые технологии для подключения компьютеров.

1.8.3 РЕЖИМЫ РАБОТЫ

Стандарт 802.16e-2005 вобрал в себя все ранее выходившие версии и на данный момент предоставляет следующие режимы.

1) Fixed WiMAX - фиксированный доступ;
2) Nomadic WiMAX - сеансовый доступ;
3) Portable WiMAX - доступ в режиме перемещения;
4) Mobile WiMAX - мобильный доступ.

Рассмотрим все эти режимы поподробнее.

Fixed WiMAX

Фиксированный доступ представляет собой альтернативу широкополосным проводным технологиям (xDSL, T1, т.п.). Стандарт использует диапазон частот 10-66 ГГц. Этот частотный диапазон из-за сильного затухания коротких волн требует прямой видимости между передатчиком и приёмником сигнала (рис. 1.66).

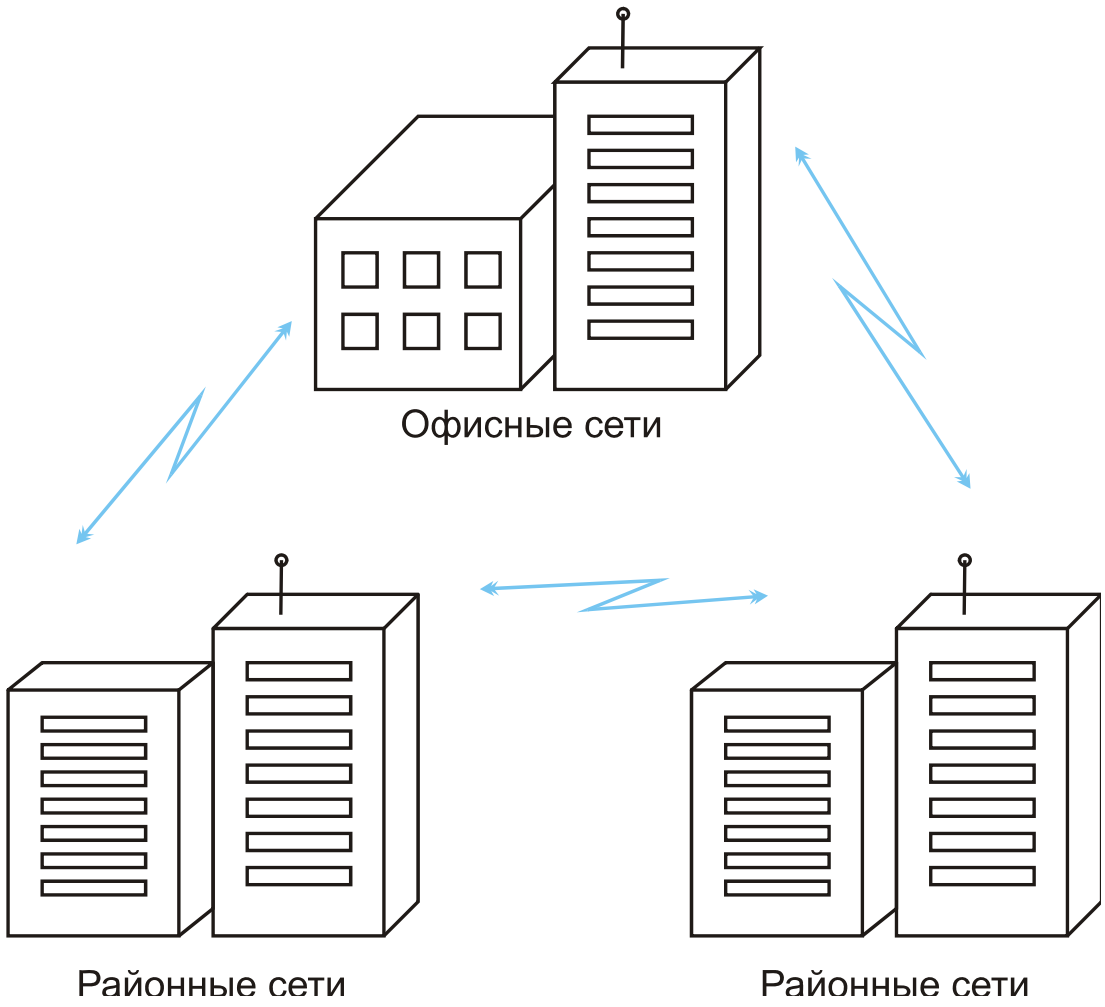


Рис. 1.66

С другой стороны, данный частотный диапазон позволяет избежать одной из главных проблем радиосвязи - многолучевого распространения сигнала. При этом ширина каналов связи в этом частотном диапазоне довольно велика (типичное значение - 25 или 28 МГц), что позволяет достигать скоростей передачи до 120 Мбит/с. Фиксированный режим включался в версию стандарта 802.16d-2004 и уже используется в ряде стран. Однако большинство компаний, предлагающих услуги Fixed WiMAX, ожидают скорого перехода на портативный и в дальнейшем мобильный WiMAX.

Nomadic WiMAX

Сеансовый (кочующий) доступ добавил понятие сессий к уже существующему Fixed WiMAX. Наличие сессий позволяет свободно перемещать клиентское оборудование между сессиями и восстанавливать соединение уже с помощью других вышек WiMAX, нежели тех, что были использованы во время предыдущей сессии. Такой режим разработан в основном для портативных устройств, таких, как ноутбуки, КПК. Введение сессий позволяет также уменьшить расход энергии клиентского устройства, что тоже немаловажно для портативных устройств.

Portable WiMAX

Для режима Portable WiMAX добавлена возможность автоматического переключения клиента от одной базовой станции WiMAX к другой без потери соединения. Однако для данного режима всё ещё ограничена скорость передвижения клиентского оборудования – 40 км/ч. Впрочем, уже в таком виде можно использовать

клиентские устройства в дороге (в автомобиле при движении по жилым районам города, где скорость ограничена, на велосипеде, двигаясь пешком, т.д.).

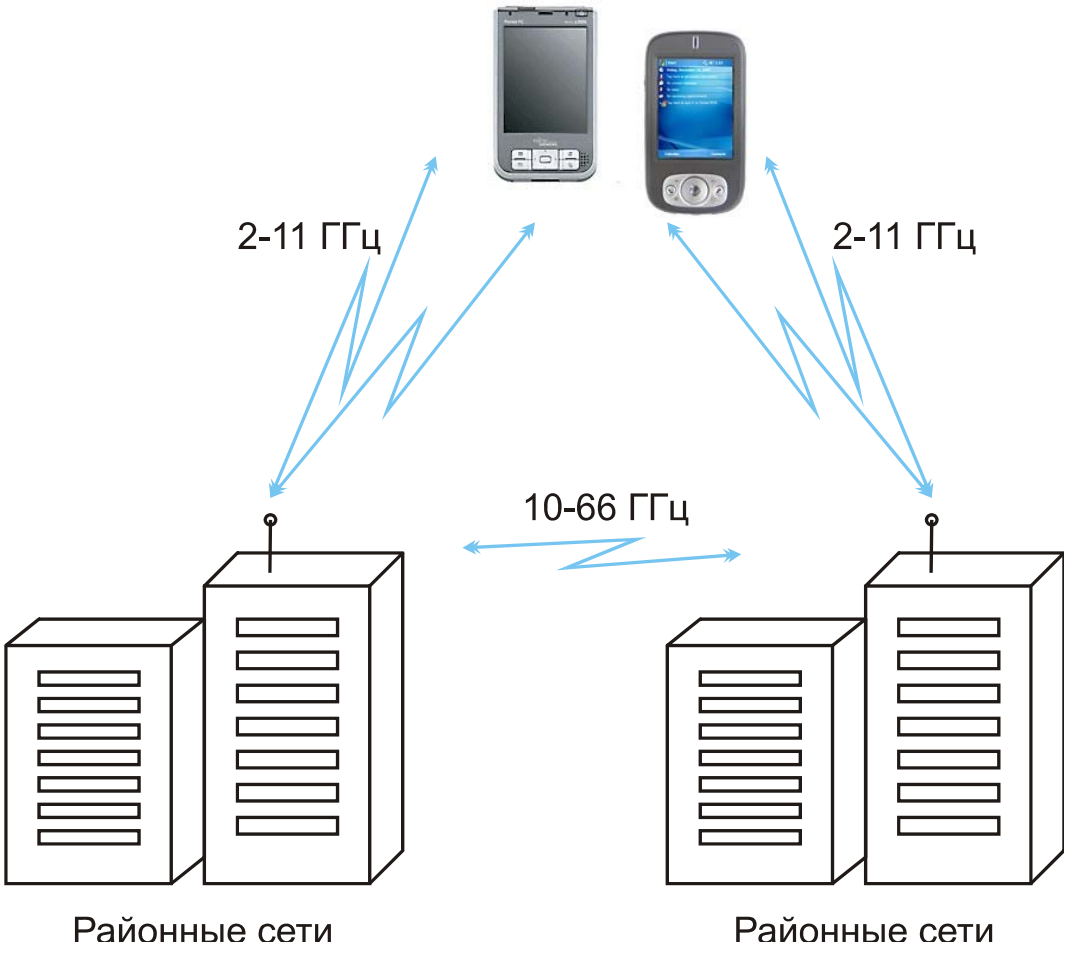


Рис. 1.67

Введение данного режима сделало целесообразным использование технологии WiMAX для смартфонов и КПК (рис. 1.67). В 2006 году начат выпуск устройств, работающих в портативном режиме WiMAX. Считается, что до 2008 года внедрение и продвижение на рынок именно этого режима будет приоритетным.

Mobile WiMAX

Был разработан в стандарте 802.16e-2005 и позволил увеличить скорость перемещения клиентского оборудования до более 120 км/ч.

Основные достижения этого режима:

1) Устойчивость к многолучевому распространению сигнала и собственным помехам.
2) Масштабируемая пропускная способность канала.
3) Технология Time Division Duplex (TDD), которая позволяет эффективно обрабатывать асимметричный трафик и упрощает управление сложными системами антенн за счёт эстафетной передачи сессии между каналами.
4) Технология Hybrid-Automatic Repeat Request (H-ARQ), которая позволяет сохранять устойчивое соединение при резкой смене направления движения клиентского оборудования.
5) Распределение выделяемых частот и использование субканалов при высокой загрузке позволяет оптимизировать передачу данных с учётом силы сигнала клиентского оборудования.

6) Управление энергосбережением позволяет оптимизировать затраты энергии на поддержание связи портативных устройств в режиме ожидания или простоя.
7) Технология Network-Optimized Hard Handoff (HHO), которая позволяет до 50 миллисекунд и менее сократить время на переключение клиента между каналами.
8) Технология Multicast and Broadcast Service (MBS), которая объединяет функции DVB-H, MediaFLO и 3GPP E-UTRA для:
   - достижения высокой скорости передачи данных с использованием одночастотной сети;
   - гибкого распределения радиочастот;
   - низкого потребления энергии портативными устройствами;
   - быстрого переключения между каналами.
9) Технология Smart Antenna, поддерживающая субканалы и эстафетную передачу сессии между каналами, что позволяет использовать сложные системы антенн, включая формирование диаграммы направленности, простанственно-временное маркирование, пространственное мультиплексирование (уплотнение).
10) Технология Fractional Frequency Reuse, которая позволяет контролировать наложение/пересечение каналов для повторного задействования частот с минимальными потерями.
11) Размер фрейма в 5 миллисекунд создает оптимальный компромисс между надёжностью передачи данных за счёт использования малых пакетов и накладными расходами за счёт увеличения числа пакетов (и как следствие, заголовков).

Стандарт WiMAX на данный момент находится на стадии тестирования. Единственная конкурентоспособная версия стандарта, для которой существует лицензия на оборудование, - это Fixed WiMAX. Однако провайдеры не спешат заменять дорогостоящее, но уже работающее оборудование на новое, ибо это требует существенных инвестиций без возможности поднять производительность (и как следствие, цену на услуги) и вернуть вложенные средства быстро.

Развёртывание WiMAX-сетей там, где доступа к Интернету ещё не было ранее, приводит к вопросу о наличии в малонаселенных или удалённых регионах достаточного числа потенциальных пользователей, обладающих оборудованием или денежными средствами на его приобретение. Та же проблема возникает при переходе на Mobile WiMAX после его лицензирования, так как, помимо затрат провайдеров на модернизацию операторского оборудования, следует учитывать затраты пользователей на модернизацию клиентского оборудования: приобретение WiMAX-карт, обновление портативных устройств.

Вторым останавливающим фактором является убеждённость многих специалистов, которые считают недопустимым использование сверхвысоких частот радиосвязи прямой видимости из-за вреда, наносимого при этом здоровью человека. Наличие вышек на расстоянии десятков метров от жилых объектов (а базовые станции рекомендуется устанавливать на крышах домов) может пагубно сказаться на здоровье жителей, особенно детей. Однако результатов медицинских экспериментов, способных чётко доказать наличие или высокую вероятность вреда, пока не опубликовано.

Третьим останавливающим фактором является, как ни странно, быстрое развитие стандарта. Появление новых, принципиально различных версий стандарта WiMAX приводит к вопросу о неизбежной смене оборудования через несколько лет. Так, станции, сейчас работающие в режиме Fixed WiMAX, не смогут поддерживать Mobile WiMAX. При переходе на следующий стандарт понадобится обновление части оборудования, что отпугивает крупных провайдеров. На данный момент внедрение и использование Fixed WiMAX на коммерческой основе могут позволить себе только небольшие компании, которые не планируют значительного расширения (в том числе территориального) и используют новизну технологии для привлечения клиентов.

И, наконец, четвертым фактором является наличие конкурентного стандарта широкополосной связи, использующего близкие диапазоны радиочастот - WiBro. Этот стандарт тоже до конца не лицензирован, однако он уже получил определённую известность. А потому всегда существует вероятность, что через несколько лет предпочтительным окажется не WiMAX, а WiBro. И компании, вложившие средства в разработку и внедрение WiMAX-систем, серьёзно пострадают. Впрочем, из-за схожести стандартов существует также вероятность слияния и в дальнейшем использования оборудования, поддерживающего оба стандарта одновременно.

Таким образом, при видимых преимуществах стандарта ещё рано говорить о тотальном внедрении технологии или даже о возможности перехода на неё и отказа от существующих сетевых решений. Необходимо сначала получить первое лицензированное оборудование стандарта Mobile WiMAX, а также результаты полевых испытаний. Затем можно ожидать утверждения стандартов версии 802.16f (Full Mobile WiMAX) и 802.16m.

Первый из них включает в себя алгоритмы обхода препятствий и оптимизацию сотовой топологии покрытия между базовыми станциями. Второй стандарт должен поднять скорость передачи данных со стационарным клиентским оборудованием до 1 Гбит/с и с мобильным клиентским оборудованием до 100 Мбит/с. Эти стандарты планируется утвердить в 2008 и 2009 годах, соответственно.

Далее можно ожидать лицензирования оборудования с поддержкой новых стандартов, появления конкуренции на рынке производства оборудования и услуг доступа через WiMAX. И только тогда можно будет говорить о действительных преимуществах и недостатках этой технологии по сравнению с ныне существующими.

ГЛАВА 2. БЕЗОПАСНОСТЬ БЕСПРОВОДНЫХ СЕТЕЙ

2.1 УГРОЗЫ И РИСКИ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ

Главное отличие между проводными и беспроводными сетями связано с абсолютно неконтролируемой областью между конечными точками сети. В достаточно широком пространстве сетей беспроводная среда никак не контролируется. Современные беспроводные технологии предлагают ограниченный набор средств управления всей областью развертывания сети. Это позволяет атакующим, находящимся в непосредственной близости от беспроводных структур, производить целый ряд нападений, которые были невозможны в проводном мире. Обсудим характерные только для беспроводного окружения угрозы безопасности, оборудование, которое используется при атаках, проблемы, возникающие при роуминге от одной точки доступа к другой, укрытия для беспроводных каналов и криптографическую защиту открытых коммуникаций.

Подслушивание

Наиболее распространенная проблема в таких открытых и неуправляемых средах, как беспроводные сети, – возможность анонимных атак. Анонимные вредители могут перехватывать радиосигнал и расшифровывать передаваемые данные, как показано на рисунке 2.1.

Рис. 2.1 Атака «подслушивание»

Оборудование, используемое для подслушивания в сети, может быть не сложнее того, которое используется для обычного доступа к этой сети. Чтобы перехватить передачу, злоумышленник должен находиться вблизи от передатчика. Перехваты такого типа практически невозможно зарегистрировать, и еще труднее им помешать. Использование антенн и усилителей дает злоумышленнику возможность находиться на значительном удалении от цели в процессе перехвата.

Подслушивание ведут для сбора информации в сети, которую впоследствии предполагается атаковать. Первичная цель злоумышленника – понять, кто использует сеть, какая информация в ней доступна, каковы возможности сетевого оборудования, в какие моменты его эксплуатируют наиболее и наименее интенсивно и какова территория развертывания сети. Все это пригодится для того, чтобы организовать атаку на сеть. Многие общедоступные сетевые протоколы передают такую важную информацию, как имя пользователя и пароль, открытым текстом. Перехватчик может использовать добытые данные для того, чтобы получить доступ к сетевым ресурсам. Даже если передаваемая информация зашифрована, в руках злоумышленника оказывается текст, который можно запомнить, а потом уже раскодировать.

Другой способ подслушивания – подключиться к беспроводной сети. Активное подслушивание в локальной беспроводной сети обычно основано на неправильном использовании протокола *Address Resolution Protocol (ARP)*. Изначально эта технология была создана для «прослушивания» сети. В действительности мы имеем дело с атакой типа MITM (man in the middle, «человек посередине») на уровне связи данных. Они могут принимать различные формы и используются для разрушения конфиденциальности и целостности сеанса связи. Атаки MITM более сложны, чем большинство других атак: для их проведения требуется подробная информация о сети. Злоумышленник обычно подменяет идентификацию одного из сетевых ресурсов. Когда жертва атаки инициирует соединение, мошенник перехватывает его и затем завершает соединение с требуемым ресурсом, а потом пропускает все соединения с этим ресурсом через свою станцию. При этом, атакующий может посылать информацию, изменять посланную или подслушивать все переговоры и потом расшифровывать их.

Атакующий посылает ARP-ответы, на которые не было запроса, к целевой станции локальной сети, которая отправляет ему весь проходящий через нее трафик. Затем злоумышленник будет отсылать пакеты указанным адресатам.

Таким образом, беспроводная станция может перехватывать трафик другого беспроводного клиента (или проводного клиента в локальной сети).

Отказ в обслуживании (Denial of Service, DOS)

Полную парализацию сети может вызвать атака типа DOS. Во всей сети, включая базовые станции и клиентские терминалы, возникает такая сильная интерференция, что станции не могут связываться друг с другом (рис. 2.2). Эта атака выключает все коммуникации в определенном районе. Если она проводится в достаточно широкой области, то может потребовать значительных мощностей. Атаку DOS на беспроводные сети трудно предотвратить или остановить. Большинство беспроводных сетевых технологий использует нелицензированные частоты – следовательно, допустима интерференция от целого ряда электронных устройств.

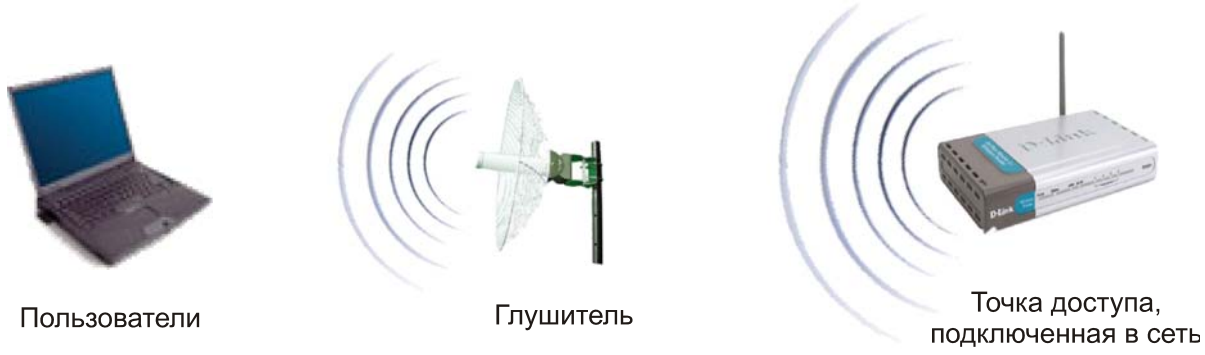


Рис. 2.2 Атака «отказ в обслуживании» в беспроводных коммуникациях

Глушение клиентской станции

Глушение в сетях происходит тогда, когда преднамеренная или непреднамеренная интерференция превышает возможности отправителя или получателя в канале связи, таким образом, выводя этот канал из строя. Атакующий может использовать различные способы глушения.

Глушение клиентской станции дает возможность мошеннику подставить себя на место заглушенного клиента, как показано на рисунке 2.3. Также глушение могут использовать для отказа в обслуживании клиента, чтобы ему не удавалось реализовать соединение. Более изощренные атаки прерывают соединение с базовой станцией, чтобы затем она была присоединена к станции злоумышленника.

Рис. 2.3 Атака глушения клиента для перехвата соединения

Глушение базовой станции

Глушение базовой станции предоставляет возможность подменить ее атакующей станцией, как показано на рисунке 2.4. Такое глушение лишает пользователей доступа к услугам.

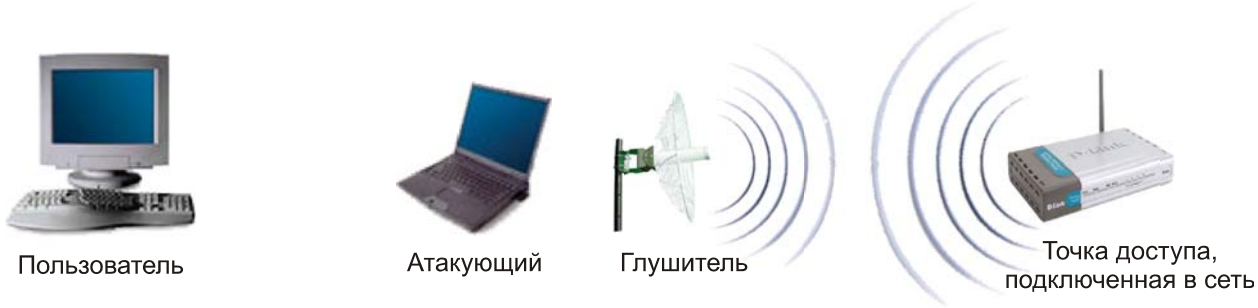


Рис. 2.4 Атака глушения базовой станции для перехвата соединения

Как отмечалось выше, большинство беспроводных сетевых технологий использует нелицензированные частоты. Поэтому многие устройства, такие как радиотелефоны, системы слежения и микроволновые печи, могут влиять на работу беспроводных сетей и глушить беспроводное соединение. Чтобы предотвратить такие случаи непреднамеренного глушения, прежде чем покупать дорогостоящее беспроводное

оборудование, надо тщательно проанализировать место его установки. Такой анализ поможет убедиться в том, что другие устройства никак не помешают коммуникациям.

Угрозы криптозащиты

В беспроводных сетях применяются криптографические средства для обеспечения целостности и конфиденциальности информации. Однако оплошности приводят к нарушению коммуникаций и злонамеренному использованию информации.

WEP – это криптографический механизм, созданный для обеспечения безопасности сетей стандарта 802.11. Этот механизм разработан с единственным статическим ключом, который применяется всеми пользователями. Управляющий доступ к ключам, частое их изменение и обнаружение нарушений практически невозможны. Исследование WEP-шифрования выявило уязвимые места, из-за которых атакующий может полностью восстановить ключ после захвата минимального сетевого трафика. В Интернет есть средства, которые позволяют злоумышленнику восстановить ключ в течение нескольких часов. Поэтому на WEP нельзя полагаться как на средство аутентификации и конфиденциальности в беспроводной сети.

Использовать описанные криптографические механизмы лучше, чем не использовать их вовсе, но благодаря известной уязвимости нужны другие методы защиты от перечисленных выше атак. Все беспроводные коммуникационные сети подвержены атакам прослушивания в период контакта (установки соединения, сессии связи и прекращения соединения). Сама природа беспроводного соединения устраняет возможность его контроля, и потому оно требует защиты. Управление ключом, как правило, вызывает дополнительные проблемы, когда применяется при роуминге и в случае общего пользования открытой средой. Далее в этом мы более внимательно рассмотрим проблемы криптографии и их решения.

Анонимность атак

Беспроводной доступ обеспечивает полную анонимность атаки. Без соответствующего оборудования в сети, позволяющего определять местоположение, атакующий может легко сохранять анонимность и прятаться где угодно на территории действия беспроводной сети. В таком случае злоумышленника трудно поймать и еще сложнее передать дело в суд.

В недалеком будущем прогнозируется ухудшение распознаваемости атак в Интернет из-за широкого распространения анонимных входов через небезопасные точки доступа. Уже есть много сайтов, где публикуются списки таких точек, которые можно использовать с целью вторжения. Важно отметить, что многие мошенники изучают сети не для атак на их внутренние ресурсы, а для получения бесплатного анонимного доступа в Интернет, прикрываясь которым они атакуют другие сети. Если операторы связи не принимают мер предосторожности против таких нападений, то будут отвечать за вред, причиняемый при использовании их доступа к Интернет другим сетям.

Физическая защита

Устройства беспроводного доступа к сети, сами по своей природе должны быть маленькими, и переносимыми (КПК, Ноутбуки), а также точки доступа также имеют небольшой размер и компактность. Кража таких устройств во многом приводит к тому, что злоумышленник может попасть в сеть, не используя сложных атак, т. к. основные

механизмы аутентификации в стандарте 802.11 рассчитаны на регистрацию именно физического аппаратного устройства, а не учетной записи пользователя. Так что потеря одного сетевого интерфейса и не своевременное извещение администратора может привести к тому, что злоумышленник получит доступ к сети без особых хлопот.

2.2 ОСНОВЫ КРИПТОГРАФИИ

2.2.1 БАЗОВЫЕ ТЕРМИНЫ И ИХ ОПРЕДЕЛЕНИЯ

Аутентификация: определение источника информации, то есть конечного пользователя или устройства (центрального компьютера, сервера, коммутатора, маршрутизатора и т. д.).
Целостность данных: обеспечение неизменности данных в ходе их передачи.
Конфиденциальность данных: обеспечение просмотра данных в приемлемом формате только для лиц, имеющих право на доступ к этим данным.
Шифрование: метод изменения информации таким образом, что прочитать ее не может никто, кроме адресата, который должен ее расшифровать.
Расшифровка: метод восстановления измененной информации и приведения ее в читаемый вид.
Ключ: цифровой код, который может использоваться для шифрования и расшифровки информации, а также для ее подписи.
Общий ключ: цифровой код, используемый для шифрования/расшифровки информации и проверки цифровых подписей; этот ключ может быть широко распространен; общий ключ используется с соответствующим частным ключом.
Частный ключ: цифровой код, используемый для шифрования/расшифровки информации и проверки цифровых подписей; владелец этого ключа должен держать его в секрете; частный ключ используется с соответствующим общим ключом.
Секретный ключ: цифровой код, совместно используемый двумя сторонами для шифрования и расшифровки данных.
Хэш-функция: математический расчет, результатом которого является последовательность битов (цифровой код). Имея этот результат, невозможно восстановить исходные данные, использованные для расчета.
Хэш: последовательность битов, полученная в результате расчета хэш-функции.
Результат обработки сообщения (Message digest): величина, выдаваемая хэш-функцией (то же, что и «хэш»).
Шифр: любой метод шифрования данных.
Цифровая подпись: последовательность битов, прилагаемая к сообщению (зашифрованный хэш), которая обеспечивает аутентификацию и целостность данных.
AAA (Authentication, Authorization, Accounting): архитектура аутентификации, авторизации и учета.
VPN (Virtual Private Networks): виртуальные частные сети.
IDS (Intrusion Detection System): системы обнаружения вторжений.

2.2.2 КРИПТОГРАФИЯ

Криптографией называется наука составления и расшифровки закодированных сообщений. Криптография является важным элементом для механизмов *аутентификации, целостности и конфиденциальности*.

Аутентификация является средством подтверждения личности отправителя или получателя информации. Целостность означает, что данные не были изменены, а конфиденциальность создает ситуацию, при которой данные не может понять никто, кроме их отправителя и получателя. Обычно криптографические механизмы существуют в виде алгоритма (математической функции) и секретной величины (ключа).

Аутентификация, целостность данных и конфиденциальность данных поддерживаются тремя типами криптографических функций: симметричным шифрованием, асимметричным шифрованием и хэш-функциями.

Симметричное шифрование

Симметричное шифрование, которое часто называют шифрованием с помощью секретных ключей, в основном используется для обеспечения конфиденциальности данных. Для того чтобы обеспечить конфиденциальность данных абоненты должны совместно выбрать единый математический алгоритм, который будет использоваться для шифрования и расшифровки данных. Кроме того, им нужно выбрать общий ключ (секретный ключ), который будет использоваться с принятым ими алгоритмом шифрования/расшифровки.

Пример симметричного шифрования показан на рисунке 2.5.

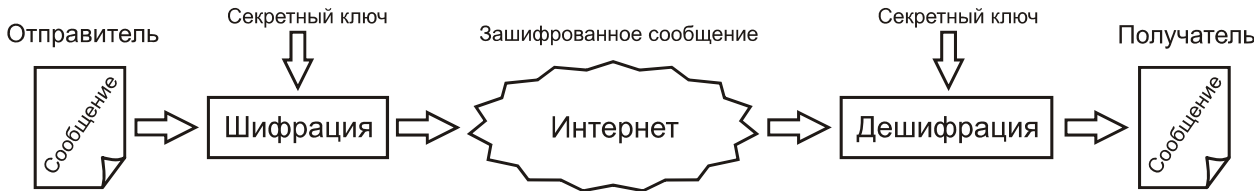


Рис. 2.5 Симметричное шифрование

Сегодня широко используются такие алгоритмы секретных ключей, как Data Encryption Standard (DES), 3DES (или «тройной DES») и International Data Encryption Algorithm (IDEA). Эти алгоритмы шифруют сообщения блоками по 64 бита. Если объем сообщения превышает 64 бита (как это обычно и бывает), необходимо разбить его на блоки по 64 бита в каждом, а затем каким-то образом свести их воедино. Такое объединение, как правило, происходит одним из следующих четырех методов:

- электронной кодовой книги (Electronic Code Book, ECB);
- цепочки зашифрованных блоков (Cipher Block Changing, CBC);
- x-битовой зашифрованной обратной связи (Cipher FeedBack, CFB-x);
- выходной обратной связи (Output FeedBack, OFB).

Шифрование с помощью секретного ключа чаще всего используется для поддержки конфиденциальности данных и очень эффективно реализуется с помощью неизменяемых «вшитых» программ (firmware). Этот метод можно использовать для аутентификации и поддержания целостности данных, но метод цифровой подписи является более эффективным. С методом секретных ключей связаны следующие проблемы:

- Необходимо часто менять секретные ключи, поскольку всегда существует риск их случайного раскрытия;
- Трудно обеспечить безопасное генерирование и распространение секретных ключей.

Асимметричное шифрование

Асимметричное шифрование часто называют шифрованием с помощью общего ключа, при котором используются разные, но взаимно дополняющие друг друга ключи и алгоритмы шифрования и расшифровки. Для того чтобы установить связь с использованием шифрования через общий ключ, обоим сторонам нужно получить два ключа: общий и частный (рис. 2.6). Для шифрования и расшифровки данных обе стороны будут пользоваться разными ключами.

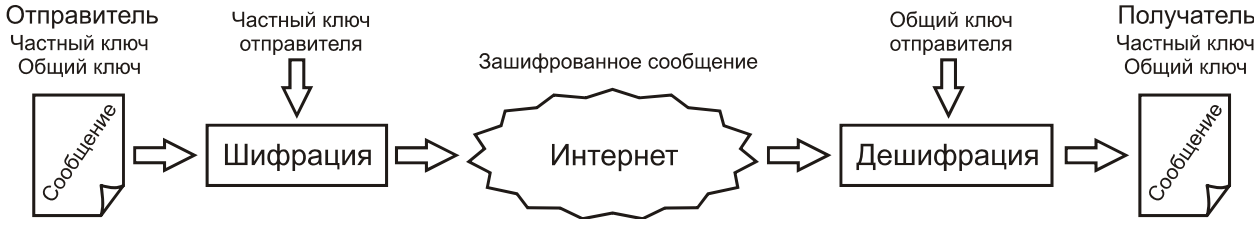


Рис. 2.6 Асимметричное шифрование

Вот некоторые наиболее типичные цели использования алгоритмов общих ключей:

- обеспечение конфиденциальности данных;
- аутентификация отправителя;
- безопасное получение общих ключей для совместного использования.

Механизмы генерирования пар общих/частных ключей являются достаточно сложными, но в результате получаются пары очень больших случайных чисел, одно из которых становится общим ключом, а другое – частным. Генерирование таких чисел требует больших процессорных мощностей, поскольку эти числа, а также их произведения должны отвечать строгим математическим критериям. Однако этот процесс генерирования абсолютно необходим для обеспечения уникальности каждой пары общих/частных ключей. Алгоритмы шифрования с помощью общих ключей редко используются для поддержки конфиденциальности данных из-за ограничений производительности. Вместо этого их часто используют в приложениях, где аутентификация проводится с помощью цифровой подписи и управления ключами.

Среди наиболее известных алгоритмов общих ключей можно назвать RSA (Rivest-Shamir-Adleman, Ривест-Шамир-Адельман) и ElGamal (Эль-Гамал).

Безопасная хэш-функция

Безопасной хэш-функцией называется функция, которую легко рассчитать, но обратное восстановление практически невозможно, так как требует непропорционально больших усилий. Входящее сообщение пропускается через математическую функцию (хэш-функцию), и в результате на выходе мы получаем некую последовательность битов (рис. 2.7). Эта последовательность называется «хэш» (или «результат обработки сообщения»). Хэш-функция принимает сообщение любой длины и выдает на выходе хэш фиксированной длины.

Рис. 2.7 Вычисление хэш-функции

Обычные хэш-функции включают:

- алгоритм Message Digest 4 (MD4);
- алгоритм Message Digest 5 (MD5);
- алгоритм безопасного хэша (Secure Hash Algorithm, SHA).

Цифровая подпись

Цифровая подпись представляет собой зашифрованный хэш, который добавляется к документу. Принцип шифрования с цифровой подписью легко понять из рисунка 2.8.

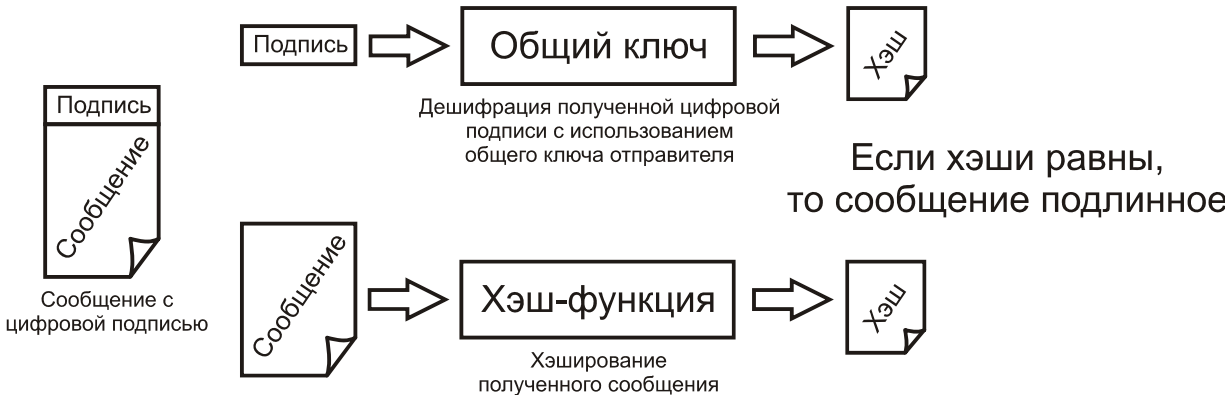


Рис. 2.8 Проверка подлинности сообщения с цифровой подписью

Она может использоваться для аутентификации отправителя и целостности документа. Цифровые подписи можно создавать с помощью сочетания хэш-функций и криптографии общих ключей.

Цифровой сертификат

Цифровым сертификатом называется сообщение с цифровой подписью, которое в настоящее время обычно используется для подтверждения действительности общего ключа. Общий формат широко распространенного сертификата X.509, включает следующие элементы:

- номер версии;
- серийный номер сертификата;
- эмитент информации об алгоритме;
- эмитент сертификата;
- даты начала и окончания действия сертификата;
- информацию об алгоритме общего ключа субъекта сертификата;
- подпись эмитирующей организации.

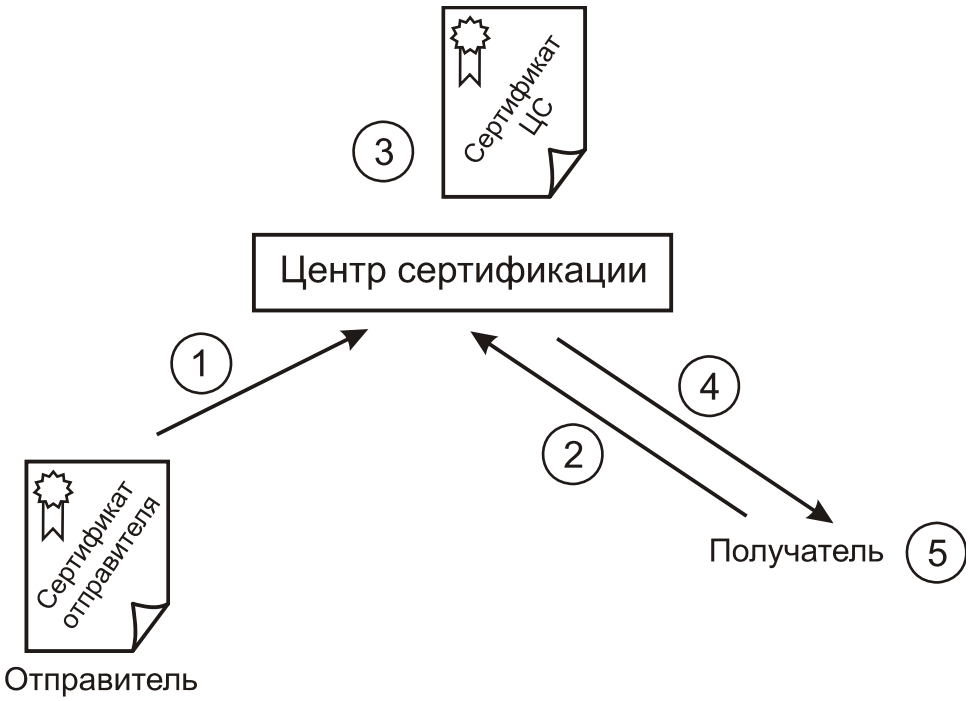


Рис. 2.9 Передача ключа с цифровым сертификатом

Эмитирующая организация, выдающая сертификат, или *центр сертификации* (Certification authority, CA), является надежной третьей стороной, которой вы полностью доверяете. Передача общего ключа происходит следующим образом (рис. 2.9):

1) отправитель создаёт сертификат, в который включает общий ключ;
2) получатель запрашивает у центра сертификации сертификат отправителя;
3) центр сертификации подписывает сертификат отправителя;
4) центр сертификации посылает подписанный сертификат получателю;
5) получатель проверяет подпись центра сертификации и извлекает общий ключ отправителя.

Для реализации этой схемы необходима надежная система распространения общего ключа CA среди пользователей. Для этого создана *инфраструктура открытых ключей PKI* (Public Key Infrastructure). Использование PKI позволяет упростить управление безопасностью путём автоматизации, усилить режим безопасности благодаря значительной сложности компрометации цифровых сертификатов, усовершенствовать и интегрировать управление защитой, усилить контроль защищенного доступа к бизнес-ресурсам.

PKI представляет собой иерархическую архитектуру управления атрибутами безопасности пользователей, участвующих в защищённом обмене информацией. Помимо живых людей в PKI также могут участвовать элементы инфраструктуры сети – межсетевые экраны, концентраторы виртуальных частных сетей, маршрутизаторы, защищенные серверы приложений и другие программно-аппаратные комплексы, нуждающиеся в проверке подлинности и шифровании.

Каждый субъект PKI имеет цифровой сертификат, эмитируемый, отзываемый и подписанный органом сертификации. Сертификат представляет собой упорядоченную структуру данных, связывающую общий ключ с его обладателем, и содержит набор элементов, используемых субъектами при установлении защищённых соединений.

2.3 ПРОТОКОЛЫ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ СЕТЕЙ

Существует множество технологий безопасности, и все они предлагают решения для важнейших компонентов политики в области защиты данных: аутентификации, поддержания целостности данных и активной проверки. Мы определяем аутентификацию как аутентификацию пользователя или конечного устройства (клиента, сервера, коммутатора, маршрутизатора, межсетевого экрана и т.д.) и его местоположения с последующей авторизацией пользователей и конечных устройств.

Целостность данных включает такие области, как безопасность сетевой инфраструктуры, безопасность периметра и конфиденциальность данных. Активная проверка помогает удостовериться в том, что установленная политика в области безопасности выдерживается на практике, и отследить все аномальные случаи и попытки несанкционированного доступа.

2.3.1 МЕХАНИЗМ ШИФРОВАНИЯ WEP

Шифрование WEP (Wired Equivalent Privacy, секретность на уровне проводной связи) основано на алгоритме RC4 (Rivest's Cipher v.4, код Ривеста), представляющем собой симметричное потоковое шифрование. Как было отмечено ранее, для нормального обмена пользовательскими данными ключи шифрования у абонента и точки радиодоступа должны быть идентичными.

Ядро алгоритма состоит из функции генерации ключевого потока. Эта функция генерирует последовательность битов, которая затем объединяется с открытым текстом посредством суммирования по модулю два. Дешифрация состоит из регенерации этого ключевого потока и суммирования его с шифрограммой по модулю два, восстанавливая исходный текст. Другая главная часть алгоритма — функция инициализации, которая использует ключ переменной длины для создания начального состояния генератора ключевого потока.

RC4 – фактически класс алгоритмов, определяемых размером его блока. Этот параметр n является размером слова для алгоритма. Обычно, n = 8, но в целях анализа можно уменьшить его. Однако для повышения безопасности необходимо увеличить эту величину. Внутреннее состояние RC4 состоит из массива размером 2n слов и двух счетчиков, каждый размером в одно слово. Массив известен как S-бокс, и далее будет обозначаться как S. Он всегда содержит перестановку 2n возможных значений слова. Два счетчика обозначены через i и j.

Алгоритм инициализации RC4 приведен ниже.

Этот алгоритм использует ключ, сохраненный в Key, и имеющий длину l байт. Инициализация начинается с заполнения массива S, далее этот массив перемешивается путем перестановок определяемых ключом. Так как только одно действие выполняется над S, то должно выполняться утверждение, что S всегда содержит все значения кодового слова.

1) Начальное заполнение массива:

```
for i = 0 to 2n – 1
    {
        S[i] = i
        j = 0
    }
```

2) Скремблирование:

```
for i = 0 to 2n − 1
{
    j = j + S[i] + Key[i mod l]
    Перестановка (S[i], S[j])
}
```

Генератор ключевого потока RC4 переставляет значения, хранящиеся в S, и каждый раз выбирает различное значение из S в качестве результата. В одном цикле RC4 определяется одно n-битное слово K из ключевого потока, которое в последующем суммируется с исходным текстом для получения зашифрованного текста.

3) Инициализация:
   i = 0
   j = 0
4) Цикл генерации:
   i = i + 1
   j = j + S[i]
   Перестановка (S[i], S[j])
   Результат: K = S[S[i] + S[j]].

Особенности WEP-протокола:

- Достаточно устойчив к атакам, связанным с простым перебором ключей шифрования, что обеспечивается необходимой длиной ключа и частотой смены ключей и инициализирующего вектора;
- Самосинхронизация для каждого сообщения. Это свойство является ключевым для протоколов уровня доступа к среде передачи, где высок уровень искажённых и потерянных пакетов;
- Эффективность: WEP может быть легко реализован;
- Открытость;
- Использование WEP-шифрования не является обязательным в сетях стандарта IEEE 802.11.

Для непрерывного шифрования потока данных используется *потоковое* и *блочное* шифрование.

Потоковое шифрование

При потоковом шифровании выполняется побитовое сложение по модулю 2 (функция “исключающее ИЛИ“, XOR) ключевой последовательности, генерируемой алгоритмом шифрования на основе заранее заданного ключа, и исходного сообщения. Ключевая последовательность имеет длину, соответствующую длине исходного сообщения, подлежащего шифрованию (рис. 2.10).

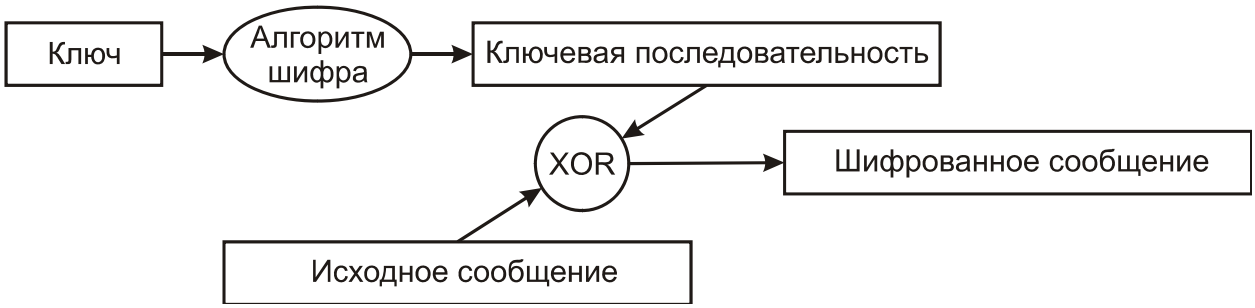


Рис. 2.10 Потоковое шифрование

Блочное шифрование

Блочное шифрование работает с блоками заранее определенной длины, не меняющейся в процессе шифрования. Исходное сообщение фрагментируется на блоки, и функция XOR вычисляется над ключевой последовательностью и каждым блоком. Размер

блока фиксирован, а последний фрагмент исходного сообщения дополняется пустыми символами до длины нормального блока (рис. 2.11). Например, при блочном шифровании с 16-байтовыми блоками исходное сообщение длиной в 38 байтов фрагментируется на два блока длиной по 16 байтов и 1 блок длиной 6 байтов, который затем дополняется 10 байтами пустых символов до длины нормального блока.

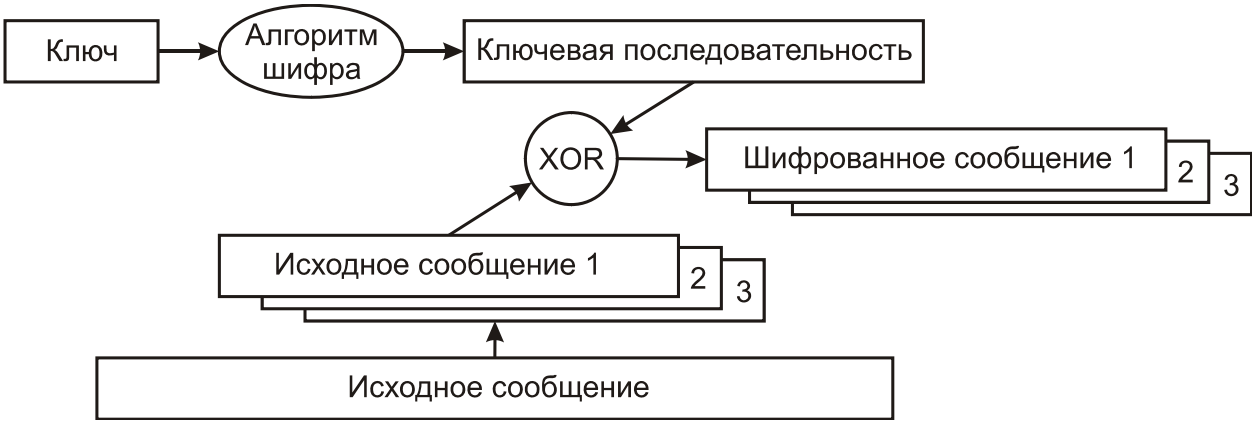


Рис. 2.11 Блочное шифрование

Потоковое шифрование и блочное шифрование используют метод электронной кодовой книги (ECB). Метод ECB характеризуется тем, что одно и то же исходное сообщение на входе всегда порождает одно и то же зашифрованное сообщение на выходе. Это представляет собой потенциальную брешь в системе безопасности, ибо сторонний наблюдатель, обнаружив повторяющиеся последовательности в зашифрованном сообщении, в состоянии сделать обоснованные предположения относительно идентичности содержания исходного сообщения.

Для устранения указанной проблемы используют:

1) Векторы инициализации (Initialization Vectors, IVs)
2) Обратную связь (feedback modes)

До начала процесса шифрования 40- или 104-битный секретный ключ распределяется между всеми станциями, входящими в беспроводную сеть. К секретному ключу добавляется вектор инициализации (IV).

Вектор инициализации (Initialization Vector, IV)

Вектор инициализации используется для модификации ключевой последовательности. При использовании вектора инициализации ключевая последовательность генерируется алгоритмом шифрования, на вход которого подаётся секретный ключ, совмещённый с IV. При изменении вектора инициализации ключевая последовательность также меняется. На рисунке 2.12 исходное сообщение шифруется с использованием новой ключевой последовательности, сгенерированной алгоритмом шифрования после подачи на его вход комбинации из секретного ключа и вектора инициализации, что порождает на выходе шифрованное сообщение.

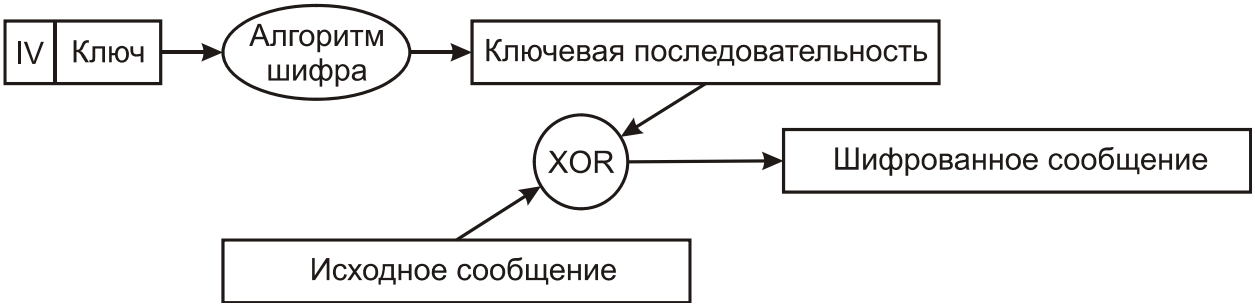


Рис. 2.12 Алгоритм шифрования WEP

Стандарт IEEE 802.11 рекомендует использование нового значения вектора инициализации для каждого нового фрейма, передаваемого в радиоканал. Таким образом, один и тот же нешифрованный фрейм, передаваемый многократно, каждый раз будет порождать уникальный шифрованный фрейм.

Вектор инициализации имеет длину 24 бита и совмещается с 40- или 104-битовым базовым ключом шифрования WEP, таким образом, что на вход алгоритма шифрования подается 64- или 128-битовый ключ. Вектор инициализации присутствует в нешифрованном виде в заголовке фрейма в радиоканале, с тем, чтобы принимающая сторона могла успешно декодировать этот фрейм. Несмотря на то, что обычно говорят об использовании шифрования WEP с ключами длиной 64 или 128 битов, эффективная длина ключа составляет лишь 40 или 104 бита по причине передачи вектора инициализации в нешифрованном виде. При настройках шифрования в оборудовании при 40-битном эффективном ключе вводятся 5 байтовых ASCII-символов (5·8=40) или 10 шестнадцатеричных чисел (10·4=40), и при 104-битном эффективном ключе вводятся 13 байтовых ASCII-символов (13·8=104) или 26 шестнадцатеричных чисел (26·4=104). Некоторое оборудование может работать со 128-битным ключом.

Обратная связь

Обратная связь модифицируют процесс шифрования и предотвращают порождение одним и тем же исходным сообщением одного и того же шифрованного сообщения. Обратная связь обычно используется при блочном шифровании. Наиболее часто встречается тип обратной связи, известный как цепочка шифрованных блоков (CBC).

В основе использования цепочки шифрованных блоков лежит идея вычисления двоичной функции XOR между блоком исходного сообщения и предшествовавшим ему блоком шифрованного сообщением. Поскольку самый первый блок не имеет предшественника, для модификации ключевой последовательности используют вектор инициализации. Работу цепочки шифрованных блоков иллюстрирует рис. 2.13.

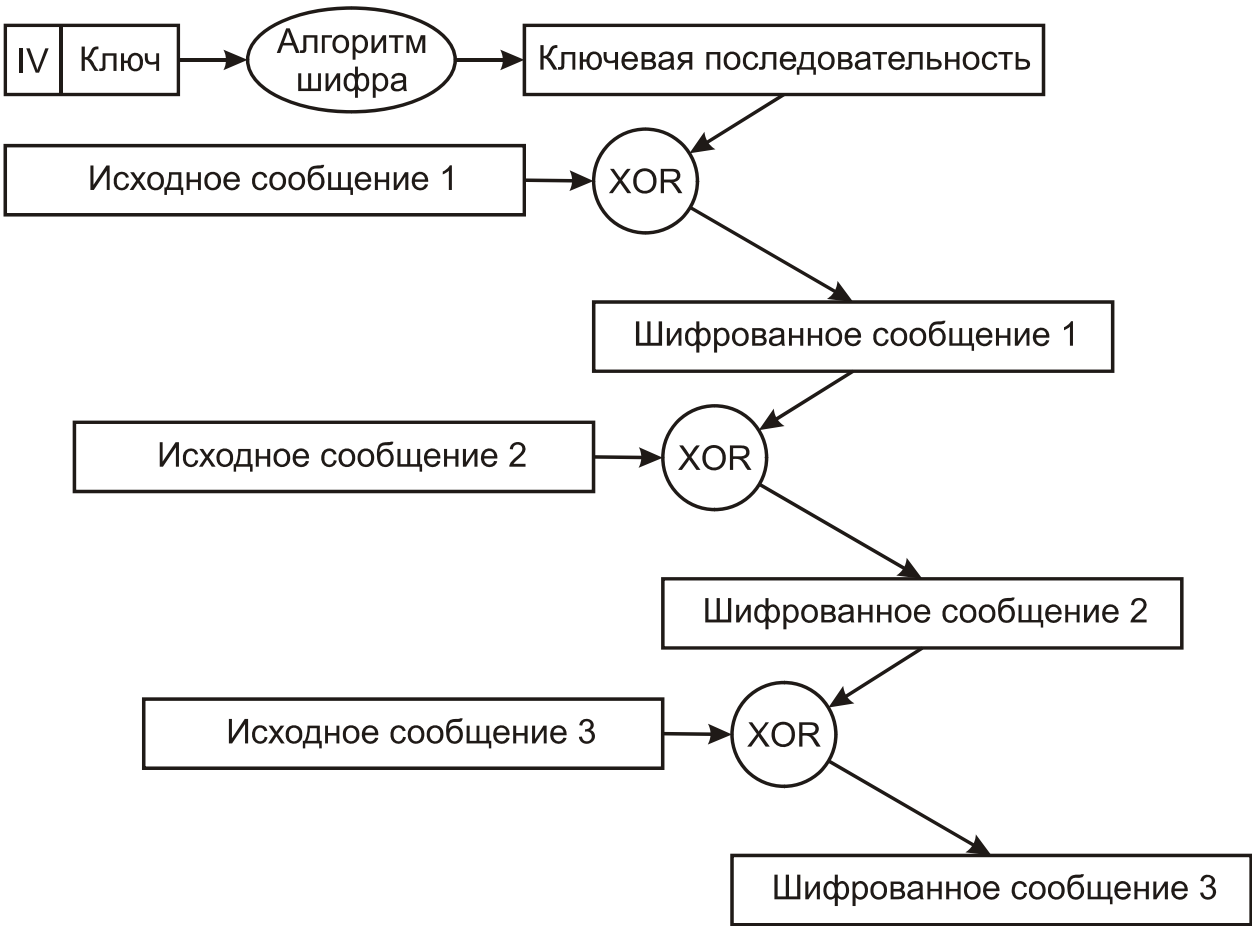


Рис. 2.13 Шифрование с обратной связью

2.3.2 УЯЗВИМОСТЬ ШИФРОВАНИЯ WEP

Атаки на зашифрованные данные с помощью технологии WEP можно подразделить на два метода: *пассивные* и *активные*.

Пассивные сетевые атаки

В августе 2001 года криптоаналитики Флурер С., Мантин И. и Шамир А. (Fluhrer S., Mantin I., Shamir A.) установили, что секретный ключ шифрования WEP может быть вычислен с использованием определенных фреймов, пассивно собранных в беспроводной локальной сети. Причиной уязвимости послужила реализация в WEP метода планирования ключей (Key Scheduling Algorithm, KSA) алгоритма потокового шифрования RC4. Некоторые векторы инициализации (так называемые «слабые» векторы) дают возможность установить побайтовый состав секретного ключа, применяя статистический анализ.

Исследователями из AT&T/Rice University и авторами программы AirSnort была продемонстрирована возможность определения секретного ключа длиной 40 и 104 битов после анализа всего лишь 4 миллионов фреймов. Для загруженной беспроводной локальной сети это эквивалентно приблизительно 4 часам работы, после чего ключ шифрования станет известен пассивному наблюдателю.

Подобная уязвимость делает шифрование с использованием WEP неэффективным, лишая его криптографической стойкости. Использование динамических секретных

ключей шифрования WEP решает проблему лишь частично, для полного устранения уязвимости требуется способ усиления самого ключа.

Активные сетевые атаки

Индуктивное вычисление секретного ключа шифрования WEP представляет собой процесс воздействия на беспроводную локальную сеть для получения определённой информации и относится к классу активных сетевых атак. Как было сказано ранее, при потоковом шифровании выполняется двоичное сложение по модулю 2 (XOR) исходного сообщения с ключевой последовательностью с целью получения шифрованного сообщения. Этот факт лёг основу данной атаки.

Высокая эффективность атаки индуктивного вычисления ключа, предпринимаемой сторонним наблюдателем в беспроводной локальной сети IEEE 802.11, объясняется отсутствием действенных средств контроля целостности сообщений (Message Intgrity Check, MIC). Принимающая сторона не в состоянии распознать факт модификации содержимого фрейма в процессе передачи по общедоступному радиоканалу. Более того, значение ICV (Integrity Check Value), предусмотренное стандартом для контроля целостности сообщений, вычисляется с помощью функции CRC32 (32-bit Cyclical Redundancy Check, контроль с помощью циклического 32-битного избыточного кода), которая подвержена атакам с манипуляцией битами. Таким образом, в отсутствии механизмов контроля целостности сообщений беспроводные локальные сети подвержены активным атакам: *повторным использованием вектора инициализации* (IV Replay) и *манипуляции битами* (Bit-Flipping).

1) Повторное использование вектора инициализации (Initialization Vector Replay Attacks)

Повторное использование вектора инициализации представляет собой разработанную теоретически и реализованную практически активную сетевую атаку в беспроводной локальной сети, существующую в нескольких разновидностях, одна из которых описана ниже и проиллюстрирована на рис. 2.14.

Рис. 2.14 Повторное использование вектора инициализации

1. Хакер многократно отправляет абоненту беспроводной локальной сети по проводной сети сообщение известного содержания (например, IP-пакет, письмо электронной почты, и т.п.).
2. Хакер пассивно прослушивает радиоканал связи абонента с точкой радиодоступа и собирает фреймы, предположительно содержащие шифрованное сообщение.
3. Хакер вычисляет ключевую последовательность, применяя функцию XOR к предполагаемому шифрованному и известному нешифрованному сообщениям.
4. Хакер «выращивает» ключевую последовательность для пары вектора инициализации и секретного ключа, породившей ключевую последовательность, вычисленную на предыдущем шаге.

В основе атаки лежит знание того, что пара вектора инициализации и секретного ключа шифрования, а значит и порождаемая ими ключевая последовательность, может быть повторно использована для воссоздания ключевой последовательности достаточной длины для нарушения конфиденциальности в беспроводной локальной сети в условиях использования шифрования WEP.

После того, как ключевая последовательность вычислена для фреймов некоторой длины, она может быть «выращена» до любого требуемого размера, как описано ниже и проиллюстрировано на рис. 2.15.

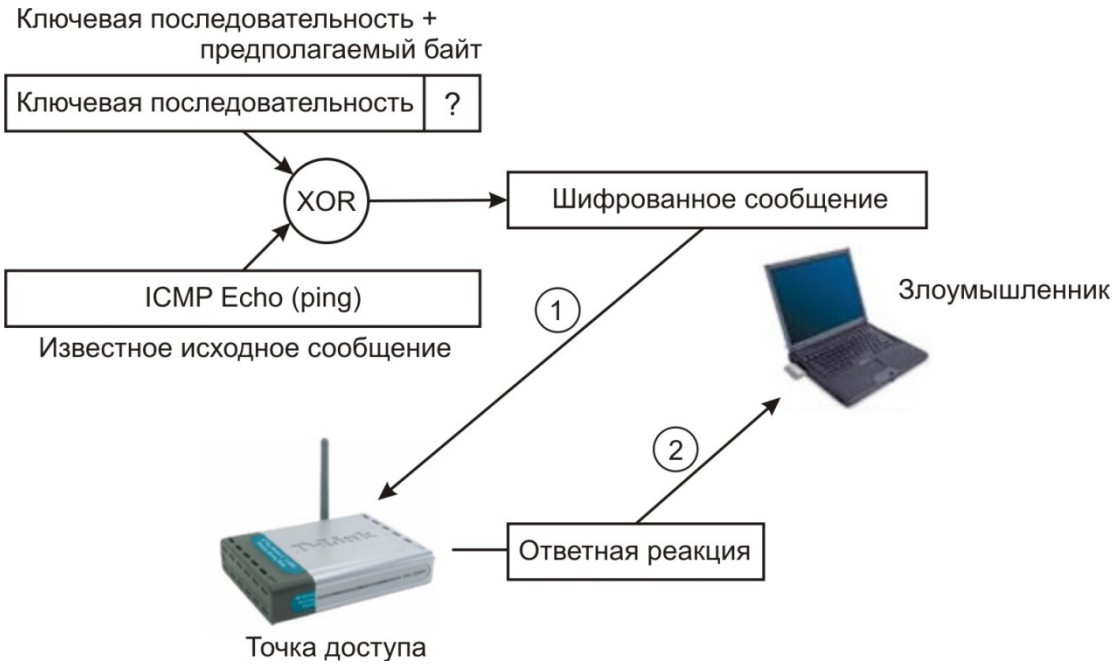


Рис. 2.15 «Выращивание» ключевой последовательности

1. Хакер создает фрейм на один байт длиннее, чем длина уже известной ключевой последовательности. Пакеты ICMP (Internet Control Message Protocol, протокол управляющих сообщений сети Интернет), посылаемые командой ping, идеальны для этих целей, ибо точка радиодоступа вынуждена на них отвечать.
2. Хакер увеличивает длину ключевой последовательности на один байт.
3. Значение дополнительного байта выбирается случайным образом из 256 возможных ASCII-символов.
4. Если предполагаемое значение дополнительного байта ключевой последовательности верно, то будет получен ожидаемый ответ от точки радиодоступа, в данном примере это ICMP.
5. Процесс повторяется до тех пор, пока не будет подобрана ключевая последовательность требуемой длины.

2) Манипуляция битами (Bit-Flipping Attacks)

Манипуляция битами преследует ту же цель, что и повторное использование вектора инициализации, и опирается на уязвимость вектора контроля целостности фрейма ICV. Пользовательские данные могут различаться от фрейма к фрейму, в то же самое время многие служебные поля и их положение внутри фрейма остаются неизменными.

Хакер манипулирует битами пользовательских данных внутри фрейма 2-го (канального) уровня модели OSI (Open Systems Interconnection) с целью искажения 3-го (сетевого) уровня пакета. Процесс манипуляции проиллюстрирован на рис. 2.16.

1. Хакер пассивно наблюдает фреймы беспроводной локальной сети с помощью средств анализа трафика протокола 802.11.
2. Хакер захватывает фрейм и произвольно изменяет биты в поле данных протокола 3-го уровня.
3. Хакер модифицирует значение вектора контроля целостности фрейма ICV (как именно будет описано ниже).
4. Хакер передаёт модифицированный фрейм в беспроводную локальную сеть.
5. Принимающая сторона (абонент либо точка радиодоступа) вычисляет значение вектора контроля целостности фрейма ICV для полученного модифицированного фрейма.

6. Принимающая сторона сравнивает вычисленное значение вектора ICV с имеющимся в полученном модифицированном фрейме.
7. Значения векторов совпадают, фрейм считается неискажённым и не отбрасывается.
8. Принимающая сторона деинкапсулирует содержимое фрейма и обрабатывает пакет сетевого уровня.
9. Поскольку манипуляция битами происходила на канальном уровне, контрольная сумма пакета сетевого уровня оказывается неверной.
10. Стек протокола сетевого уровня на принимающей стороне генерирует предсказуемое сообщение об ошибке.
11. Хакер наблюдает за беспроводной локальной сетью в ожидании зашифрованного фрейма с сообщением об ошибке.
12. Хакер захватывает фрейм, содержащий зашифрованное сообщение об ошибке и вычисляет ключевую последовательность, как это было описано ранее для атаки с повторным использованием вектора инициализации.

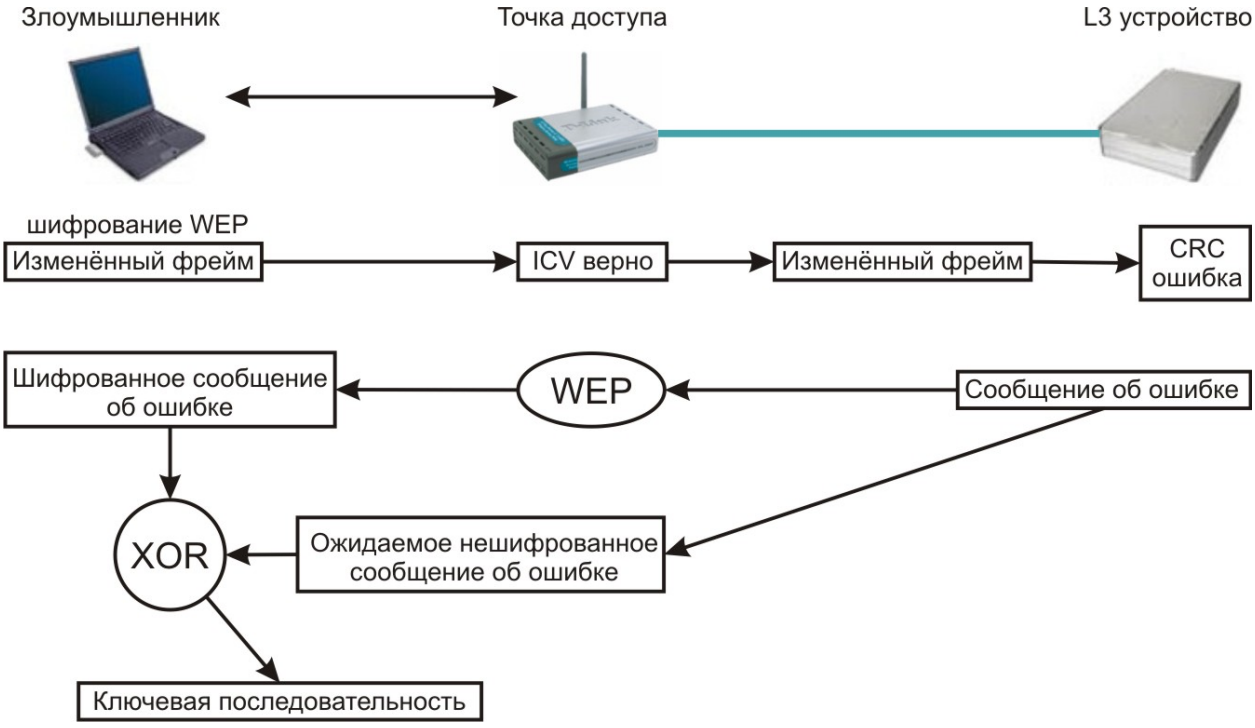


Рис. 2.16 Атака с манипуляцией битами

Вектор ICV находится в шифрованной части фрейма. С помощью следующей процедуры хакер манипулирует битами шифрованного вектора ICV и таким образом обеспечивает корректность самого вектора для нового, модифицированного фрейма (рис. 2.17):

1. Исходный фрейм F1 имеет вектор C1.
2. Создаётся фрейм F2 такой же длины, что и F1, служащий маской для модификации битов фрейма F1.
3. Создаётся фрейм F3 путём выполнения двоичной функции XOR над фреймами F1 и F2.
4. Вычисляется промежуточный вектор C2 для фрейма F3.
5. Вектор C3 для фрейма F3 вычисляется путём выполнения двоичной функции XOR над C1 и C2.

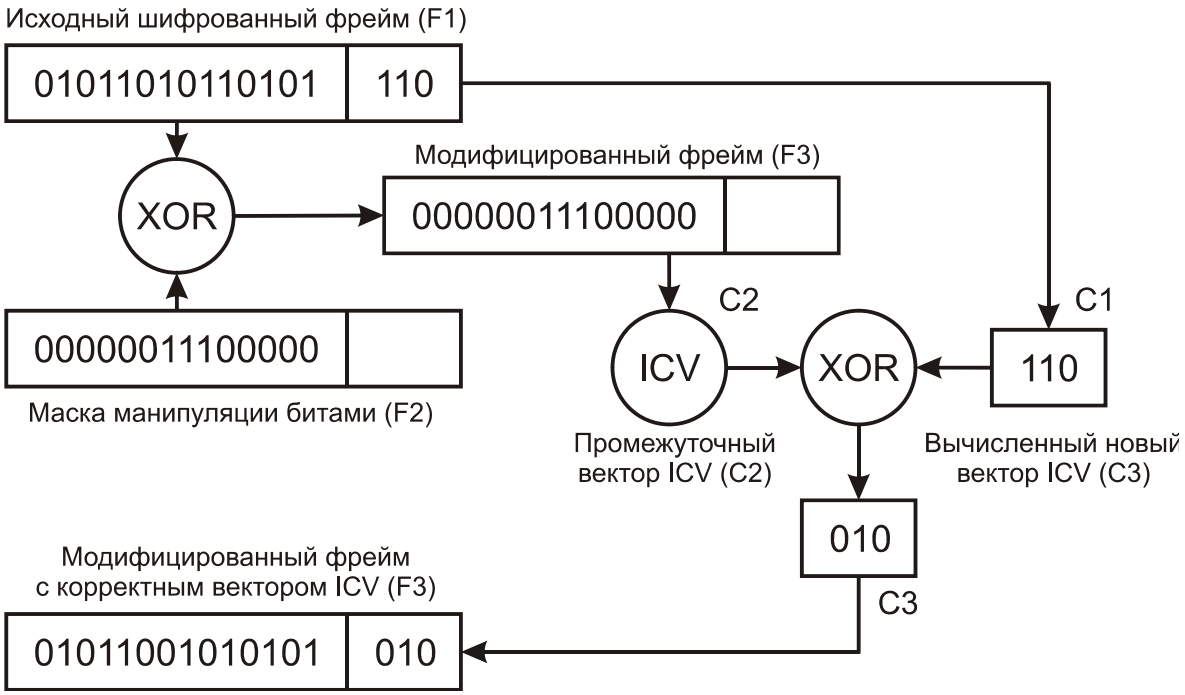


Рис. 2.17 Вычисление поля контроля целостности сообщений

Проблемы управления статическими WEP ключами

Стандартом IEEE 802.11 не предусмотрены какие либо механизмы управления ключами шифрования. По определению, алгоритм WEP поддерживает лишь статические ключи, которые заранее распространяются тем или иным способом между абонентами и точками радиодоступа беспроводной локальной сети. Поскольку IEEE 802.11 аутентифицирует физическое устройство, а не его пользователя, утрата абонентского адаптера, точки радиодоступа или собственно секретного ключа представляют опасность для системы безопасности беспроводной локальной сети. В результате при каждом подобном инциденте администратор сети будет вынужден вручную произвести смену ключей у всех абонентов и в точках доступа. Для этого во всём оборудовании D-Link отведено четыре поля для ввода ключей. И при смене всех ключей необходимо только поменять номер используемого ключа.

Эти административные действия приемлемы для небольшой беспроводной локальной сети, но совершенно неприемлемы для сетей, в которых абоненты исчисляются сотнями и тысячами, и/или распределены территориально. В условиях отсутствия механизмов генерации и распространения ключей администратор вынужден пристально охранять абонентские адаптеры и оборудование инфраструктуры сети.

2.4 АУТЕНТИФИКАЦИЯ В БЕСПРОВОДНЫХ СЕТЯХ

Основными стандартами аутентификации в беспроводных сетях являются стандарты IEEE 802.11, WPA, WPA2 и 802.1x.

Рассмотрим основы этих стандартов.

2.4.1 СТАНДАРТ IEEE 802.11 СЕТИ С ТРАДИЦИОННОЙ БЕЗОПАСНОСТЬЮ

Стандарт IEEE 802.11 с традиционной безопасностью (Tradition Security Network, TSN) предусматривает два механизма аутентификации беспроводных абонентов: *открытую аутентификацию* (Open Authentication) и *аутентификацию с общим ключом*

(Shared Key Authentication). В аутентификации в беспроводных сетях также широко используются два других механизма выходящих за рамки стандарта 802.11, а именно назначение *идентификатора беспроводной локальной сети* (Service Set Identifier, SSID) и *аутентификация абонента по его MAC-адресу* (MAC Address Authentication).

Идентификатор беспроводной локальной сети (SSID) представляет собой атрибут беспроводной сети, позволяющий логически отличать сети друг от друга. В общем случае, абонент беспроводной сети должен задать у себя соответствующий SSID для того, чтобы получить доступ к требуемой беспроводной локальной сети. SSID ни в коей мере не обеспечивает конфиденциальность данных, равно как и не аутентифицирует абонента по отношению к точке радиодоступа беспроводной локальной сети. Существуют точки доступа позволяющие разделить абонентов подключаемых к точке на несколько сегментов, это достигается тем, что точка доступа может иметь не один, а несколько SSID.

Принцип аутентификации абонента в IEEE 802.11

Аутентификация в стандарте IEEE 802.11 ориентирована на аутентификацию абонентского устройства радиодоступа, а не конкретного абонента как пользователя сетевых ресурсов. Процесс аутентификации абонента беспроводной локальной сети IEEE 802.11 состоит из следующих этапов (рис. 2.18):

1. Абонент (Client) посылает фрейм Probe Request во все радиоканалы.
2. Каждая точка радиодоступа (Access Point, AP), в зоне радиовидимости которой находится абонент, посылает в ответ фрейм Probe Response.
3. Абонент выбирает предпочтительную для него точку радиодоступа и посылает в обслуживаемый ею радиоканал запрос на аутентификацию (Authentication Request).
4. Точка радиодоступа посылает подтверждение аутентификации (Authentication Reply).
5. В случае успешной аутентификации абонент посылает точке радиодоступа фрейм ассоциации (Association Request).
6. Точка радиодоступа посылает в ответ фрейм подтверждения ассоциации (Association Response).
7. Абонент может теперь осуществлять обмен пользовательским трафиком с точкой радиодоступа и проводной сетью.

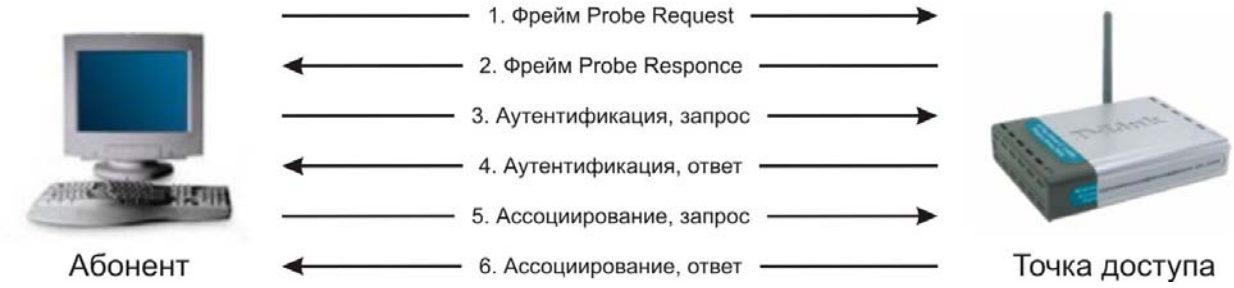


Рис. 2.18 Аутентификация по стандарту 802.11

При активизации, беспроводный абонент начинает поиск точек радиодоступа в своей зоне радиовидимости с помощью управляющих фреймов Probe Request. Фреймы Probe Request посылаются в каждый из радиоканалов, поддерживаемых абонентским радиоинтерфейсом, в попытке найти все точки радиодоступа с требуемыми клиенту идентификатором SSID и поддерживаемыми скоростями радиообмена. Каждая точка радиодоступа из находящихся в зоне радиовидимости абонента и удовлетворяющая запрашиваемым во фрейме Probe Request параметрам отвечает фреймом Probe Response,

содержащем синхронизирующую информацию и данные о текущей загрузке точки радиодоступа. Абонент определяет, с какой точкой радиодоступа он будет работать, путем сопоставления поддерживаемых ими скоростей радиообмена и загрузки. После того, как предпочтительная точка радиодоступа определена, абонент переходит в фазу аутентификации.

Открытая аутентификация

Открытая аутентификация, по сути, не является алгоритмом аутентификации в привычном понимании. Точка радиодоступа удовлетворит любой запрос открытой аутентификации. На первый взгляд, использование этого алгоритма может показаться бессмысленным, однако следует учитывать, что разработанные в 1997 году методы аутентификации IEEE 802.11 ориентированы на быстрое логическое подключение к беспроводной локальной сети. Вдобавок к этому, многие IEEE 802.11-совместимые устройства представляют собой портативные блоки сбора информации (сканеры штрих-кодов и т. п.), не имеющие достаточной процессорной мощности, требующейся для реализации сложных алгоритмов аутентификации.

В процессе открытой аутентификации происходит обмен сообщениями двух типов:

- запрос аутентификации (Authentication Request);
- подтверждение аутентификации (Authentication Response).

Таким образом, при открытой аутентификации возможен доступ любого абонента к беспроводной локальной сети. Если в беспроводной сети не используется шифрование, то любой абонент, знающий идентификатор SSID точки радиодоступа, получит доступ к сети. При использовании точками радиодоступа шифрования WEP сами ключи шифрования становятся средством контроля доступа. Если абонент не располагает корректным WEP-ключом, то даже в случае успешной аутентификации он не сможет ни передавать данные через точку радиодоступа, ни расшифровывать данные, переданные точкой радиодоступа (рис. 2.19).

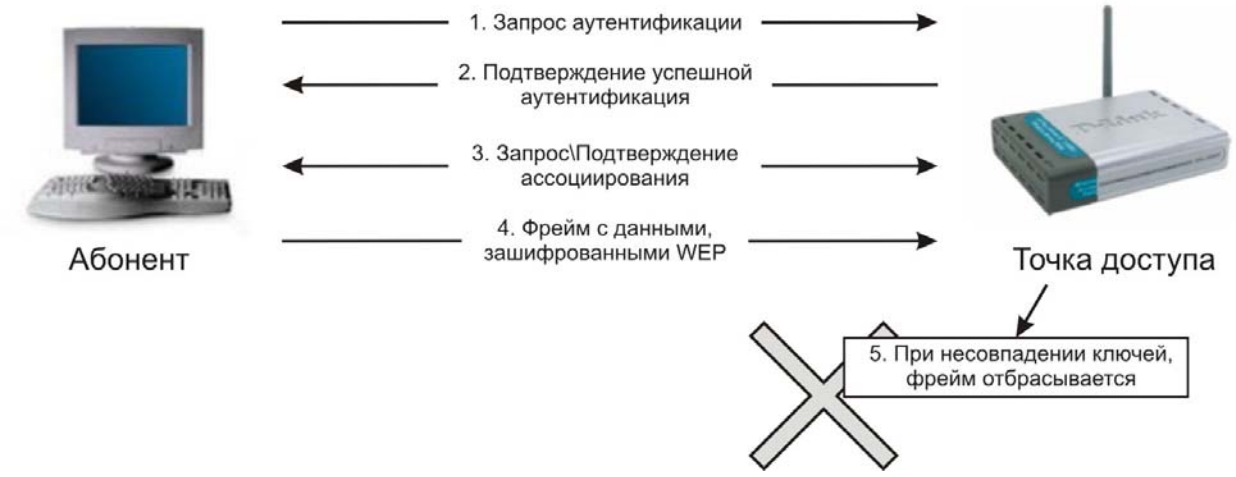


Рис. 2.19 Открытая аутентификация

Аутентификация с общим ключом

Аутентификация с общим ключом является вторым методом аутентификации стандарта IEEE 802.11. Аутентификация с общим ключом требует настройки у абонента статического ключа шифрования WEP. Процесс аутентификации иллюстрирует рис. 2.20:

1. Абонент посылает точке радиодоступа запрос аутентификации, указывая при этом необходимость использования режима аутентификации с общим ключом.

2. Точка радиодоступа посылает подтверждение аутентификации, содержащее Challenge Text.
3. Абонент шифрует Challenge Text своим статическим WEP-ключом, и посылает точке радиодоступа запрос аутентификации.
4. Если точка радиодоступа в состоянии успешно расшифровать запрос аутентификации и содержащийся в нем Challenge Text, она посылает абоненту подтверждение аутентификации, таким образом предоставляя доступ к сети.

Рис. 2.20 Аутентификация с общим ключом

Аутентификация по MAC-адресу

Аутентификация абонента по его MAC-адресу не предусмотрена стандартом IEEE 802.11, однако поддерживается многими производителями оборудования для беспроводных сетей, в том числе D-Link. При аутентификации по MAC-адресу происходит сравнение MAC-адреса абонента либо с хранящимся локально списком разрешенных адресов легитимных абонентов, либо с помощью внешнего сервера аутентификации (рис. 2.21). Аутентификация по MAC-адресу используется в дополнение к открытой аутентификации и аутентификации с общим ключом стандарта IEEE 802.11 для уменьшения вероятности доступа посторонних абонентов.

Рис. 2.21 Аутентификация с помощью внешнего сервера

Пример 2.1:

Настроим точку доступа на WEP-шифрование.

1. Для этого подключаемся к точке доступа, вводим режим, SSID, канал, как было описано в примере 1.4. Далее в поле Authentication (Аутентификация) ставим Shared Key (с общим ключом) (рис. 2.22).

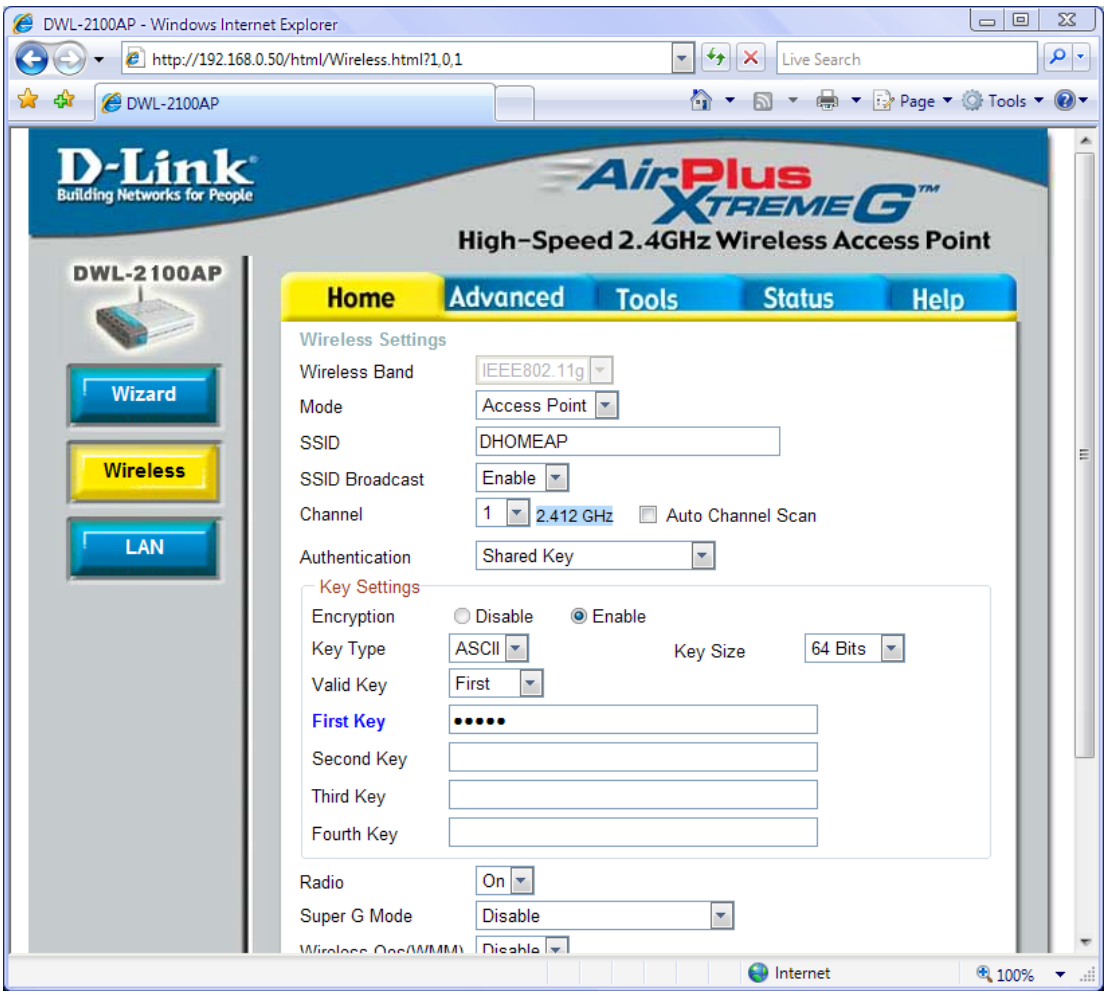


Рис. 2.22

2. Так как аутентификация с общим ключом предполагает ещё и шифрование данных по WEP, то в поле Encryption (Шифрование) активно только будет Enable.

3. Выбираем тип ключа (Key Type) и размер ключа (Key Size).

4. Вводим несколько ключей, последовательно выбирая в поле Valid Key (Действующий ключ). И при 64-битном ключе с типом ключа ASCII нужно ввести 5-значную последовательность, например *pass1*.

Теперь, после применения настроек, на клиентской стороне, надо выставить те же самые параметры, и подключиться к ней.

2.4.2 УЯЗВИМОСТЬ МЕХАНИЗМОВ АУТЕНТИФИКАЦИИ 802.11

Проблемы идентификатора беспроводной ЛВС

Идентификатор SSID регулярно передается точками радиодоступа во специальных фреймах Beacon несмотря на то, что эти фреймы играют чисто информационную роль в радиосети, т. е. совершенно «прозрачны» для абонента, сторонний наблюдатель в состоянии с легкостью определить SSID с помощью анализатора трафика протокола 802.11, например Sniffer Pro Wireless. Некоторые точки радиодоступа, в том числе D-Link, позволяют административно запретить широковещательную передачу SSID внутри фреймов Beacon. Однако и в этом случае SSID можно легко определить путем захвата фреймов Probe Response, посылаемых точками радиодоступа. Идентификатор SSID не разрабатывался для использования в качестве механизма обеспечения безопасности. Вдобавок к этому, отключение широковещательной передачи SSID точками радиодоступа

может серьёзно отразиться на совместимости оборудования беспроводных сетей различных производителей при использовании в одной радиосети.

Уязвимость открытой аутентификации

Открытая аутентификация не позволяет точке радиодоступа определить, является ли абонент легитимным или нет. Это становится серьезной брешью в системе безопасности в том случае, если в беспроводной локальной сети не используется шифрование WEP.

D-Link не рекомендует эксплуатацию беспроводных сетей без шифрования WEP. В случаях, когда использование шифрования WEP не требуется или невозможно (например, в беспроводных локальных сетях публичного доступа), методы аутентификации более высокого уровня могут быть реализованы посредством Интернет-шлюзов.

Уязвимость аутентификации с общим ключом

Аутентификация с общим ключом требует настройки у абонента статического WEP-ключа для шифрования Challenge Text, отправленного точкой радиодоступа. Точка радиодоступа аутентифицирует абонента посредством дешифрования его ответа на Challenge и сравнения его с отправленным оригиналом. Обмен фреймами, содержащими Challenge Text, происходит по открытому радиоканалу, а значит, подвержен атакам со стороны стороннего наблюдателя (Man in the middle Attack). Наблюдатель может принять как нешифрованный Challenge Text, так и тот же Challenge Text, но уже в шифрованном виде (рис. 2.23). Шифрование WEP производится путем выполнения побитовой операции XOR над текстом сообщения и ключевой последовательностью, в результате чего получается зашифрованное сообщение (Cipher-Text). Важно понимать, что выполнение побитовой операции XOR над зашифрованным сообщением и ключевой последовательностью имеет результатом текст исходного сообщения. Таким образом, наблюдатель может легко вычислить сегмент ключевой последовательности путем анализа фреймов в процессе аутентификации абонента.

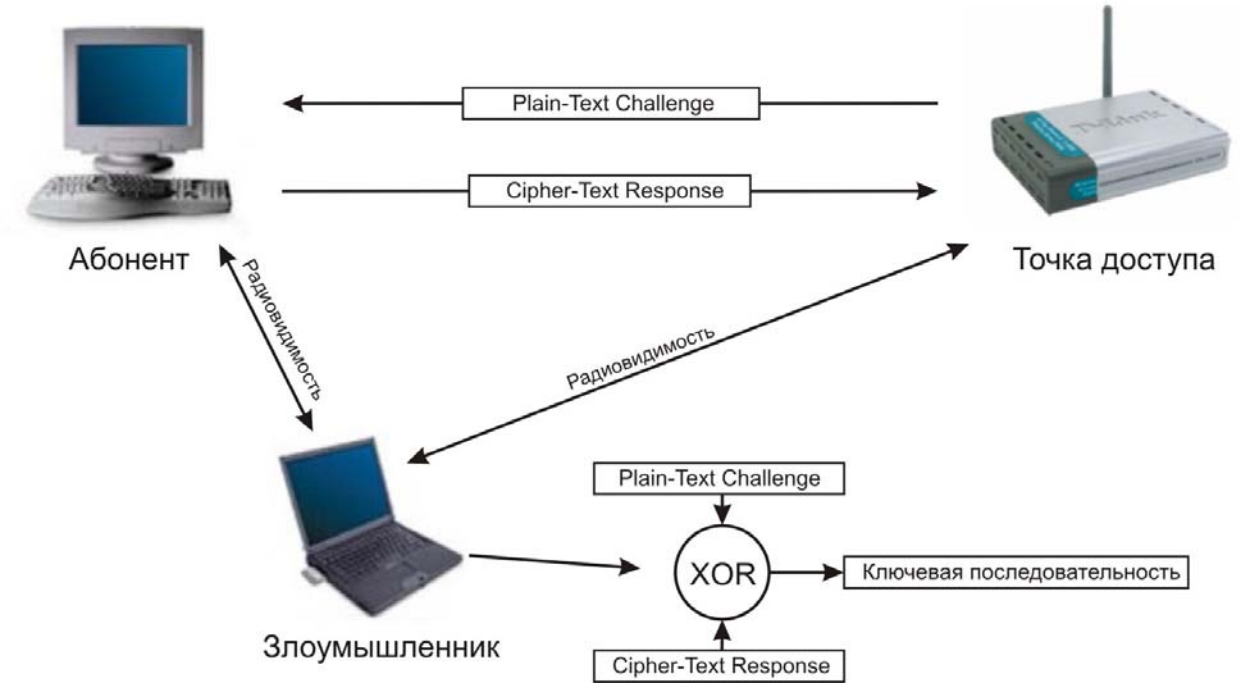


Рис. 2.23 Уязвимость аутентификации с общим ключом

Уязвимость аутентификации по MAC-адресу

Стандарт IEEE 802.11 требует передачи MAC-адресов абонента и точки радиодоступа в открытом виде. В результате этого в беспроводной сети, использующей аутентификацию по MAC-адресу, злоумышленник может обмануть метод аутентификации путём подмены своего MAC-адреса на легитимный. Подмена MAC-адреса возможна в беспроводных адаптерах, допускающих использование локально администрируемых MAC-адресов. Злоумышленник может воспользоваться анализатором трафика протокола IEEE 802.11 для выявления MAC-адресов легитимных абонентов.

2.4.3 СПЕЦИФИКАЦИЯ WPA

До мая 2001 г. стандартизация средств информационной безопасности для беспроводных сетей 802.11 относилась к ведению рабочей группы IEEE 802.11e, но затем эта проблематика была выделена в самостоятельное подразделение. Разработанный стандарт 802.11i призван расширить возможности протокола 802.11, предусмотрев средства шифрования передаваемых данных, а также централизованной аутентификации пользователей и рабочих станций.

Основные производители Wi-Fi-оборудования в лице организации WECA (Wireless Ethernet Compatibility Alliance), иначе именуемой Wi-Fi Alliance, устав ждать ратификации стандарта IEEE 802.11i, совместно с IEEE в ноябре 2002 г. анонсировали спецификацию Wi-Fi Protected Access (WPA), соответствие которой обеспечивает совместимость оборудования различных производителей.

Новый стандарт безопасности WPA обеспечивает уровень безопасности куда больший, чем может предложить WEP. Он перебрасывает мостик между стандартами WEP и 802.11i и имеет то преимущество, что микропрограммное обеспечение более старого оборудования может быть заменено без внесения аппаратных изменений.

IEEE предложила *временный протокол целостности ключа* (Temporal Key Integrity Protocol, TKIP).

Основные усовершенствования, внесенные протоколом TKIP:

- Пофреймовое изменение ключей шифрования. WEP – ключ быстро изменяется, и для каждого фрейма он другой;
- Контроль целостности сообщения. Обеспечивается эффективный контроль целостности фреймов данных с целью предотвращения проведения тайных манипуляций с фреймами и воспроизведения фреймов;
- Усовершенствованный механизм управления ключами.

Пофреймовое изменение ключей шифрования

Атаки, применяемые в WEP, использующие уязвимость слабых IV (Initialization Vectors), таких, которые применяются в приложении AirSnort, основаны на накоплении нескольких фреймов данных, содержащих информацию, зашифрованную с использованием слабых IV. Простейшим способом сдерживания таких атак является изменение WEP-ключа, используемого при обмене фреймами между клиентом и точкой доступа, до того как атакующий успеет накопить фреймы в количестве, достаточном для вывода битов ключа.

IEEE адаптировала схему, известную как пофреймовое изменение ключа (per-frame keying). Основной принцип, на котором основано пофреймовое изменение ключа, состоит в том, что IV, MAC-адрес передатчика и WEP-ключ обрабатываются вместе с помощью двухступенчатой функции перемешивания. Результат применения этой функции соответствует стандартному 104-разрядному WEP-ключу и 24-разрядному IV.

IEEE предложила также увеличить 24-разрядный вектор инициализации до 48-разрядного IV.

На рис. 2.24 представлен образец 48-разрядного IV и показано, как этот IV разбивается на части для использования при пофреймовом изменении ключа.

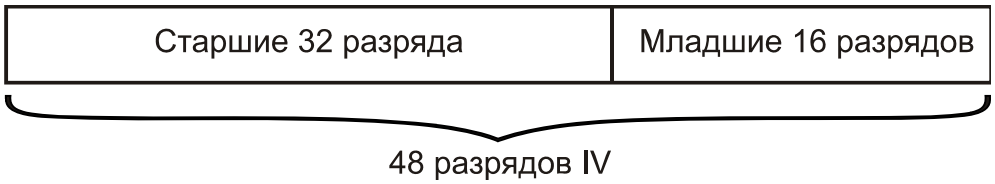


Рис. 2.24 Разбиение 48-и разрядного IV

Процесс пофреймового изменения ключа можно разбить на следующие этапы (рис. 2.25):

1) Базовый WEP-ключ перемешивается со старшими 32 разрядами 48-разрядного IV (32-разрядные числа могут принимать значения 0-4 294 967 295) и MAC-адресом передатчика. Результат этого действия называется *ключ 1-й фазы*. Этот процесс позволяет занести ключ 1-й фазы в кэш и также напрямую поместить в ключ.
2) Ключ 1-й фазы снова перемешивается с IV и MAC-адресом передатчика для выработки значения пофреймового ключа.
3) Вектор инициализации (IV), используемый для передачи фрейма, имеет размер только 16 бит (16-разрядные числа могут принимать значения 0-65 535). Оставшиеся 8 бит (в стандартном 24-битовом IV) представляют фиксированное значение, используемое как заполнитель.
4) Пофреймовый ключ используется для WEP-шифрования фрейма данных.
5) Когда 16-битовое пространство IV оказывается исчерпанным, ключ 1-й фазы отбрасывается и 32 старших разряда увеличиваются на 1.
6) Значение пофреймового ключа вычисляется заново, как на этапе 2.

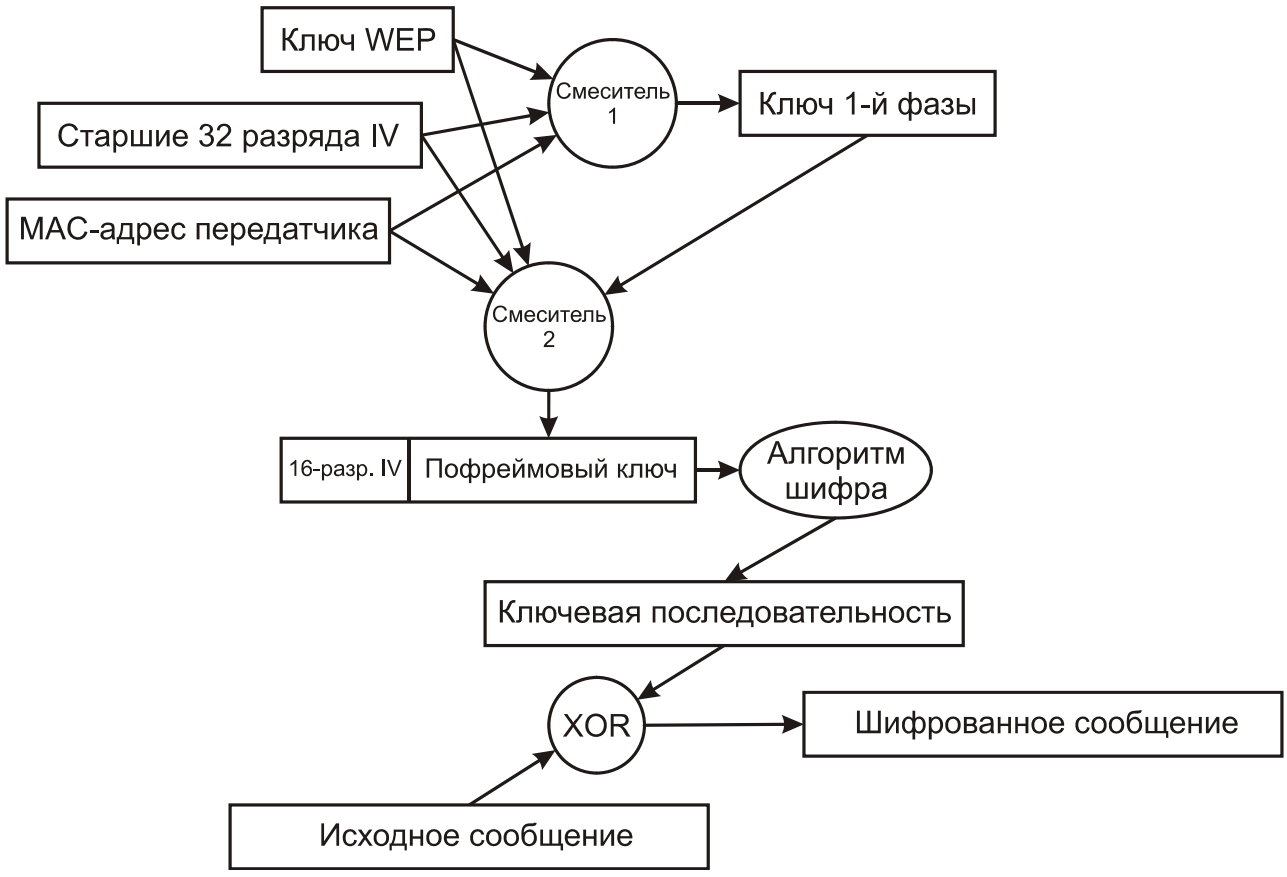


Рис. 2.25 Процесс создания шифрованного сообщения в WPA

Процесс пофреймового изменения ключа можно разбить на следующие этапы.

Устройство инициализирует IV, присваивая ему значение 0. В двоичном представлении это будет значение 00000000000000000000000000000000000000000000000000000000.

Первые 32 разряда IV (в рассматриваемом случае – первые 32 нуля) перемешиваются с WEP-ключом (например, имеющим 128-разрядное значение) и MAC-адресом передатчика (имеющим 48-разрядное значение) для получения значения ключа 1-й фазы (80-разрядное значение).

Ключ 1-й фазы вновь перемешивается с первыми (старшими) 32 разрядами IV и MAC-адресом передатчика, чтобы получить 128-разрядный пофреймовый ключ, первые 16 разрядов которого представляют собой значение IV (16 нулей).

Вектор инициализации пофреймового ключа увеличивается на 1. После того как пофреймовые возможности IV будут исчерпаны, IV 1-й фазы (32 бита) увеличивается на 1 (он теперь будет состоять из 31 нуля и одной единицы, 00000000000000000000000000000001) и т.д.

Этот алгоритм усиливает WEP до такой степени, что почти все известные сейчас возможности атак устраняются без замены существующего оборудования. Следует отметить, что этот алгоритм (и TKIP в целом) разработан с целью убрать бреши в системе аутентификации WEP и стандарта 802.11. Он жертвует слабыми алгоритмами, вместо того чтобы заменять оборудование.

Контроль целостности сообщения

Для усиления малоэффективного механизма, основанного на использовании контрольного признака целостности (ICV) стандарта 802.11, будет применяться контроль целостности сообщения (MIC). Благодаря MIC могут быть ликвидированы слабые места защиты, способствующие проведению атак с использованием поддельных фреймов и манипуляцией битами.. IEEE предложила специальный алгоритм, получивший название Michael (Майкл), чтобы усилить роль ICV в шифровании фреймов данных стандарта 802.11.

MIC имеет уникальный ключ, который отличается от ключа, используемого для шифровании фреймов данных. Этот уникальный ключ перемешивается с назначенным MAC-адресом и исходным MAC-адресом фрейма, а также со всей незашифрованной частью фрейма. На рис. 2.26 показана работа алгоритма Michael MIC.

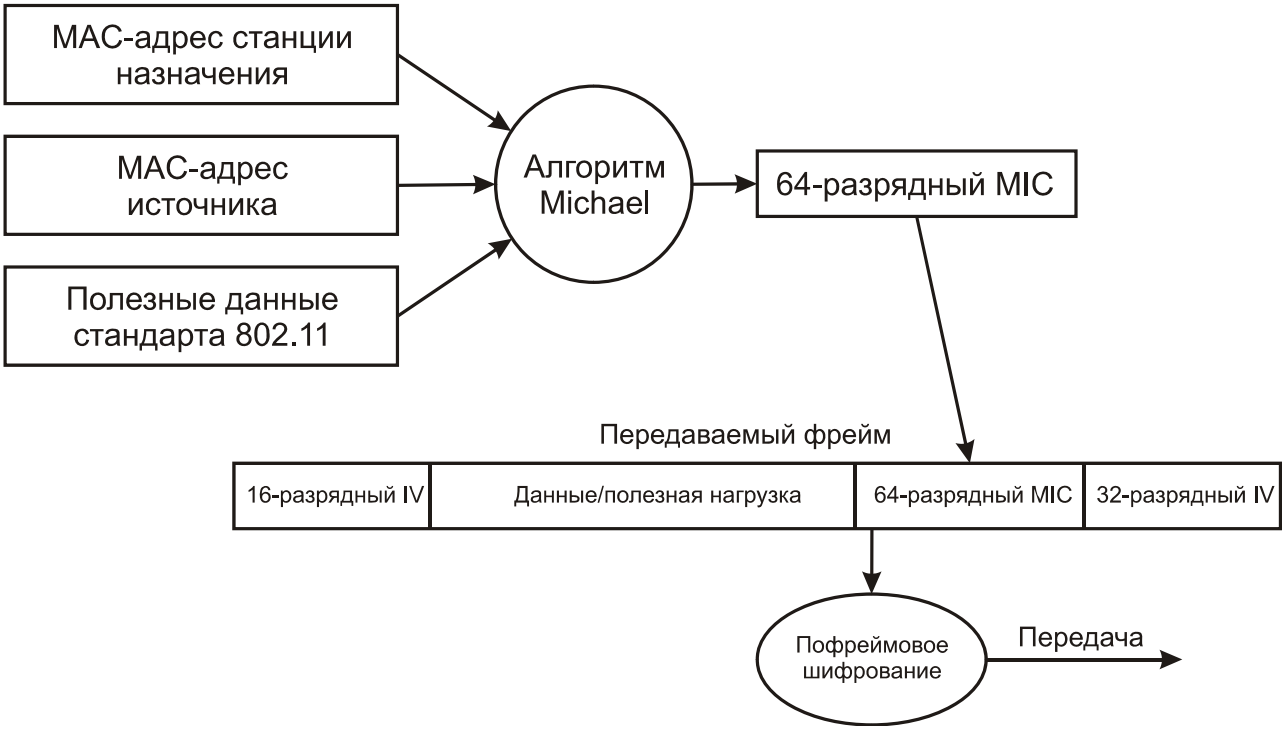


Рис. 2.26

Механизм шифрования TKIP в целом осуществляется следующим образом:

1) С помощью алгоритма пофреймового назначения ключей генерируется пофреймовый ключ (рис. 2.27).
2) Алгоритм MIC генерирует MIC для фрейма в целом.
3) Фрейм фрагментируется в соответствии с установками MAC относительно фрагментации.
4) Фрагменты фрейма шифруются с помощью пофреймового ключа.
5) Осуществляется передача зашифрованных фрагментов.

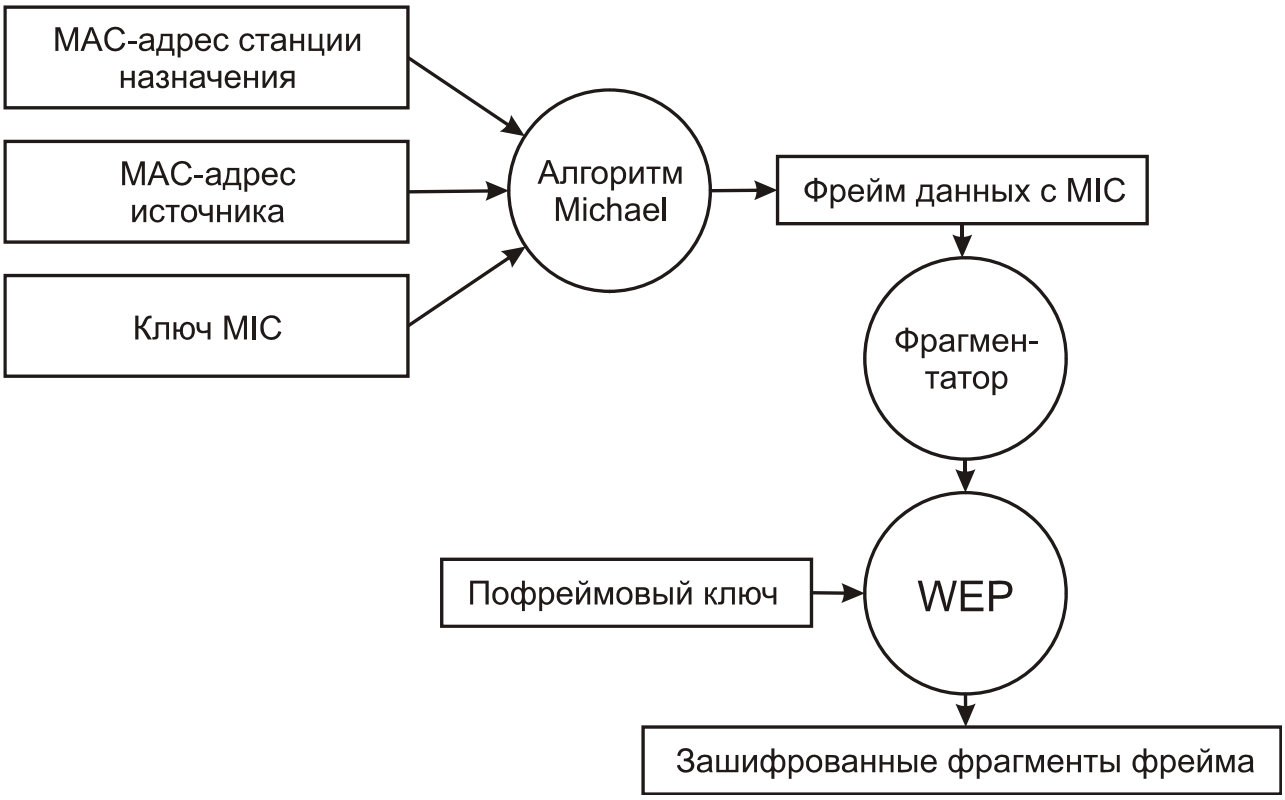


Рис. 2.27 Механизм шифрования TKIP

Аналогично процессу шифрования по алгоритму TKIP, процесс дешифрования по этому алгоритму выполняется следующим образом (рис. 2.28).

1) Предварительно вычисляется ключ 1-й фазы.
2) На основании IV, полученного из входящего фрагмента фрейма WEP, вычисляется пофреймовый ключ 2-й фазы.
3) Если полученный IV не тот, какой нужно, такой фрейм отбрасывается.
4) Фрагмент фрейма расшифровывается и осуществляется проверка признака целостности (ICV).
5) Если контроль признака целостности дает отрицательный результат, такой фрейм отбрасывается.
6) Расшифрованные фрагменты фрейма собираются, чтобы получить исходный фрейм данных.
7) Приемник вычисляет значение MIC и сравнивает его со значением, находящимся в поле MIC фрейма.
8) Если эти значения совпадают, фрейм обрабатывается приемником.
9) Если эти значения не совпадают, значит, фрейм имеет ошибку MIC и приемник принимает меры противодействия MIC.

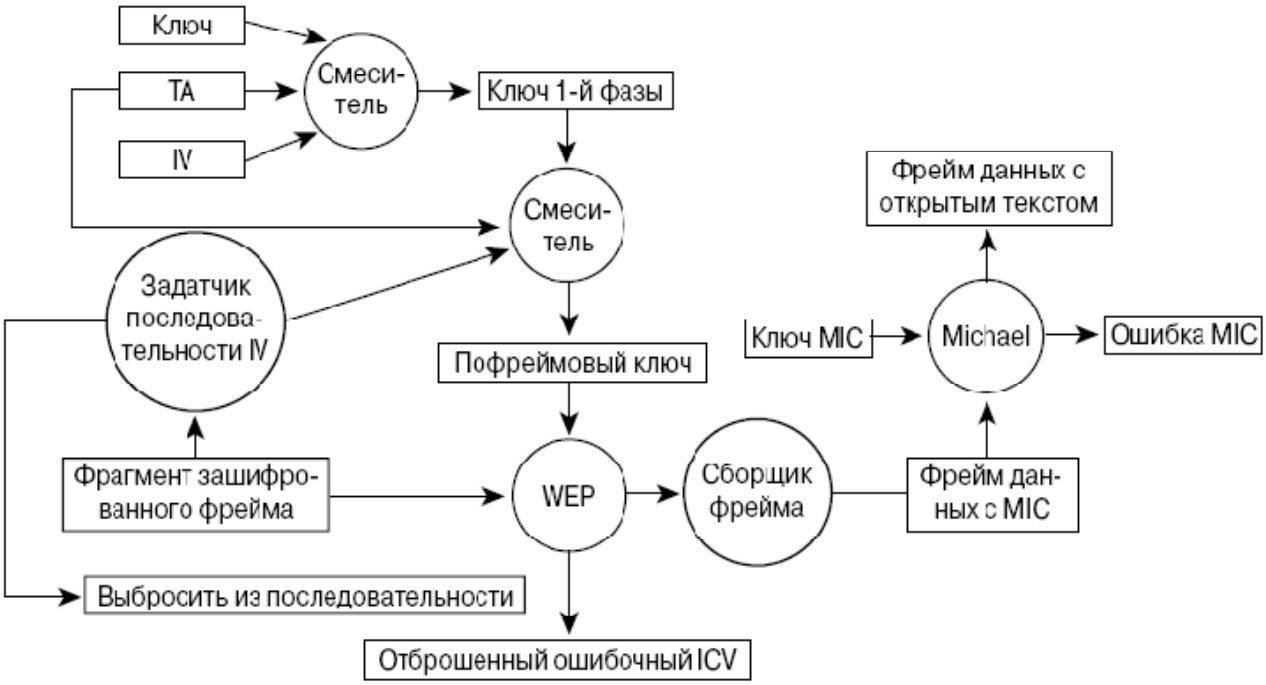


Рис. 2.28 Механизм дешифровки TKIP

Меры противодействия MIC состоят в выполнении приемником следующих задач:

1) Приемник удаляет существующий ключ на ассоциирование.
2) Приемник регистрирует проблему как относящуюся к безопасности сети.
3) Ассоциированный клиент, от которого был получен ложный фрейм, не может быть ассоциирован и аутентифицирован в течение 60 секунд, чтобы замедлить атаку.
4) Клиент запрашивает новый ключ.

WPA может работать в двух режимах: *Enterprise* (корпоративный) и *Pre-Shared Key* (персональный).

В первом случае, хранение базы данных и проверка аутентичности по стандарту 802.1x в больших сетях обычно осуществляются специальным сервером, чаще всего RADIUS (Remote Authentication Dial-In User Service). Enterprise-режим расмотрим далее в отдельной подглаве.

Во втором случае подразумевается применение WPA всеми категориями пользователей беспроводных сетей, т.е. имеет упрощенный режим, не требующий сложных механизмов. Этот режим называется WPA-PSK и предполагает введение одного пароля на каждый узел беспроводной сети (точку доступа, беспроводной маршрутизатор, клиентский адаптер, мост). До тех пор пока пароли совпадают, клиенту будет разрешен доступ в сеть. Можно заметить, что подход с использованием пароля делает WPA-PSK уязвимым для атаки методом подбора, однако этот режим избавляет от путаницы с ключами WEP, заменяя их целостной и четкой системой на основе цифро-буквенного пароля.

Таким образом, WPA/TKIP – это решение, предоставляющее больший по сравнению с WEP уровень безопасности, направленное на устранение слабостей предшественника и обеспечивающее совместимость с более старым оборудованием сетей 802.11 без внесения аппаратных изменений в устройства.

Рассмотрение пофреймового назначения ключей и MIC касалось в основном ключа шифрования и ключа MIC. Но ничего не было сказано о том, как ключи генерируются и пересылаются от клиента к точке доступа и наоборот. В разделе, посвящённому Enterprise-режиму, мы рассмотрим предлагаемый стандартом 802.11i механизм управления ключами.

2.4.4 СТАНДАРТ СЕТИ 802.11I С ПОВЫШЕННОЙ БЕЗОПАСНОСТЬЮ (WPA2)

В июне 2004 г. IEEE ратифицировал давно ожидаемый стандарт обеспечения безопасности в беспроводных локальных сетях — 802.11i.

Действительно, WPA достоин восхищения как шедевр ретроинжиниринга. Созданный с учетом слабых мест WEP, он представляет собой очень надежную систему безопасности, и обратно совместим с большинством существующего Wi-Fi-оборудования. WPA – практическое решение, обеспечивающее более чем адекватную безопасность для беспроводных сетей.

Однако WPA, в конце концов, компромиссное решение. Оно все еще основано на алгоритме шифрования RC4 и протоколе TKIP. Хотя и малая, но все же имеется вероятность открытия каких-либо слабых мест.

Абсолютно новая система безопасности, целиком лишенная брешей WEP, представляет собой лучшее долгосрочное и к тому же расширяемое решение для безопасности беспроводных сетей. С этой целью комитет по стандартам принял решение разработать систему безопасности с нуля. Это новый стандарт 802.11i, также известный как WPA2 и выпущенный тем же Wi-Fi Alliance.

Стандарт 802.11i использует концепцию повышенной безопасности (Robust Security Network, RSN), предусматривающую, что беспроводные устройства должны обеспечивать дополнительные возможности. Это потребует изменений в аппаратной части и программном обеспечении, т.е. сеть, полностью соответствующая RSN, станет несовместимой с существующим оборудованием WEP. В переходный период будет поддерживаться как оборудование RSN, так и WEP (на самом деле WPA/TKIP было решением, направленным на сохранение инвестиций в оборудование), но в дальнейшем устройства WEP будут отмирать.

802.11i приложим к различным сетевым реализациям и может задействовать TKIP, но по умолчанию RSN использует AES (Advanced Encryption Standard) и CCMP (Counter Mode CBC MAC Protocol) и, таким образом, является более мощным расширяемым решением.

В концепции RSN применяется AES в качестве системы шифрования, подобно тому, как алгоритм RC4 задействован в WPA. Однако механизм шифрования куда более сложен и не страдает от проблем, имевшихся в WEP. AES – блочный шифр, оперирующий блоками данных по 128 бит. CCMP, в свою очередь, – протокол безопасности, используемый AES. Он является эквивалентом TKIP в WPA. CCMP вычисляет MIC, прибегая к хорошо известному и проверенному методу Cipher Block Chaining Message Authentication Code (CBC-MAC). Изменение даже одного бита в сообщении приводит к совершенно другому результату.

Одним из худших аспектов WEP было управление секретными ключами. Многие администраторы больших сетей находили его неудобным. В результате чего ключи WEP не менялись длительное время (или никогда), облегчая задачу злоумышленникам.

RSN определяет иерархию ключей с ограниченным сроком действия, сходную с TKIP. В AES/CCMP, чтобы вместить все ключи, требуется 512 бит – меньше, чем в TKIP. В обоих случаях мастер-ключи используются не прямо, а для вывода других ключей. К счастью, администратор должен обеспечить единственный мастер-ключ. Сообщения составляются из 128-битного блока данных, зашифрованного секретным ключом такой же длины (128 бит). Хотя процесс шифрования сложен, администратор опять-таки не должен вникать в нюансы вычислений. Конечным результатом является шифр, который гораздо сложнее, чем даже WPA.

802.11i (WPA2) – это наиболее устойчивое, расширяемое и безопасное решение, предназначенное в первую очередь для больших предприятий, где управление ключами и администрирование были главной головной болью.

Стандарт 802.11i разработан на базе проверенных технологий. Механизмы безопасности были спроектированы с нуля в тесном сотрудничестве с лучшими специалистами по криптографии и имеют все шансы стать тем решением, которое необходимо беспроводным сетям. Хотя ни одна система безопасности полностью от взлома не гарантирована, 802.11i – это решение, на которое можно полагаться; оно свободно от слабостей предыдущих систем. И, конечно, WPA пригоден для адаптации уже существующего оборудования, и только когда его ресурсы будут окончательно исчерпаны, вы сможете заменить его новым, полностью соответствующим концепции RSN.

Производительность канала связи, как свидетельствуют результаты тестирования оборудования различных производителей, падает на 5-20% при включении как WEP, так и WPA. Однако испытания того оборудования, в котором включено шифрование AES вместо TKIP, не показали сколько-нибудь заметного падения скорости. Это позволяет надеяться, что WPA2-совместимое оборудование предоставит нам долгожданный надежно защищенный канал без потерь в производительности.

WPA2, так же как и WPA, может работать в двух режимах: *Enterprise* (корпоративный) и *Pre-Shared Key* (персональный).

Пример 2.2:

Настроим точку доступа с применением персональной спецификации WPA2-PSK.

1. Для этого подключаемся к точке доступа по проводному интерфейсу, вводим режим, SSID, канал, как было описано в примере 1.4. Далее в поле Authentication (Аутентификация) ставим WPA2-PSK (рис. 2.29).

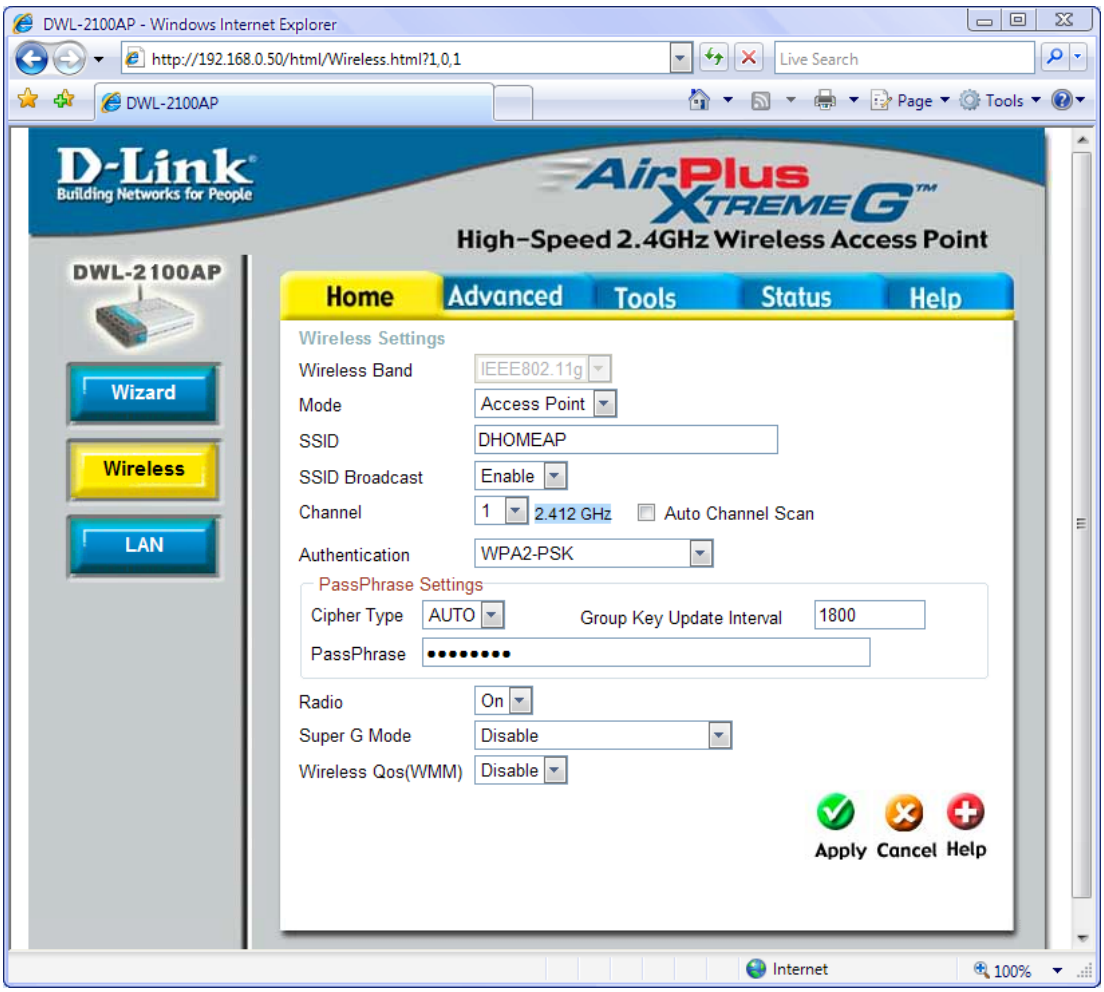


Рис. 2.29

2. Выбираем тип шифрования (Cipher Type). Возможные варианты: AUTO, TKIP, AES. Если выставлено AUTO, то точка доступа будет подстраивать тип шифрования под первого подключившегося клиента.

3. Выставляем интервал обновления группового ключа (Group Key Update Interval), который задаётся в секундах.

4. Вводим ключ в поле PassPhrase любой длины, но не менее 8 символов, например *secretpass*.

Теперь, после применения настроек, на клиентской стороне, надо выставить те же самые параметры, и подключиться к ней.

2.4.5 СТАНДАРТ 802.1X/EAP (ENTERPRISE-РЕЖИМ)

Проблемы, с которыми столкнулись разработчики и пользователи сетей на основе стандарта 802.11 вынудили искать новые решения защиты беспроводных сетей. Были выявлены компоненты, влияющие на системы безопасности беспроводной локальной сети:

1) Архитектура аутентификации;
2) Механизм аутентификации;
3) Механизм обеспечения конфиденциальности и целостности данных.

Архитектура аутентификации IEEE 802.1x – стандарт IEEE 802.1x описывает единую архитектуру контроля доступа к портам с использованием разнообразных методов аутентификации абонентов.

Алгоритм аутентификации Extensible Authentication Protocol или EAP (Расширяемый протокол идентификации) поддерживает централизованную аутентификацию элементов инфраструктуры беспроводной сети и её пользователей с возможностью динамической генерации ключей шифрования.

Архитектура IEEE 802.1x

Архитектура IEEE 802.1x включат в себя следующие обязательные логические элементы (рис. 2.30):

- Клиент (Supplicant) – находится в операционной системе абонента;
- Аутентификатор (Authenticator) – находится в программном обеспечении точки радиодоступа;
- Сервер аутентификации (Authentication Server) – находится на RADIUS-сервере.

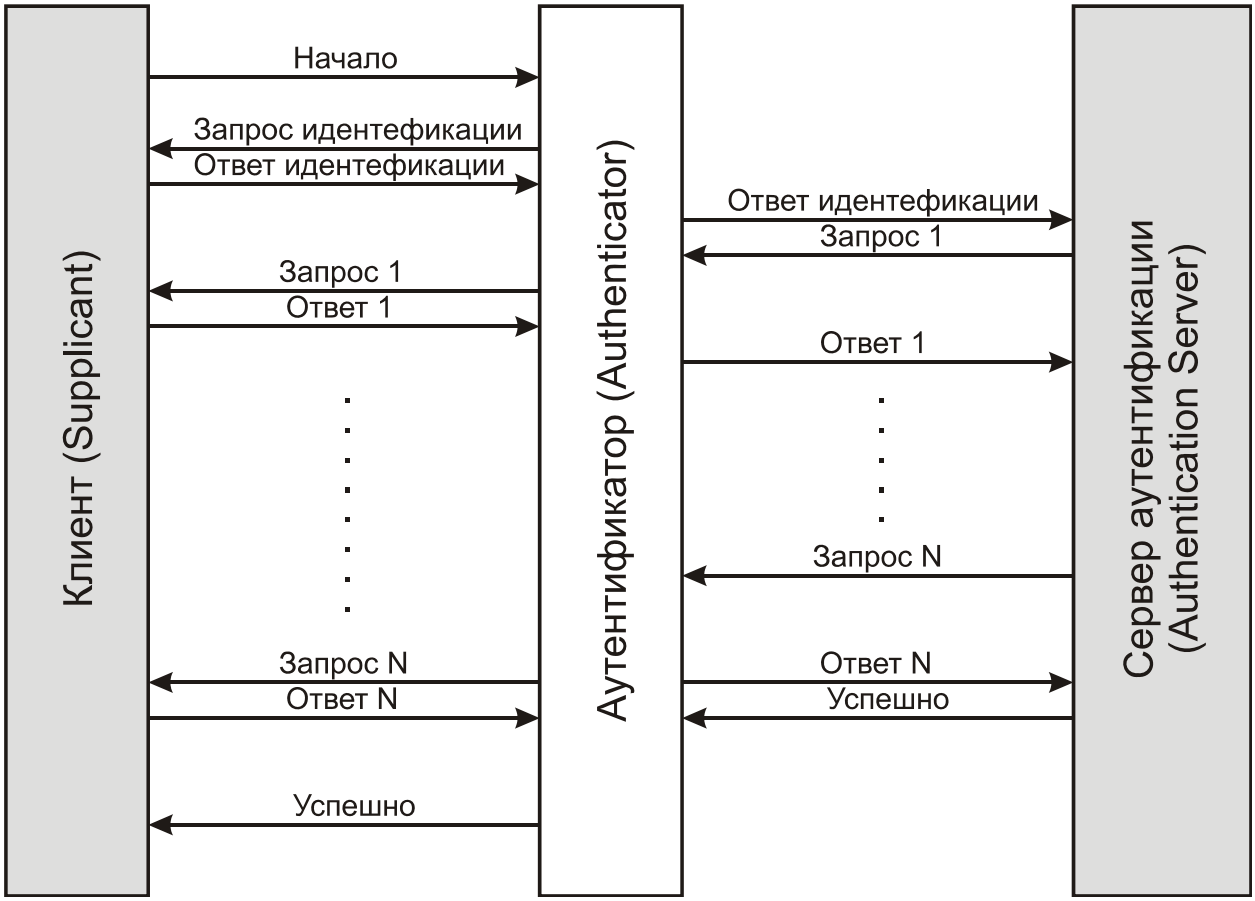


Рис. 2.30 Архитектура IEEE 802.1x

IEEE 802.1x предоставляет абоненту беспроводной локальной сети лишь средства передачи атрибутов серверу аутентификации и допускает использование различных методов и алгоритмов аутентификации. Задачей сервера аутентификации является поддержка требуемых политикой сетевой безопасностью методов аутентификации.

Аутентификатор, находясь в точке радиодоступа, создаёт логический порт для каждого клиента на основе его идентификатора ассоциирования. Логический порт имеет два канала для обмена данными. Неконтролируемый канал беспрепятственно пропускает трафик из беспроводного сегмента в проводной и обратно, в то время как контролируемый канал требует успешной аутентификации для беспрепятственного прохождения фреймов.

Таким образом, в терминологии стандарта 802.1x точка доступа играет роль коммутатора в проводных сетях Ethernet. Очевидно, что проводной сегмент сети, к которому подключена точка доступа, нуждается в сервере аутентификации. Его функции обычно выполняет RADIUS-сервер, интегрированный с той или иной базой данных пользователей, в качестве которой может выступать стандартный RADIUS, LDAP, NDS или Windows Active Directory. Коммерческие беспроводные шлюзы высокого класса могут реализовывать как функции сервера аутентификации, так и аутентификатора.

Клиент активизируется и ассоциируется с точкой радиодоступа (или физически подключается к сегменту в случае проводной локальной сети). Аутентификатор распознаёт факт подключения и активизирует логический порт для клиента, сразу переводя его в состояние «неавторизован». В результате этого через клиентский порт возможен обмен лишь трафиком протокола IEEE 802.1x, для всего остального трафика порт заблокирован. Клиент также может (но не обязан) отправить сообщение EAP Start (начало аутентификации EAP) (рис. 2.31) для запуска процесса аутентификации.

Аутентификатор отправляет сообщение EAP Request Identity (запрос имени EAP) и ожидает от клиента его имя (Identity). Ответное сообщение клиента EAP Response (ответ EAP), содержащее атрибуты, перенаправляется серверу аутентификации.

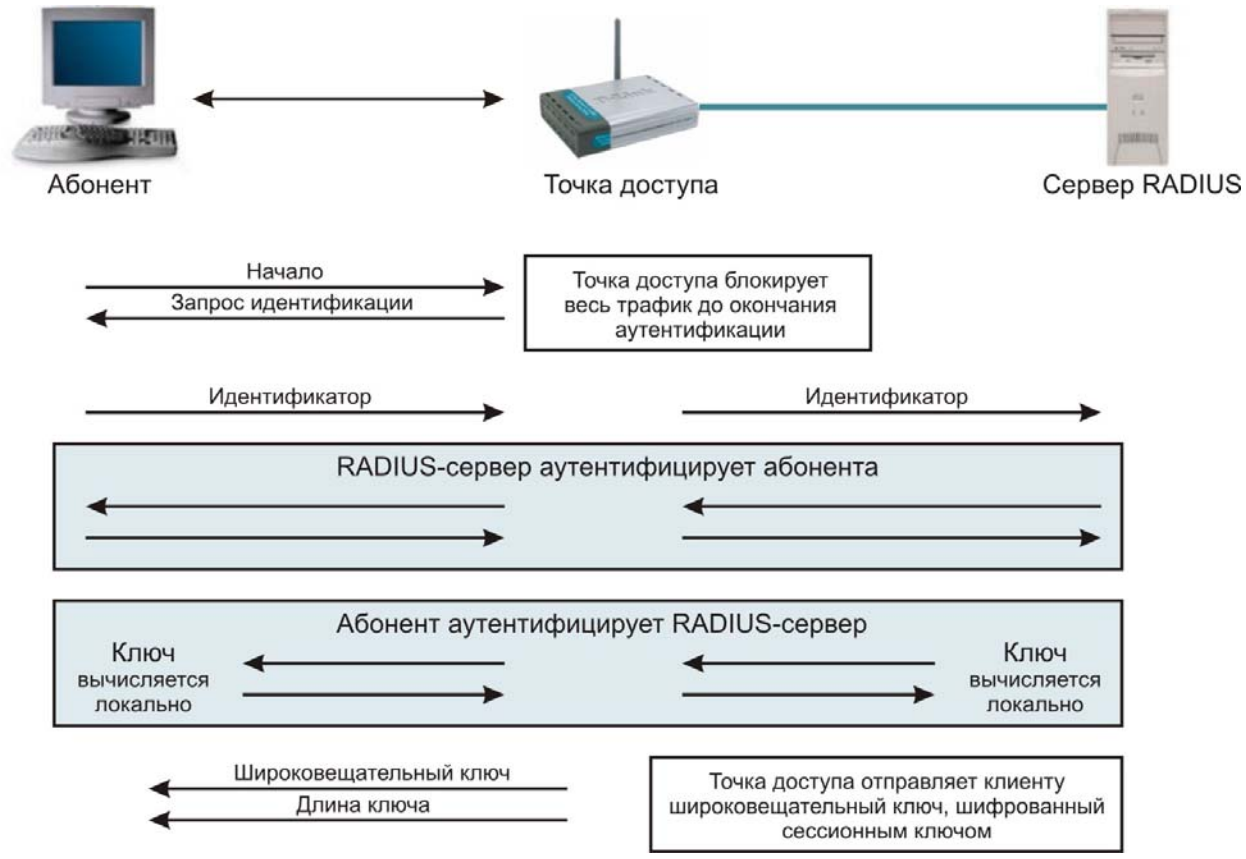


Рис. 2.31 Обмен сообщениями в 802.1x/EAP

После завершения аутентификации сервер отправляет сообщение RADIUS-ACCEPT (принять) или RADIUS-REJECT (отклонить) аутентификатору. При получении сообщения RADIUS-ACCEPT аутентификатор переводит порт клиента в состояние “авторизован“, и начинается передача всего трафика абонента.

Механизм аутентификации

Первоначально стандарт 802.1x задумывался для того, чтобы обеспечить аутентификацию пользователей на канальном уровне в коммутируемых проводных сетях.

Алгоритмы аутентификации стандарта 802.11 могут обеспечить клиента динамическими, ориентированными на пользователя ключами. Но тот ключ, который создается в процессе аутентификации, не является ключом, используемым для шифрования фреймов или проверки целостности сообщений. В стандарте WPA для получения всех ключей используется так называемый *мастер-ключ* (Master Key). На рис. 2.32 представлена иерархия ключей с учетом последовательности их создания.

Механизм генерации ключей шифрования осуществляется в четыре этапа.

1) Клиент и точка доступа устанавливают динамический ключ (он называется *парный мастер-ключ*, или PMK, от англ. Pairwise Master Key), полученный в процессе аутентификации по стандарту 802.1x.
2) Точка доступа посылает клиенту секретное случайное число, которое называется *временный аутентификатор* (Authenticator Nonce, ANonce), используя для этого сообщение EAPoL-Key стандарта 802.1x.
3) Этот клиент локально генерирует секретное случайное число, называемое *временный проситель* (Supplicant Nonce, SNonce).
4) Клиент генерирует *парный переходный ключ* (Pairwise Transient Key, PTK) путем комбинирования PMK, SNonce, ANonce, MAC-адреса клиента, MAC-адреса точки доступа и строки инициализации. MAC-адреса упорядочены, MAC-адреса низшего порядка предшествуют MAC-адресам высшего порядка. Благодаря этому гарантируется, что клиент и точка доступа “выстроят” MAC-адреса одинаковым образом (рис. 2.33).
5) Это комбинированное значение пропускается через псевдослучайную функцию (Pseudo Random Function, PRF), чтобы получить 512-разрядный PTK.
6) Клиент посылает число SNonce, сгенерированное им на этапе 3, точке доступа с помощью сообщения EAPoL-Key стандарта 802.1x, защищенное ключом EAPoL-Key MIC.
7) Точка доступа использует число SNonce для вычисления PTK таким же образом, как это сделал клиент.
8) Точка доступа использует выведенный ключ EAPoL-Key MIC для проверки целостности сообщения клиента.
9) Точка доступа посылает сообщение EAPoL-Key, показывающее, что клиент может установить PTK и его ANonce, защищенные ключом EAPoL-Key MIC. Данный этап позволяет клиенту удостовериться в том, что число ANonce, полученное на этапе 2, действительно.
10) Клиент посылает сообщение EAPoL-Key, защищенное ключом EAPoL-Key MIC, указывающее, что ключи установлены.

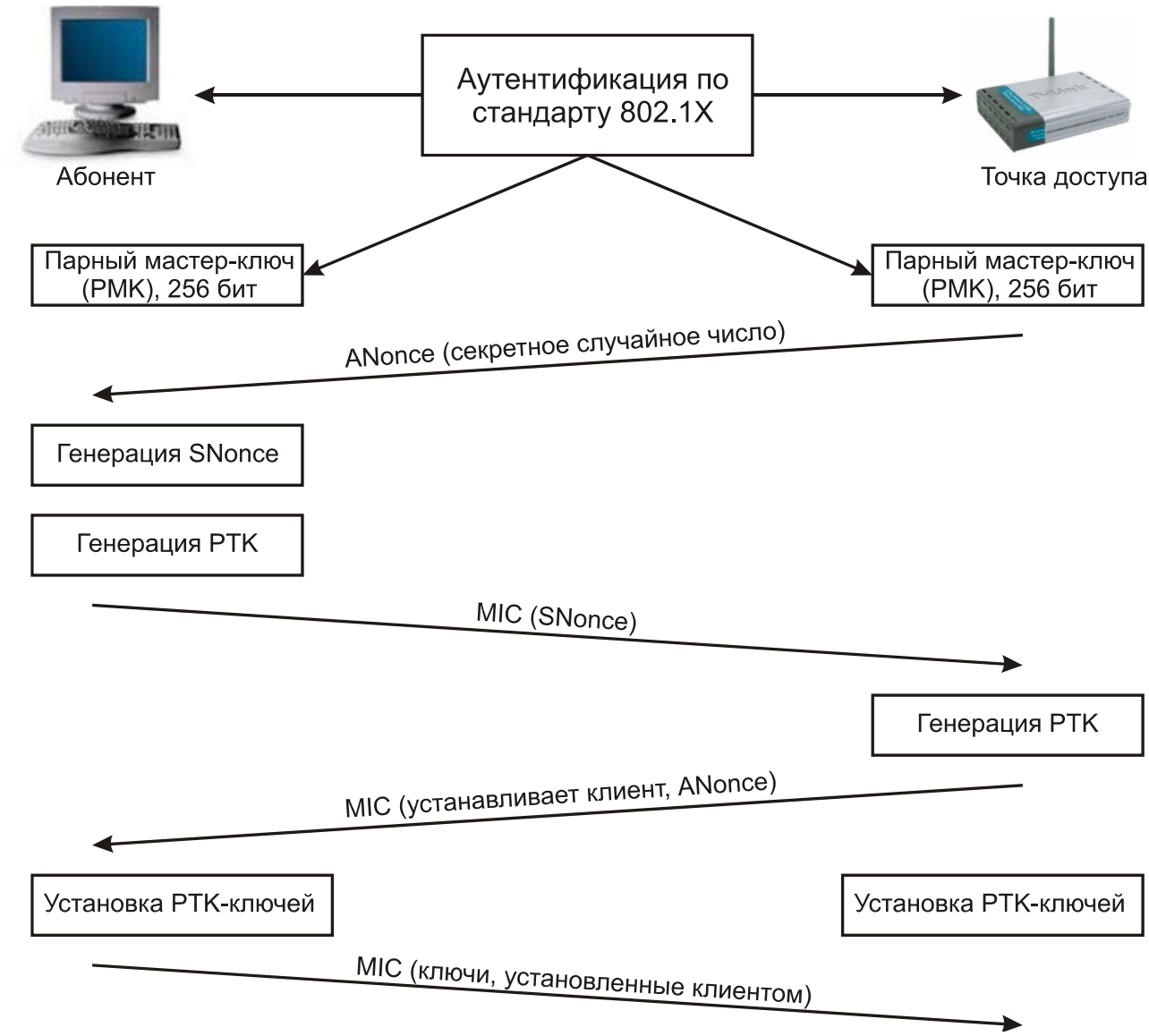


Рис. 2.32 Создание ключей

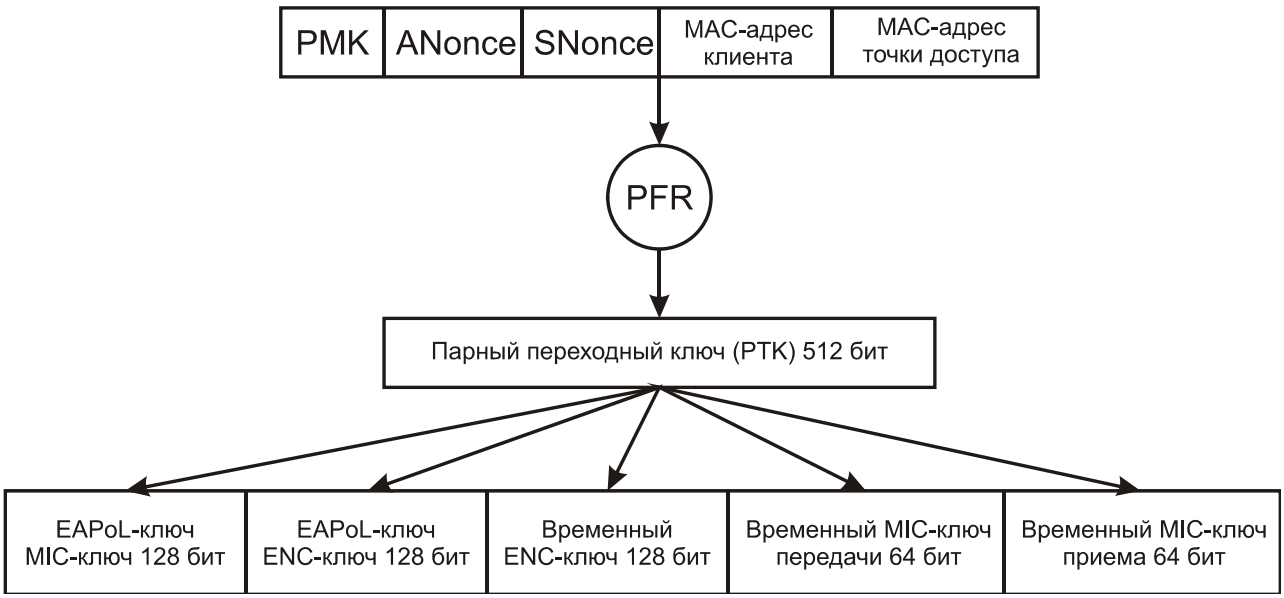


Рис. 2.33 Генерация парного переходного ключа

Парный мастер-ключ (PMK) и парный переходный ключ (PTK) являются одноадресными по своей природе. Они только шифруют и дешифруют одноадресные фреймы, и предназначены для единственного пользователя. Широковещательные фреймы требуют отдельной иерархии ключей, потому что использование с этой целью одноадресных ключей приведет к резкому возрастанию трафика сети. Точке доступа (единственному объекту BSS, имеющему право на рассылку широковещательных или многоадресных сообщений) пришлось бы посылать один и тот же широковещательный или многоадресный фрейм, зашифрованный соответствующими пофреймовыми ключами, каждому пользователю.

Широковещательные или многоадресные фреймы используют иерархию *групповых ключей*. Групповой мастер-ключ (Group Master Key, GMK) находится на вершине этой иерархии и выводится в точке доступа. Вывод GMK основан на применении PRF, в результате чего получается 256-разрядный GMK. Входными данными для PRF-256 являются шифровальное секретное случайное число (или Nonce), текстовая строка, MAC-адрес точки доступа и значение времени в формате синхронизирующего сетевого протокола (NTP). На рис. 2.34 представлена иерархия групповых ключей.

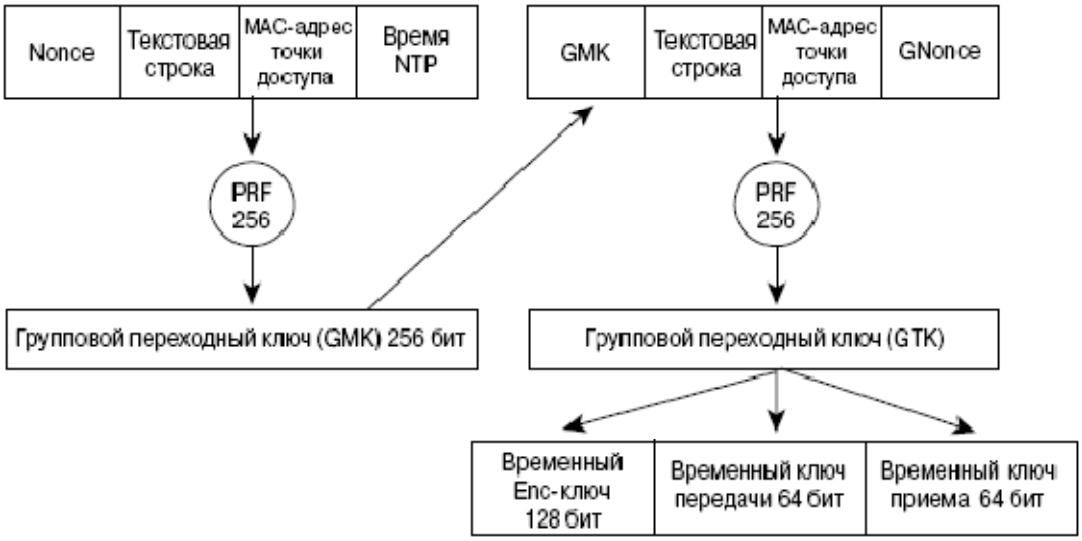


Рис. 2.34 Иерархия групповых ключей

Групповой мастер-ключ, текстовая строка, MAC-адрес точки доступа и GNonce (значение, которое берется из счетчика ключа точки доступа) объединяются и обрабатываются с помощью PRF, в результате чего получается 256-разрядный групповой переходный ключ (Group Transient Key, GTK). GTK делится на 128-разрядный ключ шифрования широковещательных/многоадресных фреймов, 64-разрядный ключ передачи MIC (transmit MIC key) и 64-разрядный ключ приема MIC (MIC receive key).

С помощью этих ключей широковещательные и многоадресные фреймы шифруются и дешифруются точно так же, как с помощью одноадресных ключей, полученных на основе парного мастер-ключа (PMK).

Клиент обновляется с помощью групповых ключей шифрования через сообщения EAPoL-Key. Точка доступа посылает такому клиенту сообщение EAPoL, зашифрованное с помощью одноадресного ключа шифрования. Групповые ключи удаляются и регенерируются каждый раз, когда какая-нибудь станция диссоциируется или деаутентифицируется в BSS. Если происходит ошибка MIC, одной из мер противодействия также является удаление всех ключей с имеющей отношение к ошибке приемной станции, включая групповые ключи.

В домашних сетях или сетях, предназначенных для малых офисов, развертывание RADIUS-сервера с базой данных конечных пользователей маловероятно. В таком случае для генерирования сеансовых ключей используется только предварительно разделенный РМК (вводится вручную). Это аналогично тому, что делается в оригинальном протоколе WEP.

Поскольку в локальных сетях 802.11 нет физических портов, то ассоциация между беспроводным клиентским устройством и точкой доступа считается сетевым портом доступа. Беспроводный клиент рассматривается как претендент, а точка доступа – как аутентификатор.

В стандарте 802.1x аутентификация пользователей на канальном уровне выполняется по протоколу EAP, который был разработан Группой по проблемам проектирования Интернет (IETF). Протокол EAP – это замена протокола CHAP (Challenge Handshake Authentication Protocol, протокол взаимной аутентификации), который применяется в PPP (Point to Point Protocol, протокол соединения «точка-точка»), он предназначен для использования в локальных сетях. Спецификация EAPOL определяет, как фреймы EAP инкапсулируются во фреймы 802.3, 802.5 и 802.11. Обмен фреймами между объектами, определенными в стандарте 802.1x, схематично изображен на рисунке 2.35.

EAP является «обобщённым» протоколом в системе аутентификации, авторизации и учёта (authentication, authorization, and accounting, AAA), обеспечивающим работу разнообразных методов аутентификаци. AAA-клиент (сервер доступа в терминологии AAA, в беспроводной сети представлен точкой радиодоступа), поддерживающий EAP, может не понимать конкретных методов, используемых абонентом и сетью в процессе аутентификации. Сервер доступа туннелирует сообщения протокола аутентификации, циркулирующие между абонентом и сервером аутентификации. Сервер доступа интересует лишь факт начала и окончания процесса аутентификации.

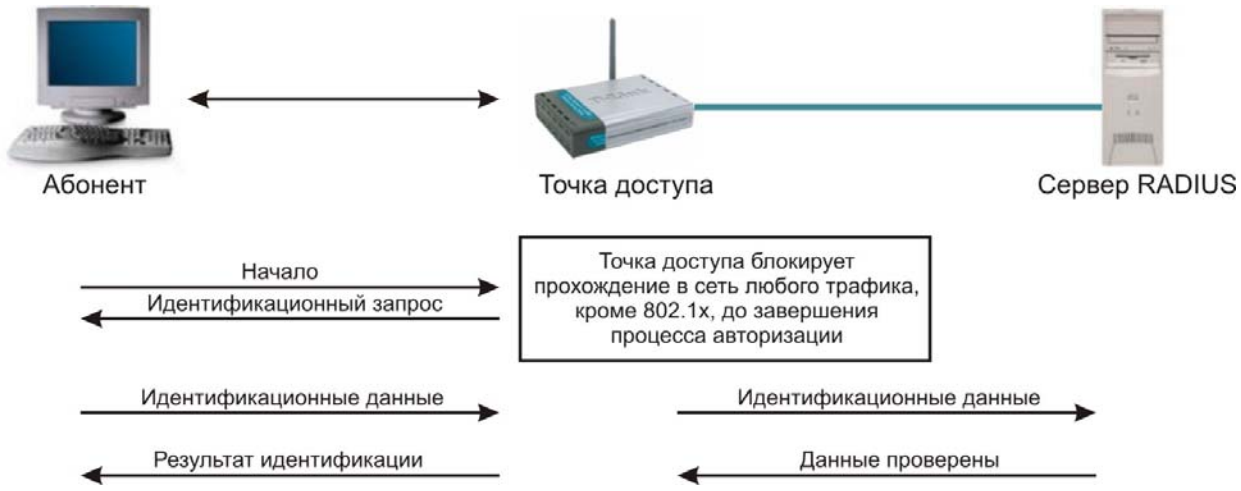


Рис. 2.35 Механизм аутентификации в 802.1x/EAP

Есть несколько вариантов EAP, спроектированных с участием различных компаний-производителей. Такое разнообразие вносит дополнительные проблемы совместимости, так что выбор подходящего оборудование и программного обеспечения для беспроводной сети становится нетривиальной задачей. При конфигурировании способа аутентификации пользователей в беспроводной сети вам, вероятно, придется столкнуться со следующими вариантами EAP:

– EAP-MD5 – это обязательный уровень EAP, который должен присутствовать во всех реализациях стандарта 802.1x, именно он был разработан первым. С точки зрения работы он дублирует протокол CHAP. Мы не рекомендуем пользоваться

протоколом EAP-MD5 по трем причинам. Во-первых, он не поддерживает динамическое распределение ключей. Кроме того, он уязвим для атаки «человек посередине» с применением фальшивой точки доступа и для атаки на сервер аутентификации, так как аутентифицируются только клиенты. И наконец, в ходе аутентификации противник может подслушать запрос и зашифрованный ответ, после чего провести атаку с известным открытым или шифрованным текстом;

– EAP-TLS (EAP-Transport Layer Security, протокол защиты транспортного уровня) поддерживает взаимную аутентификацию на базе сертификатов. EAP-TLS основан на протоколе SSLv3 и требует наличия удостоверяющего центра. Протоколы TLS и SSL используют ряд элементов инфраструктуры PKI (Public Key Infrastructure): Абонент должен иметь действующий сертификат для аутентификации по отношению к сети. AAA-сервер должен иметь действующий сертификат для аутентификации по отношению к абоненту. Орган сертификации с сопутствующей инфраструктурой управляет сертификатами субъектов PKI. Клиент и RADIUS-сервер должны поддерживать метод аутентификации EAP-TLS. Точка радиодоступа должна поддерживать процесс аутентификации в рамках 802.1x/EAP, хотя может и не знать деталей конкретного метода аутентификации. Общий вид EAP-TLS выглядит примерно так (рис. 2.36):

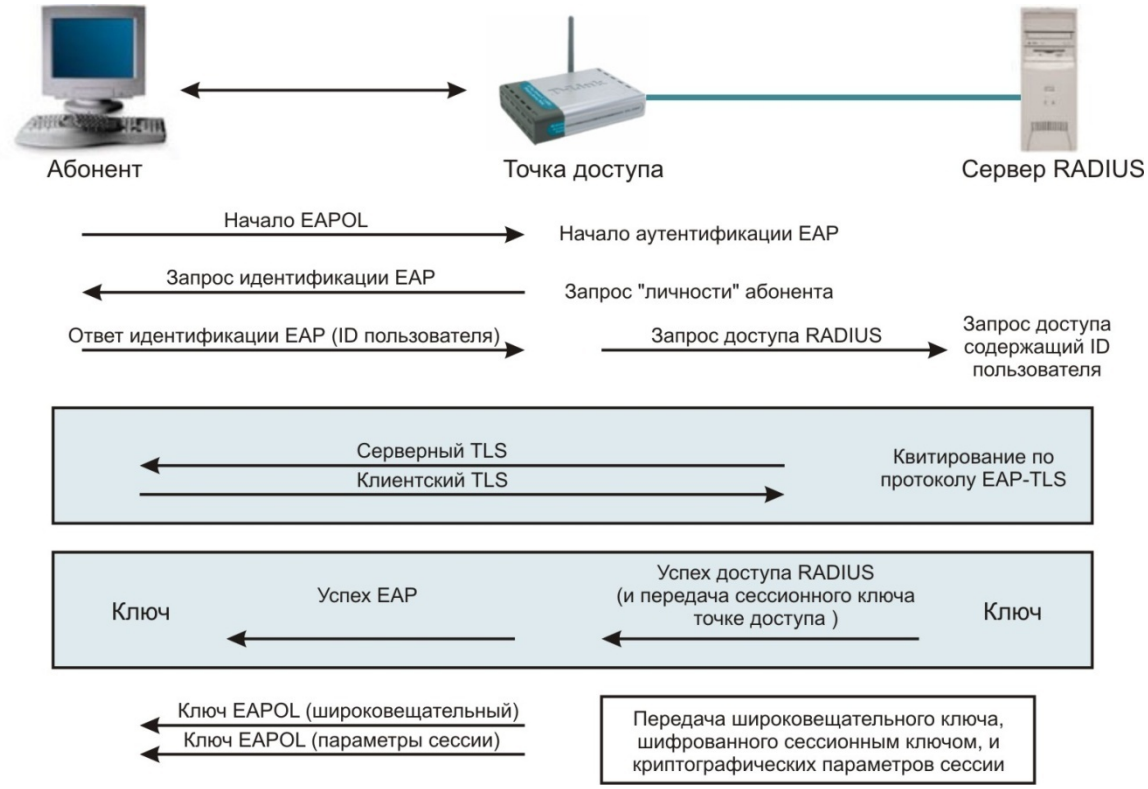


Рис. 2.36 Процесс аутентификации EAP-TLS

– EAP-LEAP (Lightweight EAP, облегчённый EAP) – это запатентованный компанией Cisco вариант EAP, реализованный в точках доступа и беспроводных клиентских картах Cisco. LEAP был первой (и на протяжении длительного времени единственной) схемой аутентификации в стандарте 802.1x, основанной на паролях. Поэтому LEAP приобрел огромную популярность и даже поддержан в сервере Free-RADIUS, несмотря на то, что это запатентованное решение. Сервер аутентификации посылает клиенту запрос, а тот должен вернуть пароль, предварительно выполнив его свертку со строкой запроса. Будучи основан на применении паролей, EAP-LEAP аутентифицирует пользователя, а не устройство.

В то же время очевидна уязвимость этого варианта для атак методом полного перебора и по словарю, не характерная для методов аутентификации с применением сертификатов.

– PEAP (Protected EAP, защищённый EAP) и EAP-TTLS (Tunneled Transport Layer Security EAP, протокол защиты транспортного уровня EAP), разработанный компанией Certicom and Funk Software. Эти варианты также достаточно развиты, и поддерживаются производителями, в частности D-link. Для работы EAP-TTLS требуется, чтобы был сертифицирован только сервер аутентификации, а у претендента сертификата может и не быть, так что процедура развертывания упрощается. EAP-TTLS поддерживает также ряд устаревших методов аутентификации, в том числе PAP, CHAP, MS-CHAP, MS-CHAPv2 и даже EAP-MD5. Чтобы обеспечить безопасность при использовании этих методов, EAP-TTLS создает зашифрованный по протоколу TLS туннель, внутри которого эти протоколы и работают. Примером практической реализации EAP-TTLS может служить программное обеспечение для управления доступом в беспроводную сеть Odyssey от компании Funk Software. Протокол PEAP очень похож на EAP-TTLS, только он не поддерживает устаревших методов аутентификации типа PAP и CHAP. Вместо них поддерживаются протоколы PEAP-MS-CHAPv2 и PEAP-EAP-TLS, работающие внутри безопасного туннеля. Поддержка PEAP реализована в пакете программ точек доступа D-link, и хорошо реализована в Windows XP начиная с Service Pack 2. В общем виде схема обмена PEAP выглядит следующим образом (рис.2.37):

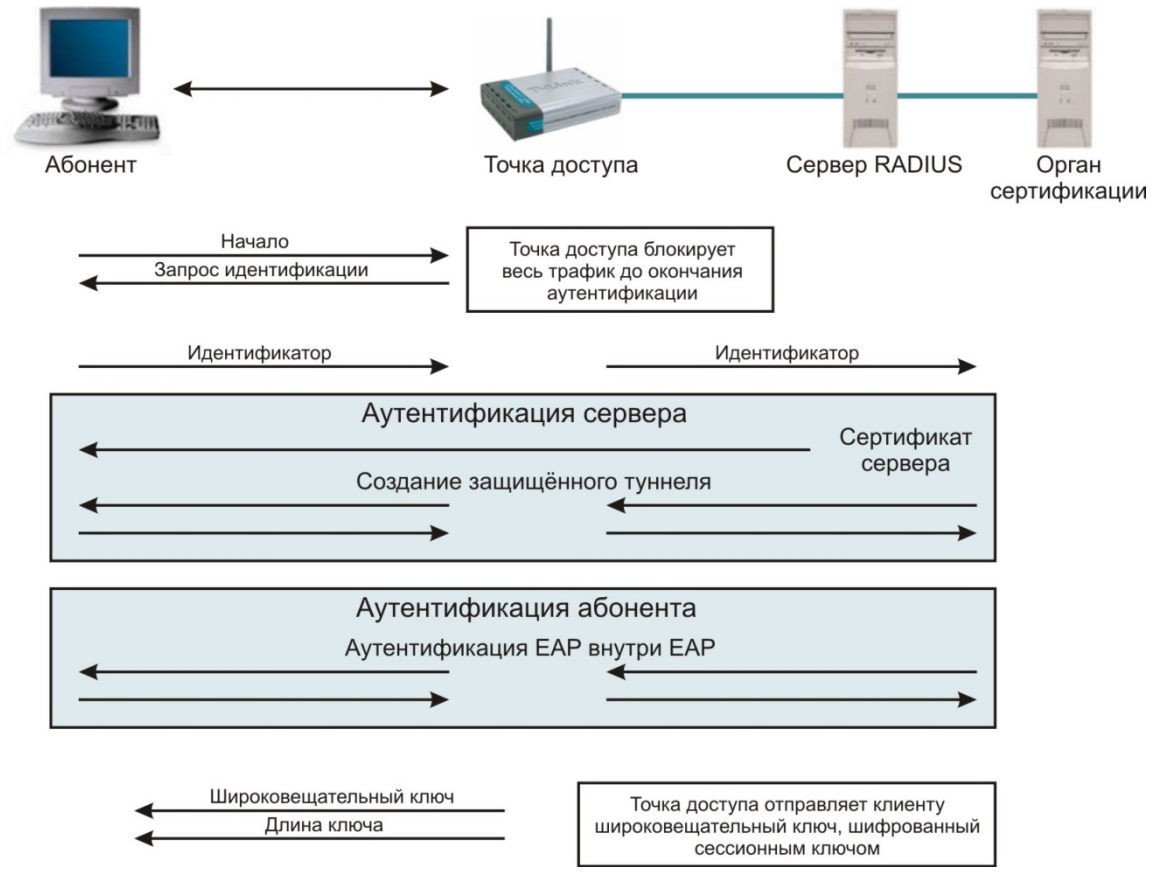


Рис. 2.37 Процесс аутентификации PEAP

– Еще два варианта EAP – это EAP-SIM и EAP-AKA для аутентификации на базе SIM и USIM. В настоящий момент оба имеют статус предварительных документов

IETF и в основном они предназначены для аутентификации в сетях GSM, а не в беспроводных сетях 802.11. Тем не менее, протокол EAP-SIM поддержан в точках доступа и клиентских устройствах некоторых производителей.

Наглядно, уровни архитектуры 802.1x показаны на рисунке 2.38.

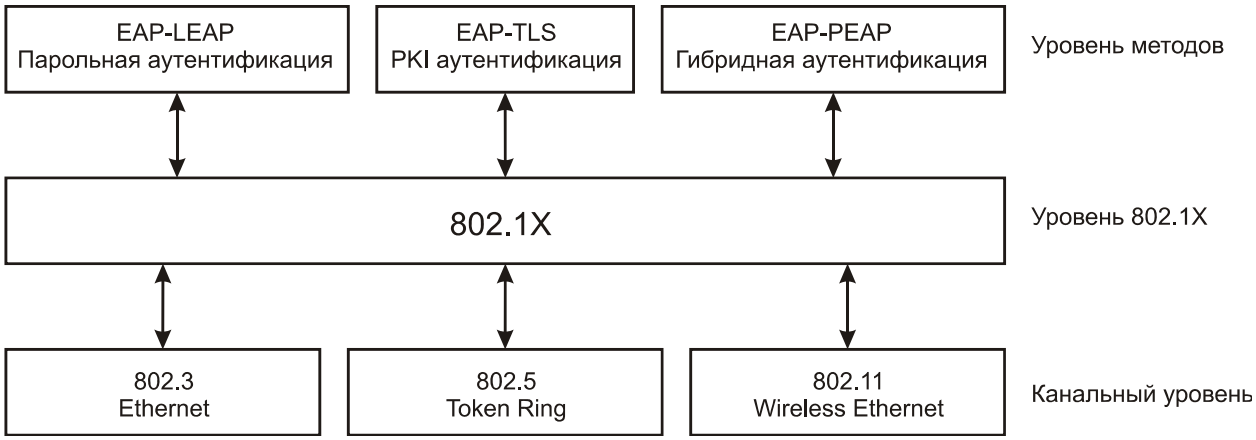


Рис. 2.38 Уровни архитектуры 802.1x

Здесь в качестве механизма обеспечения конфиденциальности и целостности данных выступают стандарты шифрования WPA и WPA2.

2.5 ТЕХНОЛОГИИ ЦЕЛОСТНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ ПЕРЕДАВАЕМЫХ ДАННЫХ

2.5.1 РАЗВЕРТЫВАНИЕ БЕСПРОВОДНЫХ ВИРТУАЛЬНЫХ СЕТЕЙ

Виртуальная частная сеть (Virtual Private Network, VPN) – это метод, позволяющий воспользоваться телекоммуникационной инфраструктурой общего пользования, например сетью Интернет для предоставления удаленным офисам или отдельным пользователям безопасного доступа к сети организации. Поскольку беспроводные сети 802.11 работают в нелицензируемом диапазоне частот и легко доступны для случайного или злонамеренного прослушивания, то именно в них развертывание и обслуживание VPN приобретает особую важность, если необходимо обеспечить высокий уровень защиты информации.

Защищать нужно как соединения между хостами в беспроводной локальной сети, так и двухточечные каналы между беспроводными мостами. Для обеспечения безопасности особо секретных данных нельзя полагаться на какой-то один механизм или на защиту лишь одного уровня сети. В случае двухточечных каналов проще и экономичнее развернуть VPN, покрывающую две сети, чем реализовывать защиту на базе стандарта 802.11i включающую RADIUS-сервер и базу данных о пользователях.

Пользоваться же реализацией стандарта на базе предварительно разделенных ключей (PSK) и протокола 802.1x при наличии высокоскоростного канала между сетями не самый безопасный метод. VPN – это полная противоположность дорогостоящей системе собственных или арендованных линий, которые могут использоваться только одной организацией. Задача VPN – предоставить организации те же возможности, но за гораздо меньшие деньги. Сравните это с обеспечением связи за счет двухточечных беспроводных каналов с мостами вместо дорогих выделенных линий.

VPN и беспроводные технологии не конкурируют, а дополняют друг друга. VPN работает поверх разделяемых сетей общего пользования, обеспечивая в то же время конфиденциальность за счет специальных мер безопасности и применения туннельных протоколов, таких как туннельный протокол на канальном уровне (Layer Two Tunneling

Protocol, L2TP). Смысл их в том, что, осуществляя шифрование данных на отправляющем конце и дешифрирование на принимающем, протокол организует «туннель», в который не могут проникнуть данные, не зашифрованные должным образом. Дополнительную безопасность может обеспечить шифрование не только самих данных, но и сетевых адресов отправителя и получателя. Беспроводную локальную сеть можно сравнить с разделяемой сетью общего пользования, а в некоторых случаях (хот-споты, узлы, принадлежащие сообществам) она таковой и является.

VPN отвечает трем условиям: конфиденциальность, целостность и доступность. Следует отметить, что никакая VPN не является устойчивой к DoS- или DDoS-атакам и не может гарантировать доступность на физическом уровне просто в силу своей виртуальной природы и зависимости от нижележащих протоколов.

Две наиболее важные особенности VPN, особенно в беспроводных средах, где имеется лишь ограниченный контроль над распространением сигнала, – это целостность и, что еще более существенно, конфиденциальность данных. Возьмем жизненную ситуацию, когда противнику удалось преодолеть шифрование по протоколу WEP и присоединиться к беспроводной локальной сети. Если VPN отсутствует, то он сможет прослушивать данные и вмешиваться в работу сети. Но если пакеты аутентифицированы, то атака «человек посередине» становится практически невозможной, хотя перехватить данные по-прежнему легко. Включение в VPN элемента шифрования уменьшает негативные последствия перехвата данных. VPN обеспечивает не столько полную изоляцию всех сетевых взаимодействий, сколько осуществление таких взаимодействий в более контролируемых условиях с четко определенными группами допущенных участников.

Есть много способов классификации VPN, но основные три вида – это сеть-сеть, хост-сеть и хост-хост.

Топология сеть-сеть

Этим термином иногда описывают VPN-туннель между двумя географически разнесенными частными сетями (рис. 2.39).

Рис. 2.39 Топология сеть-сеть

VPN такого типа обычно применяются, когда нужно объединить локальные сети с помощью сети общего пользования так, как будто они находятся внутри одного здания.

Основное достоинство такой конфигурации состоит в том, что сети выглядят как смежные, а работа VPN-шлюзов совершенно прозрачна для конечных пользователей. В этом случае важно также туннелирование, поскольку в частных сетях обычно используются описанные в RFC 1918 зарезервированные адреса, которые не могут маршрутизироваться через Интернет. Поэтому для успешного взаимодействия трафик необходимо инкапсулировать в туннель.

Типичным примером такой сети может быть соединение двух филиалов одной организации по двухточечному беспроводному каналу. Хотя трафик и не выходит за пределы внутренней инфраструктуры организации, но к ее беспроводной части нужно относиться так же внимательно, как если бы трафик маршрутизировался через сеть общего пользования. Вы уже видели, что протокол WEP можно легко преодолеть и даже TKIP иногда уязвим, поэтому мы настоятельно рекомендуем всюду, где возможно, реализовывать дополнительное шифрование.

Топология хост-сеть

При такой конфигурации удаленные пользователи подключаются к корпоративной сети через Интернет.

Сначала мобильный клиент устанавливает соединение с Интернет, а затем инициирует запрос на организацию зашифрованного туннеля с корпоративным VPN-шлюзом. После успешной аутентификации создается туннель поверх сети общего пользования и клиент становится просто еще одной машиной во внутренней сети. Все более широкое распространение надомной работы стимулирует интерес к такому применению VPN.

В отличие от VPN типа сеть-сеть, где число участников невелико и более или менее предсказуемо, VPN типа хост-сеть легко может вырасти до необъятных размеров. Поэтому системный администратор должен заранее продумать масштабируемый механизм аутентификации клиентов и управления ключами.

Топология хост-хост

Такая топология, по-видимому, встречается реже всего. Речь идет о двух хостах, обменивающихся друг с другом шифрованными и нешифрованными данными. В такой конфигурации туннель организуется между двумя хостами и весь трафик между ними инкапсулируется внутри VPN. У таких сетей не много практических применений, но в качестве примера можно назвать географически удаленный сервер резервного хранения. Оба хоста подключены к Интернет, и данные с центрального сервера зеркально копируются на резервный. Например, простые сети VPN типа хост-хост можно использовать для защиты одноранговых (Ad Hoc) сетей.

2.5.2 РАСПРОСТРАНЕННЫЕ ТУННЕЛЬНЫЕ ПРОТОКОЛЫ

Протокол IPSec

IPSec – это наиболее широко признанный, поддерживаемый и стандартизованный из всех протоколов VPN. Для обеспечения совместной работы он подходит лучше всех прочих. IPSec лежит в основе открытых стандартов, в которых описан целый набор безопасных протоколов, работающих поверх существующего стека IP. Он предоставляет службы аутентификации и шифрования данных на сетевом уровне (уровень 3) модели OSI и может быть реализован на любом устройстве, которое работает по протоколу IP. В отличие от многих других схем шифрования, которые защищают конкретный протокол верхнего уровня, IPSec, работающий на нижнем уровне, может защитить весь IP-трафик. Он применяется также в сочетании с туннельными протоколами на канальном уровне (уровень 2) для шифрования и аутентификации трафика, передаваемого по протоколам, отличным от IP.

Протокол IPSec состоит из трех основных частей:

- заголовка аутентификации (Authentication Header, AH);
- безопасно инкапсулированной полезной нагрузки (Encapsulating Security Payload, ESP);
- схемы обмена ключами через Интернет (Internet Key Exchange, IKE).

Заголовок AH добавляется после заголовка IP и обеспечивает аутентификацию на уровне пакета и целостность данных. Иными словами, гарантируется, что пакет не был изменен на пути следования и поступил из ожидаемого источника. ESP обеспечивает конфиденциальность, аутентификацию источника данных, целостность, опциональную защиту от атаки повторного сеанса и до некоторой степени скрытность механизма управления потоком. Наконец, IKE обеспечивает согласование настроек служб безопасности между сторонами-участниками.

Протокол PPTP

Двухточечный туннельный протокол (Point-to-Point Tunneling Protocol, PPTP) – это запатентованная разработка компании Microsoft, он предназначен для организации взаимодействия по типу VPN. PPTP обеспечивает аутентификацию пользователей с помощью таких протоколов, как MS-CHAP, CHAP, SPAP и PAP. Этому протоколу недостает гибкости, присущей другим решениям, он не слишком хорошо приспособлен

для совместной работы с другими протоколами VPN, зато прост и широко распространен во всем мире.

Протокол определяет следующие типы коммуникаций:

- PPTP-соединение, по которому клиент организует PPP-канал с провайдером;
- Управляющее PPTP-соединение, которое клиент организует с VPN-сервером и по которому согласует характеристики туннеля;
- PPTP-туннель, по которому клиент и сервер обмениваются зашифрованными данными.

Протокол PPTP обычно применяется для создания безопасных каналов связи между многими Windows-машинами в сети Intranet.

Протокол L2TP

Этот протокол, совместно разработанный компаниями Cisco, Microsoft и 3Com, обещает заменить PPTP в качестве основного туннельного протокола. По существу, L2TP (Layer Two Tunneling Protocol, протокол туннелирования канального уровня) представляет собой комбинацию PPTP и созданного Cisco протокола Layer Two Forwarding (L2F). Протокол L2TP применяется для туннелирования PPP-трафика поверх IP-сети общего пользования. Для установления соединения по коммутируемой линии в нем используется PPP с аутентификацией по протоколу PAP или CHAP, но, в отличие от PPTP, L2TP определяет свой собственный туннельный протокол.

Поскольку L2TP работает на канальном уровне (уровень 2), то через туннель можно пропускать и не-IP трафик. Вместе с тем L2TP совместим с любым канальным протоколом, например ATM, Frame Relay или 802.11. Сам по себе протокол не содержит средств шифрования, но может быть использован в сочетании с другими протоколами или механизмами шифрования на прикладном уровне.

2.6 СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЯ В БЕСПРОВОДНЫЕ СЕТИ

Системы обнаружения вторжения (Intrusion Detection System, IDS) – это устройства с помощью которых можно выявлять и своевременно предотвращать вторжения в вычислительные сети. Они делятся на два вида: на базе сети и на базе хоста.

Сетевые системы (Network Intrusion Detection Systems, NIDS) анализируют трафик с целью обнаружения известных атак на основании имеющихся у них наборов правил (экспертные системы). Исключение с точки зрения принципов анализа составляют системы на базе нейросетей и искусственного интеллекта. Подмножеством сетевых систем обнаружения вторжений являются системы для наблюдения только за одним узлом сети (Network Node IDS).

Другой вид систем обнаружения вторжений представляют системы на базе хоста (Host Intrusion Detection Systems, HIDS). Они устанавливаются непосредственно на узлах и осуществляют наблюдение за целостностью файловой системы, системных журналов и т.д.

NIDS делятся в свою очередь на две большие категории: на основе сигнатур и на основе базы знаний. Сигнатурные IDS наиболее распространены и проще реализуются, но их легко обойти и они не способны распознавать новые атаки. В таких системах события, происходящие в сети, сравниваются с признаками известных атак, которые и называются сигнатурами. Если инструмент взлома модифицировать с целью изменения какой-либо части сигнатуры атаки, то, скорее всего, атака останется незамеченной. Кроме того, базы данных, содержащие сигнатуры, необходимо надежно защищать и часто обновлять. IDS на основе базы знаний следят за сетью, собирают статистику о её поведении в нормальных условиях, обнаруживают различные отклонения и помечают их как

подозрительные. Поэтому такие IDS еще называют основанными на поведении или статистическими.

Простейшую архитектуру IDS можно представить на рисунке 2.40.

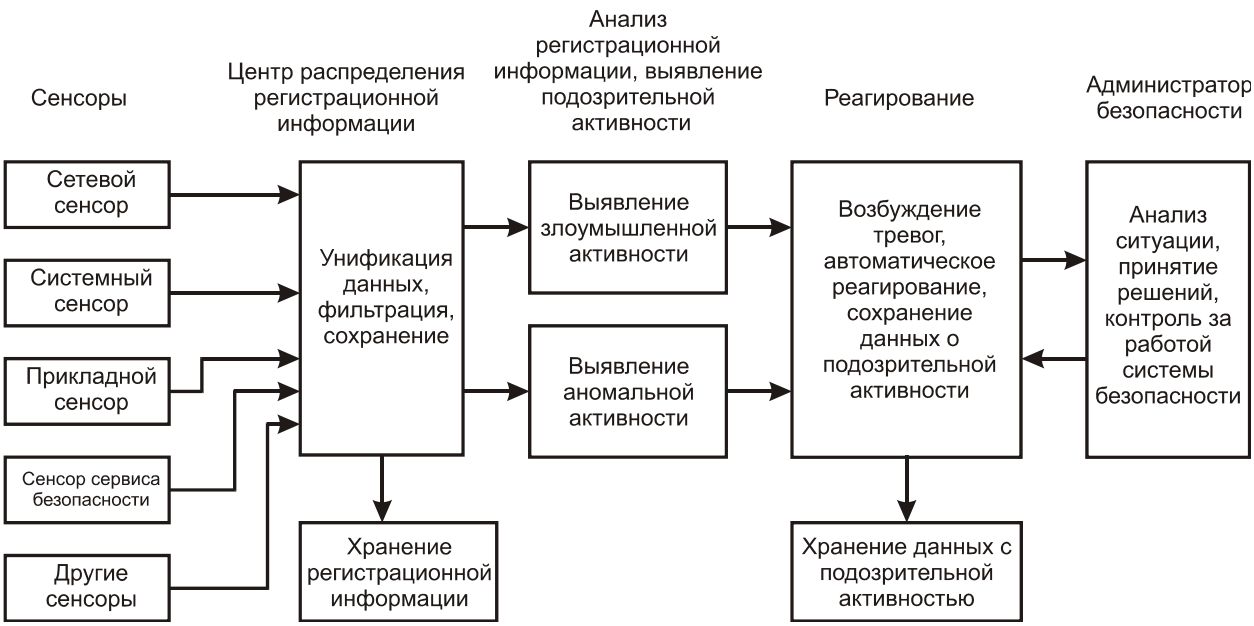


Рис. 2.40 Основные элементы архитектуры систем обнаружения вторжений

Для эффективной работы статистической IDS необходимо иметь надежную информацию о том, как ведет себя сеть в нормальных условиях, – точку отсчета. Хотя такую IDS обмануть сложнее, но и у нее есть свои проблемы – ложные срабатывания и трудности при обнаружении некоторых видов коммуникаций по скрытому каналу. Ложные срабатывания особенно вероятны в беспроводных сетях из-за нестабильности передающей среды. Кроме того, атаки, проведенные на ранних стадиях периода фиксации точки отсчета, могут исказить процедуру обучения статистической IDS, поэтому ее развертывание в промышленной сети – занятие рискованное. Как быть, если нормальное поведение сети уже изменено взломщиком в момент развертывания?

Хорошая IDS для беспроводной сети должна быть одновременно сигнатурной и статистической. Некоторые инструменты для проведения атак на беспроводные сети имеют четко выраженные сигнатуры. Если они обнаруживаются в базе данных, то можно поднимать тревогу. С другой стороны, у многих атак очевидных сигнатур нет, зато они вызывают отклонения от нормальной работы сети на нижних уровнях стека протоколов. Отклонение может быть малозаметным, например несколько пришедших не по порядку фреймов, или бросающимся в глаза, скажем, выросшая в несколько раз нагрузка. Обнаружение таких аномалий – это непростая задача, поскольку не существует двух одинаковых беспроводных сетей. То же относится и к проводным локальным сетям, но там хотя бы нет радиопомех, отражения, рефракции и рассеивания сигнала. Поэтому эффективное применение IDS в беспроводных сетях возможно только после длительного периода детального исследования сети. При разворачивании системы необходимо четко понимать, что, как и зачем мы хотим анализировать, и постараться ответить на эти вопросы чтобы сконструировать необходимую систему IDS (рис. 2.41).

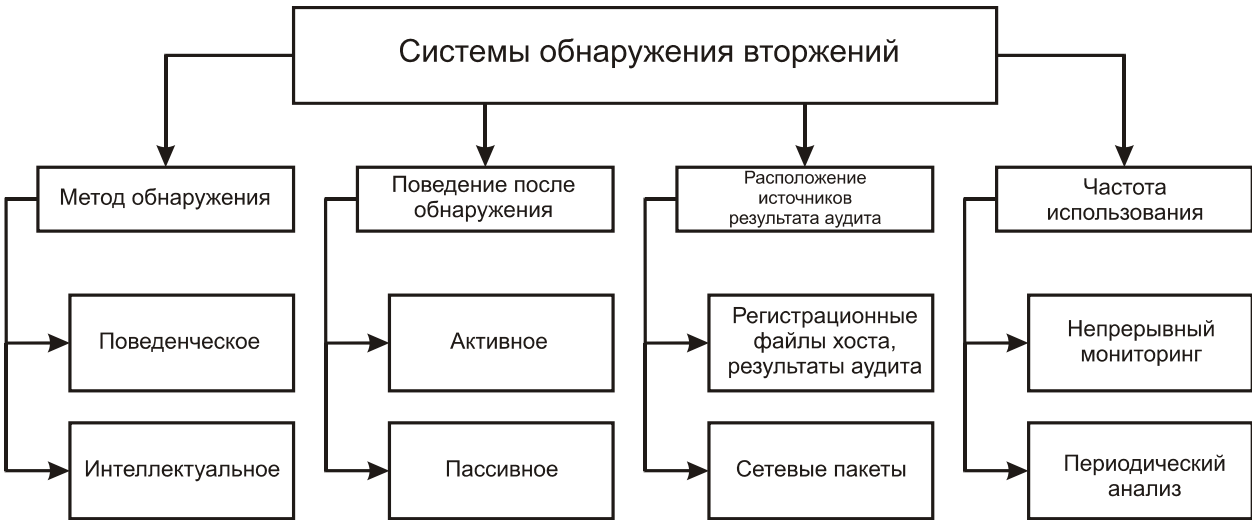


Рис. 2.41 Характеристики систем обнаружения вторжений

Только собрав значительный объем статистических данных о работе конкретной сети, можно решить, что является аномальным поведением, а что – нет, и идентифицировать проблемы со связью, ошибки пользователей и атаки. Многократные запросы на аутентификацию по протоколу 802.1x/LEAP могут свидетельствовать о попытке атаки методом полного перебора. Но это может объясняться и тем, что пользователь забыл свой пароль, или работой плохо написанного клиентского приложения, которое продолжает попытки войти в сеть, пока не будет введен правильный пароль. Увеличение числа фреймов-маяков может быть признаком DoS-атаки или присутствия в сети фальшивой точки доступа, но не исключено, что все дело в неисправной или неправильно сконфигурированной законной точке доступа. События, фиксируемые IDS на верхних уровнях стека протоколов, например большое число фрагментированных пакетов или запросов TCP SYN, может указывать на сканирование портов или DoS-атаку, но, возможно, это просто результат плохой связи на физическом уровне (уровень 1).

1) События на физическом уровне:
- наличие дополнительных передатчиков в зоне действия сети;
- использование каналов, которые не должны быть задействованы в защищаемой сети;
- перекрывающиеся каналы;
- внезапное изменение рабочего канала одним или несколькими устройствами, за которыми ведется наблюдение;
- ухудшение качества сигнала, высокий уровень шума или низкое значение отношения сигнал/шум.

Эти события могут свидетельствовать о наличии проблем со связью или с сетью, об ошибках, допущенных при конфигурировании сети, о появлении мошеннических устройств, о преднамеренном глушении либо об атаках «человек посередине» на уровень 1 или 2.

2) События, связанные с административными или управляющими фреймами:
- повышенная частота появления некоторых типов фреймов;
- фреймы необычного размера;
- фреймы неизвестных типов;
- неполные, испорченные или неправильно сформированные фреймы;
- затопление фреймами с запросами на отсоединение и прекращение сеанса;

- частое появление фреймов с запросом на повторное присоединение в сетях, где не включен роуминг;
- фреймы с неправильными порядковыми номерами;
- частое появление пробных фреймов;
- фреймы, в которых SSID отличается от SSID данной сети;
- фреймы с широковещательным SSID;
- фреймы с часто изменяющимися или случайными SSID;
- фреймы со значениями в поле SSID или других полях, типичными для некоторых инструментов вторжения;
- фреймы с MAC-адресами, отсутствующими в списке контроля доступа;
- фреймы с дублирующимися MAC-адресами;
- фреймы с часто изменяющимися или случайными MAC-адресами.

Эти события могут указывать на неправильную конфигурацию сети, проблемы со связью, сильные помехи, попытки применения инструментов активного сканирования сети, подделку MAC-адресов, присутствие в сети посторонних клиентов, попытки угадать или подобрать методом полного перебора закрытый SSID или на более изощренные атаки «человек посередине» на уровень 2, связанные с манипуляцией управляющими или административными фреймами.

3) События, связанные с фреймами протоколов 802.1x/EAP:
   - неполные, испорченные или неправильно сформированные фреймы протокола 802.1x;
   - фреймы с такими типами протокола EAP, которые не реализованы в данной беспроводной сети;
   - многократные фреймы запроса и ответа процедуры аутентификации EAP;
   - многократные фреймы с извещением о неудачной аутентификации EAP;
   - затопление фреймами начала и завершения сеанса EAP;
   - фреймы EAP аномального размера;
   - фреймы EAP с некорректным значением длины.
   - фреймы EAP с неправильными «верительными грамотами»;
   - фреймы EAP, приходящие от неизвестных аутентификаторов (фальшивая точка доступа);
   - незавершенная процедура аутентификации по протоколу 802.1x/EAP.

Эти события могут указывать на попытки прорваться через процедуру аутентификации, описанную в протоколе 802.1x, в том числе и путем размещения фальшивого устройства и проникновения в сеть с помощью атаки методом полного перебора или проведения изощренной DoS-атаки, направленной на вывод из строя механизмов аутентификации. Разумеется, неправильно сформированные фреймы могут возникать и в результате сильных радиопомех или других проблем на уровне 1.

4) События, связанные с протоколом WEP:
   - наличие незашифрованного беспроводного трафика;
   - наличие трафика, зашифрованного неизвестными WEP-ключами;
   - наличие трафика, зашифрованного WEP-ключами разной длины;
   - фреймы со слабыми IV;
   - идущие подряд фреймы с повторяющимися IV;
   - не изменяющиеся IV;
   - откат к WEP от более безопасного протокола, например TKIP;
   - ошибки при ротировании WEP-ключей.

Эти события могут указывать на серьезные ошибки при конфигурировании сети, на применение небезопасного устаревшего оборудования или на использование инструментов внедрения трафика опытным взломщиком.

5) События, связанные с общими проблемами связи:
   - потеря связи;
   - внезапный всплеск нагрузки на сеть;
   - внезапное уменьшение пропускной способности сети;
   - внезапное увеличение задержек в двухточечном канале;
   - повышенный уровень фрагментации пакетов;
   - частые повторные передачи.

Эти события заслуживают более пристального изучения для выявления точной причины ошибок. Механизм построения выводов, встроенный в IDS, должен уметь связывать события с различными возможными причинами, тем самым упрощая расследование.

6) Прочие события:
   - присоединившиеся, но не аутентифицированные хосты;
   - атаки на верхние уровни стека протоколов, вызывающие срабатывание «традиционной» IDS;
   - посторонний административный трафик, адресованный точке доступа;
   - постоянное дублирование или повтор пакетов с данными;
   - пакеты с данными, в которых испорчены контрольные суммы или MIC, формируемые на канальном уровне;
   - затопление многократными попытками одновременного присоединения к сети.

Эти события могут свидетельствовать об успешной или неудачной атаке, о наличии хоста с неправильными настройками безопасности, о попытках получить контроль над точкой доступа и изменить ее конфигурацию, о применении инструментов для внедрения трафика, о DoS-атаке против хостов с включенным протоколом 802.11i или о попытках переполнить буферы точки доступа большим числом запросов на соединение со стороны проводной или беспроводной части сети. Но, как и раньше, искажение фрейма или пакета может быть обусловлено проблемами на физическом уровне, например наличием помех или слабым уровнем сигнала.

Коммерческие системы IDS для беспроводных сетей.

Из коммерческих решений хорошо известны программы AirDefense Guard и Isomair Wireless Sentry. Они основаны на размещении сенсоров на территории.

ГЛАВА 3. АНТЕННЫ

3.1 ОПРЕДЕЛЕНИЕ АНТЕННЫ

Антенну можно определить как проводник, используемый для излучения или улавливания электромагнитной энергии из пространства. Для передачи сигнала радиочастотные электрические импульсы передатчика с помощью антенны преобразуются в электромагнитную энергию, которая излучается в окружающее пространство. При получении сигнала энергия электромагнитных волн, поступающих на антенну, преобразуется в радиочастотные электрические импульсы, после чего подаётся на приёмник.

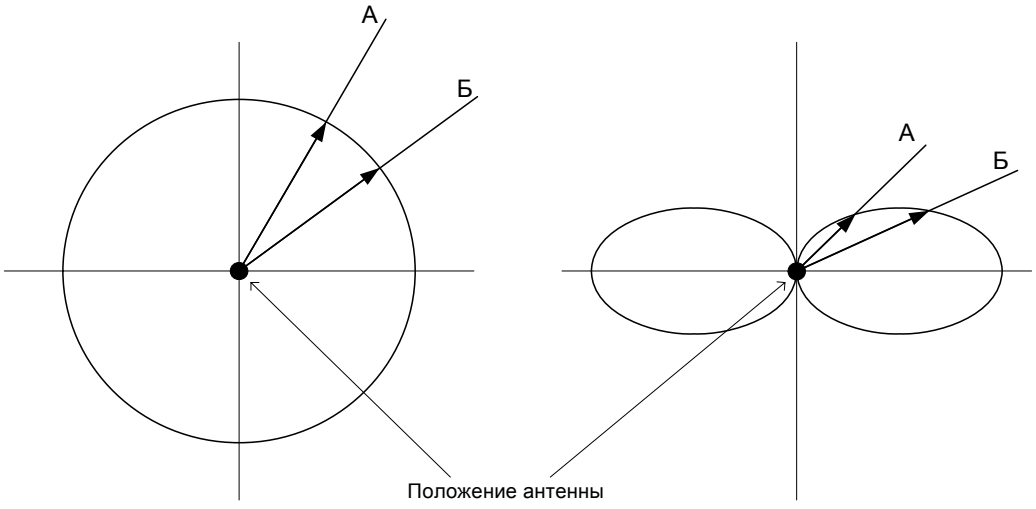
Как правило, при двусторонней связи одна и та же антенна используется как для приёма, так и для передачи сигнала. Такой подход возможен, потому что любая антенна с равной эффективностью поставляет энергию из окружающей среды к принимающим терминалам и от передающих терминалов в окружающую среду.

Для правильной настройки антенн, разберём некоторые её характеристики.

3.1.1 ДИАГРАММА НАПРАВЛЕННОСТИ

Антенны излучают энергию во всех направлениях. Однако в большинстве случаев эффективность передачи сигнала для различных направлении неодинакова. Наиболее распространенным способом определения эффективности антенны является *диаграмма направленности*, которая представляет собой зависимость излучающих свойств антенны от пространственных координат. Диаграммы направленности антенн представляются как двухмерное поперечное сечение трехмерной диаграммы.

Один из наиболее простых типов диаграммы направленности соответствует идеальному случаю так называемой изотропной антенны. Под *изотропной* антенной понимают точку в пространстве, которая излучает энергию одинаково во всех направлениях. Диаграмма направленности для изотропной антенны представляет собой сферу, центр которой совпадает с положением антенны (рис. 3.1а). Расстояние от антенны до любой точки диаграммы направленности прямо пропорционально энергии, которая была излучена антенной в данном направлении. На рис. 3.1б представлен еще один идеализированный случай — направленная антенна с одним выделенным направлением излучения (вдоль горизонтальной оси).



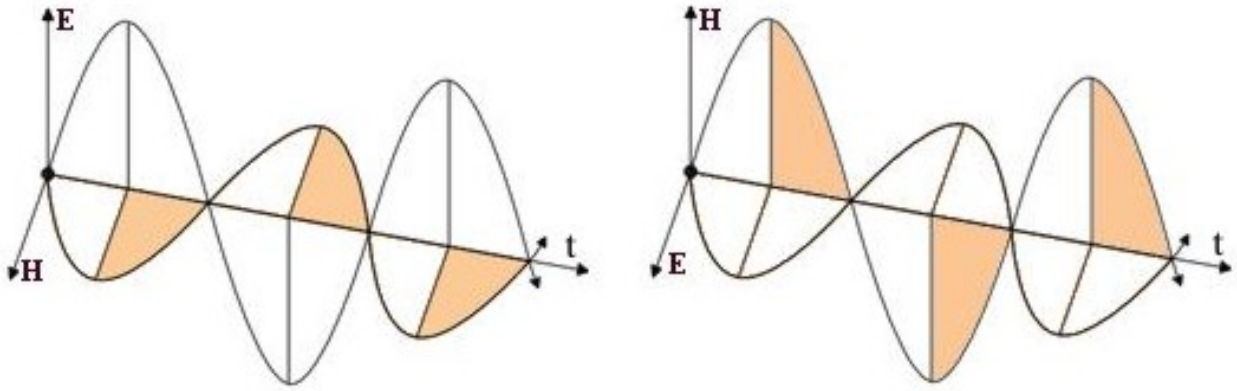
(а) Изотропная антенна (б) Направленная антенна

Рис. 3.1 Диаграммы направленности

Размер диаграммы направленности может быть произвольным. Важно лишь, чтобы в каждом направлении были соблюдены пропорции. Чтобы на основе относительного расстояния определить приведенную мощность в заданном направлении, от точки размещения антенны до пересечения с диаграммой направленности проводят прямую линию под соответствующим углом наклона. На рис. 3.1б для двух антенн сравниваются два угла передачи сигнала (А и Б). Изотропной антенне соответствует ненаправленная круговая диаграмма; векторы А и Б равны по величине.

3.1.2 ПОЛЯРИЗАЦИЯ АНТЕНН

Важной характеристикой антенны является её *поляризация*. В системах радиодоступа используют антенны с вертикальной, горизонтальной и круговой (с правым и левым вращением) поляризациями (рис. 3.2).



(а) (б)

Рис. 3.2 Вертикальная (а) и горизонтальная (б) поляризации

Учёт поляризации позволяет получить дополнительные энергетические преимущества при решении задач электромагнитной совместимости, планировании зон обслуживания и т. д. При заполнении определенного пространства точками доступа до предельного уровня, после которого взаимные радиопомехи начинают мешать нормальной работе сетей, достаточно изменить поляризацию антенн, после чего можно продолжать наращивать радиосеть.

В плоской электромагнитной волне векторы вертикального электрического ***E*** и магнитного ***H*** полей в каждый момент времени ориентированы в пространстве определённым образом. Поляризация электромагнитной волны является её пространственно-временно́й характеристикой и определяется видом траектории, описываемой концом вектора электрического поля в фиксированной точке пространства. На антеннах с поляризацией, на задней стороне есть указатель в виде стрелки, который и определяет необходимую поляризацию.

При круговой или циклической поляризации электромагнитное поле вращается вокруг оси *X* с определенным циклом, или шагом, так, что в разных точках пространства принимает или вертикальную или горизонтальную поляризацию. Такой вид поляризации сравнительно редко применяется.

3.1.3 КОЭФФИЦИЕНТЫ УСИЛЕНИЯ АНТЕНН

Коэффициент усиления является мерой направленности антенны. Данный параметр определяется как отношение мощности сигнала, излученного в определённом направлении, к мощности сигнала, излучаемого идеальной ненаправленной антенной в

любом направлении.

Коэффициент усиления антенны по отношению к дипольной антенне обычно дается в *дБ* (*dB*), а по отношению к изотропной – в *дБи* (*dBi*)

Впервые использованная для измерений интенсивности сигнала, единица измерения децибел была названа так в честь Александра Грэма Бэлла. Значения в децибелах вычисляются по логарифмической шкале, что позволяет обеспечить спецификацию характеристик в широком диапазоне напряжений или мощностей (см. (3.1) и (3.2)).

$$Б = Бел = \log_{10}\left(\frac{P_1}{P_2}\right) = 2 \cdot \log_{10}\left(\frac{V_1}{V_2}\right) \tag{3.1}$$

$$дБ = децибел = 10 \cdot \log_{10}\left(\frac{P_1}{P_2}\right) = 20 \cdot \log_{10}\left(\frac{V_1}{V_2}\right) \tag{3.2}$$

где

P_1 – измеренная мощность (*Вт*),

P_2 – эталонная мощность (*Вт*),

V_1 – измеренное напряжение (*В*),

V_2 – эталонное напряжение (*В*).

Пример 3.1:

Если на входе линии передачи уровень мощности сигнала составляет *100 мВт*, а на некотором расстоянии *50 мВт*, то ослабление сигнала можно выразить следующим образом:

$$L_{дБ} = 10 \lg \frac{100}{50} = 3 \text{ дБ}$$

В децибелах выражается относительное, а не абсолютное отличие сигналов. Ослабление сигнала с *10 Вт* на *5 Вт* также является ослаблением на *3 дБ*.

Пример 3.2:

Использование децибелов полезно при определении усиления или снижения мощности, происходящего на последовательности передающих элементов. Рассмотрим, например, последовательность элементов, на вход которой подаётся мощность *4 мВт*, первый элемент является кабельной сборкой с затуханием *12 дБ*, второй элемент - это усилитель с усилением *35 дБ*, а третий - ещё одна кабельная сборка с затуханием *10 дБ*. Суммарное усиление тракта равно *(-12+35-10)=13 дБ*. Вычисляем мощность на выходе:

$$G_{дБ} = 13 = 10 \lg \frac{P_{вых}}{4}$$

$$P_{вых} = 4 \times 10^{1,3} = 79{,}8 \text{ мВт}$$

Значения в децибелах связаны с относительными амплитудами или изменениями амплитуд, но никак не с абсолютными уровнями. Было бы удобно представить абсолютный уровень мощности также в децибелах, чтобы можно было легко вычислять усиление или снижение мощности по отношению к исходному сигналу. Поэтому в качестве эталонного уровня выбрана величина *1 Вт*, а абсолютный уровень мощности в *дБВт* или *dBW* (децибел-ватт). Он определяется следующим образом:

$$\text{мощность, дБВт} = 10 \lg \frac{\text{мощность, Вт}}{1 \text{ Вт}}$$

Широко используется и другая производная единица – *дБмВт* (*dBm*) (децибел-милливат). В этом случае за эталонный уровень мощности принимается *1 мВт*.

$$мощность, дБмВт = 10 \lg \frac{мощность, мВт}{1\ мВт}$$

Увеличение мощности сигнала в одном направлении возможно лишь за счёт остальных направлений распространения. Другими словами, увеличение мощности сигнала в одном направлении влечёт за собой уменьшение мощности в других направлениях. Необходимо отметить, что коэффициент усиления характеризует направленность сигнала, а не увеличение выходной мощности по отношению к входной (как может показаться из названия), поэтому данный параметр часто ещё называют коэффициентом направленного действия.

3.2 РАСПРОСТРАНЕНИЕ СИГНАЛА

При распространении сигнал, излученный антенной, может огибать поверхность Земли, отражаться от верхних слоев атмосферы либо распространяться вдоль линии прямой видимости.

3.2.1 ДИФРАКЦИЯ ЭЛЕКТРОМАГНИТНЫХ ВОЛН

При огибании поверхности Земли (см. рис. 3.3) путь распространения сигнала в той или иной степени повторяет контур планеты. Передача может производиться на значительные расстояния, намного превышающие пределы прямой видимости. Данный эффект имеет место для частот до 2 МГц. На способность сигналов, принадлежащих данной полосе частот, повторять кривизну земной поверхности влияет фактор *дифракции электромагнитных волн*. Данное явление связано с поведением электромагнитных волн при наличии препятствии.

Рис. 3.3 Распространение околоземных волн (частота до 2 МГц)

Рассеяние электромагнитных волн указанного диапазона в атмосфере происходит таким образом, что в верхние атмосферные слои эти волны не попадают.

3.2.2 РАСПРОСТРАНЕНИЕ ВОЛН ВДОЛЬ ЛИНИИ ПРЯМОЙ ВИДИМОСТИ

Если частота радиосигнала превышает 30 МГц, то огибание им земной поверхности и отражение от верхних слоев атмосферы становятся невозможными. В этом случае связь должна осуществляться в пределах прямой видимости (рис. 3.4).

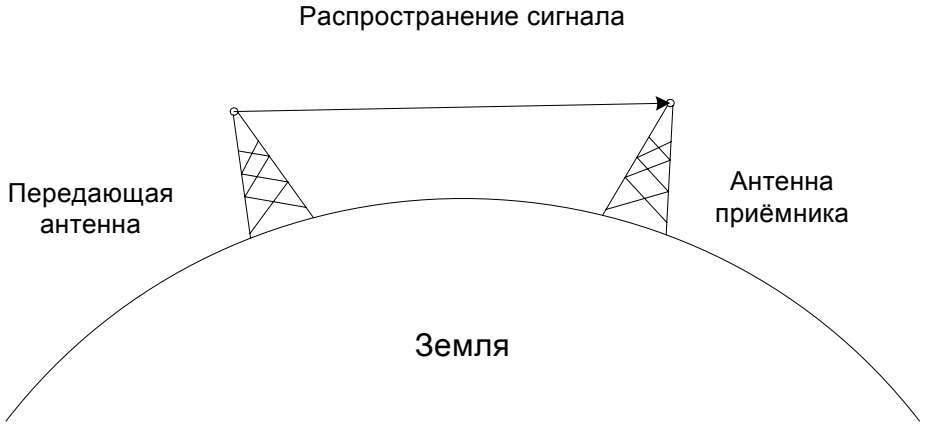


Рис. 3.4 Распространение сигнала вдоль линии видимости (частота свыше 30 МГц)

При связи через спутник сигнал с частотой свыше 30 МГц не будет отражаться ионосферой. Такой сигнал может передаваться от наземной станции к спутнику и обратно при условии, что спутник не находится за пределами горизонта. При наземной связи передающая и принимающая антенны должны находиться в пределах эффективной линии прямой видимости. Использование термина «эффективный» связано с тем, что волны сверхвысокой частоты искривляются и преломляются атмосферой. Степень и направление искривления зависят от различных факторов. Однако, как правило, искривления сверхвысокочастотных волн повторяют кривизну поверхности Земли. Поэтому такие волны распространяются на расстояние, превышающее оптическую линию прямой видимости. Так как связь между точками доступа, работающая в стандартах 802.11a, 802.11b и 802.11g обычно рассчитывается на линию прямой видимости, то в следующей главе рассмотрим, как влияет окружающая среда на полезный сигнал.

3.3 ПЕРЕДАЧА СИГНАЛА В ПРЕДЕЛАХ ЛИНИИ ПРЯМОЙ ВИДИМОСТИ

Для любой системы связи справедливо утверждение, что принимаемый сигнал отличается от переданного сигнала. Данный эффект является следствием различных искажений в процессе передачи. При передаче аналогового сигнала искажения приводят к его случайному изменению, что проявляется в ухудшении качества связи. Если же передаются цифровые данные, искажения приводят к появлению двоичных ошибок – двоичная единица может преобразоваться в нуль и наоборот. Рассмотрим различные типы искажений, а также их влияние на пропускную способность каналов связи в пределах прямой видимости. Наиболее важными являются следующие типы искажений:

- затухание или амплитудное искажение сигнала;
- потери в свободном пространстве;
- шум;
- атмосферное поглощение;

3.3.1 ЗАТУХАНИЕ

При передаче сигнала в любой среде его интенсивность уменьшается с расстоянием. Такое ослабление, или *затухание*, в общем случае логарифмически зависит от расстояния. Как правило, затухание можно выразить как постоянную потери интенсивности (в децибелах) на единицу длины. При рассмотрении затухания важны три фактора.

1) Полученный сигнал должен обладать мощностью, достаточной для его обнаружения и интерпретации приёмником.
2) Чтобы при получении отсутствовали ошибки, мощность сигнала должна

поддерживаться на уровне, в достаточной мере превышающем шум.

3) При повышении частоты сигнала затухание возрастает, что приводит к искажению.

Первые два фактора связаны с затуханием интенсивности сигнала и использованием усилителей или ретрансляторов. Для двухточечного канала связи мощность сигнала передатчика должна быть достаточной для четкого приема. В то же время интенсивность сигнала не должна быть слишком большой, так как в этом случае контуры передатчика или приемника могут оказаться перегруженными, что также приведет к искажению сигнала. Если расстояние между приемником и передатчиком превышает определенную постоянную, свыше которой затухание становится неприемлемо высоким, для усиления сигнала в заданных точках пространства располагаются ретрансляторы или усилители. Задача усиления сигнала значительно усложняется, если существует множество приемников, особенно если расстояние между ними и передающей станцией непостоянно.

Третий фактор списка известен как амплитудное искажение. Вследствие того, что затухание является функцией частоты, полученный сигнал искажается по сравнению с переданным, что снижает четкость приема. Для устранения этой проблемы используются методы выравнивания искажения в определенной полосе частот. Одним из возможных подходов может быть использование устройств, усиливающих высокие частоты в большей мере, чем низкие.

3.3.2 ПОТЕРИ В СВОБОДНОМ ПРОСТРАНСТВЕ

Для любого типа беспроводной связи передаваемый сигнал рассеивается по мере его распространения в пространстве. Следовательно, мощность сигнала, принимаемого антенной, будет уменьшаться по мере удаления от передающей антенны. Для спутниковой связи упомянутый эффект является основной причиной снижения интенсивности сигнала. Даже если предположить, что все прочие причины затухания и ослабления отсутствуют, переданный сигнал будет затухать по мере распространения в пространстве. Причина этого – распространение сигнала по всё большей площади. Данный тип затухания называют *потерями в свободном пространстве* и вычисляют через отношение мощности излучённого сигнала P_t к мощности полученного сигнала P_r. Для вычисления того же значения децибелах следует взять десятичный логарифм от указанного отношения, после чего умножить полученный результат на 10.

$$\frac{P_t}{P_r} = \frac{(4\pi)^2 (d)^2}{G_r G_t \lambda^2} \tag{3.3}$$

P_t – мощность сигнала передающей антенны;

P_r – мощность сигнала, поступающего на антенну приемника;

λ – длина волны несущей;

d – расстояние, пройденное сигналом между двумя антеннами;

G_t – коэффициент усиления передающей антенны;

G_r – коэффициент усиления антенны приемника.

Следовательно, если длина волны несущей и их разнесение в пространстве остаются неизменными, увеличение коэффициентов усиления передающей и приёмной антенн приводит к уменьшению потерь в свободном пространстве.

3.3.3 ШУМ

Для любой передачи данных справедливо утверждение, что полученный сигнал состоит из переданного сигнала, модифицированного различными искажениями, которые вносятся самой системой передачи, а также из дополнительных нежелательных сигналов,

взаимодействующих с исходной волной во время ее распространения от точки передачи к точке приема. Эти нежелательные сигналы принято называть *шумом*. Шум является основным фактором, ограничивающим производительность систем связи.

Шумы можно разделить на четыре категории:

- тепловой шум;
- интермодуляционные шумы;
- перекрестные помехи;
- импульсные помехи.

Тепловой шум является результатом теплового движения электронов. Данный тип помех оказывает влияние на все электрические приборы, а также на среду передачи электромагнитных сигналов.

Если сигналы разной частоты передаются в одной среде, может иметь место *интермодуляционный шум*. Интермодуляционным шумом являются помеха, возникающие на частотах, которые представляют собой сумму, разность или произведение частот двух исходных сигналов. Например, смешивание двух сигналов, передаваемых на частотах f_1 и f_2 соответственно, может привести к передаче энергии на частоте $f_1 + f_2$. При этом данный паразитный сигнал может интерферировать с сигналом связи, передаваемым на частоте $f_1 + f_2$.

С *перекрёстными помехами* сталкивался каждый, кто во время использования телефона переменно слышал разговор посторонних людей. Данный тип помех возникает вследствие нежелательного объединения трактов передачи сигналов. Такое объединение может быть вызвано сцеплением близко расположенных витых пар, по которым передаются множественные сигналы. Перекрестные помехи могут возникать во время приема посторонних сигналов антеннами. Несмотря на то, что для указанного типа связи используют высокоточные направленные антенны, потерь мощности сигнала во время распространения избежать все же невозможно. Как правило, мощность перекрёстных помех равна по порядку (или ниже) мощности теплового шума. Все указанные выше типы помех являются предсказуемыми и характеризуются относительно постоянным уровнем мощности. Таким образом, вполне возможно спроектировать систему передачи сигнала, которая была бы устойчивой к указанным помехам.

Однако кроме вышеперечисленных типов помех существуют так называемые *импульсные помехи*, которые по своей природе являются прерывистыми и состоят из нерегулярных импульсов или кратковременных шумовых пакетов с относительно высокой амплитудой. Причин возникновения импульсных помех может быть множество, в том числе внешние электромагнитные воздействия (например, молнии) или дефекты (поломки) самой системы связи.

3.3.4 АТМОСФЕРНОЕ ПОГЛОЩЕНИЕ

Причиной дополнительных потерь мощности сигнала между передающей и принимающей антеннами является атмосферное поглощение, при этом основной вклад в ослабление сигнала вносят водные пары и кислород. Дождь и туман (капли воды, находящиеся во взвешенном состоянии в воздухе) приводят к рассеиванию радиоволн и, в конечном счете, к ослаблению сигнала. Указанные факторы могут быть основной причиной потерь мощности сигнала. Следовательно, в областях, для которых характерно значительное выпадение осадков, необходимо либо сокращать расстояние между приемником и передатчиком, либо использовать для связи более низкие частоты.

3.4 ОТНОШЕНИЕ СИГНАЛ/ШУМ В ЦИФРОВЫХ СИСТЕМАХ СВЯЗИ

Очень важной характеристикой производительности цифровых систем связи

является отношение сигнал/шум.

Отношение сигнал/шум – это отношение энергии сигнала на 1 бит к плотности мощности шумов на 1 герц (E_b/N_0). Рассмотрим сигнал, содержащий двоичные цифровые данные, передаваемые с определенной скоростью – R бит/с. Напомним, что 1 Вт = 1 Дж/с, и вычислим удельную энергию одного бита сигнала: $E_b = ST_b$ (где S – мощность сигнала; T_b – время передачи одного бита). Скорость передачи данных R можно выразить в виде $R = 1/T_b$. Учитывая, что тепловой шум, присутствующий в полосе шириной 1 Гц, для любого устройства или проводника составляет

$$N_0 = kT \text{ (Вт/Гц)}, \tag{3.4}$$

где

N_0 – плотность мощности шумов в ваттах на 1 Гц полосы;

k – постоянная Больцмана, $k = 1{,}3803 \times 10^{-23}$ *Дж/К*;

T – температура в Кельвинах (абсолютная температура),

то, следовательно,

$$\frac{E_b}{N_0} = \frac{S/R}{N_0} = \frac{S}{kTR}. \tag{3.5}$$

Отношение E_b/N_0 имеет большое практическое значение, поскольку скорость появления ошибочных битов является (убывающей) функцией данного отношения. При известном значении E_b/N_0, требуемом для получения желаемого уровня ошибок, можно выбирать все прочие параметры в приведенном уравнении. Необходимо отметить, что для сохранения требуемого значения E_b/N_0 при повышении скорости передачи данных R потребуется увеличивать мощность передаваемого сигнала по отношению к шуму.

Довольно часто уровень мощности шума достаточен для изменения значения одного из битов данных. Если же увеличить скорость передачи данных вдвое, биты будут «упакованы» в два раза плотнее, и тот же посторонний сигнал приведёт к потере двух битов информации. Следовательно, при неизменной мощности сигнала и шума увеличение скорости передачи данных влечет за собой возрастание уровня возникновения ошибок.

Пример 3.3:

Рассмотрим метод кодирования сигнала, для которого необходимо, чтобы отношение E_b/N_0 равнялось *8,4 дБ* при частоте возникновения ошибок 10^{-4} (ошибочным является 1 бит из каждых 10000). Если эффективная температура теплового шума равна *290 К*, а скорость передачи данных 1 Мбит/с, какой должна быть мощность сигнала, чтобы преодолеть тепловой шум?

Решение:

По формуле (3.5) находим S:

$$S = \frac{E_b}{N_0} kTR$$

Для упрощения расчётов переведём это выражение в логарифмы:

$$S_{дБВт} = 10\log_{10}\left(\frac{E_b}{N_0} kTR\right) = \left(\frac{E_b}{N_0}\right)_{дБ} + 10\log_{10}(kTR)$$

Так как 1 Мбит = 1048576 бит, то

$$S_{дБВт} = 8{,}4 + 10\log_{10}(1{,}38 \cdot 10^{-23} \cdot 290 \cdot 1048576) = -135{,}37$$

или

$$S = 10^{\frac{S_{дБВт}}{10}} = 2{,}904 \cdot 10^{-14} \text{ Вт}$$

Следовательно, для того чтобы преодолеть тепловой шум необходима мощность - *135,37 дБВт*.

3.5 РАСЧЁТ ЗОНЫ ДЕЙСТВИЯ СИГНАЛА

3.5.1 РАСЧЁТ ДАЛЬНОСТИ РАБОТЫ БЕСПРОВОДНОГО КАНАЛА СВЯЗИ

Без вывода приведём формулу для расчёта дальности. Она берётся из инженерной формулы расчёта потерь в свободном пространстве:

$$FSL = 33 + 20(\lg F + \lg D)$$

где

FSL (free space loss) – потери в свободном пространстве (*дБ*);

F – центральная частота канала на котором работает система связи (*МГц*);

D – расстояние между двумя точками (*км*).

FSL определяется суммарным усилением системы. Оно считается следующим образом:

$$Y_{дБ} = P_{t,дБмВт} + G_{t,дБи} + G_{r,дБи} - P_{\min,дБмВт} - L_{t,дБ} - L_{r,дБ} \quad (3.6)$$

где

$P_{t,дБмВт}$ – мощность передатчика;

$G_{t,дБи}$ – коэффициент усиления передающей антенны;

$G_{r,дБи}$ – коэффициент усиления приемной антенны;

$P_{\min,дБмВт}$ – чувствительность приемника на данной скорости;

$L_{t,дБ}$ – потери сигнала в коаксиальном кабеле и разъемах передающего тракта;

$L_{r,дБ}$ – потери сигнала в коаксиальном кабеле и разъемах приемного тракта.

Для каждой скорости приёмник имеет определённую чувствительность. Для небольших скоростей (например, *1-2* Мегабита) чувствительность наименьшая: от *–90 дБмВт* до *–94 дБмВт*. Для высоких скоростей, чувствительность намного выше. В качестве примера в таблице 3.1 приведены несколько характеристик обычных точек доступа 802.11a,b,g.

Таблица 3.1 Зависимость чувствительность от скорости передачи данных

Скорость	**Чувствительность**
54 Мбит/с	-66 дБмВт
48 Мбит/с	-71 дБмВт
36 Мбит/с	-76 дБмВт
24 Мбит/с	-80 дБмВт
18 Мбит/с	-83 дБмВт
12 Мбит/с	-85 дБмВт
9 Мбит/с	-86 дБмВт
6 Мбит/с	-87 дБмВт.

В зависимости от марки радио-модулей максимальная чувствительность может немного варьироваться. Ясно, что для разных скоростей максимальная дальность будет разной.

FSL вычисляется по формуле:

$$FSL = Y_{дБ} - \mathrm{SOM} \quad (3.7)$$

где

SOM (*System Operating Margin*) – запас в энергетике радиосвязи (дБ). Учитывает возможные факторы отрицательно влияющие на дальность связи, такие как:

- температурный дрейф чувствительности приемника и выходной мощности передатчика;
- всевозможные погодные аномалии: туман, снег, дождь;
- рассогласование антенны, приёмника, передатчика с антенно-фидерным трактом.

Параметр *SOM* обычно берётся равным *10 дБ*. Считается, что *10*-ти децибельный запас по усилению достаточен для инженерного расчета.

Центральная частота канала *F* берётся из таблицы 3.2.

Таблица 3.2 Вычисление центральной частоты

Канал	Центральная частота (*МГц*)
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462
12	2467
13	2472
14	2484

В итоге получим формулу дальность связи:

$$D = 10^{\left(\frac{FSL}{20} - \frac{33}{20} - \lg F\right)}. \qquad (3.8)$$

Пример 3.4:

Найти расстояние, на котором будет стабильно работать связь на скоростях 56 Мбит/с и 6 Мбит/с для точки доступа DWL-2100AP и беспроводного адаптера DWL-G132. Их паспортные характеристики:

Мощность передатчиков DWL-2100AP и DWL-G132: 16 дБмВт;
Чувствительность DWL-2100AP на скорости 54 Мбит/с: -66 дБмВт;
Чувствительность DWL-2100AP на скорости 6 Мбит/с: -88 дБмВт;
Чувствительность DWL-G132 на скорости 54 Мбит/с: -66 дБмВт;
Чувствительность DWL-G132 на скорости 6 Мбит/с: -87 дБмВт;
Коэффициент усиления штатной антенны DWL-2100AP: 2 дБи.
Коэффициент усиления штатной антенны DWL-G132: 0 дБи.

Потерь в антенно-фидерном тракте, т.е. между беспроводными точками и их антеннами нет.

Решение:

1) Найдём расстояние на скорости 54 Мбит/с.

Параметр *FSL* равен

$$FSL = 16 + 2 - (-66) - 10 = 74 \text{ дБ}$$

По формуле (3.8) находим дальность работы беспроводного оборудования на данной скорости (в качестве примера возьмём шестой канал):

$$D_{54} = 10^{\left(\frac{74}{20} - \frac{33}{20} - \lg 2437\right)} = 0{,}046\ км \approx 50\ м$$

2) Найдём расстояние на скорости 6 Мбит/с.

FSL равен

$$FSL = 16 + 2 - (-88) - 10 = 96\ дБ$$

По формуле (3.8) находим дальность работы беспроводного оборудования на данной скорости:

$$D_6 = 10^{\left(\frac{96}{20} - \frac{33}{20} - \lg 2437\right)} = 0{,}579\ км \approx 580\ м$$

3.5.2 РАСЧЁТ ЗОНЫ ФРЕНЕЛЯ

Радиоволна в процессе распространения в пространстве занимает объем в виде эллипсоида вращения с максимальным радиусом в середине пролета, который называют *зоной Френеля* (рис. 3.5). Естественные (земля, холмы, деревья) и искусственные (здания, столбы) преграды, попадающие в это пространство, ослабляют сигнал.

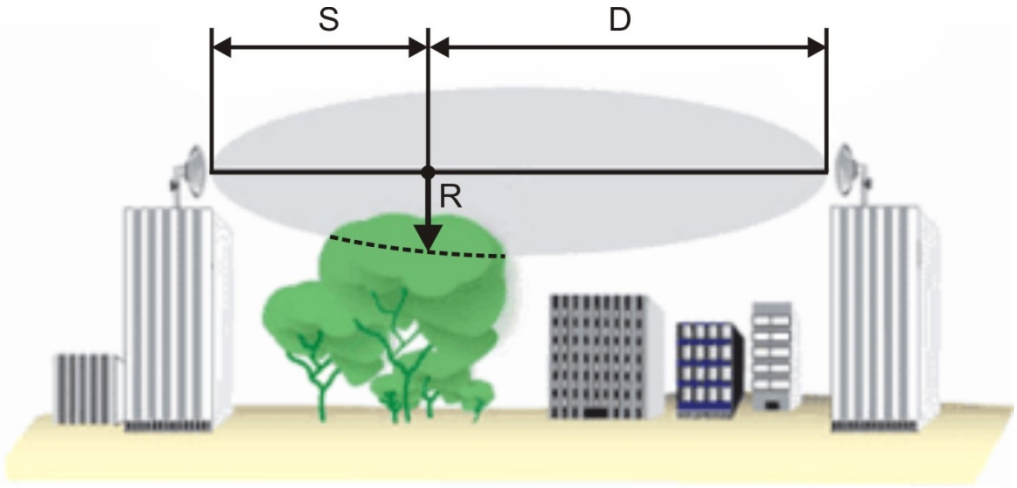


Рис. 3.5 Зона Френеля

Радиус первой зоны Френеля над предполагаемой преградой, может быть рассчитан с помощью формулы:

$$R = 17{,}3\sqrt{\frac{1}{f}\frac{SD}{S+D}} \qquad (3.9)$$

где

R – радиус зоны Френеля (м);

S, D – расстояние от антенн до самой высшей точки предполагаемого препятствия (км);

f – частота (ГГц).

Замечания:

- Обычно блокирование 20% зоны Френеля вносит незначительное затухание в канал. Свыше 40% затухание сигнала будет уже значительным, следует избегать попадания препятствий на пути распространения.
- Этот расчет сделан в предположении, что земля плоская. Он не учитывает кривизну земной поверхности. Для протяженных каналов следует проводить совокупный расчет, учитывающий рельеф местности и естественные преграды на пути распространения. В случае больших расстояний между антеннами следует

стараться увеличивать высоту подвеса антенн, принимая во внимание кривизну земной поверхности.

Пример 3.5:

Пусть расстояние между антеннами равно 10 км (см. рис. 3.5), предполагаемое препятствие от правой антенны находится на расстоянии 7 км и беспроводное оборудование работает на шестом канале.

Решение:

Подставив данные *S*, *D* и частоту канала из таблицы 3.2 в формулу (3.9), получим:

$$R = 17{,}3\sqrt{\frac{1}{2{,}437}\frac{3\cdot 7}{3+7}} = 16{,}06\ м\,.$$

Следовательно, чтобы затухание сигнала было минимальным, необходимо чтобы препятствие не заходило в зону Френеля с радиусом 16 *м*.

3.6 ПОСТРОЕНИЕ АНТЕННО-ФИДЕРНЫХ ТРАКТОВ И РАДИОСИСТЕМ С ВНЕШНИМИ АНТЕННАМИ

Задачи по подключению к беспроводному оборудованию дополнительных антенн, усилению мощности передатчика, включению в систему дополнительных фильтров довольно часто встречается в практике построения беспроводных сетей. И, как правило, на эту тему возникает много вопросов, самыми распространёнными из которых являются вопросы по соответствию разъемов на используемом оборудовании и дополнительных кабелях, а также вопросы по расчёту полученных систем.

Сразу необходимо отметить, что вынос антенны – это дело неблагодарное, потому как возникающие при этом негативные факторы, такие как затухание сигнала на кабельных сборках и увеличение уровня паразитных шумов, значительно ухудшают характеристики исходной радиосистемы. Вместе с тем, подключенные антенны (особенно с большими коэффициентами усиления) во многом компенсируют все эти негативные факторы, но, несмотря на это, при проектировании всё же стараются максимально сократить расстояние от порта активного оборудования точек доступа до вынесенной антенны и, по возможности, подключить антенну напрямую к точке доступа.

Очень часто бывают случаи, когда необходимо увеличить зону охвата внутри помещений, для этого используют антенны во внутреннем (*indoor*) исполнении. Для связи между домами или районами используют более дорогое оборудование во внешнем (*outdoor*) исполнении.

3.6.1 АНТЕННО-ФИДЕРНЫЙ ТРАКТ С УСИЛИТЕЛЕМ

На рис. 3.6 показана беспроводная система с антенно-фидерным трактом, в который включено множество элементов. Их может быть значительно больше, но здесь показаны наиболее часто используемые. Далее поясним, для чего используется тот или иной элемент, как он называется, и какие нюансы необходимо учесть при его использовании.

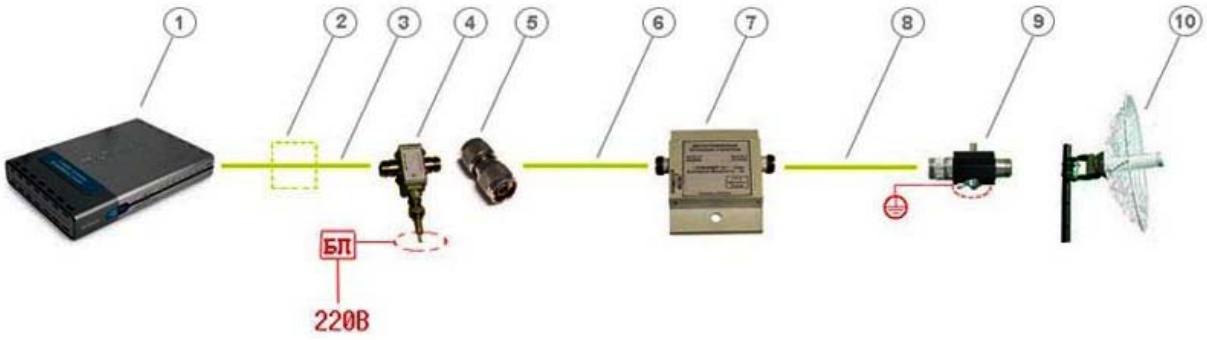


Рис. 3.6 Антенно-фидерный тракт с усилителем

1. *Точка доступа со съёмной антенной*

Почти всё беспроводное оборудование *D-Link* комплектуется съемными штатными антеннами 2–5 *дБи* (например, *DWL-2100AP, DWL-3200AP, DWL-8200AP, DWL-2700AP, DWL-7700AP, DWL-G520* и т.д.) – это означает, что штатную антенну можно легко снять и подключить вместо неё более мощную антенну с необходимым коэффициентом усиления и диаграммой направленности. В технических характеристиках беспроводного оборудования всегда сказано, каким типом антенн оно комплектуется по умолчанию.

Кроме поддерживаемых технологий и скоростных характеристик точка доступа имеет несколько важных физических характеристик, которые являются исходными данными для расчёта антенно-фидерного тракта и энергетических характеристик системы. К таким характеристикам относятся:

- мощность передатчика, которая измеряется или в милливаттах (*мВт*) или в децибел-милливаттах (*дБмВт*).
- чувствительность приёмника для определённой скорости – чем она выше, тем выше скорость.

2. *Полосовой фильтр*

Он показан пунктиром, потому как его довольно редко включают в систему, но, тем не менее, он присутствует в системах профессионального уровня. Принято думать, что кабель вносит только потери, связанные с длиной кабеля и достаточно выбрать кабель с малым затуханием или поставить усилитель, и все проблемы будут решены. Однако это не совсем так. В первую очередь, длинный кабель собирает помехи во всем диапазоне частот, поэтому работе будут мешать все радиоустройства, способные создать на входе приемника карты достаточно сильную помеху. Поэтому, часто случается, что в городской среде, в которой присутствует сильное зашумление, связь между точками доступа в системах с вынесенной на большое расстояние антенной работают крайне нестабильно, и поэтому в кабель необходимо включать дополнительный полосовой фильтр непосредственно перед входным разъемом точки доступа, который внесет еще потери не менее *1,5 дБ*.

Полосовые фильтры бывают настраиваемыми и с фиксированной центральной частотой, которая настраивается в процессе производства, например как у фильтров серии *NCS F24XXX*, поэтому желательно заранее определиться с требованиями по настройке и указать их при заказе. Фильтры различаются шириной полосы пропускания, которая определяет диапазон частот, которые не ослабляются.

3. *Кабельная сборка SMA-RP-plug↔N-type-male*

Часто её ещё называют «*pigtale*» – это небольшой переходник с антенного вывода *indoor* точки доступа, который называется *SMA-RP* (реверс *SMA*), на широко

используемый в антенно-фидерном оборудовании высокочастотный разъем *N-type* (рис. 3.7).

Рис. 3.7 Кабельная сборка «pigtale»

Pigtale-кабель входит в комплект поставки всех внешних (*outdoor*) антенн *D-Link*, антенны для внутреннего использования также комплектуются необходимыми кабелями. Вносит дополнительное затухание около 0,5 дБ.

4. *Инжектор питания*

Включается в тракт между активным оборудованием и входным портом усилителя (вносит затухание не более *0,5 дБ*) и подключается к блоку питания, который подключается к розетке *220В*. Инжектор имеет *2* порта – оба *N-type-female*. Инжектор питания и блок питания входят в комплект поставки усилителей.

5. *Переходник TLK-N-type-MM*

Переходник *N-Type Male-Male* (рис. 3.8) служит для изменения конфигурации порта с *female* на *male*, здесь мы его используем, чтобы подключить к инжектору следующую за ним кабельную сборку (стандартные кабельные сборки обычно имеют разъемы *N-type-male*↔*N-type-female*).

Рис. 3.8 Переходник TLK-N-type-MM

Общепринятым является, что коаксиальный разъем, устанавливаемый стационарно, например входы или выходы усилителей, фильтров, генераторов сигналов, разъемы для подключения, устанавливаемые на антеннах, имеют конфигурацию «гнездо» (*female*), а разъемы на подключаемых к ним кабелях, имеют конфигурацию «штекер» (*male*). Однако данное правило не всегда соблюдается, поэтому иногда возникают проблемы при сборке

тракта на элементах от различных производителей. Легко разрешить эту проблему позволяет использование переходника *N-type-male↔N-type-male*.

6. *Кабельная сборка (например, HQNf-Nm15)*

Это *15* метровая кабельная сборка *N-type (female)↔N-type (male)* (рис. 3.9).

Рис. 3.9 Кабельная сборка N-type (female)↔N-type (male)

Можно также использовать кабельные сборки больших длин, например, последовательно объединив две *15*-метровые сборки (или другие длины), важно только чтобы:

- уровень сигнала на входном порту усилителя попадал в допустимый диапазон, который указан в характеристиках усилителя
- уровень принятого от удалённой точки доступа сигнала и усиленного в усилителе, имел достаточную интенсивность для восприятия приёмником точки после прохождения кабельной сборки.

7. *Усилитель 2,4 ГГц (например, NCS24XX)*

Двунаправленный магистральный усилитель (рис. 3.10) предназначен для увеличения мощности передаваемого сигнала и повышения чувствительности канала приема в беспроводных сетях передачи данных, а также компенсации потерь в канале между радиомодемом и антенной.

Рис. 3.10 Усилитель 2,4 ГГц

Усилитель имеет внешнее исполнение и может быть установлен непосредственно на антенном посту. Использование усилителя позволяет организовать связь даже при самых неблагоприятных условиях соединения. При включении усилителя в радиосистему в значительной степени увеличивается зона её покрытия.

При использовании усилителей необходимо учитывать следующие моменты:

- если мощность передатчика точки доступа слишком велика и не попадает в диапазон допустимой интенсивности сигнала на входном порту усилителя, то использовать её с усилителем всё-таки можно, но необходимо включить в тракт между усилителем и точкой доступа кабельную сборку или какой-либо специальный элемент, затухание на котором обеспечит необходимое ослабление сигнала, с тем чтобы его интенсивность попала в допустимый диапазон. Ослабляя переданный сигнал, следует также помнить, что одновременно ослабляется и принятый сигнал, поэтому ослаблением не стоит увлекаться.

Пример 3.6:

Подключим к точке доступа с мощностью передатчика *200 мВт* усилитель *NCS2405*, на входе которого должно быть *10-100 мВт*, выходная мощность *500 мВт*. Для этого необходимо ослабить исходный сигнал на *100 мВт*, т.е. в два раза или на *3 дБ*, для этого включаем в схему десятиметровую кабельную сборку на основе кабеля с затуханием *0,3 дБ/м* на частоте *2,4 ГГц*.

- максимальное расстояние, на которое можно вынести усилитель от порта радиомодема, зависит от затухания на используемых элементах тракта; при этом необходимо чтобы уровень сигнала на входном порту усилителя попадал в допустимый диапазон, который указан в характеристиках усилителя, а так же чтобы уровень принятого от удалённого передатчика сигнала и усиленного в усилителе, имел достаточную интенсивность для восприятия приёмником после прохождения данной кабельной сборки.

Пример 3.7:

Посчитаем максимальное расстояние от активного порта *indoor* точки доступа (мощность *16 дБмВт*) до входного порта усилителя *NCS2401* для схемы на рис. 3.6. Погонное затухание на кабеле на частоте *2,4 ГГц* возьмём по *0,3 дБ/м*.

Решение:

Найдём суммарное затухание тракта до порта усилителя (считаем схему без фильтра):

Y = 0,5 дБ (pigtale)+0,5 дБ (инжектор)+6 дБ (*15*-метровая кабельная сборка (затухание на кабеле *0,3 дБ/м)+3* разъёма по *0,75 дБ*) = 7,75 дБ,

следовательно, мощность, которая попадёт на вход усилителя, будет равняться

16-7,75 = 8,25 дБмВт.

Для усилителя *NCS2401* нижняя граница допустимой интенсивности сигнала на входном порту равняется *4 мВт* (*6 дБмВт*). Следовательно, можно ещё увеличить длину кабельной сборки:

8,25-6=2,25 дБмВт;

2,25/0,3=7,5 м,

т.е. ещё примерно на *7,5* метров. Следовательно, максимальное расстояние кабельной сборки будет *22,5* метра.

Теперь посмотрим, что происходит с принятым сигналом. Предположим, что от удалённого передатчика на усилитель поступает сигнал мощностью *-98 дБмВт*; в режиме приёма коэффициент усиления усилителя равен *30 дБ*. Затухание тракта до порта радиомодема равно *10 дБ* (*7,75 дБ+2,25 дБ*). Найдём интенсивность сигнала поступившего на приёмник точки доступа: *-98+30-10=(-78 дБмВт)*. В таблице 3.1 смотрим чувствительность приёмника и находим скорость, на которой он может работать:

(-78 дБмВт) < (-76 дБмВт)

следовательно, при такой длине кабельной сборки точка доступа может работать на скорости 24 Мбит/с. Если нужна большая скорость, то необходимо, либо уменьшить длину кабельной сборки, либо взять усилитель с большим коэффициентом усиления.

В таблице 3.3 сведены все величины затухания от среды распространения сигнала.

Таблица 3.3 Затухание от среды распространения сигнала

Наименование	**Ед. изм.**	**Значение**
Окно в кирпичной стене	дБ	2
Стекло в металлической раме	дБ	6
Офисная стена	дБ	6
Железная дверь в офисной стене	дБ	7
Железная дверь в кирпичной стене	дБ	12,4
Стекловолокно	дБ	0,5 - 1
Стекло	дБ	3- 20
Дождь и туман	дБ/км	0,02 – 0,05
Деревья	дБ/м	0,35
Кабельная сборка pigtale	дБ	0,5
Полосовой фильтр NCS F24XXX	дБ	1,5
Коаксиальный кабель	дБ/м	0,3
Разъём N-type	дБ	0,75
Инжектор питания	дБ	0,5

8. *Кабельная сборка* (например, *HQNf-Nm1,5*)

HQNf-Nm1,5 – кабель (переходник) *N-type(female)↔N-type(male) длинной 1,5 м.*

9. *Модуль грозовой защиты*

В оборудовании *D-Link* идёт со всеми внешними антеннами. Имеет разъёмы *N-type(female)↔N-type(male)*.

10. *Внешняя направленная* (*например, ANT24-2100*)

Антенна с коэффициентом усиления *21 дБи*. Антенны имеют разъём: *N-type-female*.

3.6.2 ПРОСТОЙ АНТЕННО-ФИДЕРНЫЙ ТРАКТ

На рис. 3.11 представлена простая беспроводная система, в которой отсутствует усилитель, и антенно-фидерный тракт состоит только из пассивных элементов.

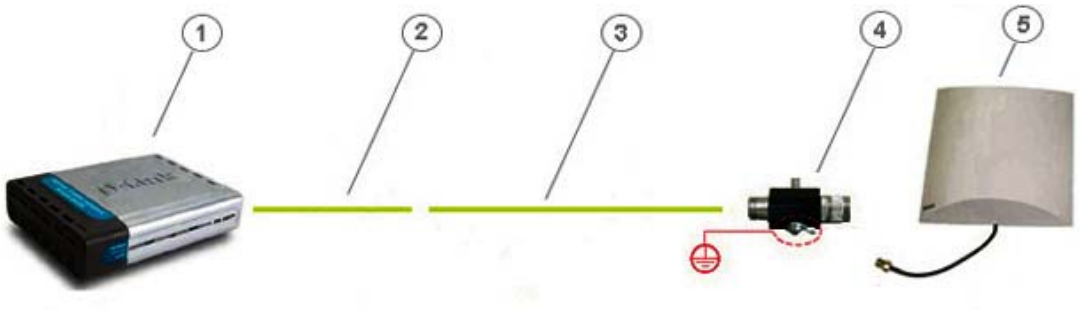


Рис. 3.11 Простой антенно-фидерный тракт

На рисунке 3.11 показаны:

1. точка доступа DWL-2100AP;
2. *pigtale* (в комплекте с антенной);
3. кабельная сборка;
4. модуль грозовой защиты (в комплекте с антенной);
5. антенна *ANT24-1400.*

Расстояние, на которое возможно вынести антенну в данном случае, сильно ограничивается мощностью передатчика точки доступа и затуханием, вносимым пассивными элементами. При выносе антенны на большое расстояние как принятый, так переданный сигнал может полностью поглотиться кабельными сборками и переходниками.

При использовании даже самой короткой кабельной сборки к антенне подводится мощность значительно меньшая исходной, что незамедлительно отразится на дальности действия радиосистемы. Поэтому мы рекомендуем использовать в таких схемах кабельные сборки не длиннее *6* метров и, по возможности, антенны с максимальным коэффициентом усиления.

3.6.3 ТОЧКА ДОСТУПА, ПОДКЛЮЧЁННАЯ НАПРЯМУЮ К АНТЕННЕ

Если подключить точку доступа напрямую к антенне, как это показано на рис. 3.12, исключив промежуточную кабельную сборку, то будет достигнута максимальная возможная для данного комплекта оборудования дальность связи.

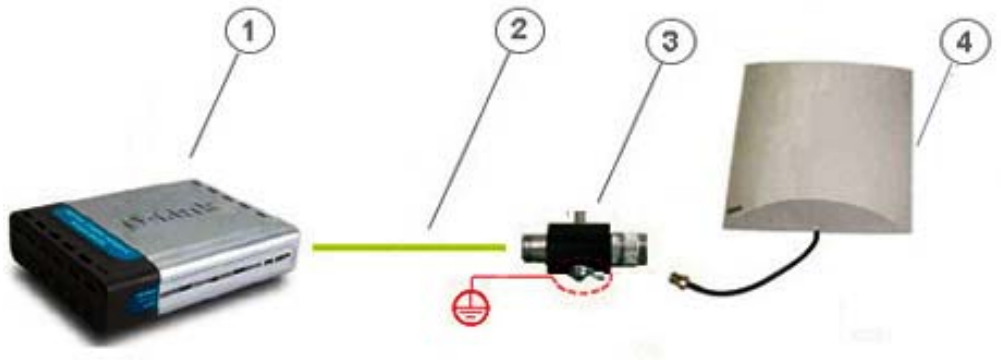


Рис. 3.12 Точка доступа, подключённая напрямую к антенне

На рисунке 3.12 показаны:

1. точка доступа *DWL-2100AP;*
2. *pigtale* (в комплекте с антенной);

3. модуль грозовой защиты (в комплекте с антенной);
4. антенна *ANT24-1400.*

В принципе, ради дальности иногда можно пожертвовать и модулем грозовой защиты, чтобы исключить вносимое им затухание, но лучше этого не делать. Эта схема довольно широко используется – это позволяет установить *indoor* точку доступа в непосредственной близости от антенного поста и минимизировать потери мощности сигнала.

Наиболее часто используемые антенны представлены в Приложении В.

ПРИЛОЖЕНИЕ А. ОБЗОР БЕСПРОВОДНОГО ОБОРУДОВАНИЯ D-LINK

Беспроводное оборудование компании D-Link представлено следующими сериями продуктов:

- Серия AirPlusG - предназначена для создания экономичных беспроводных сетей стандарта 802.11g в диапазоне частот 2,4 ГГц;
- Серия AirPlusXtremeG - предназначена для создания высокоскоростных беспроводных сетей стандарта 802.11g в диапазоне частот 2,4 ГГц;
- Серия AirPlusXtremeG с поддержкой технологии MIMO - предназначена для создания высокоскоростных беспроводных сетей стандарта 802.11g в диапазоне частот 2,4 ГГц с увеличенным радиусом действия;
- Серия AirPremierAG - предназначена для создания беспроводных сетей масштаба предприятия стандартов 802.11a/b/g в диапазоне частот 2,4/5 ГГц;
- Серия AirPremier - предназначена для создания беспроводных сетей масштаба предприятия и внешних сетей стандартов 802.11b/g в диапазоне частот 2,4 ГГц;

Экономичные решения для создания беспроводных сетей стандарта 802.11g

Оборудование серии AirPlusG является экономически-эффективным решением для создания беспроводных сетей дома или малого офиса. Данная серия продуктов включает беспроводную точку доступа, беспроводные маршрутизаторы, принт-серверы и PCI/CardBus/USB-адаптеры. Все оборудование функционирует на базе стандарта 802.11g на скорости до 54 Мбит/с и обратно совместимо с устройствами стандарта 802.11b. Для обеспечения защиты беспроводной сети в устройствах реализована поддержка современных протоколов шифрования данных WPA/WPA2. Настройка и управление осуществляется через удобный в использовании Web-интерфейс.

DWL-G700AP
AirPlusG беспроводная точка доступа 802.11g, до 54 Мбит/с

Рис. А.1 Беспроводная точка доступа DWL-G700AP

- Поддержка стандартов 802.11b/g
- 1 порт 10/100Base-TX
- Режимы работы: точка доступа, беспроводной повторитель
- Шифрование WEP, WPA и WPA2
- Поддержка протокола 802.1x

- Фильтрация MAC-адресов
- Функция отключения широковещания SSID
- DHCP клиент/сервер
- Web-интерфейс управления

DI-524/524UP
AirPlusG беспроводные маршрутизаторы 802.11g, до 54 Мбит/с

Рис. А.2 Беспроводной маршрутизатор DI-524UP

- Поддержка стандартов 802.11b/g
- 4 порта 10/100Base-TX LAN
- 1 порт USB 1.1 для подключения принтера (DI-524UP)
- Шифрование WEP, WPA и WPA2
- Поддержка протокола 802.1x
- NAT, VPN pass-through, фильтрация MAC/IP/URL
- DHCP клиент/сервер
- Web-интерфейс управления

Решения для создания высокоскоростных беспроводных сетей стандарта 802.11g

Для бизнес-приложений D-Link предлагает семейства оборудования AirPlusXtremeG, AirPremierAG и AirPremier позволяющие обеспечить высокий уровень защиты информации и поддерживающие скорость соединения в обоих диапазонах до 108 Мбит/с. Каждая серия беспроводных устройств представлена точкой доступа, многофункциональным шлюзом доступа и сетевыми адаптерами для шин PCI, PCMCIA, USB. Точки доступа, входящие в семейства AirPremier и AirPremierAG поддерживают стандарт 802.3af Power over Ethernet (PoE). В дополнение к этому все точки доступа поддерживают протокол сетевого управления SNMP v.3, который позволяет осуществлять настройку и удаленный мониторинг устройств в режиме реального времени из любого удобного места.

Скорость соединения до 108 Мбит/с достигается при работе в Турбо-режиме (*Turbo mode*). Этот режим может быть использован в двух подрежимах - *Dynamic Turbo* и *Static Turbo*.

При работе в режиме *Dynamic Turbo* устройства отслеживают эфир и анализируют возможные режимы работы взаимодействующих друг с другом клиентов. В случае если условия окружающей среды позволяют, радиолиния переводится в режим расширенной

полосы частот и устройства периодически отслеживают, не появился ли не поддерживающий Турбо-режимы клиент 802.11g. Если да, то система возвращается в обычный режим работы со скоростью соединения до 54 Мбит/с.

При работе в *Static Turbo* режим расширенного использования радиочастотного диапазона включен постоянно, при этом оборудование без поддержки Турбо-режимов такую сеть обнаружить не сможет. Скорость соединения в такой беспроводной сети будет максимально возможной, т.к. устройствам не приходится постоянно переключаться в обычный режим функционирования.

Функция *Super G without Turbo mode* включает в себя следующие механизмы повышения производительности (максимальная скорость соединения остается равной 54 Мбит/с):

Packet Bursting (Пакетная передача данных): техника пакетной передачи позволяющая увеличить пропускную способность благодаря отправке большего количества кадров за тот же временной интервал и уменьшению стандартных накладных расходов за счет отказа от промежуточных периодов ожидания DIFS (Distributed InterFrame Space).

Fast Frames (Быстрые кадры): технология пакетной агрегации повышает пропускную способность путём увеличения размера передаваемых кадров и уменьшения межкадровых интервалов.

Hardware Compression and Encryption (Аппаратное сжатие и шифрование): применение аппаратного сжатия по алгоритму Lempel-Ziv и шифрования данных. Увеличение пропускной способности осуществляется за счет предварительного сжатия информации

Функция *Super G with Turbo mode* включает в себя следующие механизмы повышения производительности Packet Bursting, Fast Frames, Hardware Compression and Encryption и Multi-Channel Bonding.

Multi-Channel Bonding (Объединение каналов): максимальное увеличение пропускной способности осуществляется за счет использования нескольких (двух) каналов передачи одновременно.

DWL-2100AP
AirPlusXtremeG беспроводная точка доступа 802.11g, до 108 Мбит/с

Рис. А.3 Беспроводная точка доступа DWL-2100AP

- Поддержка стандартов 802.11b/g
- 1 порт 10/100Base-TX

- Режимы работы: точка доступа, WDS с точкой доступа, WDS (мост), беспроводной повторитель, беспроводной клиент
- Шифрование WEP, WPA и WPA2
- Поддержка протокола 802.1x
- Фильтрация MAC-адресов
- Разделение WLAN STA
- 8 SSID для сегментации сети
- Функция отключения широковещания SSID
- 802.1Q VLAN Tagging
- Поддержка WMM (Wi-Fi Multimedia)
- DHCP клиент/сервер
- Web-интерфейс управления, протокол SNMP v.1, v.3, Telnet

DI-624/624S
AirPlusXtremeG беспроводные маршрутизаторы 802.11g, до 108 Мбит/с

Рис. А.4 Беспроводной маршрутизатор DI-624S

- Поддержка стандартов 802.11b/g
- 4 порта 10/100Base-TX LAN
- 2 порта USB 2.0 (DI-624S)
- Шифрование WEP, WPA и WPA2
- IP-маршрутизация
- NAT, SPI, DMZ, VPN pass-through, фильтрация MAC/IP/URL
- Поддержка QoS (DI-624S)
- 6 встроенных серверов (DI-624S)
- Web-интерфейс управления

DGL-4300
GamerLounge игровой маршрутизатор 802.11g, до 108 Мбит/с

Рис. А.5 Игровой маршрутизатор DGL-4300

- Поддержка стандартов 802.11b/g
- 4 порта 10/100/1000Base-T LAN
- 1 порт 10/100Base-TX WAN
- Антенна с коэффициентом усиления 5 dBi
- Поддержка WDS
- Поддержка технологии GameFuel™ Priority
- Шифрование WEP, WPA и WPA2
- NAT, VPN в режиме pass-through
- До 256 конфигураций межсетевых экранов для портов
- Политики контроля доступа («родительский» контроль)
- Ведение журнала событий на самом устройстве и внешнем сервере
- Статическая/динамическая маршрутизация
- Уведомления по электронной почте
- Высокопроизводительный центральный процессор для поддержки до 1000 одновременных соединений
- Web-интерфейс управления

DWL-2200AP
AirPremier управляемая точка доступа 802.11g с поддержкой PoE, до 108 Мбит/с

Рис. А.6 Беспроводная точка доступа DWL-2200AP

- Поддержка стандартов 802.11b/g
- 1 порт 10/100Base-TX
- Антенна с коэффициентом усиления 5 dBi
- Поддержка стандарта 802.3af PoE
- Режимы работы: точка доступа, WDS с точкой доступа, WDS (мост)
- Шифрование WEP, WPA и WPA2
- Поддержка шифрования AES
- Фильтрация MAC-адресов
- Функция отключения широковещания SSID
- 802.11i-ready
- DHCP клиент/сервер
- Web-интерфейс управления, протокол SNMP v.3, Telnet

DWL-3200AP
AirPremier управляемая точка доступа 802.11g с поддержкой PoE, до 108 Мбит/с

Рис. А.7 Беспроводная точка доступа DWL-3200AP

- Поддержка стандартов 802.11b/g
- 1 порт 10/100Base-TX
- 2 антенны с коэффициентом усиления 5 dBi
- Поддержка стандарта 802.3af PoE
- Металлический корпус с вентиляцией
- Режимы работы: точка доступа, мост «точка-точка», мост «точка- много точек»
- Шифрование WEP, WPA и WPA2
- Поддержка протокола 802.1x
- Фильтрация MAC-адресов
- 8 SSID для сегментации сети
- Функция отключения широковещания SSID
- 802.11i-ready
- DHCP клиент/сервер
- Web-интерфейс управления, протокол SNMP v.3, Telnet

DWL-7100AP
AirPremier AG трехрежимная двухдиапазонная беспроводная точка доступа 802.11a/b/g, до 108 Мбит/с

Рис. А.8 Беспроводная точка доступа DWL-7100AP

- Поддержка стандартов 802.11a/b/g
- 1 порт 10/100Base-TX
- Режимы работы: точка доступа, WDS с точкой доступа, WDS (мост), беспроводной повторитель, беспроводной клиент
- Шифрование WEP, WPA и WPA2
- Поддержка протокола 802.1x
- Фильтрация MAC-адресов
- Разделение WLAN STA
- Функция отключения широковещания SSID
- DHCP клиент/сервер
- Web-интерфейс управления, протокол SNMP v.3, Telnet

DI-784
AirPremier AG трехрежимный двухдиапазонный беспроводный маршрутизатор 802.11a/b/g, до 108 Мбит/с

Рис. А.9 Беспроводный маршрутизатор DI-784

- Поддержка стандартов 802.11a/b/g

- 4 порта 10/100Base-TX LAN
- 1 порт 10/100Base-TX WAN с поддержкой PPPoE
- Шифрование WEP, WPA и WPA2
- IP-маршрутизация
- NAT, SPI, DMZ, VPN pass-through, фильтрация MAC/IP/URL, виртуальный сервер
- Поддержка протокола Network Timing Protocol (NTP)
- Web-интерфейс управления

Решения на базе технологии MIMO

Благодаря поддержке технологии MIMO (Multiple Input Multiple Output) можно в 8 раз увеличить дальность передачи беспроводного сигнала..

MIMO-устройства, которые представлены беспроводным маршрутизатором DI-634M и беспроводными PCI и CardBus-адаптерами DWL-G520M и DWL-G650M передают информацию через множество антенн с высоким коэффициентом усиления. В процессе распространения радиосигналы обычно отражаются от объектов, встречающихся на их пути, создавая множество маршрутов, что приводит к их интерференции и затуханию. Устройства используют эффект многолучевого распространения для увеличения дальности передачи информации, объединяя сигналы принятые несколькими антеннами на разных частотах и повышая, за счет этого, мощность исходного сигнала. В результате сокращается количество «мертвых» зон и осуществляется передача мощных сигналов на большие расстояния с высокими скоростями, достаточными для работы потоковых приложений и передачи больших файлов.

Помимо технологии MIMO DI-634M, DWL-G520M и DWL-G650M поддерживают технологию 108G, благодаря чему на их основе можно строить надежные беспроводные сети, обеспечивающие высокую производительность и большой радиус действия. Поддержка устройствами расширенных функций сетевой безопасности обеспечивает защиту беспроводного соединения и доступа в Интернет.

DI-634M
AirPlusXtremeG беспроводной маршрутизатор 802.11g с поддержкой технологии MIMO, до 108 Мбит/с

Рис. А.10 Беспроводный MIMO-маршрутизатор DI-634M

- Поддержка стандартов 802.11b/g
- Поддержка технологии MIMO
- 4 порта 10/100Base-TX LAN
- 1 порт 10/100Base-TX WAN
- Шифрование WEP, WPA и WPA2
- Поддержка протокола 802.1x
- NAT, DMZ, VPN pass-through, DHCP, виртуальный сервер
- Web-интерфейс управления

Решения для создания внешних беспроводных сетей

Беспроводное оборудование, предназначенное для внешнего использования, специально разработано для функционирования в сложных климатических условиях и оборудовано прочным, водонепроницаемым корпусом со встроенным обогревателем и температурным датчиком. Кроме того, данное оборудование поддерживают стандарт IEEE 802.3af, что позволяет осуществлять его установку в местах, где нет доступных силовых розеток.

Семейство беспроводных устройств для внешнего использования представлено двумя точками доступа DWL-2700AP и DWL-7700AP. Устройства обладают расширенными функциями обеспечения безопасности, сетевого управления, включая протокол SNMP, и поддерживают несколько режимов работы, позволяя использовать их для создания надежных и хорошо управляемых беспроводных магистралей.

При объединении двух удаленных офисов или соединении двух локальных сетей, дальность действия, обеспечиваемая внешними точками доступа со штатными антеннами, может оказаться недостаточной. Расстояние передачи в этом случае можно значительно увеличить с помощью направленных и всенаправленных антенн, предназначенных для внешнего использования.

DWL-2700AP
AirPremier внешняя беспроводная точка доступа 802.11b/g, до 54 Мбит/с

Рис. А.11 Внешняя беспроводная точка доступа DWL-2700AP

- Поддержка стандартов 802.11b/g
- 1 порт 10/100Base-TX
- 2 антенны с коэффициентом усиления 5 dBi
- Поддержка стандарта 802.3af PoE
- Прочный корпус со встроенным обогревателем
- Режимы работы: точка доступа, WDS с точкой доступа, WDS (мост)
- Шифрование WEP, WPA и WPA2
- Поддержка протокола 802.1x
- Фильтрация MAC-адресов
- Multiple SSID для сегментации сети
- Разделение WLAN STA
- Функция отключения широковещания SSID
- 802.1Q VLAN Tagging
- Web-интерфейс управления, протокол SNMP v.3, Telnet

DWL-7700AP
AirPremier внешняя трехрежимная двухдиапазонная беспроводная точка доступа/мост802.11a/b/g, до 108 Мбит/с

Рис. А.12 Внешняя беспроводная точка доступа DWL-7700AP

- Поддержка стандартов 802.11a/b/g
- 1 порт 10/100Base-TX
- 2 антенны с коэффициентом усиления 5 dBi
- Поддержка стандарта 802.3af PoE
- Прочный корпус со встроенным обогревателем
- Режимы работы: точка доступа, WDS с точкой доступа, WDS (мост)
- Шифрование WEP, WPA и WPA2
- Поддержка протокола 802.1x
- Фильтрация MAC-адресов
- Multiple SSID для сегментации сети
- Разделение WLAN STA
- Функция отключения широковещания SSID
- 802.1Q VLAN Tagging
- Поддержка WMM (Wi-Fi Multimedia)
- Web-интерфейс управления, протокол SNMP v.3, Telnet

ПРИЛОЖЕНИЕ Б. ПРАВИЛА ИСПОЛЬЗОВАНИЯ РАДИОЧАСТОТНОГО СПЕКТРА

В соответствии со статьей 22 «**Регулирование использования радиочастотного спектра**» Федерального закона «О связи» в редакции от 09.02.2007 N 14-ФЗ:

Выдержка из статьи 22 ФЗ «О связи»
4. Использование в Российской Федерации радиочастотного спектра осуществляется в соответствии со следующими принципами:
разрешительный порядок доступа пользователей к радиочастотному спектру;
……..
платность использования радиочастотного спектра;
недопустимость бессрочного выделения полос радиочастот, присвоения радиочастот или радиочастотных каналов;
……
прозрачность и открытость процедур распределения и использования радиочастотного спектра.
5. Средства связи, иные радиоэлектронные средства и высокочастотные устройства, являющиеся источниками электромагнитного излучения, подлежат регистрации. Перечень радиоэлектронных средств и высокочастотных устройств, подлежащих регистрации, и порядок их регистрации определяются Правительством Российской Федерации.
Радиоэлектронные средства, используемые для индивидуального приема программ телевизионного вещания и радиовещания, сигналов персональных радиовызовов (радиопейджеры), электронные изделия бытового назначения и средства персональной радионавигации, не содержащие радиоизлучающих устройств, используются на территории Российской Федерации с учетом ограничений, предусмотренных законодательством Российской Федерации, и регистрации не подлежат.
Использование без регистрации радиоэлектронных средств и высокочастотных устройств, подлежащих регистрации в соответствии с правилами настоящей статьи, не допускается.

В соответствии со статьей 24 «**Выделение полос радиочастот и присвоение (назначение) радиочастот или радиочастотных каналов**», право на использование радиочастотного спектра предоставляется посредством выделения полос радиочастот и присвоения радиочастот или радиочастотных каналов. Использование радиочастотного спектра без соответствующего разрешения не допускается.

Присвоение радиочастот или радиочастотных каналов для радиоэлектронных средств (РЭС) гражданского назначения осуществляется Федеральным агентством связи (Россвязь) по заключению радиочастотной службы при Россвязи на основании заявлений граждан Российской Федерации или заявлений российских юридических лиц.

Порядок получения разрешений для беспроводных сетей в диапазоне 2,4 ГГц в России

1) Внутриофисные системы беспроводной передачи данных.

Порядок использования полосы радиочастот 2400-2483,5 МГц для внутриофисных систем передачи данных определен Решением ГКРЧ (Государственной Комиссии по радиочастотам) № 04-03-04-003 от 6 декабря 2004 г.. Это Решение значительно упростило процедуру получения разрешительных документов и определило возможность использования внутриофисного оборудования Wi-Fi без оформления разрешений на использование радиочастот.

Выдержка из Решения ГКРЧ № 04-03-04-003 от 6 декабря 2004 г.
3. Разрешить гражданам Российской Федерации и российским юридическим лицам использование на вторичной основе радиочастот в пределах полосы радиочастот 2400 - 2483,5 МГц для эксплуатации внутриофисных систем передачи данных, указанных в прилагаемом перечне (приложение № 2), на территории Российской Федерации без оформления разрешений на использование радиочастот, при выполнении следующих условий:
эксплуатации РЭС внутриофисных систем передачи данных только внутри зданий, закрытых складских помещений и производственных территорий;
регистрации РЭС внутриофисных систем передачи данных установленным в Российской Федерации порядком.

В приложение № 2 к Решению ГКРЧ № 04-03-04-003 включено, в частности, следующее внутриофисное оборудование D-Link:

DWL-1000AP+, DWL-1040AP+, DWL-900AP+, DWL-650+, DWL-520+, DWL-120+, DI-714P+, DI-614+, DWL-G520, DWL-G650, DWL-2100AP, DI-624, DWL-G520+, DWL-G650+, DWL-2000AP+, DI-624+, DI-724P+, DI-824VUP+, DSL-G604T, DWL-G120, DWL-G122, DWL-G510, DWL-G630, DWL-G730AP, DI-524, DWL-3200AP.

2) Уличные операторские сети беспроводной передачи данных.

Для получения разрешения на использование полосы частот 2400 – 2483,5 МГц (стандарты 802.11b/g) для эксплуатации РЭС этой группы применяется частично упрощенный порядок на основе Решения ГКРЧ от 25 сентября 2000 г. (протокол № 2/7). Для этих систем не требуется оформления частных решений ГКРЧ для каждого конкретного заявителя, при условии соответствия технических параметров беспроводного оборудования основным тактико-техническим характеристикам, определенным в Решении ГКРЧ №05-10-01-001 от 28 ноября 2005 года.

3) Bluethooth.

Порядок использования на территории Российской Федерации радиоэлектронных средств технологии Bluetooth, работающих в полосе частот 2400-2483,5 МГц определен Решением ГКРЧ № 25/2 от 31.03.03**.**

Данное Решение ГКРЧ определяет возможность использования, приобретения и эксплуатации радиоэлектронных средств технологи Bluetooth с максимальной излучаемой мощностью не более 2,5 мВт без оформления разрешений органов государственной радиочастотной службы и без последующей регистрации этих РЭС в указанных органах.

Радиоэлектронные средства технологи Bluetooth с максимальной излучаемой мощностью не более 100 мВт разрешается использовать при условии выполнения требований Решения ГКРЧ № 04-03-04-003.

Порядок получения разрешений для беспроводных сетей в диапазоне 5 ГГц в России

В диапазоне 5 ГГц порядок назначения радиочастот одинаковый как для уличных операторских сетей, так и для внутриофисных сетей беспроводной передачи данных.

Для получения разрешения на использование радиочастот в других диапазонах, в том числе в диапазоне 5 ГГц (стандарт 802.11a), необходимо предварительно получить частное Решение ГКРЧ.

Действующие решения ГКРЧ:

Решение ГКРЧ от 30 июля 2001 г. протокол № 11/1

Решение ГКРЧ от 23 декабря 2002 г.протокол № 23/5

Решение ГКРЧ №05-10-01-001 от 28 ноября 2005 г.

Ответственность

Статьи 24 «**Выделение полос радиочастот и присвоение (назначение) радиочастот или радиочастотных каналов**» и 25 «**Контроль за излучениями радиоэлектронных средств и (или) высокочастотных устройств**» Федерального закона «О связи» N 126-ФЗ в редакции от 09.02.2007 N 14-ФЗ определяют процедуры, связанные с нарушением условий, установленных при выделении полосы радиочастот и правил использования радиочастотного спектра.

Выдержка из статьи 24 ФЗ «О связи»

10. В случае выявления нарушения условий, установленных при выделении полосы радиочастот либо присвоении (назначении) радиочастоты или радиочастотного канала, разрешение на использование радиочастотного спектра пользователями радиочастотным спектром для радиоэлектронных средств гражданского назначения может быть приостановлено органом, выделившим полосу радиочастот либо присвоившим (назначившим) радиочастоту или радиочастотный канал в соответствии с пунктами 2 и 3 настоящей статьи на срок, необходимый для устранения этого нарушения, но не более чем на девяносто дней.

11. Разрешение на использование радиочастотного спектра прекращается во внесудебном порядке или срок действия такого разрешения не продлевается по следующим основаниям:

заявление пользователя радиочастотным спектром;

аннулирование лицензии на осуществление деятельности в области оказания услуг связи, если такая деятельность связана с использованием радиочастотного спектра;

истечение срока, указанного при присвоении (назначении) радиочастоты или радиочастотного канала, если этот срок не был продлен в установленном порядке или если заблаговременно, не менее чем за тридцать дней, не была подана заявка на его продление;

использование радиоэлектронных средств и (или) высокочастотных устройств в противоправных целях, наносящих вред интересам личности, общества и государства;

невыполнение пользователем радиочастотным спектром условий, установленных в решении о выделении полосы радиочастот либо присвоении (назначении) радиочастоты или радиочастотного канала;

невнесение пользователем радиочастотным спектром платы за его использование в течение тридцати дней со дня установленного срока платежа;

ликвидация юридического лица, которому было выдано разрешение на использование радиочастотного спектра;

неустранение нарушения, послужившего основанием для приостановления разрешения на использование радиочастотного спектра.

12. При наличии в документах, представленных заявителем, недостоверной или искаженной информации, повлиявшей на принятие решения о выделении полосы радиочастот либо присвоении (назначении) радиочастоты или радиочастотного канала, орган, выделивший полосу радиочастот либо присвоивший (назначивший) радиочастоту или радиочастотный канал, вправе обратиться в суд с требованием о прекращении или непродлении срока действия разрешения на использование радиочастотного спектра.

13. При прекращении или приостановлении разрешения на использование радиочастотного спектра плата, внесенная за его использование, не возвращается.

Выдержка из статьи 25 ФЗ «О связи»

1. Контроль за излучениями радиоэлектронных средств и (или) высокочастотных

устройств (радиоконтроль) осуществляется в целях:
проверки соблюдения пользователем радиочастотным спектром правил его использования;
выявления не разрешенных для использования радиоэлектронных средств и прекращения их работы;
выявления источников радиопомех;
выявления нарушения порядка и правил использования радиочастотного спектра, национальных стандартов, требований к параметрам излучения (приема) радиоэлектронных средств и (или) высокочастотных устройств;
обеспечения электромагнитной совместимости;
обеспечения эксплуатационной готовности радиочастотного спектра.
2. Радиоконтроль является составной частью государственного управления использованием радиочастотного спектра и международно-правовой защиты присвоения (назначения) радиочастот или радиочастотных каналов. Радиоконтроль за радиоэлектронными средствами гражданского назначения осуществляется радиочастотной службой. Порядок осуществления радиоконтроля определяется Правительством Российской Федерации.
В процессе радиоконтроля для изучения параметров излучений радиоэлектронных средств и (или) высокочастотных устройств, подтверждения нарушения установленных правил использования радиочастотного спектра может проводиться запись сигналов контролируемых источников излучений.
Такая запись может служить только в качестве доказательства нарушения порядка использования радиочастотного спектра и подлежит уничтожению в порядке, установленном законодательством Российской Федерации.
Использование такой записи в иных целях не допускается, и виновные в таком использовании лица несут установленную законодательством Российской Федерации ответственность за нарушение неприкосновенности частной жизни, личной, семейной, коммерческой и иной охраняемой законом тайны.

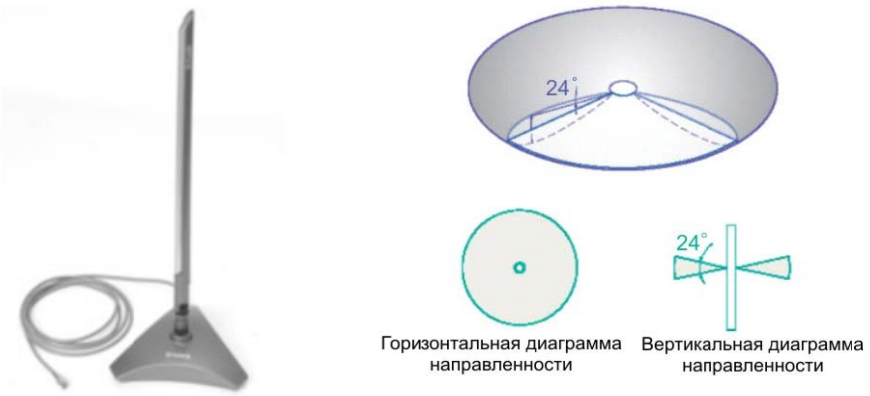
В соответствии с постановлением Правительства РФ от 30 июня 2004 г. № 318 контроль за излучением радиоэлектронных средств осуществляется Федеральной службой по надзору в сфере связи (Россвязьнадзор), территориальными органами Россвязьнадзора и их структурных подразделениями на основании Постановления Правительства РФ от 1 апреля 2005 г. N 175 «Об утверждении правил осуществления радиоконтроля в Российской Федерации».

Согласно статье 68 ФЗ «О связи» «**Ответственность за нарушение законодательства Российской Федерации в области связи**» случаях и в порядке, которые установлены законодательством Российской Федерации, лица, нарушившие законодательство Российской Федерации в области связи, несут уголовную, административную и гражданско-правовую ответственность.

ПРИЛОЖЕНИЕ В. ОБЗОР АНТЕНН D-LINK

Антенна ANT24-0700

Это всенаправленная антенна с высоким коэффициентом усиления 7 *дБи* (рис. В.1(а)). Диаграмма направленности показана на рис. В.1(б)



(а) (б)

Рис. В.1 Антенна ANT24-0700

Антенна *D-Link ANT24-0700* – это всенаправленная антенна с высоким коэффициентом усиления, предназначенная для использования в помещении в диапазоне частот *2,4 ГГц*. Ее можно использовать с беспроводными устройствами *802.11b* и *802.11g*, такими как точки доступа и удаленные маршрутизаторы. Антенну можно использовать для замены стандартной антенны беспроводного устройства для увеличения радиуса действия. Она может быть подключена к беспроводному устройству через кабель (входящий в комплект поставки антенны) или напрямую.

Антенна ANT24-0800

Это всенаправленная антенна для внутреннего и внешнего использования с коэффициентом усиления 8 *дБи* (рис. В.2(а)). Диаграмма направленности показана на рис. В.2(б).

(а) (б)

Рис. В.2 Антенна ANT24-0800

D-Link ANT24-0800 подключается к беспроводным устройствам, работающим в частотном диапазоне *2,4 ГГц* для увеличения площади покрытия беспроводной сети. Данная модель имеет 360-градусную зону охвата (в горизонтальной плоскости) и 15-градусную зону охвата по вертикали. *D-Link ANT24-0800* поставляется с кабелем – переходником, позволяющим подключать антенну к беспроводным устройствам с реверсным разъемом *SMA-RP-plug*. Комплект поставки включает в себя: набор крепежа, модуль грозовой защиты и заземления, кабель-переходник.

Корпус антенны сделан устойчивым к погодным явлениям, что позволяет использовать ее не только внутри помещений. Антенна также имеет шарнирное соединение, позволяющее точнее настроить угол наклона антенны для хорошего приема.

Антенна ANT24-0801

Это всенаправленная антенна для внутреннего и внешнего использования с коэффициентом усиления 8,5 *дБи* (рис. В.3(а)). Диаграмма направленности показана на рис. В.3(б).

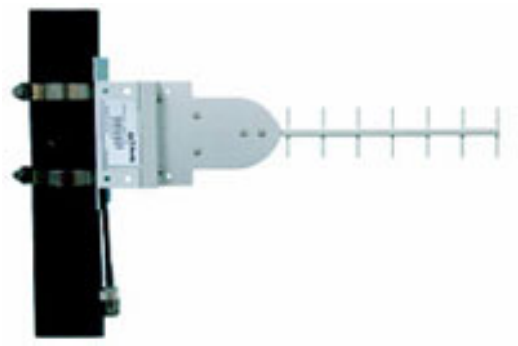
(а) (б)

Рис. В.3 Антенна ANT24-080

Антенна работает в диапазоне частот *2,4 ГГц*, что позволяет ее использовать совместно с аппаратурой, выпускаемой для медицины и науки. Антенна *ANT24-0801* подключается к беспроводным устройствам, имеющим реверсный *SMA-RP*-разъем и предоставляет возможность расширить площадь покрытия существующей беспроводной сети, работающей в диапазоне *2,4 ГГц*. Корпус антенны сделан устойчивым к погодным явлениям, что позволяет использовать ее не только внутри помещений. В комплект поставки антенны включен модуль грозовой защиты и 3-х метровый кабель расширения.

Антенна ANT24-1201

Это направленная внешняя антенна, коэффициент усиления *12 дБи* (рис. В.4(а)). Диаграмма направленности показана на рис. В.4(б).



(а)

(б)

Рис. В.4 Антенна ANT24-1201

Направленная внешняя антенна *D-Link ANT24-1201* подключается к беспроводным устройствам, работающим в частотном диапазоне *2,4 ГГц* для увеличения площади покрытия беспроводной сети.

Корпус антенны сделан из устойчивого к погодным явлениям материала.

Антенна поставляется с кабелем – переходником, позволяющим подключать антенну к беспроводным устройствам с реверсным разъемом *SMA-RP*. Комплект поставки состоит из набора крепежа, модуля грозовой защиты и заземления, кабеля–переходника.

Теоретическое расстояние передачи при скорости *1 Мбит/с/11 Мбит/с*:

- при работе с внутренними точками доступа до *1,5км/500м*;
- при работе с внешними точками доступа до *2,5км/1км*.

Антенна ANT24-1801

Это направленная антенна, коэффициент усиления *18 дБи* (рис. В.5(а)). Диаграмма направленности показана на рис. В.5(б).

(а) (б)

Рис. В.5 Антенна ANT24-1801

Антенна работает в диапазоне частот *2,4 –2,5 ГГц*, что позволяет ее использовать совместно с аппаратурой, выпускаемой для медицины и науки.

Антенна *ANT24-1801* подключается к беспроводным устройствам, имеющим реверсный *SMA-RP*-разъем и предоставляет возможность расширения площади покрытия существующей беспроводной сети, работающей в диапазоне *2,4 ГГц*.

В комплект поставки антенны входит крепеж для монтажа, кабель-переходник для разъема *RP-SMA* и модуль грозовой защиты.

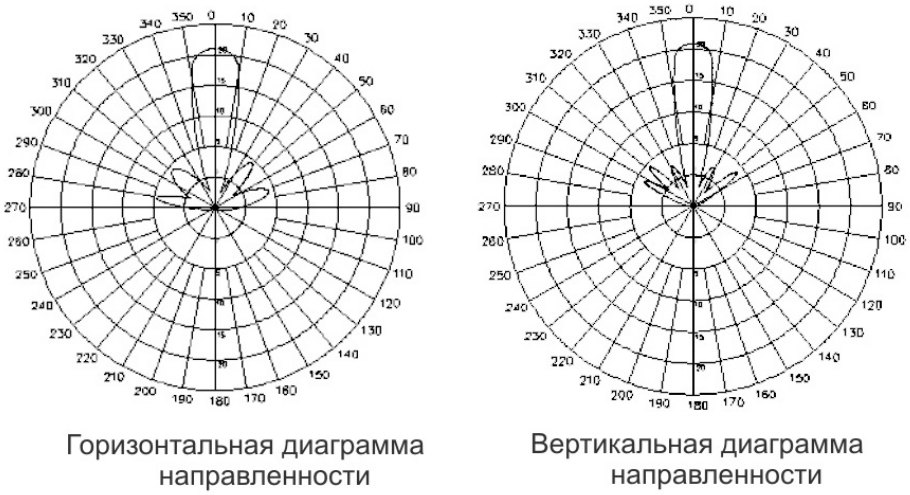
Теоретическое расстояние передачи при скорости *1 Мбит/с/11 Мбит/с*:

- при работе с внутренними точками доступа до *5км/2км*;
- при работе с внешними точками доступа до *8км/3км*.

Антенна ANT24-2100

Параболическая антенна с высоким коэффициентом усиления, 21 *дБи* (рис. В.6(а)). Диаграмма направленности показана на рис. В.6(б).

(а)



(б)

Рис. В.6 Антенна ANT24-2100

D-Link ANT24-2100 подключается к беспроводным устройствам стандартов *802.11b* и *802.11g* (*2,4 ГГц*).

Антенна предоставляет возможность существенно расширить площадь покрытия существующей беспроводной сети и/или создать беспроводной мост для передачи данных на большие расстояния.

Через кабель-переходник *SMA-RP↔N-Type*, входящий в комплект поставки антенны, *ANT24-2100* легко подключается к любым внутриофисным точкам доступа и беспроводным адаптерам *D-Link*, со съемными штатными антеннами. Сама антенна имеет разъем для подключения *N*-типа (*N-type-female*) , что позволяет подключать её к внешним точкам доступа *D-Link*, а так же к активному оборудованию других производителей.

Высокий коэффициент направленности антенны (*21 дБи*) позволяет строить радиомосты на большие расстояния. Теоретическая дальность передачи при использовании *ANT24-2100* совместно с активным оборудованием *2,4 ГГц* мощностью *35 мВт* (такую мощность имеют внутриофисные точки доступа *D-Link*, например *DWL-2100AP*, *DWL-3200AP*, *DWL-8200AP*) на обоих концах беспроводного канала связи (без использования дополнительных кабельных сборок) для скорости *1 Мбит/с* составляет около *10 км*.

В комплект поставки *ANT24-2100* входит модуль грозовой защиты и крепеж на мачту и на стену.

ГЛОССАРИЙ

801.11 - стандарт IEEE, в котором определяется порядок доступа к передающей среде и приводятся спецификации физического уровня для беспроводных локальных сетей со скоростью до 2 Мбит/с. Стандарт 802.11 распространяется на высокочастотные радиоканалы DSSS и FHSS, а также на инфракрасные каналы.
802.11a - редакция стандарта 802.11 IEEE, в которой рассматриваются сети, работающие со скоростями до 54 Мбит/с по технологии DSSS.
802.11b - редакция стандарта 802.11 IEEE, в которой рассматриваются сети, работающие со скоростями до 11 Мбит/с по технологии DSSS.
802.1lg - редакция стандарта 802.11 IEEE, в которой рассматриваются сети, работающие со скоростями до 54 Мбит/с по технологии DSSS, обратно совместимые со стандартом 802.11b.
802.1li - стандарт IEEE, относящийся к безопасности беспроводных сетей. В нем объединены протоколы 802.1x и TKIP/CCMP с целью обеспечить аутентификацию пользователей, конфиденциальность и целостность данных в беспроводных локальных сетях.
802.1x - стандарт IEEE аутентификации и контроля доступа на канальном уровне.
Access point (точка доступа) - тип базовой станции, которую беспроводная локальная сеть использует для обеспечения взаимодействия беспроводных пользователей с проводной сетью и осуществления роуминга в пределах здания.
Ad Hoc mode (режим одноранговой сети) - конфигурация беспроводной сети, при которой пользователи могут непосредственно устанавливать соединения между своими устройствами, обходясь без услуг базовой станции. В этом режиме могут работать беспроводные персональные и локальные сети.
Autentificator (Аутентификатор) - в протоколе 802.1x посредник между сервером аутентификации, например RADIUS, и претендентом. В беспроводных сетях обычно размещается на точке доступа; в проводных сетях эту функцию могут выполнять высококлассные коммутаторы.
Bluetooth - часть спецификации 802.15 для беспроводных персональных сетей, разработанная и поддерживаемая группой Bluetooth SIG, которая была основана компаниями Ericsson, Nokia, IBM, Intel и Toshiba.
BSS (Basic Service Set) (Базовый набор служб) - базовая сота в сети 802.11, состоящая из одной точки доступа и присоединившихся к ней клиентов.
CCMP (Counter Mode with CBC MAC) - основанный на алгоритме AES протокол шифрования, который должен заменить WEP и TKIP. Считается обязательным в спецификации WPA версии 2.
CDMA (Code Division Multiple Access) - множественный доступ с кодовым разделением каналов. Процесс, при котором каждый пользователь модулирует свои сигналы отличным от других кодом во избежание возникновения взаимных помех.
Clear-To-Send (CTS) (Готов к передаче) - управляющий фрейм в стандарте 802.11, применяемый для обнаружения виртуальной несущей. Фрейм CTS посылается в ответ на фрейм RTS. Он разрешает запрашивающему хосту передавать данные в течение времени, указанного в поле Network Allocation Vector.
CRC (Cyclic Redundancy Check) (Код циклической избыточности) - основной математический алгоритм вычисления контрольной суммы для проверки целостности передаваемых данных. Часто вычисляется путем деления длины фрейма на простое число, легко может быть изменён противником.
CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) - протокол второго уровня, применяемый для устранения коллизий в сетях 802.11 с множественным доступом с контролем несущей. Станции только тогда пытаются осуществить передачу, когда этого

не делает ни одна другая станция сети. В противном случае происходит коллизия и станции приходится повторно передавать данные.
dBi - децибелы, отнесенные к идеальной изотропной антенне.
dB - децибелы, отнесенные к полуволновому диполю.
DCF (Distributed Coordination Function) - распределенная функция координации. Часть стандарта 802.11, определяющая, как станции должны конкурировать за право доступа к среде передачи. Для регулирования трафика сети DCF использует технологию CSMA.
DSSS (Direct Sequence Spread Spectrum) - один из двух подходов к передаче радиосигналов с изменяемым спектром. При использовании технологии DSSS поток передаваемых данных разбивается на небольшие кусочки, каждому из которых выделяется широкополосный канал. На передающем конце информационный сигнал комбинируется с последовательностью битов, передаваемых с более высокой скоростью, которая разделяет данные в соответствии с коэффициентом изменения.
EAP (Extensible Authentication Protocol) - гибкий протокол аутентификации, первоначально спроектированный для аутентификации в протоколе PPP, а позже включенный в стандарт 802.1x.
EAPOL (EAP over LAN EAP) - инкапсуляции фреймов протокола EAP в проводных локальных сетях. Определяется отдельно для Ethernet и Token Ring.
EIRP (Эффективная изотропно излучаемая мощность) - реальная выходная мощность, излучаемая антенной, рассчитываемая как IR + коэффициент усиления антенны.
ESSID (Extended Service Set ID) - имя, идентифицирующее сеть 802.11. Чтобы присоединиться к беспроводной локальной сети, нужно знать ее ESSID.
ETSI (European Telecommunications Standards Institute) (Европейский институт стандартов телекоммуникаций) некоммерческая организация, выпускающая стандарты и правила в области телекоммуникаций для всей Европы.
FDMA (Frequency Division Multiple Access) - множественный доступ с частотным разделением. Процесс, в ходе которого относительно широкий частотный диапазон делится на узкие поддиапазоны. Каждый пользователь передает речь и данные в выделенном для него поддиапазоне.
FHSS (Frequency Hopping Spread Spectrum) - изменение спектра скачкообразной перестройкой частоты). Один из двух подходов к передаче радиосигнала с изменяемым спектром. Характеризуется тем, что несущая частота псевдослучайным образом «скачет» в пределах определенного диапазона.
FSK (Frequency Shift Keying) – частотная манипуляция. Процесс модуляции, при которой слегка изменяется частота несущего сигнала, за счет чего осуществляется представление информации способом, подходящим для ее передачи через воздушную среду.
ICV (Integrity Check Value) (Код контроля целостности) - простая контрольная сумма, вычисляемая для фрейма 802.11 перед началом шифрования по протоколу WEP.
IV (Initialization Vectors) (Вектор инициализации) – дополнительные несекретные двоичные данные для шифрования известного или предсказуемого открытого текста с целью введения добавочной криптографической изменчивости. Кроме того, векторы инициализации используются для синхронизации криптографического оборудования.
Hotspot («горячая точка») – место, где развернута общедоступная беспроводная локальная сеть. «Горячие точки» располагаются в зонах, где концентрируются люди с компьютерными устройствами, таких как аэропорты, гостиницы, дворцы съездов и кафе.
MIC (Message Integrity Check) (Код целостности сообщения) - алгоритм, используемый в стандарте 802.11i для обеспечения аутентификации и целостности пакетов.
OFDM (Orthogonal Frequency Division Multiplexing) - мультиплексирование с разделением по ортогональным частотам. Процесс, в ходе которого сигнал перед передачей его через воздушную среду распределяется по многим поднесущим. Используется с целью повышения характеристик беспроводных локальных сетей

стандартов 802.11a и 802.11g и в некоторых патентованных беспроводных региональных сетях.

Point-To-Multipoint System (система типа «точка-несколько точек») – система, позволяющая одному пользователю напрямую связываться с несколькими другими.

Point-To-Point System (система типа «точка-точка») – система, в которой связь между двумя пользователями осуществляется напрямую.

Point-To-Point Tunneling Protocol (PPTP) (Двухточечный туннельный протокол) - очень широко распространенный туннельный протокол, запатентованный Microsoft.

PSK (Phase Shift Keying) – фазовая модуляция. Процесс модуляции, при котором для представления информации используются небольшие изменения фазы несущей, в результате чего возможна передача данных через радиоэфир.

PSK (Pre Shared Key) (Режим с предварительным распределением ключей) - описанный в спецификации WPA режим обеспечения безопасности, основанный на предварительном размещении ключей на всех хостах, имеющих доступ к беспроводной локальной сети. Применяется в тех случаях, когда распределение ключей по протоколу 802.1x невозможно.

QAM (Quadrature Amplitude Modulation) – квадратурная амплитудная модуляция. Процесс модуляции, при котором для представления информации используются небольшие изменения фазы и амплитуды несущей, в результате чего передача данных возможна через радиоэфир.

RADIUS (Remote Authentication Dial-In User Service) - служба дистанционной аутентификации пользователей по коммутируемым линиям. Система аутентификации и учета, которую многие поставщики услуг широкополосного доступа к Internet используют для управления доступом к Internet и выписки счетов за пользование беспроводной сетью.

Request-To-Send (RTS) (Запрос на передачу) - тип управляющего фрейма в стандарте 802.11, применяется в механизме обнаружения виртуальной несущей. Если такой механизм используется в сети 802.11, то станция, желающая отправить данные, должна предварительно послать фрейм RTS.

Spanning Tree Protocol (STP) (Протокол остовного дерева) - определенный в стандарте 802.Id протокол уровня 2, позволяющий избежать зацикливания в сетях с несколькими коммутаторами и избыточными соединениями.

Supplicant (Претендент) - в протоколе 802.1x клиентское устройство, нуждающееся в аутентификации.

TDMA (Time Division Multiple Access) - множественный доступ с временным разделением каналов. Процесс, позволяющий только одному пользователю осуществлять передачу в данный промежуток времени. Каждый пользователь занимает всю полосу канала в течение выделенного для него временного интервала.

TKIP (Temporal Key Integrity Protocol) (Протокол целостности временных ключей) - основанный на алгоритме RC4 протокол шифрования, который избавлен от многих слабостей оригинального статического протокола WEP. Протокол TKIP это необязательная часть стандарта 802.11i. Он обратно совместим с WEP и не требует замены оборудования.

VPN (Virtual Private Network) - виртуальная частная сеть, использующая специальное программное обеспечение на клиентском устройстве, которое управляет доступом к отдаленным приложениям и обеспечивает безопасность соединения за счет сквозного шифрования.

WDS (Wireless Distribution System) (Беспроводная распределенная система) - элемент беспроводной системы, состоящий из взаимосвязанных базовых наборов служб, которые образуют расширенный набор служб.

WEP (Wired Equivalent Privacy) - в стандарте 802.11 необязательный механизм обеспечения безопасности, в котором для шифрования трафика в беспроводной сети применяется алгоритм RC4.

Wi Fi (Wireless Fidelity) - процедура сертификации, разработанная организацией Wi-Fi Alliance, которая гарантирует возможность совместной работы различных продуктов, реализующих стандарт 802.11.

Wi-Fi Protected Access (WPA) - защищенный доступ к Wi-Fi. Протокол безопасности, определенный Альянсом Wi-Fi, позволяющий компьютерным устройствам периодически получать новые ключи шифрования. В WPA версии 1 применяются временный протокол целостности ключа TKIP и WEP; в WPA версии 2 используется весь стандарт 802.11i, включающий AES.

WLAN (Wireless Local Area Network) (Беспроводная локальная сеть) – локальные сети стандарта 802.11.

ИСТОЧНИКИ ИНФОРМАЦИИ

1) Столлингс В. Беспроводные линии связи и сети.: Пер. с англ. – М.: Издательский дом «Вильямс», 2003. – 640 с.
2) Вишневский В., Ляхов А., Портной С., Шахнович И. Широкополосные беспроводные сети передачи информации. - М.:Эко-Трендз, 2005. – 592 с.
3) Олифер В.Г.,. Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. – Спб.: Питер, 2006. – 958 с.
4) Григорьев В.А., Лагутенко О.И., Распаев Ю.А. Сети и системы радиодоступа. – М.:Эко-Трендз, 2005. – 384 с.
5) Рошан Педжман, Лиэри Джонатан. Основы постороения беспроводных локальных сетей стандарта 802.11. : Пер. с англ. - М.: Издательский дом «Вильямс», 2004. – 304 с.
6) Максим М. Безопасность беспроводных сетей / Мерит Максим, Дэвид Полино; Пер. с англ. Семенова А.В. – М.: Компания АйТи; ДМК Пресс, 2004.- 288с.
7) Владимиров А.А.Wi-фу: «боевые» приемы взлома и защиты беспроводных сетей / Андрей А. Владимиров, Константин В. Гавриленко, Андрей А. Михайловский; пер. с англ. АА. Слинкина. М.: НТ Пресс, 2005. — 463с.
8) http://www.tayle.com – сайт компании ТАЙЛЕ.
9) http://www.airdata.ru – сайт компании Air Data Communications.
10) http://www.dlink.ru – сайт компании D-LINK.
11) http://wifi-wiki.ru
12) http://www.wireless.bape3.org
13) http://www.alpha-teleport.info – сайт компании alpha-teleport.info.
14) http://www.ixbt.com – информационный портал.
15) http://www.wireless.ru – специализированный портал, посвященный беспроводным технологиям.
16) http://www.umd.ru – сайт компании УМДпроект.
17) http://www.ferra.ru – информационный портал.
18) http://ru.wikipedia.org – википедия, русский проект свободной многоязычной энциклопедии.
19) http://pcweek.ru – сайт журнала PCWeek Russian Edition.
20) http://www.thg.ru – Русский Tom's Hardware Guide, информационный портал.