СОДЕРЖАНИЕ

ГЛАВА СТРАНИЦА

1 Аспекты организации сети Wi-Fi

Довольно распространенная сегодня аббревиатура Wi-Fi расшифровывается как торговая марка Wi-Fi Alliance для беспроводных сетей на базе стандарта IEEE 802.11. Под аббревиатурой Wi-Fi (от английского словосочетания Wireless Fidelity (перевод – «беспроводное качество» или «беспроводная точность»)) уже несколько лет высокими темпами развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам. Отчасти и поэтому любое оборудование, соответствующее стандарту IEEE 802.11, может быть протестировано в Wi-Fi Alliance и получить соответствующий сертификат и право нанесения логотипа Wi-Fi. По другой версии, термин «Wi-Fi» изначально был придуман как игра слов для привлечения внимания потребителя «намеком» на Hi-Fi (англ. High Fidelity – высокая точность). Несмотря на то что поначалу в некоторых пресс-релизах WECA фигурировало словосочетание «Wireless Fidelity» («беспроводная точность»), на данный момент от такой формулировки отказались, и термин «Wi-Fi» никак не расшифровывается.

История создания Wi-Fi такова. В 1991 году NCR Corporation/AT&T (впоследствии – Lucent Technologies и Agere Systems) в Сига, Нидерланды, разработали новый продукт, предназначавшийся для систем кассового обслуживания, который был выведен на рынок под маркой WaveLAN и обеспечивал скорость передачи данных от 1 до 2 Мбит/с. Один из создателей Wi-Fi – Вик Хейз (Vic Hayes) – разработчик таких стандартов, как IEEE 802.11b, IEEE 802.11a и IEEE 802.11g, покинул компанию в 2003 году, и Agere Systems не смогла конкурировать на равных с другими, несмотря на то что продукция занимала нишу относительно бюджетных Wi-Fi-решений. 802.11abg all-in-one-чипсет Agere (кодовое имя: WARP) плохо продавался, и Agere Systems решила уйти с рынка Wi-Fi еще в конце 2004 года.

Широко известный сегодня стандарт IEEE 802.11n утвержден 11 сентября 2009 года. Его применение позволило повысить скорость передачи данных практически в четыре раза, по сравнению с устройствами стандартов 802.11g (максимальная скорость которых равна 54 Мбит/с), при условии использования в режиме 802.11n с другими устройствами 802.11n. Теоретически 802.11n способен обеспечить скорость передачи данных до 600 Мбит/с [2]. С 2011 по 2013 год разрабатывался стандарт IEEE 802.11ac, окончательное принятие стандарта было запланировано на начало 2014 года. Скорость передачи данных при использовании 802.11ac может достигать нескольких Гбит/с. Большинство ведущих производителей оборудования уже анонсировали устройства, поддерживающие данный

стандарт. Эволюция продолжалась, и в 2011 году Институт инженеров электротехники и электроники (IEEE) выпустил официальную версию стандарта IEEE 802.22. Системы и устройства, поддерживающие этот стандарт, позволят принимать данные на скорости до 22 Мбит/с в радиусе 100 км от ближайшего передатчика.

1.1. Особенности Wi-Fi

Блок-схема сети Wi-Fi содержит не менее одной точки доступа и не менее одного клиента. Также возможно подключение двух клиентов в режиме точка-точка (Ad-hoc), когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров «напрямую». Точка доступа передаёт свой идентификатор сети (SSID) с помощью специальных сигнальных пакетов на скорости 0,1 Мбит/с каждые 100 мс. Поэтому 0,1 Мбит/с – наименьшая скорость передачи данных для Wi-Fi. Зная SSID сети, клиент может выяснить, возможно ли подключение к данной точке доступа. При попадании в зону действия двух точек доступа с идентичными SSID приемник может выбирать между ними на основании данных об уровне сигнала. Стандарт Wi-Fi дает клиенту полную свободу при выборе критериев для соединения. Более подробно принцип работы описан в официальном тексте стандарта. Однако сей стандарт не описывает всех аспектов построения беспроводных локальных сетей Wi-Fi. Поэтому каждый производитель оборудования решает эту задачу посвоему, применяя те подходы, которые он считает наилучшими с той или иной точки зрения. Поэтому возникает необходимость классификации способов построения беспроводных локальных сетей.

По способу объединения точек доступа в единую систему можно выделить:

- автономные точки доступа (называются также самостоятельные, децентрализованные, умные);
- точки доступа, работающие под управлением контроллера (называются также «легковесные», централизованные);
- бесконтроллерные, но не автономные (управляемые без контроллера).

По способу организации и управления радиоканалами можно выделить беспроводные локальные сети:

- со статическими настройками радиоканалов;
- с динамическими (адаптивными) настройками радиоканалов;
- со «слоистой» или многослойной структурой радиоканалов.

1.2. Преимущества и недостатки перед другими формами передачи данных на небольшие расстояния

1.2.1. Общеизвестные преимущества Wi-Fi

Беспроводной Интернет позволяет развернуть сеть без прокладки кабеля, что может уменьшить стоимость развертывания и/или расширения сети. Места, где нельзя проложить кабель, к примеру вне помещений и в зданиях, имеющих историческую ценность, могут обслуживаться беспроводными сетями. Также такое решение позволяет иметь доступ к сети мобильным устройствам. Для всех Wi-Fi-устройств гарантируется совместимость оборудования благодаря обязательной сертификации оборудования с логотипом Wi-Fi. Другим отличительным фактором использования Wi-Fi-устройств и сетей являются их доступность в бытовом плане, легкий монтаж и мобильность. Пользователь больше не привязан к одному месту и может пользоваться Интернетом в комфортной для вас обстановке. В пределах Wi-Fi-зоны в сеть Интернет могут выходить несколько пользователей с компьютеров, ноутбуков, телефонов и т. д. Излучение от Wi-Fi-устройств в момент передачи данных на порядок (в 10 раз) меньше, чем у сотового телефона. И тем не менее мы еще вернемся к вопросу безопасности применения Wi-Fi в этом разделе далее, поскольку с медицинской точки зрения известны несколько противоречий на сей счет.

1.2.2. Недостатки

Как ни странно, но недостатки Wi-Fi тоже имеют место быть.

В диапазоне 2,4 ГГц работает множество устройств, таких как устройства, поддерживающие Bluetooth, и др., и даже микроволновые печи, что ухудшает электромагнитную совместимость. Производителями оборудования указывается скорость на L1 (OSI), в результате чего создается иллюзия, что производитель оборудования завышает скорость, но на самом деле в Wi-Fi весьма высоки служебные «накладные расходы». Получается, что скорость передачи данных на L2 (OSI) в Wi-Fi-сети всегда ниже заявленной скорости на L1 (OSI). Реальная скорость зависит от доли служебного трафика, которая зависит уже от наличия между устройствами физических преград (мебель, стены), наличия помех от других беспроводных

устройств или электронной аппаратуры, расположения устройств относительно друг друга и т. п.

Частотный диапазон и эксплуатационные ограничения в различных странах не одинаковы. Во многих европейских странах разрешены два дополнительных канала, которые запрещены в США; в Японии есть ещё один канал в верхней части диапазона, а другие страны, к примеру Испания, запрещают использование низкочастотных каналов. Более того, некоторые страны, к примеру Россия, Белоруссия и Италия, требуют регистрации всех сетей Wi-Fi, работающих вне помещений, или требуют регистрации Wi-Fi-оператора. О том, как можно заглушить Wi-Fi, тоже будет рассказано далее.

Внимание, важно!
Добавлю, что в России точки беспроводного доступа, а также адаптеры Wi-Fi с ЭИИМ, превышающей 100 мВт (20 дБм), подлежат обязательной регистрации.

1.3. Защита от вторжения: разные варианты

Стандарт шифрования WEP может быть относительно легко взломан даже при правильной конфигурации (из-за слабой стойкости алгоритма). Новые устройства поддерживают более совершенные протоколы шифрования данных WPA и WPA2. Принятие стандарта IEEE 802.11i (WPA2) в июне 2004 года сделало возможным применение более безопасной схемы связи, которая доступна в новом оборудовании. Обе схемы требуют более стойкого пароля, чем те, которые обычно назначаются пользователями. Многие организации используют дополнительное шифрование (VPN) для защиты от вторжения.

Сегодня основным методом взлома WPA2 является подбор пароля, поэтому рекомендуется использовать сложные цифробуквенные пароли, для того чтобы максимально усложнить задачу подбора пароля. В режиме точка-точка (Ad-hoc) стандарт предписывает лишь реализовать скорость 11 Мбит/сек (802.11b). Шифрование WPA(2) недоступно, только «легковзламываемый» WEP.

Актуальные вопросы безопасности беспроводных сетей

Безопасности беспроводных сетей стоит уделять особое внимание. Ведь Wi-Ai является беспроводной сетью с относительно боль-

шим радиусом действия. Соответственно, злоумышленник может перехватывать информацию или же атаковать пользовательскую сеть, находясь на относительно безопасном расстоянии. Существует множество различных способов защиты, и при условии правильной настройки можно быть уверенным в обеспечении необходимого уровня безопасности. Разберемся в них предметно.

WEP – это протокол шифрования, использующий довольно нестойкий алгоритм RC4 на статическом ключе. Существует 64-, 128-, 256- и 512-битное WEP-шифрование. Чем больше бит используется для хранения ключа, тем больше возможных комбинаций ключей, а соответственно, более высокая стойкость сети к взлому. Часть wep-ключа является статической (40 бит в случае 64-битного шифрования), а другая часть (24 бит) – динамическая (вектор инициализации), то есть меняющаяся в процессе работы сети. Основной уязвимостью протокола WEP является то, что векторы инициализации повторяются через некоторый промежуток времени, и взломщику потребуется лишь собрать эти повторы и вычислить по ним статическую часть ключа. Для повышения уровня безопасности можно дополнительно к wep-шифрованию использовать стандарт 802.1x или VPN.

WPA – более стойкий протокол шифрования, чем WEP, хотя используется тот же алгоритм RC4. Более высокий уровень безопасности достигается за счет использования протоколов TKIP и MIC.

TKIP (Temporal Key Integrity Protocol). Протокол динамических ключей сети, которые меняются довольно часто. При этом каждому устройству также присваивается ключ, который тоже меняется.

MIC (Message Integrity Check). Протокол проверки целостности пакетов. Защищает от перехвата пакетов и из перенаправления. Также возможно использование 802.1x и VPN, как и в случае с wep-протоколом.

Существует два вида WPA: WPA-PSK (Pre-shared key). Для генерации ключей сети и для входа в сеть используется ключевая фраза. Оптимальный вариант для домашней или небольшой офисной сети – WPA-802.1x. Вход в сеть осуществляется через сервер аутентификации. Оптимально для сети крупной компании.

Усовершенствование протокола WPA активно происходит все предыдущие годы. В отличие от WPA, используется более стойкий алгоритм шифрования AES. По аналогии с WPA, WPA2 также делится на два типа: WPA2-PSK и WPA2-802.1x.

Протоколы разных стандартов безопасности сети

- EAP (Extensible Authentication Protocol). Протокол расширенной аутентификации. Используется совместно с RADIUS-сервером в крупных сетях.
- TLS (Transport Layer Security). Протокол, который обеспечивает целостность и шифрование передаваемых данных между сервером и клиентом, их взаимную аутентификацию, предотвращая перехват и подмену сообщений.
- RADIUS (Remote Authentication Dial-In User Server). Сервер аутентификации пользователей по логину и паролю.
- VPN (Virtual Private Network) – виртуальная частная сеть. Протокол был создан для безопасного подключения клиентов к сети через общедоступные интернет-каналы. Принцип работы VPN – создание так называемых безопасных «туннелей» от пользователя до узла доступа или сервера. Хотя VPN изначально был создан не для WI-Fi, его можно использовать в любом типе сетей. Для шифрования трафика в VPN чаще всего используется протокол IPSec. Он обеспечивает практически стопроцентную безопасность. Случаев взлома VPN на данный момент неизвестно. Мы рекомендуем использовать эту технологию для корпоративных сетей.

Дополнительные методы защиты пользовательской сети

Фильтрация по MAC-адресу – важное звено в обеспечении безопасности работы. MAC-адрес – это уникальный идентификатор устройства (сетевого адаптера), «зашитый» в него производителем. На некотором оборудовании можно задействовать данную функцию и разрешить доступ в сеть необходимым адресам. Это создаст дополнительную преграду взломщику, хотя не очень серьезную – в принципе, MAC-адрес можно подменить.

Приватное скрытие SSID обеспечивает сети еще большую безопасность.

SSID – это идентификатор вашей беспроводной сети. Большинство оборудования позволяет его скрыть, таким образом, при сканировании Wi-Fi-сетей вашей сети видно не будет. Но опять же, это не слишком серьезная преграда, если взломщик использует более продвинутый сканер сетей, чем стандартная утилита в Windows.

Запрет доступа к настройкам точки доступа или роутера через беспроводную сеть реализуется следующим образом. Активацией этой функции можно запретить доступ к настройкам точки доступа

через Wi-Fi-сеть, однако это не защитит пользователя от перехвата трафика или от проникновения в сеть. Поэтому неправильная настройка оборудования, поддерживающего даже самые современные технологии защиты, не обеспечит должного уровня безопасности сети. В каждом стандарте есть дополнительные технологии и настройки для повышения уровня безопасности, которые опытный пользователь умело применяет на практике, не манкируя обеспечением безопасности собственных данных.

1.4. Перспективы технологии Wi-Fi на разных уровнях

На промышленном уровне суперсовременные технологии Wi-Fi предлагаются пока ограниченным числом поставщиков. Так, несколько лет назад компания Siemens Automation & Drives предложила Wi-Fi-решения для своих контроллеров SIMATIC в соответствии со стандартом IEEE 802.11g в свободном ISM-диапазоне 2,4 ГГц, обеспечивающем максимальную скорость передачи 54 Мбит/с. Данные технологии применяются для управления движущимися объектами и в складской логистике, а также в тех случаях, когда по какой-либо причине невозможно прокладывать проводные сети Ethernet. Использование Wi-Fi-устройств на предприятиях обусловлено высокой помехоустойчивостью, что делает их применимыми на предприятиях со множеством металлических конструкций. Wi-Fi электронные устройства не создают существенных помех для узкополосных радиосигналов. Технология находит широкое применение на удаленном или опасном производстве, там, где нахождение оперативного персонала связано с повышенной опасностью или вовсе затруднительно. К примеру, для задач телеметрии на нефтегазодобывающих предприятиях, а также для контроля за перемещением персонала и транспортных средств в шахтах и рудниках, для определения нахождения персонала в аварийных ситуациях.

На рис. 1.1 представлена иллюстрации организации сети Wi-Fi.

1.5. Взаимодействие сетей Wi-Fi и сотовой связи

Теоретически и перспективно Wi-Fi и подобные ему технологии со временем могут заменить сотовые сети, такие как GSM. Препятствия-

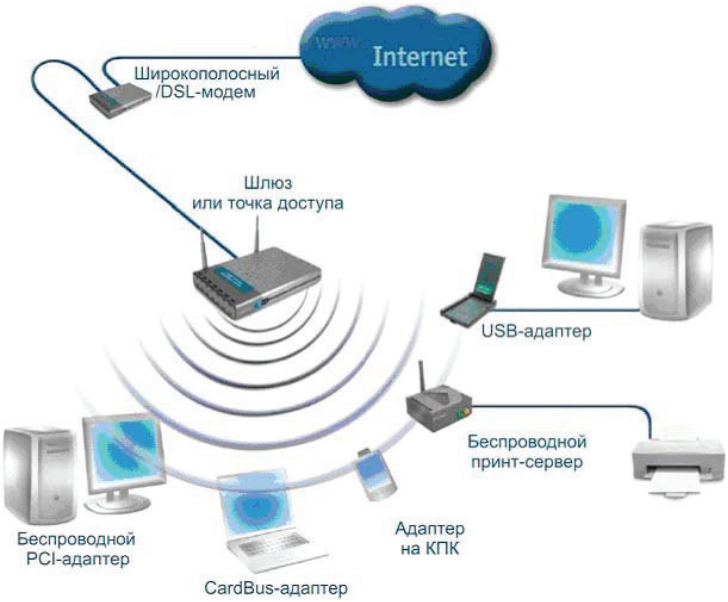

Рис. 1.1. Организации сети Wi-Fi

ми для такого развития событий в ближайшем будущем являются отсутствие глобального роуминга, ограниченность частотного диапазона и сильно ограниченный радиус действия Wi-Fi. Более правильным выглядит сравнение сотовых сетей с другими стандартами беспроводных сетей, таких как UMTS, CDMA или WiMAX. Тем не менее уже сегодня Wi-Fi пригоден для использования VoIP в корпоративных сетях или в среде SOHO. Первые образцы оборудования появились еще в начале 2000-х, они серийно вышли на широкий рынок в 2005 году. Тогда такие компании, как Zyxel, UT Starcomm, Samsung, Hitachi, и многие другие представили на рынок VoIP Wi-Fi-телефоны по «разумным» ценам. В те далекие годы ADSL ISP-провайдеры начали предоставлять услуги VoIP своим клиентам (ISP XS4All). Когда звонки с помощью VoIP стали очень дешёвыми, а зачастую вообще бесплатными, провайдеры, способные предоставлять услуги VoIP, получили возможность открыть новый рынок – услуг VoIP. Телефоны GSM с интегрированной поддержкой возможностей Wi-Fi и VoIP стали выводиться на рынок, и потенциально они планировались такими, чтобы заменить проводные телефоны. Но сегодня непосредственное сравнение Wi-Fi и сотовых сетей нецелесообразно

по целому ряду причин. Телефоны, использующие только Wi-Fi, имеют очень ограниченный радиус действия, поэтому развертывание таких сетей обходится довольно дорого. И тем не менее развертывание подобных сетей может быть наилучшим решением для локального использования, например в корпоративных сетях. Однако устройства, поддерживающие несколько стандартов, могут занять значительную долю рынка. При наличии в данном конкретном месте покрытия как GSM, так и Wi-Fi, экономически намного более выгодно использовать Wi-Fi, разговаривая посредством сервисов интернет-телефонии. К примеру, программное обеспечение – клиент Skype давно существует в версиях как для смартфонов, так и для КПК.

Всех пользователей Wi-Fi сегодня условно можно разделить на три категории:

- linus – выделяющие бесплатный доступ в Интернет;
- bills – продающие свой частотный диапазон;
- aliens – использующие доступ через bills.

Таким образом, система аналогична пиринговым сервисам. Несмотря на то что FON получает финансовую поддержку от таких компаний, как Google и Skype, лишь со временем можно уточнить, будет ли эта идея действительно работать.

У этого сервиса есть три основные проблемы. Первая заключается в том, что для перехода проекта из начальной стадии в основную требуется больше внимания со стороны общественности и СМИ. Нужно также учитывать тот факт, что предоставление доступа к вашему интернет-каналу другим лицам может быть ограничено вашим договором с интернет-провайдером. Поэтому интернет-провайдеры будут пытаться защитить свои интересы. Так же, скорее всего, поступят звукозаписывающие компании, выступающие против свободного распространения MP3.

Возможные решения по организации беспроводного доступа представлены на рис. 1.2.

Внимание, важно!

По ряду причин в России основное количество точек доступа сообщества FON расположено в Московском регионе. Посему говорить о распространении и какой-либо перспективе развертывания системы по всей стране, полагаю, преждевременно.

Wi-Fi совместим с игровыми консолями и КПК и позволяет вести сетевую игру через любую точку доступа или в режиме точка-точка.