ФЕДЕРАЛЬНОЕ АГЕНСТВО ПО ОБРАЗОВАНИЮ

ГОУ ВПО

Кафедра математики и информатики

Беспроводные локальные сети Wlan

(Реферат)

Выполнил:

студенты1 курса

Ф.И.О.

Проверил:

Кандидат математических наук, доктор:

Ф.И.О.

Нижний Новгород

2007г.

*Содержание:*

***Введение***

***Глава 1.***

***1.1.*** Архитектура, компоненты сети и стандарты

***1.2.*** Сравнение стандартов беспроводной передачи данных

***1.3***. Организация сети

***1.4.*** Типы и разновидности соединений

***1.5***. Безопасность Wi-Fi сетей

***Глава 2***.

***2.1*** Адаптер Wi-Fi ASUS WL-138g V2

***2.2* Интернет-центр ZyXEL P-330W**

***2.3* Плата маршрутизатора Hi-Speed 54G**

***2.4*** PCI-адаптер HWP54G

***Глава 3.***

 ***3. Новинки***

***Заключение***

**Список используемой литературы**

***Введение.***

Так сложилось, что в нашей стране большую распространенность получили районные Ethernet сети, затягивающие в квартиру витую пару. Когда дома всего один компьютер, вопросов с подключением кабеля обычно не возникает. Но когда появляется желание лазить в Интернет с компьютера, лэптопа и КПК с возможностью беспроводного подключения, задумываешься о том, как все это грамотно осуществить. Разделить один Интернет-канал на всех домочадцев нам помогают многофункциональные роутеры.

Потребность в создании дома персональной Wi-fi сети испытывает, наверное, любой обладатель ноутбука или КПК. Конечно, можно купить точку доступа и организовать беспроводный доступ через нее. Но куда удобнее иметь устройство всё в одном», ведь роутеры справляются с этой функцией ничуть не хуже точек доступа. Главное, на что стоит обращать внимание, это поддерживаемые стандарты Wi-fi. Ибо в последние несколько лет среди производителей появилась тенденция выпускать устройства с поддержкой еще не существующих стандартов. Безусловно, в этом есть определенная польза. Мы получаем большую производительность и дальнобойность wi-fi при использовании оборудования от одного производителя. Однако, поскольку каждый из них реализует новшества так, как ему больше нравится (стандарт ведь пока не принят), совместимости оборудования от разных производителей мы не наблюдаем.

Обычно беспроводные сетевые технологии группируются в три типа, различающиеся по масштабу действия их радиосистем, но все они с успехом применяются в бизнесе.

PAN (персональные сети) — короткодействующие, радиусом до 10 м сети, которые связывают ПК и другие устройства — КПК, мобильные телефоны, принтеры и т. п. С помощью таких сетей реализуется простая синхронизация данных, устраняются проблемы с обилием кабелей в офисах, реализуется простой обмен информацией в небольших рабочих группах. Наиболее перспективный стандарт для PAN — это Bluetooth.

WLAN (беспроводные локальные сети) — радиус действия до 100 м. С их помощью реализуется беспроводной доступ к групповым ресурсам в здании, университетском кампусе и т. п. Обычно такие сети используются для продолжения проводных корпоративных локальных сетей. В небольших компаниях WLAN могут полностью заменить проводные соединения. Основной стандарт для WLAN — 802.11.

WWAN (беспроводные сети широкого действия) — беспроводная связь, которая обеспечивает мобильным пользователям доступ к их корпоративным сетям и Интернету. Пока здесь нет доминирующего стандарта, но наиболее активно внедряется технология GPRS — быстрее всего в Европе и с некоторым отставанием в США.

На современном этапе развития сетевых технологий, технология беспроводных сетей Wi-Fi является наиболее удобной в условиях требующих мобильность, простоту установки и использования. Wi-Fi (от англ. wireless fidelity - беспроводная связь) - стандарт широкополосной беспроводной связи семейства 802.11 разработанный в 1997г. Как правило, технология Wi-Fi используется для организации беспроводных локальных компьютерных сетей, а также создания так называемых горячих точек высокоскоростного доступа в Интернет.

**Глава 1.**

***1.1 Архитектура, компоненты сети и стандарты***

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

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

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

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

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

В основу стандарта 802.11 положена сотовая архитектура. Сеть может состоять из одной или нескольких ячеек (сот). Каждая сота управляется базовой станцией, называемой точкой доступа (Access Point, AP). Точка доступа и находящиеся в пределах радиуса ее действия рабочие станции образуют базовую зону обслуживания (Basic Service Set, BSS). Точки доступа многосотовой сети взаимодействуют между собой через распределительную систему (Distribution System, DS), представляющую собой эквивалент магистрального сегмента кабельных ЛС. Вся инфраструктура, включающая точки доступа и распределительную систему, образует расширенную зону обслуживания (Extended Service Set). Стандартом предусмотрен также односотовый вариант беспроводной сети, который может быть реализован и без точки доступа, при этом часть ее функций выполняется непосредственно рабочими станциями.

В настоящее время существует множество стандартов семейства IEEE 802.11:

1. 802.11 - первоначальный основополагающий стандарт. Поддерживает передачу данных по радиоканалу со скоростями 1 и 2 (опционально) Мбит/с.
2. 802.11a - высокоскоростной стандарт WLAN. Поддерживает передачу данных со скоростями до 54 Мбит/с по радиоканалу в диапазоне около 5 ГГц.
3. 802.11b - самый распространенный стандарт. Поддерживает передачу данных со скоростями до 11 Мбит/с по радиоканалу в диапазоне около 2,4 ГГц.
4. 802.11c - Стандарт, регламентирующий работу беспроводных мостов. Данная спецификация используется производителями беспроводных устройств при разработке точек доступа.
5. 802.11d - Стандарт определял требования к физическим параметрам каналов (мощность излучения и диапазоны частот) и устройств беспроводных сетей с целью обеспечения их соответствия законодательным нормам различных стран.
6. 802.11e - Создание данного стандарта связано с использованием средств мультимедиа. Он определяет механизм назначения приоритетов разным видам трафика - таким, как аудио- и видеоприложения. Требование качества запроса, необходимое для всех радио интерфейсов IEEE WLAN.
7. 802.11f - Данный стандарт, связанный с аутентификацией, определяет механизм взаимодействия точек связи между собой при перемещении клиента между сегментами сети. Другое название стандарта - Inter Access Point Protocol. Стандарт, описывающий порядок связи между равнозначными точками доступа.
8. 802.11g - устанавливает дополнительную технику модуляции для частоты 2,4 ГГц. Предназначен, для обеспечения скоростей передачи данных до 54 Мбит/с по радиоканалу в диапазоне около 2,4 ГГц.
9. 802.11h – Разработка данного стандарта связана с проблемами при использовании 802.11а в Европе, где в диапазоне 5 ГГц работают некоторые системы спутниковой связи. Для предотвращения взаимных помех стандарт 802.11h имеет механизм "квазиинтеллектуального" управления мощностью излучения и выбором несущей частоты передачи. Стандарт, описывающий управление спектром частоты 5 ГГц для использования в Европе и Азии.
10. 802.11i (WPA2) – Целью создания данной спецификации является повышение уровня безопасности беспроводных сетей. В ней реализован набор защитных функций при обмене информацией через беспроводные сети - в частности, технология AES (Advanced Encryption Standard) - алгоритм шифрования, поддерживающий ключи длиной 128, 192 и 256 бит. Предусматривается совместимость всех используемых в данное время устройств - в частности, Intel Centrino - с 802.11i-сетями. Затрагивает протоколы 802.1X, TKIP и AES.
11. 802.11j - Спецификация предназначена для Японии и расширяет стандарт 802.11а добавочным каналом 4,9 ГГц.
12. 802.11n - Перспективный стандарт, находящийся на сегодняшний день в разработке, который позволит поднять пропускную способность сетей до 100 Мбит/сек.
13. 802.11r - Данный стандарт предусматривает создание универсальной и совместимой системы роуминга для возможности перехода пользователя из зоны действия одной сети в зону действия другой.

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

***1.2***  ***Сравнение стандартов беспроводной передачи данных:***

802.11b. В окончательной редакции широко распространенный стандарт 802.11b был принят в 1999 г. и благодаря ориентации на свободный от лицензирования диапазон 2,4 ГГц завоевал наибольшую популярность у производителей оборудования. Пропускная способность (теоретическая 11 Мбит/с, реальная — от 1 до 6 Мбит/с) отвечает требованиям большинства приложений. Поскольку оборудование 802.11b, работающее на максимальной скорости 11 Мбит/с, имеет меньший радиус действия, чем на более низких скоростях, то стандартом 802.11b предусмотрено автоматическое понижение скорости при ухудшении качества сигнала.
К началу 2004 года в эксплуатации находилось около 15 млн. радиоустройств 802.11b.

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

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

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

***1.3. Организация сети***

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

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

***1.4.Типы и разновидности соединений***

**1. Соединение Ad-Hoc (**точка-точка)**.**

Все компьютеры оснащены беспроводными картами (клиентами) и соединяются напрямую друг с другом по радиоканалу работающему по стандарту 802.11b и обеспечивающих скорость обмена 11 Mбит/с, чего вполне достаточно для нормальной работы.

**2. Инфраструктурное соединение.**

Все компьютеры оснащены беспроводными картами и подключаются к точке доступа. Которая, в свою очередь, имеет возможность подключения к проводной сети.

Данная модель используется когда необходимо соединить больше двух компьютеров. Сервер с точкой доступа может выполнять роль роутера и самостоятельно распределять интернет-канал.

**3. Точка доступа, с использованием роутера и модема.**

Точка доступа включается в роутер, роутер — в модем (эти устройства могут быть объединены в два или даже в одно). Теперь на каждом компьютере в зоне действия Wi-Fi , в котором есть адаптер Wi-Fi, будет работать интернет.

**4. Соединение мост.**

Компьютеры объединены в проводную сеть. К каждой группе сетей подключены точки доступа, которые соединяются друг с другом по радио каналу. Этот режим предназначен для объединения двух и более проводных сетей. Подключение беспроводных клиентов к точке доступа, работающей в режиме моста невозможно.

**5. Репитер.**

Точка доступа просто расширяет радиус действия другой точки доступа, работающей в инфраструктурном режиме.

***1.5. Безопасность Wi-Fi сетей***

Как и любая компьютерная сеть, Wi-Fi – является источником повышенного риска несанкционированного доступа. Кроме того, проникнуть в беспроводную сеть значительно проще, чем в обычную, — не нужно подключаться к проводам, достаточно оказаться в зоне приема сигнала.

Беспроводные сети отличаются от кабельных только на первых двух - физическом (Phy) и отчасти канальном (MAC) - уровнях семиуровневой модели взаимодействия открытых систем. Более высокие уровни реализуются как в проводных сетях, а реальная безопасность сетей обеспечивается именно на этих уровнях. Поэтому разница в безопасности тех и других сетей сводится к разнице в безопасности физического и MAC-уровней.

Хотя сегодня в защите Wi-Fi-сетей применяются сложные алгоритмические математические модели аутентификации, шифрования данных и контроля целостности их передачи, тем не менее, вероятность доступа к информации посторонних лиц является весьма существенной. И если настройке сети не уделить должного внимания злоумышленник может:

* заполучить доступ к ресурсам и дискам пользователей Wi-Fi-сети, а через неё и к ресурсам LAN;
* подслушивать трафик, извлекать из него конфиденциальную информацию;
* искажать проходящую в сети информацию;
* воспользоваться интернет-траффиком;
* атаковать ПК пользователей и серверы сети
* внедрять поддельные точки доступа;
* рассылать спам, и совершать другие противоправные действия от имени вашей сети.

Для защиты сетей 802.11 предусмотрен комплекс мер безопасности передачи данных.

 На раннем этапе использования Wi-Fi сетей таковым являлся пароль SSID (Server Set ID) для доступа в локальную сеть, но со временем оказалось, что данная технология не может обеспечить надежную защиту.

Главной же защитой долгое время являлось использование цифровых ключей шифрования потоков данных с помощью функции Wired Equivalent Privacy (WEP). Сами ключи представляют из себя обыкновенные пароли с длиной от 5 до 13 символов ASCII. Данные шифруются ключом с разрядностью от 40 до 104 бит. Но это не целый ключ, а только его статическая составляющая. Для усиления защиты применяется так называемый вектор инициализации Initialization Vector (IV), который предназначен для рандомизации дополнительной части ключа, что обеспечивает различные вариации шифра для разных пакетов данных. Данный вектор является 24-битным. Таким образом, в результате мы получаем общее шифрование с разрядностью от 64 (40+24) до 128 (104+24) бит, в результате при шифровании мы оперируем и постоянными, и случайно подобранными символами.

Но, как оказалось, взломать такую защиту можно соответствующие утилиты присутствуют в Интернете (например, AirSnort, WEPcrack). Основное её слабое место — это вектор инициализации. Поскольку мы говорим о 24 битах, это подразумевает около 16 миллионов комбинаций, после использования этого количества, ключ начинает повторяться. Хакеру необходимо найти эти повторы (от 15 минут до часа для ключа 40 бит) и за секунды взломать остальную часть ключа. После этого он может входить в сеть как обычный зарегистрированный пользователь.

Как показало время, WEP тоже оказалась не самой надёжной технологией защиты. После 2001 года для проводных и беспроводных сетей был внедрён новый стандарт IEEE 802.1X, который использует вариант динамических 128-разрядных ключей шифрования, то есть периодически изменяющихся во времени. Таким образом, пользователи сети работают сеансами, по завершении которых им присылается новый ключ. Например, Windows XP поддерживает данный стандарт, и по умолчанию время одного сеанса равно 30 минутам. IEEE 802.1X — это новый стандарт, который оказался ключевым для развития индустрии беспроводных сетей в целом. За основу взято исправление недостатков технологий безопасности, применяемых в 802.11, в частности, возможность взлома WEP, зависимость от технологий производителя и т. п. 802.1X позволяет подключать в сеть даже PDA-устройства, что позволяет более выгодно использовать саму идею беспроводной связи. С другой стороны, 802.1X и 802.11 являются совместимыми стандартами. В 802.1X применяется тот же алгоритм, что и в WEP, а именно — RC4, но с некоторыми отличиями. 802.1X базируется на протоколе расширенной аутентификации (EAP), протоколе защиты транспортного уровня (TLS) и сервере доступа Remote Access Dial-in User Server. Протокол защиты транспортного уровня TLS обеспечивает взаимную аутентификацию и целостность передачи данных. Все ключи являются 128-разрядными по умолчанию.

В конце 2003 года был внедрён стандарт Wi-Fi Protected Access (WPA), который совмещает преимущества динамического обновления ключей IEEE 802.1X с кодированием протокола интеграции временного ключа TKIP, протоколом расширенной аутентификации (EAP) и технологией проверки целостности сообщений MIC. WPA — это временный стандарт, о котором договорились производители оборудования, пока не вступил в силу IEEE 802.11i. По сути, WPA = 802.1X + EAP + TKIP + MIC, где:

* WPA — технология защищённого доступа к беспроводным сетям
* EAP — протокол расширенной аутентификации (Extensible Authentication Protocol)
* TKIP — протокол интеграции временного ключа (Temporal Key Integrity Protocol)
* MIC — технология проверки целостности сообщений (Message Integrity Check).

Стандарт TKIP использует автоматически подобранные 128-битные ключи, которые создаются непредсказуемым способом и общее число вариаций которых достигает 500 миллиардов. Сложная иерархическая система алгоритма подбора ключей и динамическая их замена через каждые 10 Кбайт (10 тыс. передаваемых пакетов) делают систему максимально защищённой.
От внешнего проникновения и изменения информации также обороняет технология проверки целостности сообщений (Message Integrity Check). Достаточно сложный математический алгоритм позволяет сверять отправленные в одной точке и полученные в другой данные. Если замечены изменения и результат сравнения не сходится, такие данные считаются ложными и выбрасываются.

Правда, TKIP сейчас не является лучшим в реализации шифрования, поскольку в силу вступают новые алгоритмы, основанные на технологии Advanced Encryption Standard (AES), которая, уже давно используется в VPN. Что касается WPA, поддержка AES уже реализована в Windows XP, пока только опционально.

Помимо этого, параллельно развивается множество самостоятельных стандартов безопасности от различных разработчиков, в частности, в данном направлении преуспевают Intel и Cisco. В 2004 году появляется WPA2, или 802.11i, который, в настоящее время является максимально защищённым.

Таким образом, на сегодняшний день у обычных пользователей и администраторов сетей имеются все необходимые средства для надёжной защиты Wi-Fi, и при отсутствии явных ошибок (пресловутый человеческий фактор) всегда можно обеспечить уровень безопасности, соответствующий ценности информации, находящейся в такой сети.

Сегодня беспроводную сеть считают защищенной, если в ней функционируют три основных составляющих системы безопасности: аутентификация пользователя, конфиденциальность и целостность передачи данных. Для получения достаточного уровня безопасности необходимо воспользоваться рядом правил при организации и настройке частной Wi-Fi-сети:

 Шифровать данные путем использования различных систем. Максимальный уровень безопасности обеспечит применение VPN;

 использовать протокол 802.1X;

 запретить доступ к настройкам точки доступа с помощью беспроводного подключения;

 управлять доступом клиентов по MAC-адресам;

 запретить трансляцию в эфир идентификатора SSID;

 располагать антенны как можно дальше от окон, внешних стен здания, а также ограничивать мощность радиоизлучения;

 использовать максимально длинные ключи;

 изменять статические ключи и пароли;

 использовать метод WEP-аутентификации “Shared Key" так как клиенту для входа в сеть необходимо будет знать WEP-ключ;

 пользоваться сложным паролем для доступа к настройкам точки доступа;

 по возможности не использовать в беспроводных сетях протокол TCP/IP для организации папок, файлов и принтеров общего доступа. Организация разделяемых ресурсов средствами NetBEUI в данном случае безопаснее;

 не разрешать гостевой доступ к ресурсам общего доступа, использовать длинные сложные пароли;

 не использовать в беспроводной сети DHCP. Вручную распределить статические IP-адреса между легитимными клиентами безопаснее;

 на всех ПК внутри беспроводной сети установить файерволлы, не устанавливать точку доступа вне брандмауэра, использовать минимум протоколов внутри WLAN (например, только HTTP и SMTP);

 регулярно исследовать уязвимости сети с помощью специализированных сканеров безопасности (например NetStumbler)

 использовать специализированные сетевые операционные системы такие как, Windows Nt, Windows 2003, Windows Xp.

Так же угрозу сетевой безопасности могут представлять природные явления и технические устройства, однако только люди (недовольные уволенные служащие, хакеры, конкуренты) внедряются в сеть для намеренного получения или уничтожения информации и именно они представляют наибольшую угрозу.

**Глава 2.**

***2.* Точка доступа D-link и ZyXel**

***2.1. Адаптер Wi-Fi ASUS WL-138g V2***

Стандарты: IEEE 802.11b, IEEE 802.11g

Дополнительные параметры:

ASUS WL-138g V2 Wireless LAN PCI Card, 54Mbps

PCI адаптер для подключения настольного компьютера к беспроводным сетям Wi-Fi

Радиус действия: 30 метров в помещении или 60 метров на открытой местности для 802.11g; 40 метров в помещении или 310 метров на открытойместностидля 802.11b

Скорость передачи:

802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Мбит/сек;

802.11b: 1, 2, 5.5, 11 Мбит/сек

Стандарты: IEEE 802.11g, IEEE 802.11b

Антенна: Съемная; коннектор RP-SMA

Диапазон частот: 2.412 - 2.472 ГГц

Защита данных: WEP-кодирование с 64- или 128-битным ключом; поддержка WPA и WPA2 (включая 802.1x, TKIP, AES)

**2.2. *Интернет-центр ZyXEL P-330W***

**Интернет-центр ZyXEL P-330W предназначен для безопасного подключения к Интернету по выделенной линии Ethernet через домовые сети. С его помощью все домашние компьютеры и сетевые устройства могут совместно использовать высокоскоростной выделенный канал. Благодаря фирменной технологии ZyXEL Link Duo интернет-центр P-330W обеспечивает не только выход в Интернет, но и одновременный доступ к серверам локальных ресурсов домовой сети.**

***Основные преимущества***

**Рекомендован ведущими интернет-провайдерами. Постоянное подключение к Интернету на скорости до 100 Мбит/с при свободном телефонеОдновременная работа в Интернете и домовой сети благодаря технологии Link Duo для PPTP/PPPoE**

**Двойная защита сети от угроз из ИнтернетаКоммутатор для непосредственного подключения четырех сетевых устройств**

**Универсальное применение в качестве: интернет-центра с подключением по Ethernet, интернет-центра с подключением по Wi-Fi, точки доступа Wi-Fi или беспроводного адаптера Wi-Fi**

**Безопасное беспроводное соединение на скорости до 54 Мбит/с и увеличенная дальность благодаря антенне с усилением 5 дБи.**

***Характеристики***

**Четыре режима работы:**

**Интернет-центр с подключением по выделенной линии Ethernet**

**Интернет-центр с подключением к провайдеру по Wi-Fi**

**Беспроводная точка доступа Wi-Fi**

**Беспроводной Ethernet-адаптер Wi-Fi**

**1 разъем RJ-45 «WAN» (10BASE-T/100BASE-TX) с автоопределением типа кабеля**

**4 разъема RJ-45 «LAN» (10BASE-T/100BASE-TX) с автоопределением типа кабеля**

**1 разъем RP-SMA для подключения антенны**

**Съемная всенаправленная антенна 5 дБи**

**7 индикаторов состояния (PWR/SYS, WAN, WLAN, LAN1-4)**

**Кнопка возврата к заводским установкам**

***Беспроводная сеть***

**Беспроводная точка доступа стандарта 802.11g 54 Мбит/с, совместимая с устройствами стандарта 802.11b**

**Беспроводной клиент стандарта 802.11g 54 Мбит/с, совместимый с устройствами стандарта 802.11b Радиус действия до 100 м в помещении, до 300 м на открытом пространстве.**

***2.3 Плата маршрутизатора Hi-Speed 54G***

**На сегодняшний день в беспроводном секторе компания предлагает линейку беспроводных устройств Hi-Speed 54G, в которую входят роутеры и другие клиентские устройства, а также линейку Wi - Fi антенн Hi-Gain 24. Еще, все используемое оборудование работает в стандарте 802.11G, который обеспечивает максимальную канальную скорость 54 Mbit, что по сегодняшним меркам не так уж и много (мы уже писали от 108Mb оборудовании), однако, наш выбор не случаен. Дело в том, что в нашей сети должны работать устройства, использующие стандарт 802.11G (компьютеры, ноутбуки и беспроводные принт-серверы), так и 802.11B, обеспечивающ ие скорость обмена 11Mb ( карманные компьютеры, коммуникаторы, и некоторые модели ноутбуков).**

***Стандарты* IEEE 802.11b и 802.11g**

***Частота* 2,4 ГГц**

***Максимальное расстояние* 300 м**

***Скорости работы* 1/2/5,5/6/9/11/12/18/24/36/48/54 Мбит/с**

***Антенна* Внешняя, с возможностью поворота в двух плоскостях**

***Особенности антенны*. Есть возможность подключения внешней антенны (разъём Reversed-SMA)**

***Мощность* Передача 13 dBm**

***Приём* -80 dBm**

***Безопасность* WEP 64-ех и 128-ми и 256-битный**

***Характеристики проводной части***

***LAN интерфейс* 4 порта 10BASE-T/100BASE-TX**

***Особенности* Автоматическое определение MDI/MDI-X**

***2.4 PCI-адаптер HWP54G***

**В целом, беспроводный контроллер Hawking Wireless-G PCI ничем не отличается от других подобных контроллеров. Она основана на базе чипа Ralink RT2560F и радиоблока RT2525, расположенного под миниатюрным экраном.**

**На тыльном бреккете располагается разъем для подключения антенны и два светодиода, отображающие наличие и статус соединения.**

**Глава 3.**

***3. Новинки***

***ASUS WL-160W - адаптер Wi-Fi с поддержкой 802.11n***

***28.12.2006***

Тайваньская компания ASUS, авторитетный производитель компьютерной электроники, в том числе решений для беспроводных сетей, представила адаптер WL-160W.

Новое устройство отличает поддержка черновой версии протокола IEEE 802.11n (Draft), который обеспечивает повышенную скорость передачи данных и увеличенную зону охвата беспроводной сети по сравнению с существующими продуктами для стандартов IEEE 802.11b/g.

Поддержка технологии Multiple Input, Multiple Output (MIMO) позволяет добиться скорости свыше 100 Мбит/с, что превышает возможности проводных сетей Fast Ethernet. ASUS WL-160W совместим с основными стандартами шифрования WEP, WPA и WPA2, что должно гарантировать надёжную защиту данных при работе в беспроводной сети.

Новый адаптер Wi-Fi от ASUS подключается к персональному компьютеру или ноутбуку посредством интерфейса USB 2.0. Производитель рекомендует использовать WL-160W вместе с беспроводным маршрутизатором WL-500W Super Speed N. Стоит также отметить, что представленный адаптер достаточно прост в настройке и эксплуатации. Конфигурацию упрощает интуитивный мастер установки. ***abit выпустила Wi-Fi карту под PCI-Express 1x***

***13.12.2006***

Производители потихоньку начинают «обживать» до сих пор все больше пустующие слоты PCI-Express 1x: abit выпустила выполненный в этом формате адаптер беспроводного доступа стандарта 802.11b/g AirPace Wi-Fi.

Никаких технологий для «сверхстандартной» пропускной способности не предлагается, максимум – штатные 54 Мбит/с, но «изюминка» все же присутствует – это возможность работать в режиме программной имитации точки доступа, при этом локальные ресурсы компьютера остаются доступными для внешних подключений.

Изображенный на снимке черный предмет, присоединенный к карте, при всей своей схожести с вантуcом, на самом деле, конечно, является комплектной внешней антенной. Производителем заявлено «низкое энергопотребление» и «расширенная поддержка безопасности», последняя выражается в совместимости со стандартами 64/128-бит WEP и WPA.

**Заключение.**

Беспроводные локальные сети (WLAN – wireless LAN) могут использоваться в офисе для подключения мобильных сотрудников (ноутбуки, носимые терминалы) в местах скопления пользователей - аэропортах, бизнес-центрах, гостиницах и т. д.

Мобильный Интернет и мобильные локальные сети открывают корпоративным и домашним пользователям новые сферы применения карманных ПК, ноутбуков. Одновременно с этим постоянно снижаются цены на беспроводное оборудование Wi-Fi и расширяется его ассортимент. Wi-Fi также подходит для людей, которым по долгу необходимо перемещаться по помещению, к примеру, на складе или в магазине. В этом случае для учета (отгрузки, приема и т. п.) товаров используются носимые терминалы, которые постоянно соединены с корпоративной сетью по протоколу Wi-Fi, и все изменения сразу отражаются в центральной базе данных. WLAN применим и в организации временных сетей, когда долго и нерентабельно прокладывать провода, а потом их демонтировать.

Еще один вариант использования – в исторических постройках, где прокладка проводов невозможна или запрещена. Иногда не хочется портить внешний вид помещения проводами или коробами для их прокладки. Кроме того, Wi-Fi-протокол подходит и для бытового применения, где тем более неудобно прогладывать провода.

  Что касается мобильных компьютеров, 12 марта 2003 года корпорация Intel представила технологию Intel Centrino для мобильных ПК — основу для мобильных компьютеров нового поколения со встроенными функциями беспроводной связи, которые предоставят корпоративным и домашним пользователям большую свободу и новые возможности подключения к компьютерным сетям. Технология, которую представляет торговая марка Intel Centrino для мобильных ПК, включает в себя процессор Intel Pentium M, семейство наборов микросхем Intel 855 и сетевой интерфейс Intel Pro/Wireless 2100. Все компоненты технологии оптимизированы, проверены и протестированы для совместной работы в мобильных системах.

Сетевой интерфейс Intel PRO/Wireless 2100 разработан и проверен на полную совместимость с узлами доступа 802.11b, сертифицированными по стандарту Wi-Fi. Он оснащен мощными встроенными средствами безопасности для беспроводных локальных сетей, включая технологии 802.11x, WEP и VPN, с возможностью программного обновления до поддержки WPA.

Wi-Fi технологии становятся все более совершенными и качество их соединения и безопасность стремительно приближается к возможностям обычного, широко используемого, проводного соединения.