Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Кафедра сетей и устройств телекоммуникаций

УНИВЕРСАЛЬНЫЙ ТЕЛЕКОММУНИКАЦИОННЫЙ ШЛЮЗ 2 WIRE 1701 HG: ПРИНЦИП ПОСТРОЕНИЯ И ТЕХНИЧЕСКОЙ ЭКСПЛУАТАЦИИ

Методические указания к лабораторной работе
по дисциплинам «Документальные службы и терминальные устройства телекоммуникаций» и «Защищенные терминальные устройства и цифровой абонентский телетрафик» для студентов специальностей 1-45 01 03 «Сети телекоммуникаций», 1-45 01 05 «Системы распределения мультимедийной информации», 1-98 01 02 «Защита информации в телекоммуникациях» всех форм обучения

Минск БГУИР 2011

УДК 621.391.(076)
ББК 32.811я73
И39

С о с т а в и т е л и:
А. И. Королёв, В. В. Рыжиков

Универсальный телекоммуникационный шлюз 2 Wire 1701 HG: принцип построения и технической эксплуатации : метод. указания к лаб. работе по дисц. «Документальные службы и терминальные устройства телекоммуникаций» и «Защищенные терминальные устройства и цифровой абонентский телетрафик» для студ. спец. 1-45 01 03 «Сети телекоммуникаций», 1-45 01 05 «Системы распределения мультимедийной информации», 1-98 01 02 «Защита информации в телекоммуникациях» всех форм обуч. /сост. А. И. Королев, В. В. Рыжиков. – Минск : БГУИР, 2011. –22 с.: ил.

И39

Излагаются принципы построения, функционирования, основные характеристики и общие правила технической эксплуатации универсального телекоммуникационного шлюза 2 Wire 1701 HG, предназначенного для организации беспроводных локальных сетей WLAN по технологии Wi-Fi. Приведены описание лабораторной установки и методики выполнения лабораторной работы с использованием универсального телекоммуникационного шлюза 2 Wire 1701 HG.

УДК 621.391(076)
ББК 32.811я73

Перечень основных сокращений

ЛС – локальная сеть

Модем – модулятор (MOD) и демодулятор (DEMOD)

ПК – персональный компьютер

ТВ – телевизионное вещание

Факс – факсимильный аппарат

Шлюз – устройство распределения (коммутации) информации

ADSL (Asynchronous Digital Subscriber Loop) – асинхронная цифровая абонентская линия связи

Broadband Link – широкополосная линия связи

EAP (Extensible Authentification Protocol) – протокол расширенной аутентификации

Home PNA – имя

Local Network – локальная сеть

MIC (Message Integrity Check) – технология проверки целостности сообщений

Network – сеть

Power – индикатор электропитания

TKIP (Temporal Key Integrity Protocol) – протокол интеграции временного ключа

USB (Universal Serial Bus) – кабельная шина

VPN (Virtual Path Network) – частная виртуальная сеть

WEP (Wired Equivalent Privacy) – функция шифрования потоков данных

Wi-Fi – беспроводная сеть

WPAC (Wi-Fi Protected Acces) – технология защищенного доступа к беспроводным сетям

2 Wire Gateway – двухпроводный шлюз

Лабораторная работа №2

ИЗУЧЕНИЕ ПРИНЦИПА ПОСТРОЕНИЯ И ТЕХНИЧЕСКОЙ ЭКСПЛУАТАЦИИ УНИВЕРСАЛЬНОГО ШЛЮЗА ТИПА 2 WIRE 1701 HG

Цель работы

Изучить принцип построения, функционирования универсального шлюза; получить практические навыки в настройке и технической эксплуатации универсального шлюза типа 2 Wire 1701 HG.

2.1. Домашнее задание

Изучить основные технические характеристики; принцип построения и функционирования шлюза 2 Wire 1701 HG; основные принципы и этапы его технической эксплуатации.

Рассмотреть методику настройки шлюза при его использовании в проводном и беспроводном режимах.

2.2. Состав лабораторной установки

В состав лабораторной установки входят шлюз 2 Wire 1701 HG, четыре компьютера с сетевыми платами, поддерживающими протокол Wi-Fi, локальная сеть лаборатории 501, являющаяся составной частью мультисервисной сети кафедры СиУТ.

Обобщенная структурная схема лабораторной установки представлена на рис. 2.1.

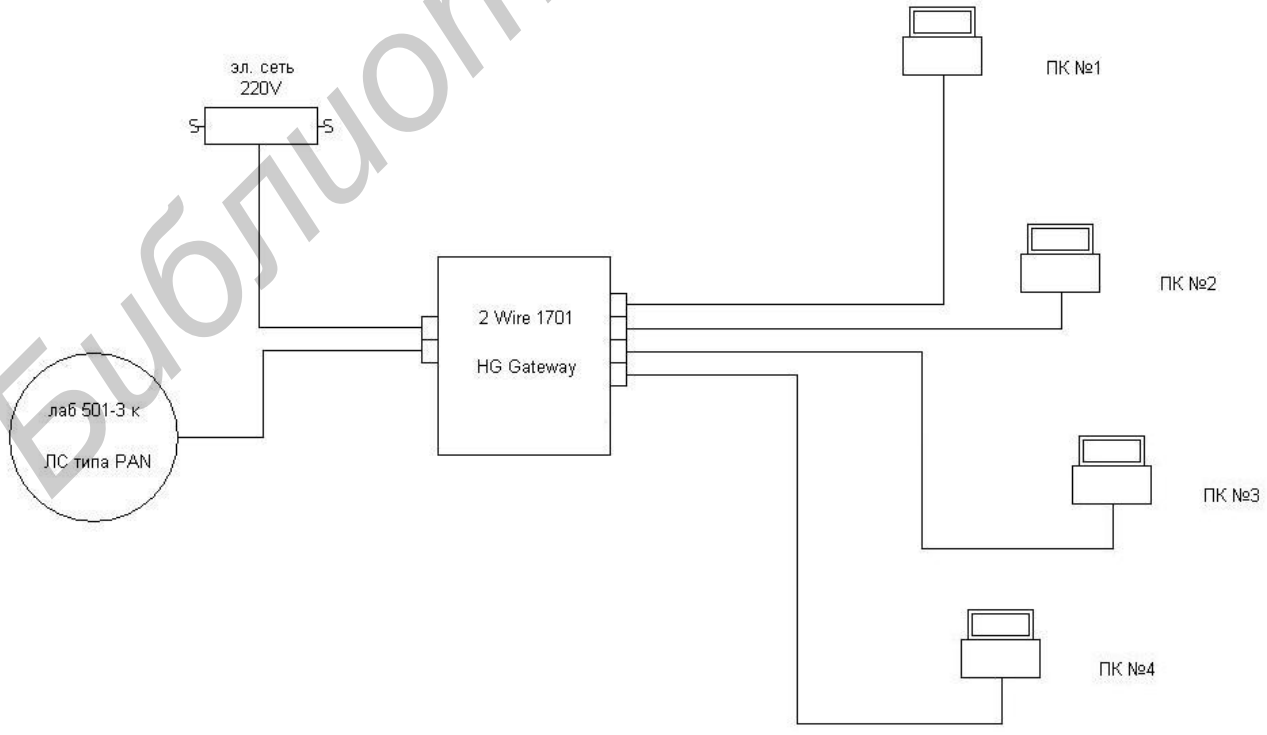

Рис. 2.1

2.3. Назначение, принцип построения и основные технические характеристики шлюза 2 Wire 1701 HG

2.3.1. Назначение и принцип организации сети

Шлюз 2 Wire 1701 HG (двухпроводный шлюз) предназначен для организации беспроводных (по технологии Wi-Fi) локальных сетей WLAN с радиусом действия до 100 м и возможностью использования проводных корпоративных локальных сетей.

Устройство 2 Wire 1701 HG обеспечивает возможность подключения до четырех хостов по проводному интерфейсу Fast Ethernet (FE) и до 254 беспроводных устройств по радиоинтерфейсу 802.11 b/g. Если требуется подключить более четырех хостов по проводному интерфейсу FE, то можно использовать любой недорогой коммутатор (Switch) с необходимым количеством портов.

Устройство 2 Wire 1701 HG по своей сути – это Wi-Fi-маршрутизатор со встроенным модемом, поддерживающий технологию ADSL; по способу организации сети данное устройство обеспечивает структуру сети, получившую название «инфраструктура». Обобщенная структура данной сети представлена на рис. 2.2

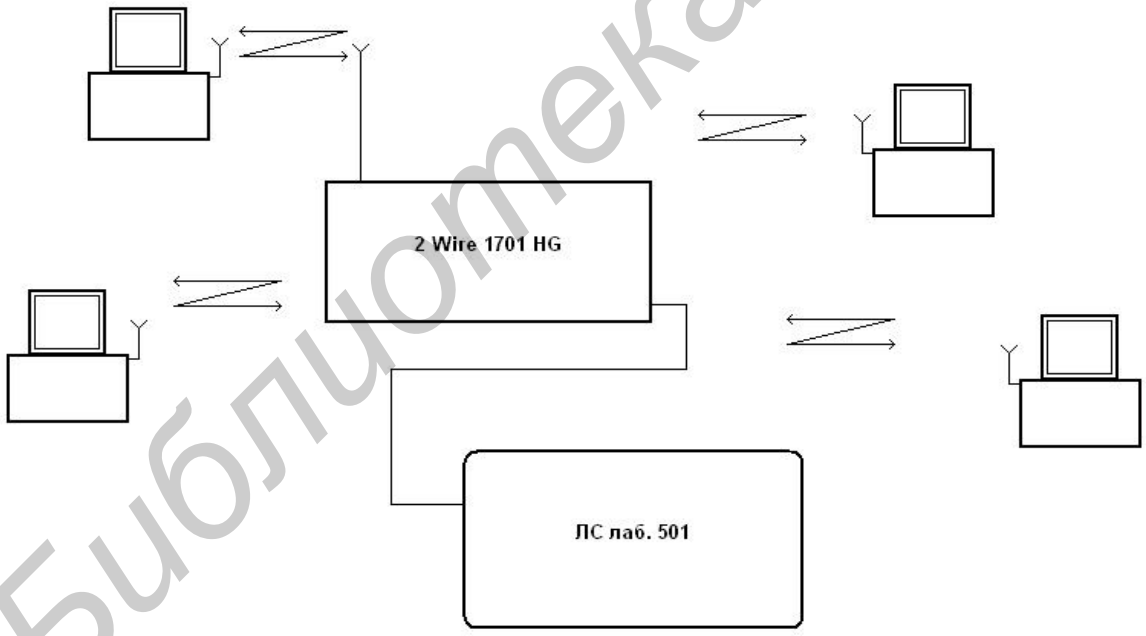

Рис. 2.2

При организации сети данной структуры все компьютеры должны быть оснащены беспроводными сетевыми картами и подключены к точке доступа 2 Wire 1701 HG; точка доступа должна быть подключена к проводной сети.

Кроме организации сети данной структуры 2 Wire 1701 HG может обеспечивать следующие варианты связей:

1) соединение по принципу Ad-Hoc «точка – точка». Данное соединение абонентов или ПК можно представить в виде следующей схемы (рис. 2.3);

Рис. 2.3

2) соединение с использованием роутера (маршрутизатора) и модема, что условно можно представить в виде схемы (рис. 2.4).

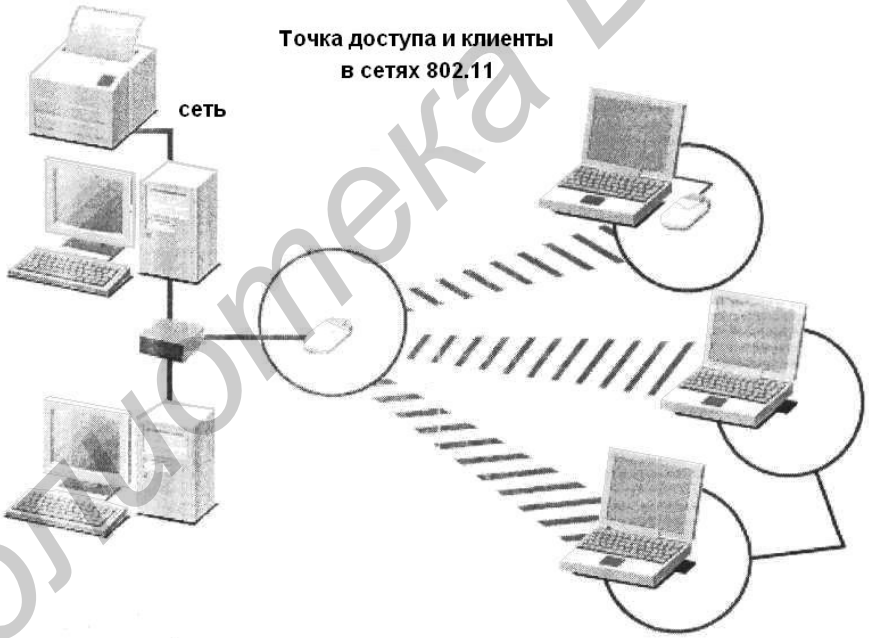

Рис. 2.4

Данное соединение – это соединение по принципу организации «клиентской точки». В этом режиме точка доступа работает как клиент и может соединяться с точкой доступа, работающей в инфраструктурном режиме. К такой точке можно подключить только один MAC-адрес. Поэтому задача состоит в том, чтобы объединить только два компьютера; два Wi-Fi-адаптера могут работать друг с другом напрямую без центральных антенн;

3) соединение по принципу «мост»; условно данное соединение можно представить в виде схемы (рис. 2.5);

Рис. 2.5

4) использование 2 Wire l701 HG в качестве репитера (повторителя) по следующей схеме (рис. 2.6).

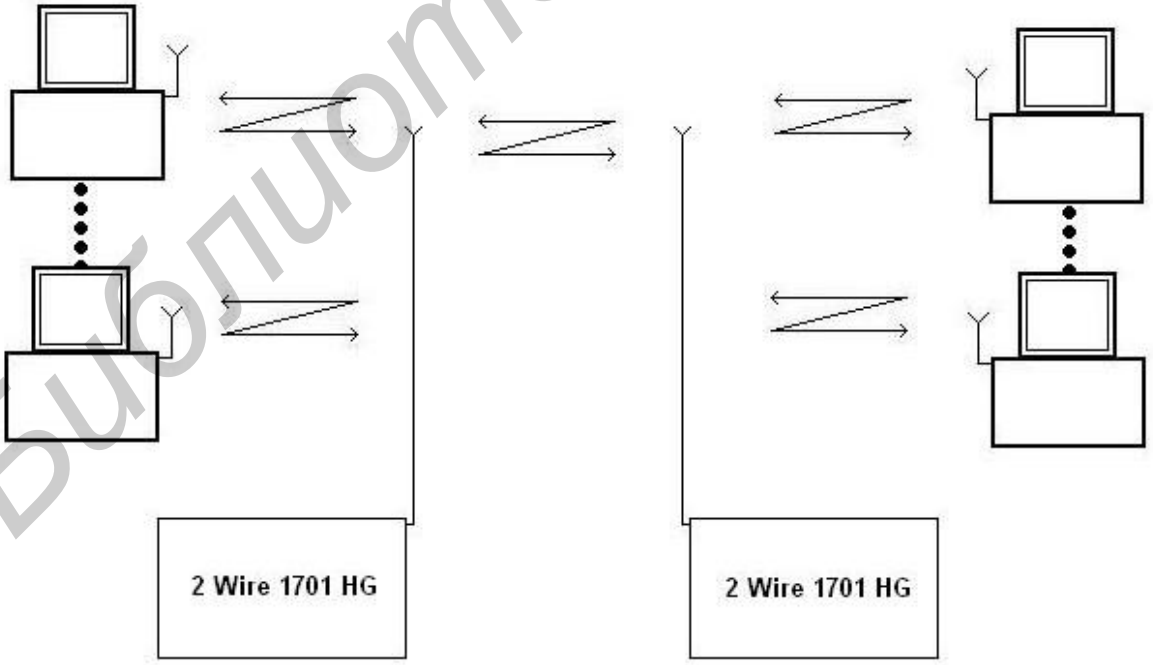

Рис. 2.6

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

2.3.2. Основные технические характеристики 2 Wire l701 HG

1. Интерфейсы местной сети: Ethernet; Home PNA; USB; беспроводной стандарт 802.11 b/g.

2. Совместимость стандартов:

– ADSL G.dmt (r992.1 ITU); внутренняя или внешняя пара;

– ASNI T1.413; внутренняя или внешняя пара;

– Home PNA 2.0 (10 Мбит/с) и 1.0 (1 Мбит/с);

– USB 1.1;

– TCP/IP, DHCP и доменная система имен DNS (клиент-сервер для DHCP и доменной системы имен DNS);

– VPN-передача с PPTP, L2TP, IP Sec;

– PPPoE, PPPoA (RFC2364) и RFC2684;

– Ethernet 802.3;

– Wi-Fi 802.11 b/g беспроводной;

– прямое подключение USB поддерживается на следующих операционных системах (ОС):

а) Windows 98 SE, ME, 2000, XP;

б) Mac OS 9.X или Mac 10.2;

– компакт-диск установки поддерживается на следующих операционных системах (ОС):

а) Windows 98 SE, ME, 2000, XP;

б) Mac 10.1 или выше;

– web-браузер: Netscape 7.1, Microsoft Internet Explorer или выше.

2.3.3. Общие сведения о стандартах беспроводной связи IEEE 802.11

Первый промышленный стандарт для организации беспроводных локальных сетей Wireless Local Area Networks (WLAN) был принят в 90-х гг. прошлого века. Аналогично проводному Ethernet 802.3 стандарт IEEE 802.11 определяет протокол использования единой среды передачи, получивший название Carrier Sense Multiple Access Collision Avoidance (CSMA/CA). Вероятность коллизий (конфликтов) беспроводных узлов минимизируется путем предварительной посылки короткого сообщения, называемого ready to send (RTS), которое 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). Такая посылка позволяет передающему узлу узнать, свободна ли среда и готов ли приемный узел к приему. После получении пакета данных приемный узел должен передать сигнал подтверждения (АСК) факта безошибочного приема. Если АСК 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, авторизирован в ней, а также шифрование для защиты от подслушивания.

На физическом уровне стандарт предусматривает использование двух радиоканалов и один канал инфракрасного диапазона.

В основу стандарта IEEE 802.11 положена сотовая архитектура (структура) организации сети. Сеть может состоять из одной или нескольких сот (ячеек). 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 Servise Set (BSS). Точки доступа многосотовой сети взаимодействуют между собой через распределительную систему Distribution System (DS), представляющую собой эквивалент магистрального сегмента кабельных ЛС. Вся инфраструктура, включая точки доступа и распределительную систему, образует расширенную зону обслуживания Extended Service Set (ESS). 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, которые имеют разную буквенную индексацию, а именно, IEEE 802.11a – IEEE 802.11x. На практике наибольшее применение получили три стандарта, а именно, IEEE 802.11a, 802.11b, 802.11g. В табл. 2.1 приведены основные характеристики данных стандартов.

Таблица 2.1

Основные характеристики стандартов беспроводной связи
(IEEE 802.11a, IEEE 802.11b, IEEE 802.11g)

Основные технические параметры стандартов	Стандарт IEEE 802.11		
	802.11a	802.11b	802.11g
Количество используемых радиоканалов	Три неперекрывающихся радиоканала	Три неперекрывающихся радиоканала	Три неперекрывающихся радиоканала
Частотный диапазон, ГГц	5	2,4	2,4
Максимальная скорость передачи данных, Мбит/с	54	11	54
Ориентировочная дальность передачи данных, м	12 м при 54 Мбит/с; 100 м при 11 Мбит/с	30 м при 11 Мбит/с; 100 м при 1 Мбит/с	15 м при 54 Мбит/с; 50 м при 11 Мбит/с

Шлюз, или маршрутизатор, 2 Wire l701 HG функционирует на основе реализации протоколов двух нижних уровней модели ISO/OSI, а именно, физического и канального. Основными функциональными блоками шлюза являются приемопередатчик, интерфейс проводной сети, встроенный микропроцессор и программное обеспечение. Обобщенная структурная схема шлюза приведена на рис. 2.7.

Рис. 2.7

Физический уровень стандарта IEEE 802.11 предусматривает передачу сигнала одним из двух методов: прямой последовательности Direct Sequence Spread Spectrum (DSSS) и частотных скачков Frequency Hopping Spread Spectrum (FHSS).

Данные методы различаются способом используемой модуляции, но характеризуются одной и той же технологией расширения спектра. Основной принцип технологии расширения спектра Spread Spectrum (SS) заключается в том, чтобы от узкополосного спектра сигнала, возникающего при обычном потенциальном кодировании, перейти к широкополосному спектру, что позволяет значительно повысить помехоустойчивость передаваемых данных.

Обе технологии расширения спектра DSSS и FHSS основаны на применении процедуры двухэтапной модуляции несущей.

По методу DSSS каждый бит исходного сообщения представляется специальными 11-разрядными кодовыми комбинациями (путем выполнения логической операции «исключающее ИЛИ»), и уже результирующая последовательность модулирует передаваемый в эфир радиосигнал (при этом используется фазовая модуляция несущей; при каждом переходе логического уровня из 0 в 1 или 1 в 0 происходит смещение фазы синусоидального колебания). Псевдослучайные кодовые комбинации придают радиосигналу характер шума, в 11 раз увеличивая спектр частот исходного узкополосного сигнала и распределяя его мощность по всему диапазону частот радиоканала.

Для выделения полезной информации приемная сторона использует ту же кодовую последовательность. Поддержание синхронности фазы несущего колебания в приемнике и передатчике осуществляется передатчиком посредством формирования через определенные промежутки времени специального синхросигнала.

Согласно методу FHSS модулирование несущего радиосигнала выполняется непосредственно исходным сообщением с использованием частотной модуляции, при которой передача логических уровней 0 и 1 осуществляется на частотах, расположенных несколько выше или ниже центральной. Расширение спектра производится в соответствии с заданной последовательностью, используемой передатчиком и приемником.

Стандартом IEEE 802.11 предусмотрено 79 возможных значений несущего колебания, причем длительность удержания частоты на каждом уровне (dwell time) составляет 20 мс. В этом случае сигнал FHSS можно считать широкополосным только на достаточно большом интервале времени, включающем много периодов удержания, поскольку на каждом из последних диапазон частот передаваемого радиосигнала определяется спектром исходного сообщения, т. е. фактически является узкополосным.

Канальный уровень включает в себя два подуровня: управление логическим соединением Logical Link Control (LLC) и управление доступом к среде передачи Media Access Control (MAC). У проводной сети Ethernet и 2 Wire l701 HG один и тот же LLC, что значительно упрощает объединение проводных и беспроводных сетей. Подуровни MAC данных сетей имеют тонкие различия. Эти различия состоят в следующем.

В сетях Ethernet для обобщения возможности множественного доступа к общей среде передачи, например, к кабелю связи, используется протокол CSMA/CD, а в сетях 802.11 используется полудуплексный режим передачи. В этом случае каждая станция может либо принимать, либо передавать информацию, а поэтому обнаружить конфликты в процессе передачи невозможно.

Для сетей стандартов IEEE 802.11, как отмечалось выше, был разработан модифицированный вариант протокола CSMA/CD, получивший название CSMA/CA. Работает он следующим образом. Станция, которая собирается передавать информацию, сначала «слушает эфир» и, если среда передачи данных все еще свободна, осуществляет передачу. Наличие случайной задержки необходимо для того, чтобы сеть не «зависала», если несколько станций одновременно захотят получить доступ к частоте. Если информационный пакет приходит без искажений, принимающая станция посылает обратно подтверждение.

Целостность пакета проверяется методом контрольной суммы. Получив подтверждение, передающая станция считает процесс передачи данного информационного пакета завершенным. Если подтверждение не получено, станция считает, что произошла коллизия (конфликт), и пакет передается снова через случайный промежуток времени.

Еще одна специфичная для беспроводных сетей проблема – две клиентские станции имеют плохую связь друг с другом, но при этом качество связи каждой из них с точкой доступа хорошее. В таком случае передающая клиентская станция может посылать на точку доступа запрос на очистку эфира. Тогда по команде с точки доступа другие клиентские станции прекращают передачу на

время «общения» двух точек с плохой связью. Режим принудительной очистки эфира (протокол Request to Send/Clear to Send – RTS/CTS) реализован далеко не во всех моделях оборудования стандарта IEEE 802.11 и если он есть, то включается лишь в крайних случаях. В Ethernet при передаче потоковых данных используется управление с точки доступа к каналу связи, распределенное между всеми станциями. Напротив, в стандарте IEEE 802.11 в таких случаях применяется централизованное управление с точки доступа. Клиентские станции последовательно опрашиваются на предмет передачи потоковых данных. Если какая-нибудь из станций сообщает, что она будет передавать потоковые данные, точка доступа выделяет ей промежуток времени, в который из всех станций сети будет передавать только она.

Следует отметить, что принудительная очистка эфира снижает эффективность работы беспроводной сети, поскольку связана с передачей дополнительной служебной информации и кратковременными перерывами в связи. Кроме этого, в проводных сетях Ethernet при необходимости можно реализовать не только полудуплексный, но и дуплексный вариант передачи, когда коллизия обнаруживается в процессе передачи (это повышает реальную пропускную способность сети). Поэтому при прочих равных условиях реальная пропускная способность беспроводной сети стандарта IEEE 802.11b будет ниже, чем у проводного Ethernet. Таким образом, если сетям Ethernet 10 Мбит/с и IEEE 802.11b (максимальная скорость передачи 11 Мбит/с) с одинаковым числом пользователей давать одинаковую нагрузку, постепенно увеличивая ее, то начиная с некоторого порога сеть IEEE 802.11b начнет «тормозить», а Ethernet все еще будет функционировать нормально.

Поскольку клиентские станции могут быть мобильными устройствами с автономным питанием, в стандарте IEEE 802.11 большое внимание уделено вопросам управления питанием. В частности, предусмотрен режим, когда клиентская станция через определенные промежутки времени «просыпается», чтобы принять сигнал включения, который, возможно, передает точка доступа. Если этот сигнал принят, клиентское устройство включается, в противном случае оно снова «засыпает» до следующего цикла приема информации.

2.3.4. Методы организации защиты информации в беспроводных Wi-Fi-сетях

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

Беспроводные сети отличаются от кабельных (проводных) сетей только на первых двух уровнях: физическом (Phy) и отчасти канальном 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 реализации

безопасности тех и других сетей сводится к разнице в реализации безопасности физического и канального уровней.

В настоящее время для защиты 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. Установлено, что если на стадии запуска настройке сети не уделить должного внимания, то злоумышленник может [1 – 4]:

а) заполучить доступ к ресурсам и дискам пользователей Wi-Fi, а через нее и к ресурсам сети LAN;

б) контролировать трафик и извлекать из него конфиденциальную информацию;

в) искажать проходящую в сети информацию;

г) воспользоваться интернет-трафиком;

д) атаковать ПК пользователей и серверы сети;

е) внедрять поддельные точки доступа;

ж) рассылать спам и совершать другие противоправные действия от имени вашей сети.

Для защиты сетей стандарта IEEE 802.11 предусмотрен комплекс мер безопасности передачи данных.

На раннем этапе использования Wi-Fi-сетей таковым являлся пароль Server Set ID (SSID) для доступа в локальную сеть. Однако данная технология не обеспечивает надежную защиту.

Главной защитой долгое время было использование цифровых ключей шифрования потоков данных с помощью функции Wired Equivalent Privacy (WEP). Ключи являются обыкновенными паролями длиной от 5 до 13 символов кода ASCII.

Данные шифруются ключом разрядностью от 40 до 104 бит. Но это не целый ключ, а только его статическая составляющая. Для усиления защиты применяется 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 кодовым словом. Таким образом, общее шифрование реализуется разрядностью кода от 64 (40 + 24) до 128 (104 + 24) бит. В результате при шифровании используются как постоянные, так и случайно подобранные символы.

Однако взломать такую защиту можно соответствующими утилитами из Интернета, например Airsnot WEPcrack и др. Слабое место такой защиты – это вектор инициализации, так как используется 24 бита и формируется около 16 миллионов комбинаций, после использования которых ключ начинает повторяться, поэтому хакеру необходимо найти эти повторы (для этого потребуется менее часа времени) и за секунды взломать остальную часть ключа. После этого он может входить в сеть как обычный зарегистрированный пользователь.

Так как стандарт WEP не обеспечивает надежной защиты данных для проводных и беспроводных сетей, то в 2001 г. был внедрен новый стандарт IEEE 802.1X, который использует вариант динамических 128-разрядных ключей шифрования, т. е. 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.

Стандарт IEEE 802.1X позволяет подключать в сеть даже PDA-устройства, что способствует более выгодному использованию самой идеи беспроводной связи. Стандарты IEEE 802.1X и 802.11 являются совместимыми. В стандарте IEEE 802.1X применяется тот же алгоритм, что и в WEP, а именно, алгоритм RC4, но с некоторыми различиями. Стандарт IEEE 802.1X базируется на протоколе расширенной аутентификации (EAP), протоколе защиты транспортного уровня (TLS) и сервере доступа Remote Acces 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 г. был внедрен стандарт Wi-Fi Protected Acces (WPA), который совмещает преимущества динамического обновления ключей стандарта IEEE 802.1X с кодированием протокола интеграции временного ключа TKIP, протоколом расширенной аутентификации (EAP) и технологической проверки целостности сообщений MIC. WPA – это современный стандарт, о котором договорились производители оборудования, пока не вступил в силу IEEE 802.11i. По сути WPA = 802.1X + EAP + TKIP + + MIC, где:

а) WPA – технология защищенного доступа к беспроводным сетям;

б) EAP – протокол расширенной аутентификации (Extensible Authentification Protocol);

в) TKIP – протокол интеграции временного ключа (Temporal Key Integrity Protocol);

г) MIC – технология проверки целостностей сообщений (Message Integrity Check).

Стандарт TKIP использует автоматически подобранные 128-битные ключи, которые создаются непредсказуемым способом и общее число вариации которых достигает 500 миллиардов. Сложная иерархическая система алгоритма подбора ключей и динамическая их замена через 10 Кбайт (10 тыс. передаваемых пакетов) делают систему максимально защищенной.

От внешнего проникновения и изменения информации также защищает технология поверки целостности сообщений (MIC). Достаточно сложный математический алгоритм реализации позволяет сверять данные, отправленные в одной точке и полученные в другой. Если замечены изменения и результат сравнения не сходится, такие данные считаются ложными и выбрасываются.

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

Помимо этого, параллельно разрабатывается множество самостоятельных стандартов безопасности: в данном направлении преуспевают Intel и Cisco. В 2004 г. появляется WPA2, или стандарт 802.11 I, который в настоящее время является максимально защищенным.

Беспроводная сеть считается защищенной, если в ней функционируют три основные составляющие 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, а именно:

– шифровать данные путем использования различных алгоритмов и систем. Максимальный уровень безопасности обеспечит применение VPN;

– использовать протокол стандарта 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 NetBEUI в данном случае безопаснее;

– не разрешать гостевой доступ к ресурсам общего доступа и 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, устанавливать точку доступа вне брэндмауэра, использовать минимум протоколов внутри WLAN (например только HTTP и SMTP);

– регулярно исследовать уязвимость сети с помощью специализированных сканеров безопасности (например NetStumbler);

– использовать специализированные сетевые операционные системы, такие, как Windows NT, Windows 2003, Windows XP.

Также угрозу сетевой безопасности могут представлять природные явления, технические устройства и люди (недовольные уволенные служащие, хакеры, конкуренты).

2.4. Порядок выполнения лабораторной работы

2.4.1. Порядок включения проверки и работоспособности шлюза 2 Wire 1701 HG

Для включения и проверки работоспособности шлюза необходимо:

а) чтобы все устройства, которые подключены к шлюзу, имели сетевой интерфейс, совместимый с моделью используемого шлюза 2 Wire 1701 HG;

б) проверить подключение шлюза к электросети, локальной сети лаборатории 501 и мультимедийной сети кафедры;

в) проверить подключение четырех ПК к шлюзу (см. рис. 2.2);

г) включить электропитание шлюза и ПК. Далее проверка функционирования шлюза выполняется в режимах POWER (электропитание), Local Network (локальная сеть) и Broadbank Link (широкополосная линия связи) по методике, приведенной в табл. 2.2, 2.3 и 2.4 соответственно.

Таблица 2.2

Индикатор POWER (электропитание)

Цвет индикатора Power (питания)	Состояние шлюза
OFF (выключено)	Не подключено питание
Мигающий зеленый	Шлюз загружается
Зеленый	Шлюз включен
Красный	Системная ошибка. Обратитесь в службу поддержки

Таблица 2.3

Индикатор Local NetWork (локальная сеть)

Цвет индикатора Local NetWork	Состояние шлюза
OFF (выключено)	Шлюз не подключен к розетке питания, компьютеру или главному компьютеру путем Home PNA, USB, Ethernet или Wireless
ON (включено)	Шлюз подключен

Таблица 2.4

Индикатор «Broadbank Link» (широкополосная линия связи)

Цвет индикатора Broadbank Link	Состояние шлюза
OFF (выключено)	Нет широкополосного сигнала. Шлюз не подключен или нет подключения к нужному сервису
Мигающий оранжевый	Шлюз устанавливает соединение
Красный	Шлюз не обнаружил сигнала
Оранжевый	Шлюз обнаружил сигнал, но не смог подключиться к провайдеру сети Internet либо (или) не было настроено соединение
Мигающий зеленый	Шлюз подключает доступные сервисы
Зеленый	Шлюз полностью подключил доступные сервисы

2.4.2. Порядок проверки работоспособности шлюза 2 Wire 1701 HG в режиме проводного соединения

Для проверки работоспособности шлюза в режиме проводного соединения необходимо выполнить следующее:

1. В папке «Сетевое окружение» найти текущее проводное соединение. При работоспособности шлюза и правильном подключении статус соединения будет отображаться как «Подключено».

2. Зайти в свойства сетевого соединения. В свойствах протокола TCP/IP необходимо установить IP-адрес для проводной сетевой платы. Вводим IP-адрес 192.168.1.X (X – любое число от 2 до 63).Маска подсети – 255.255.255.0. Шлюз – 192.168.1.254;

3. Для проверки работоспособности сети проверить обмен пакетами компьютера со шлюзом. Если обмен происходит, можно считать, что соединение установлено правильно.

В меню «Пуск» —> «Выполнить» выполнить команду ping 192.168.1.254.

4. После настройки другого компьютера аналогичным образом можно проверить работоспособность соединения между двумя компьютерами. Для этого на обоих компьютерах выполнить команду ping с IP-адресом соседа. IP-адрес можно узнать, посмотрев «Состояние» —> «Поддержка» в свойствах соединения.

5. Еще одним способом проверки правильности соединения является проверка свойств локальной сети в самом шлюзе. Чтобы попасть в эти свойства, в браузере (например Internet Explorer) наберем адрес шлюза 192.168.1.254. Попадаем во внутренние настройки шлюза. Выбираем пункт «Home NetWork» и на панели «Local Devices» видим компьютеры, включенные в локальную сеть, а также способ соединения – проводной или беспроводной.

6. Также можно не устанавливать IP-адреса вручную, а оставить «получить IP-адрес автоматически». Тогда по технологии DHCP шлюз сам раздаст IP-адреса по порядку, начиная с 192.168.1.64.

В этом случае для проверки работоспособности следует зайти в «Состояние» —> «Поддержка» и узнать полученный IP-адрес.

Таким образом, узнав IP-адреса всех компьютеров в сети, можно выполнить команду ping, воспользовавшись известными нам IP-адресами. Следовательно, будет проверена работоспособность всей сети.

2.4.3. Порядок проверки работоспособности шлюза 2 Wire 1701 HG в режиме беспроводного соединения

Для проверки работоспособности шлюза в режиме беспроводного соединения необходимо выполнить следующее:

1. В папке «Сетевое окружение» найти текущее беспроводное соединение. Выбрать его и нажать «Подключить». При запросе ключа шифрования ввести: 6860489106 (указан на наклейке снизу шлюза).

Далее повторить пп. 2 – 6 (см. п. 2.4.2) для беспроводной сети.

2. Проверить работоспособность беспроводной сети:

а) вручную физически вытащить кабель из соответствующего порта шлюза 2 Wire 1701 HG. В «Сетевых подключениях» проводное соединение станет недоступно, останется лишь беспроводное. Командой ping можно проверить доступность обоих интерфейсов. Обмен пакетами по проводному интерфейсу происходить не будет;

б) в «Сетевых подключениях» можно использовать функцию «Отключить» на проводном соединении. Командой ping снова проверить доступность интерфейсов.

2.4.4. Настройка и соединение шлюза 2 Wire 1701 HG , подключенного к ПК, с сетью Интернет

1. Зайдем в настройки широкополосного соединения, для чего в браузеренаберем адрес шлюза 192.168.1.254. Выберем пункт «Broadbank Link» —> «Advanced Setting».

Для подключения к сети Интернет по технологии ADSL установим следующие параметры:

1) «ATM Circuit Identifier» – VPI и VCI. Данные параметры определены

провайдером услуг ADSL (в частности, для провайдера «Белтелеком» данные параметры равны: VPI = O, VCI = 33). Эти параметры уникальны для каждого провайдера;

2) «ATM Encapsulation» – метод формирования ATM-кадра. Выберем значение «Bridged LLC». Это позволит прописать имя пользователя и пароль внутри шлюза и избавит от необходимости каждый раз вручную подключаться к Интернету. Подключение будет происходить автоматически при включении шлюза;

3) в разделе «Broadband Connection» установим тип соединения «Connection Type». Для ADSL – соединения используем тип соединения PPP (Point to Point – «точка – точка»). Далее пропишем параметры PPP:

«Username» – имя пользователя.

«Password» – пароль.

«Confirm password» – подтверждение пароля.

Эти параметры также выдаются провайдером. Остальные параметры являются необязательными, и их можно не изменять.

После окончания настроек нажмем кнопку «Save» («Сохранить настройки»).

2.4.5. Настройка параметров безопасности шлюза 2 Wire 1701 HG

Настройка параметров безопасности шлюза выполняется по следующей методике:

1. В устройство 2 Wire 1701 HG встроен сетевой защитник – брандмауэр (Firewall). Изменяя его настройки, можно либо полностью запретить/разрешить как входящий, так и исходящий трафик, либо гибко настроить под необходимые протоколы или конкретные приложения.

Для настройки параметров безопасности наберем в браузере адрес шлюза 192.168.1.254. Выберем пункт «Firewall» —> «Advanced Setting».

В разделе «Setting» —> «Security» есть три главные опции, обеспечивающие сетевую защиту:

1) «Stealth Mode» – режим «невидимый». Если данный режим включен, шлюз 2 Wire 1701 HG при попытке запроса на подключение к сети извне, не возвращает никакого сообщения в ответ, и таким образом сети как бы не существует. В противном случае посылается ответ «подключение недоступно», таким образом, подтверждается, что сеть существует, но доступ к ней запрещен;

2) «Block Ping» – блокировка запроса. Обычно команда ping (запрос) используется для проверки доступности сетевого интерфейса по его IP-адресу и диагностики. Но в последнее время злоумышленники научились использовать эту безвредную команду с целью получения конфиденциальной информации. Поэтому иногда целесообразно заблокировать эту возможность;

3) «Strict VDP Session Control» – строгий контроль сеанса VDP.

Эта возможность сетевой защиты обеспечивает уровень повышенной безопасности, которая позволяет не принимать пакеты, посланные из неизвестного источника по существующему подключению.

В дополнение к проверке информации об адресате шлюз также будет проверять информацию об источнике подключения.

2. «Inbound and Outbound Control» – управление входящим и исходящим трафиком.

В данном разделе можно запрещать/разрешать входящий (Inbound) или исходящий (Outbound) трафик для определенного типа протокола (например FTP, HTTP, Net BIOS). Протоколы, отмеченные галочкой, будут разрешены.

3. Шлюз также имеет возможность гибко настроить параметры безопасности для отдельных программ, посылающих или принимающих сетевой трафик:

1) выберем «Firewall» —> «Firewall Settings»;

2) выберем пункт «Allow Individual Applications» и далее «Add a new user-defined Application»;

3) «Application name» – имя приложения можно ввести любое (например «test»);

4) «Protocol» – определяется протокол передачи TCP или VDP;

5) «Port (or Range)» – ввести конкретный порт (или диапазон портов), который будет использовать данное приложение;

6) «Protocol Timeout» – время работы протокола (или другими словами, нашего приложения). Эта функция очень полезна, если нужно ограничить время пользования сетью для пользователя;

7) «Map to Host Port» – переназначение порта. Эта функция используется, когда нужно скрыть порты, по которым работает наше приложение во внешней сети. Это применяется с той целью, чтобы злоумышленник не мог однозначно определить, какое именно приложение работает в сети, и не мог остановить наш компьютер, «замаскировавшись» под это приложение.

Это означает, что если реально используются порты 101 – 110 и значение «Map to Host Port» установлено в 4000, то во внешней сети будут видны порты 4001 – 4010;

8) «Application Type» – этот параметр необязателен и используется лишь тогда, когда точно известен тип приложения (например FTP, PPTP, IRC);

9) после того как все параметры установлены, нажимаем «Add Definition»;

10) далее возвращаемся к пункту «Firewall Setting». В списке приложений находим наше приложение «test». Выделяем его и нажимаем «Add». После чего приложение «test» появится в списке «Hosted Application».

Следовательно, подобным образом можно настроить несколько приложений и использовать их одновременно;

11) удалить приложения можно кнопкой «Remove».

3. Оформление отчета

Отчет должен содержать:
– титульный лист, форма которого установлена кафедрой;
– результаты выполнения домашнего задания;
– основные технические характеристики аппаратуры шлюза 2 Wire 1701 HG;
– обобщенная структурная схема шлюза 2 Wire 1701HG и сети;
– связи на основе данного устройства;
– результаты выполнения лабораторной работы.

4. Контрольные вопросы

1. Перечислите основные качественные и количественные характеристики шлюза 2 Wire 1701 HG.
2. Поясните принцип построения и функционирования шлюза 2 Wire 1701 HG.
3. Поясните варианты построения сетей связи на основе шлюза 2 Wire 1701 HG.
4. Перечислите основные методы защиты информации, используемые в шлюзе 2 Wire 1701 HG, и их основные свойства.
5. Поясните порядок выполнения следующих процедур:
– включения и проверки работоспособности шлюза;
– проверки работоспособности в режиме проводного соединения;
– проверки работоспособности в режиме беспроводного соединения;
– настройки и соединения шлюза и подключенных к нему ПК с сетью Интернет;
– настройки шлюза для организации защиты ПК лабораторной установки от несанкционированного доступа.

Литература

1. Феер, К. Беспроводная цифровая связь. Методы модуляции и расширения спектра / К. Феер; пер. с англ.– М. : Радио и связь, 2001.
2. Универсальный телекоммуникационный шлюз 2 Wire 1701HG : техническое описание, 4.1.
3. Универсальный телекоммуникационный шлюз 2 Wire 1701HG : руководство пользователя, 4.2.
4. Стандарт IEEE 802.11.
5. Стандарт IEEE 802.15.

Св. план 2010, поз. 96

Учебное издание

УНИВЕРСАЛЬНЫЙ ТЕЛЕКОММУНИКАЦИОННЫЙ ШЛЮЗ 2 WIRE 1701 HG: ПРИНЦИП ПОСТРОЕНИЯ И ТЕХНИЧЕСКОЙ ЭКСПЛУАТАЦИИ

Методические указания
к лабораторной работе по дисциплинам
«Документальные службы и терминальные устройства телекоммуникаций»
и «Защищенные терминальные устройства и цифровой абонентский телетрафик» для студентов специальностей 1-45 01 03 «Сети телекоммуникаций», 1-45 01 05 «Системы распределения мультимедийной информации», 1-98 01 02 «Защита информации в телекоммуникациях»
всех форм обучения

Составители:
Королев Алексей Иванович
Рыжиков Валентин Владимирович

Редактор Л. А. Шичко
Корректор Е. Н. Батурчик
Компьютерная верстка М. В. Гуртатовская

Подписано в печать | Формат 60x84 1/16. | Бумага офсетная.
Гарнитура «Таймс». | Отпечатано на ризографе. | Усл. печ. л.
Уч.-изд. л. 1,2. | Тираж 50 экз. | Заказ 188.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0494371 от 16.03.2009. ЛП №02330/0494175 от 03.04.2009.
220013, Минск, П. Бровки, 6