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

Факультет инфокоммуникаций

Кафедра инфокоммуникационных технологий

А. И. Королёв, В. К. Конопелько, В. Ю. Цветков

ПЕРЕДАЧА И ЗАЩИТА ДАННЫХ В СЕТЯХ ИНФОКОММУНИКАЦИЙ. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

Рекомендовано УМО по образованию в области информатики и радиоэлектроники в качестве учебно-методического пособия для специальности 1-45 80 02 «Телекоммуникационные системы и компьютерные сети»

Минск БГУИР 2017

УДК [654:004.056](076.5)
ББК 32.88я73
К68

Р е ц е н з е н т ы:

кафедра систем телекоммуникаций учреждения образования
«Белорусская государственная академия связи»
(протокол №1 от 31.08.2016);

главный научный сотрудник государственного научного учреждения
«Объединенный институт проблем информатики Национальной академии
наук Беларуси», доктор технических наук, профессор С. Ф. Липницкий

Королёв, А. И.

К68 Передача и защита данных в сетях инфокоммуникаций. Лабораторный практикум : учеб.-метод. пособие / А. И. Королёв, В. К. Конопелько, В. Ю. Цветков. – Минск : БГУИР, 2017. – 106 с. : ил.

ISBN 978-985-543-340-9.

Излагаются методы организации передачи и защиты данных в Wi-Fi сетях, а также техническая диагностика универсального телекоммуникационного шлюза 2Wire1701HG, предназначенного для организации беспроводных сетей WLAN. Приведены описания восьми лабораторных работ и методика их выполнения.

УДК [654:004.056](076.5)
ББК 32.88я73

ISBN 978-985-543-340-9

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ ОСНОВНЫХ СОКРАЩЕНИЙ

АФУ – антенно-фидерное устройство
БЛС – беспроводная линия связи
БМ – беспроводной мост
БС – беспроводная связь
ЛС – локальная сеть
Модем – модулятор (MOD) и демодулятор (DEMOD)
ПД – передача данных
ПИ – передача информации
ПК – персональный компьютер
РК – радиоканал
ТД – точка доступа
ТмТ – точка – много точек
ТТ – точка – точка
ШЛС – широкополосная линия связи
ШПС – шумоподобный сигнал

ADSL (Asymmetric Digital Subscriber Link) – асимметричная цифровая абонентская линия
AHm (Ad-Hoc mode) – режим одноранговой сети
AP (Access Point) – точка (пункт) доступа
ApL (Application List) – список приложений
At (Authenticator) – аутентификатор
ATM (Asynchronous Transfer Mode) – асинхронный способ передачи
BL (Broadband Link) – широкополосная линия связи
Cnf (Configure) – настройка
DHCP (Dynamic Host Configuration Protocol) – динамический протокол конфигурации хоста
DL (Device List) – список устройств
DSL (Digital Subscriber Link) – цифровая абонентская линия
EAP (Extensible Authentication Protocol) – протокол расширенной аутентификации
Gateway – шлюз
LAN (Local Area Network) – локальная сеть
MDC (Management/Diagnostic Console) – консоль управления и диагностики
MIC (Message Integrity Check) – технология проверки целостности сообщения
NAP (Network Access Point) – точка сетевого доступа
NW (Network) – сеть

Router – маршрутизатор
TKIP (Temporal Key Integrity Protocol) – протокол целостности временного ключа
USB (Universal Serial Bus) – универсальная последовательная шина
VPI (Virtual Path Identifier) – идентификатор виртуального пути
VCI (Virtual Chanel Identifier) – идентификатор виртуального канала
WAN (Wide Area Network) – территориально распределенная сеть
WAP (Wireless Application Protocol) – протокол беспроводных приложений
WDS (Wireless Distribution System) – беспроводная распределенная система
WEP (Wired Equivalent Privacy) – функция шифрования потоков данных
WLAN (Wireless LAN) – беспроводная локальная сеть
WPA (Wireless Protocol Access) – технология защищенного доступа к беспроводным сетям
WWAN (Wireless WAN) – беспроводная территориально распределенная сеть
2 Wire Gateway – двухпроводный шлюз

ЛАБОРАТОРНАЯ РАБОТА №1

Методы организации и режимы передачи данных в Wi-Fi сетях

1.1 Цель работы

Изучить методы организации и режимы передачи данных в Wi-Fi сетях, реализуемые на основе оборудования фирмы D-Link.

1.2 Домашнее задание к лабораторной работе

1. Согласно данному методическому руководству и рекомендованной литературе подготовиться к выполнению лабораторной работы.
2. Изучить состав и основные технические характеристики комплекса технических средств, используемых для организации Wi-Fi сетей.
3. Изучить методы организации Wi-Fi сетей.
4. Изучить режимы передачи данных, используемые в современных Wi-Fi сетях применительно к оборудованию фирмы D-Link.

1.3 Методы организации Wi-Fi сетей

1.3.1 Классификация и краткая характеристика топологий Wi-Fi сетей

Методы организации сетей связи определяются их топологией, или структурой. *Топология* сети есть проекция сети на плоскость, определяющая места расположения оконечных устройств и коммутационного оборудования сети на обслуживаемой территории, а также их взаимосвязь друг с другом на основе соответствующих беспроводных каналов связи и в случае необходимости проводных каналов связи. При организации беспроводных сетей на основе технологий сети Wi-Fi наибольшее применение получили следующие топологии.

1.3.1.1 Топология сети типа «кольцо»

Сеть с топологией «кольцо» организуется таким образом, что каждая точка доступа сети имеет связь только с двумя соседними точками доступа. Условно топологию данного типа для четырех офисных зданий, каждое из которых может представлять собой беспроводную распределенную систему, можно представить в виде следующей схемы (рисунок 1.1).

В данной топологии сети нет четко выделенного центра, все точки доступа могут быть одинаковыми и иметь равные права. Подключение новых абонентов в сеть осуществляется, как правило, без всяких проблем, хотя и требует обязательной остановки работы двух крайних точек от вновь включаемой.

Важнейшее достоинство данной топологии сети состоит в том, что ретрансляция сигналов каждым абонентом позволяет существенно увеличить размеры всей сети в целом в общем случае до нескольких километров [1–4].

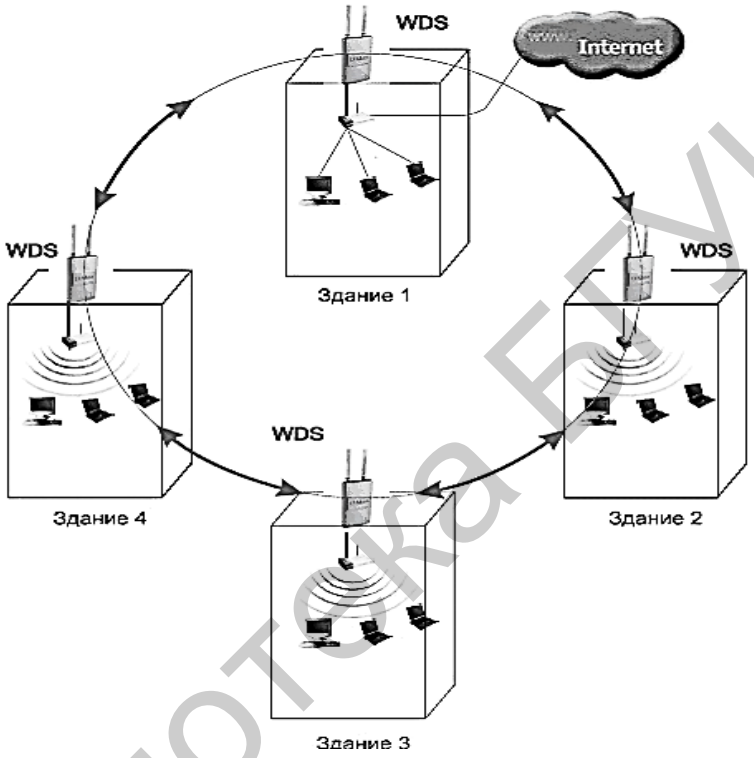


Рисунок 1.1 – Топология сети типа «кольцо»

Принцип связи между точками доступа в этом случае представляет собой ациклический (неправильный) граф типа «дерево», т. е. данные из сети Интернет к точке доступа 2 (Здание 2) могут приходить по двум направлениям, а именно: первое направление – через точку доступа 1 (Здание 1), второе направление – через точки доступа 1, 4, 3.

Для устранения лишних связей, способных приводить к появления циклов в графе, реализуется алгоритм Spanning tree (кодовое дерево). Его работа приводит к выявлению и блокированию лишних связей.

При изменении топологии сети, например, из-за отключения некоторых точек доступа или невозможности работы каналов радиосвязи, алгоритм Span-

ningtree запускается заново, и прежде заблокированные связи (радиоканалы) могут использоваться взамен вышедших из строя.

1.3.1.2 Топология сети типа «звезда»

Беспроводная сеть данной топологии имеет выделенную точку доступа, или выделенный центр сети, к которому подключаются все остальные абоненты сети. Обобщенная схема беспроводной сети данной топологии имеет следующее построение (рисунок 1.2).

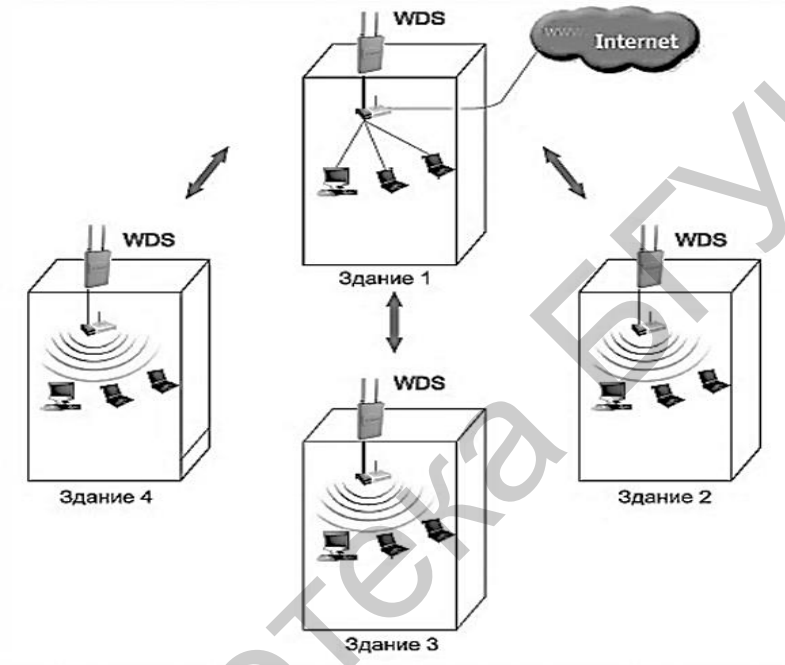


Рисунок 1.2 – Топология сети типа «звезда»

В сети связи с топологией «звезда» весь обмен информацией ведется только через центральную точку доступа, на которую, таким образом, ложится большая нагрузка.

Важнейшими недостатками данной топологии являются:

а) низкая надежность функционирования сети, которая обусловлена наличием одной центральной точки доступа. Для повышения надежности функционирования сети данной топологии требуется резервирование центральной точки доступа;

б) жесткое ограничение в количестве обслуживаемых абонентов. Это обусловлено тем, что все точки доступа работают на одном радиоканале, а центральная точка доступа одновременно может обслуживать порядка 10–15 периферийных точек доступа из-за большого падения скорости ПД.

К достоинствам сети данной топологии относятся:

а) высокая оперативность подключения новых пользователей сети;

б) выход из строя любой периферийной точки доступа не влияет на функционирование сети.

Общий вывод по данной топологии сети: целесообразно использовать в комбинации с другими типами топологий.

1.3.1.3 Топология сети типа «шина»

Топология данного типа носит также название «магистраль» и самой своей структурой предполагает использование однотипного сетевого оборудования ПК и КПК, а также равноправия в сети всех абонентов.

Обобщенная структурная схема сети данной топологии имеет данное построение (рисунок 1.3)

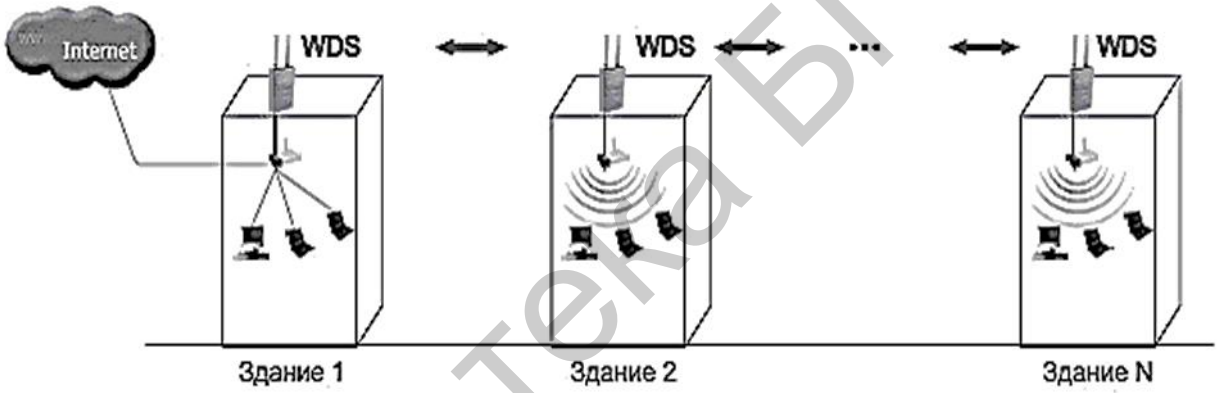


Рисунок 1.3 – Топология сети типа «шина»

В сети связи данной топологии отсутствует точка доступа с функциями центральной станции, что увеличивает надежность функционирования сети. К достоинствам сети связи данной топологии следует отнести:

а) высокая оперативность включения новых абонентов в сеть. Для этого необходимо ввести параметры новой точки доступа в последнюю точку доступа сети, что приведет только к кратковременной перегрузке данной точки доступа;

б) на работу сети связи почти не влияют отказы остальных точек доступа, т. к. все остальные ПК сети могут продолжать обмен информацией между собой и только ПК аварийной точки доступа не сможет получить доступ в сеть Интернет.

К недостатку сети связи с данной топологией следует отнести минимальную дальность радиосвязи: радиус зоны покрытия территории точки доступа определяется мощностью и типом антенны передатчика.

Следует отметить, что на практике в большинстве случаев Wi-Fi сети используют комбинированные топологии, из которых наиболее известными являются следующие.

1.3.1.4 Топология сети типа «точка – точка»

Сеть связи с данной топологией выполняет (реализует) функции «моста». Для ее реализации требуется две точки доступа. Сеть связи с данной топологией имеет следующее построение (рисунок 1.4).

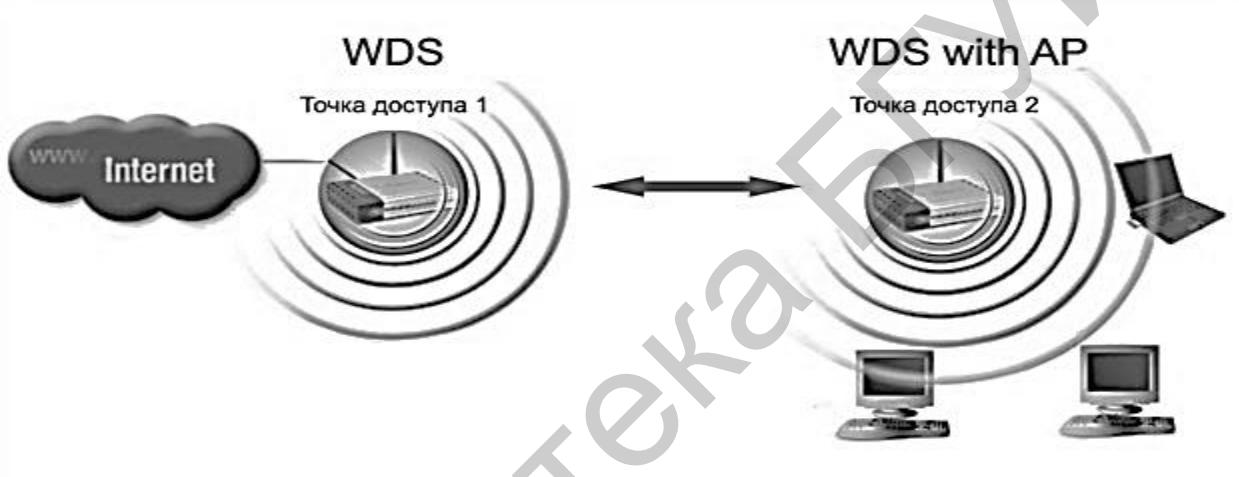


Рисунок 1.4 – Топология сети типа «точка – точка» (мост)

Сеть связи с топологией «точка – точка» достаточно просто преобразуется в сеть связи с топологией «точка – много точек».

1.3.1.5 Топология сети типа «точка – много точек»

Сеть связи с данной топологией, так же как и предыдущий тип связи, выполняет функцию «моста». Для ее реализации требуется не менее трех точек доступа. Обобщенная структурная схема Wi-Fi сети имеет следующее построение (рисунок 1.5).

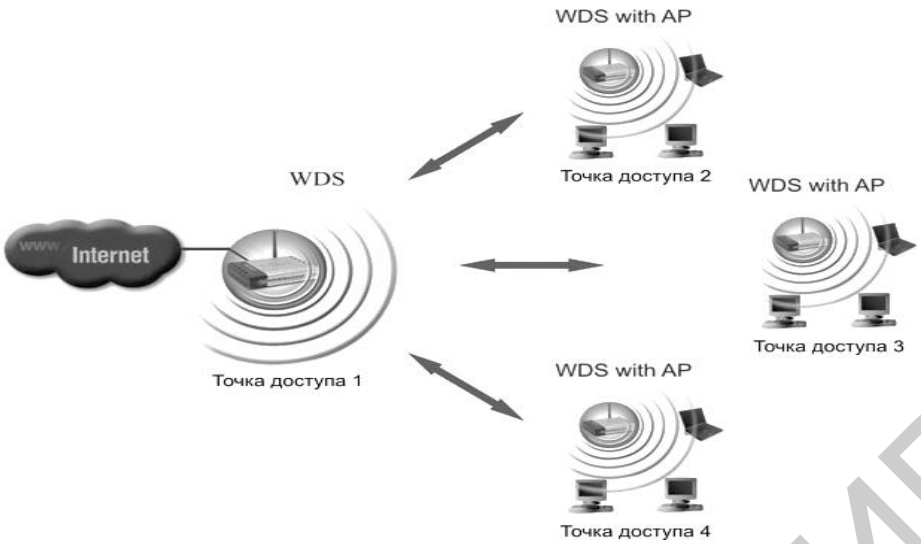


Рисунок 1.5 – Топология сети типа «точка – много точек»

На рисунке 1.6 представлена структурная схема одного из вариантов построения Wi-Fi сети данной топологии на основе использования беспроводного маршрутизатора типа Di-724P+ фирмы D-Link, а также с указанием конкретного типа периферийного оборудования.

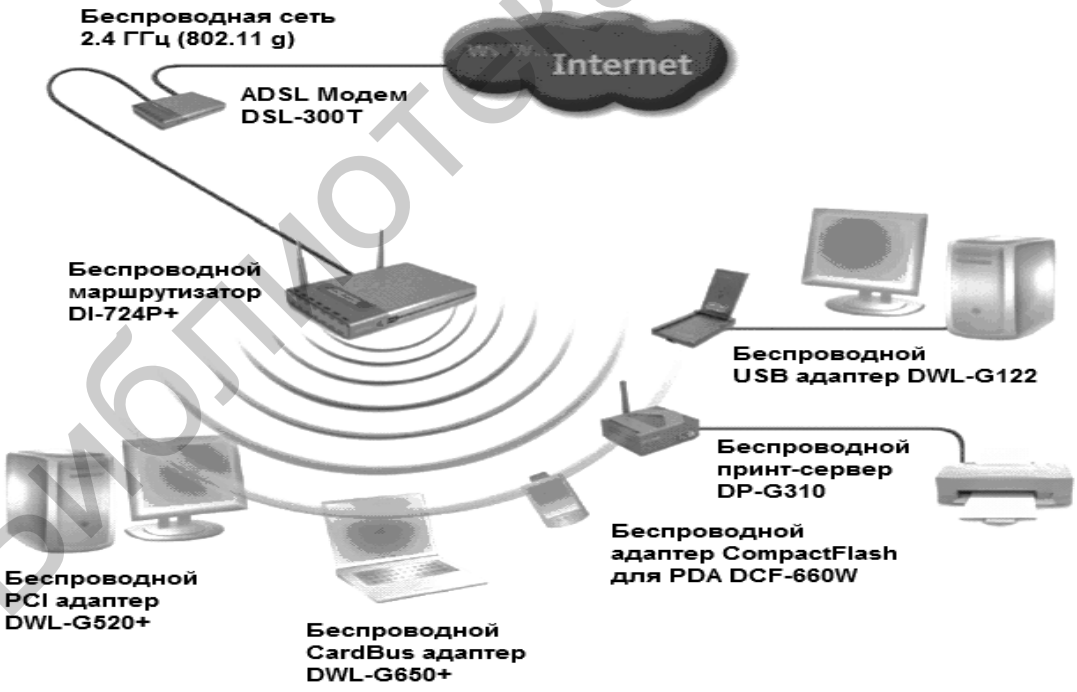


Рисунок 1.6 – Топология сети типа «точка – много точек»
с использованием беспроводного маршрутизатора

На практике очень часто используются Wi-Fi сети с комбинированной топологией типа «звезда – точка – много точек». Обобщенная структурная схема данной топологии сети представлена на рисунке 1.7.

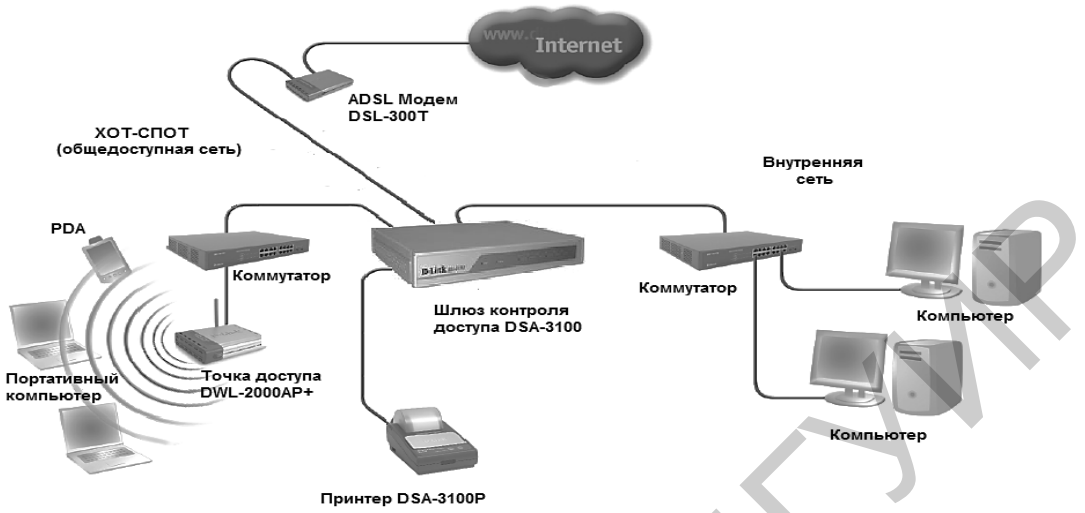


Рисунок 1.7 – Топология сети типа «звезда – точка – много точек»

В качестве связующего центрального устройства в данном варианте построения Wi-Fi сети используется шлюз контроля доступа типа DSA-3100 фирмы D-Link.

Следует отметить, что наличие большого количества оборудования Wi-Fi сетей обеспечивает возможность построения данных сетей с наиболее оптимальной топологией как в ее функциональном назначении, так и в стоимостной оценке.

1.3.2 Режимы передачи данных Wi-Fi сетей

1.3.2.1 Режим Ad-Hoc (к случаю)

В данном режиме ПД абоненты сети устанавливают связь непосредственно друг с другом. Устанавливается одноранговое взаимодействие по топологии сети «точка – точка», и ПК взаимодействуют друг с другом напрямую, без применения точек доступа. На рисунке 1.8 представлена обобщенная схема данного режима ПД.

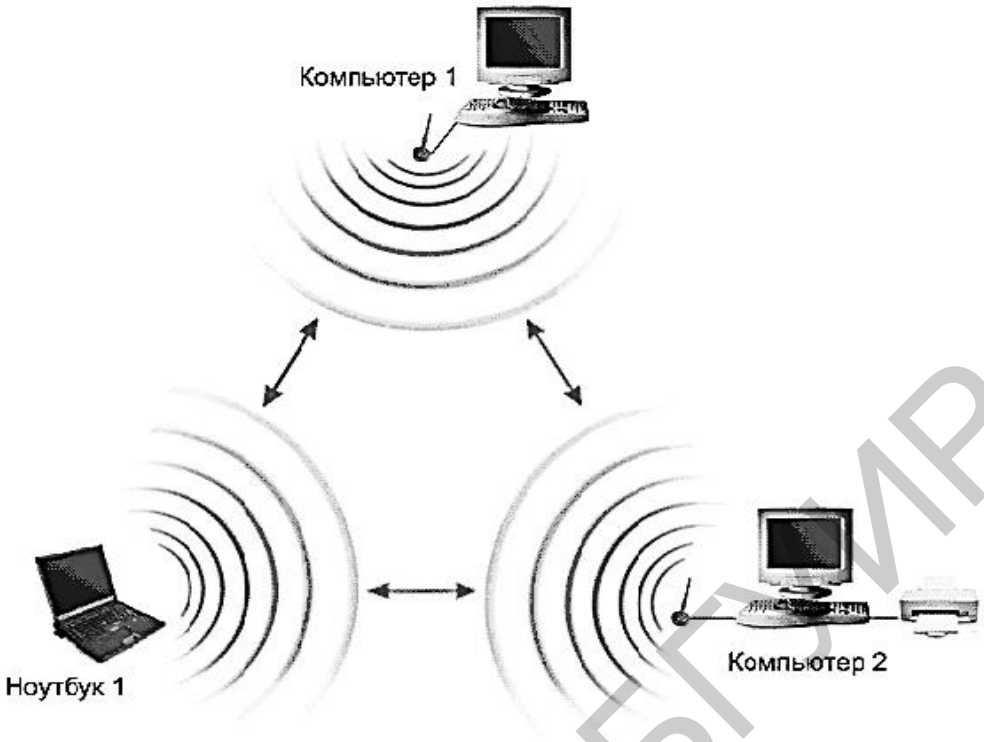


Рисунок 1.8 – Режим передачи данных Ad-Hoc

Основное достоинство данного режима ПД – простота организации: режим не требует дополнительного оборудования (точки доступа). Кроме того, он позволяет оперативно создавать кратковременные сети ПД. Однако необходимо иметь в виду, что режим Ad-Hoc позволяет устанавливать соединения на скорости не более 11 Мбит/с независимо от используемого оборудования. Реальная скорость обмена данных будет еще ниже, составляя не более 11/N Мбит/с, где N – число устройств в сети, а дальность связи не более 100 м. Скорость ПД быстро падает с увеличением расстояния между абонентами.

1.3.2.2 Инфраструктурный режим передачи данных

Для организации долговременных беспроводных сетей следует использовать инфраструктурный режим ПД.

Данный режим установления соединения и ПД организуется по схеме, представленной на рисунке 1.9. В инфраструктурном режиме точку доступа можно рассматривать как беспроводной коммутатор, благодаря чему она обеспечивает связь абонентам ПК ноутбуков.

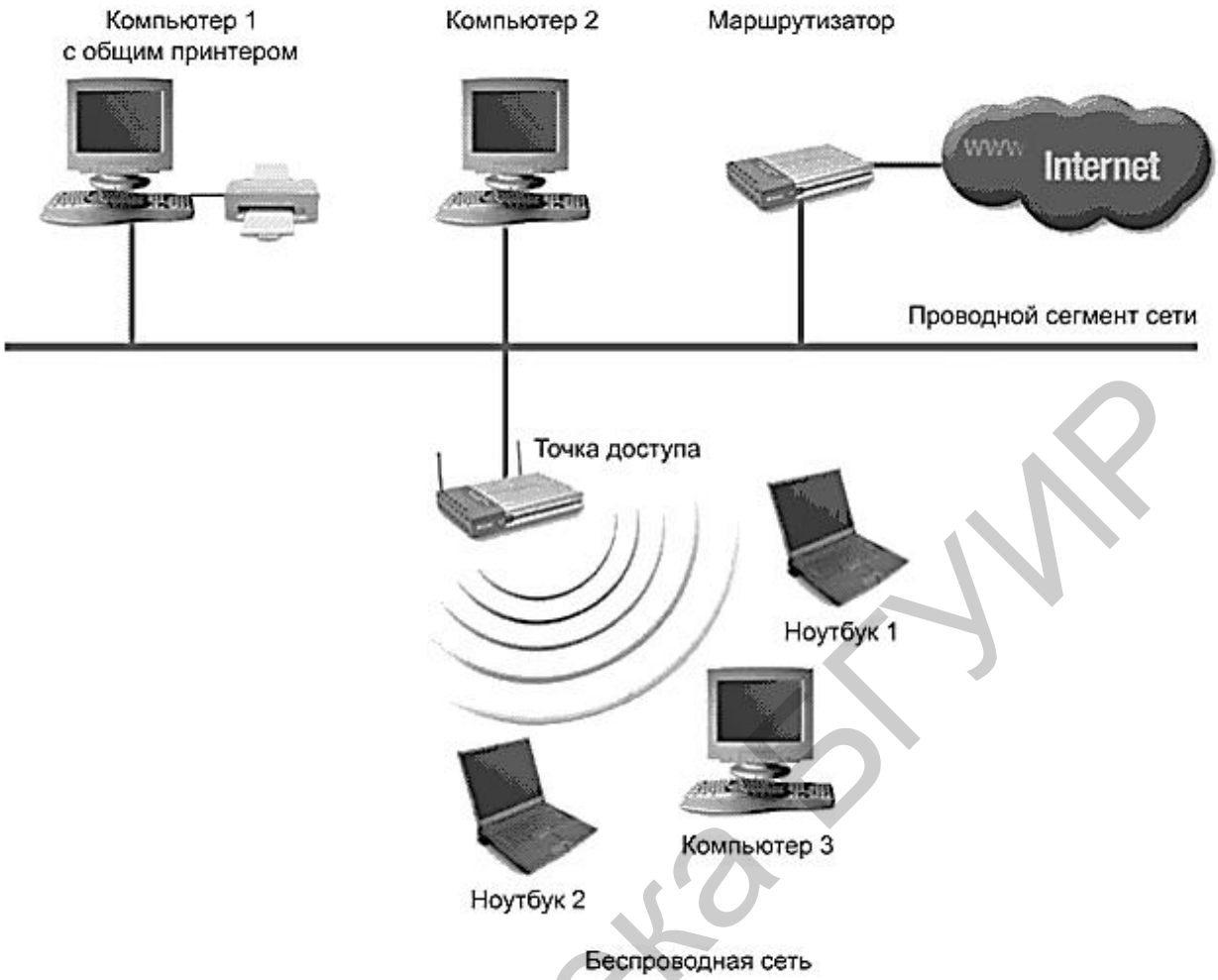


Рисунок 1.9 – Инфраструктурный режим передачи данных

Абонентские оконечные устройства не связываются непосредственно друг с другом, а связываются с точкой доступа, и она направляет пакеты данных нужным адресам сети.

1.3.2.3 Режим «Повторитель»

Данный режим организации работы беспроводной сети связи может возникнуть, когда оказывается невозможным или неудобным соединить точку доступа с проводной инфраструктурой (с проводным сегментов сети) или какое-либо препятствие затрудняет напрямую осуществление связи точки доступа с местом расположения беспроводных абонентских устройств. В таких ситуациях можно использовать точку доступа в режиме работы повторителя (рисунок 1.10).

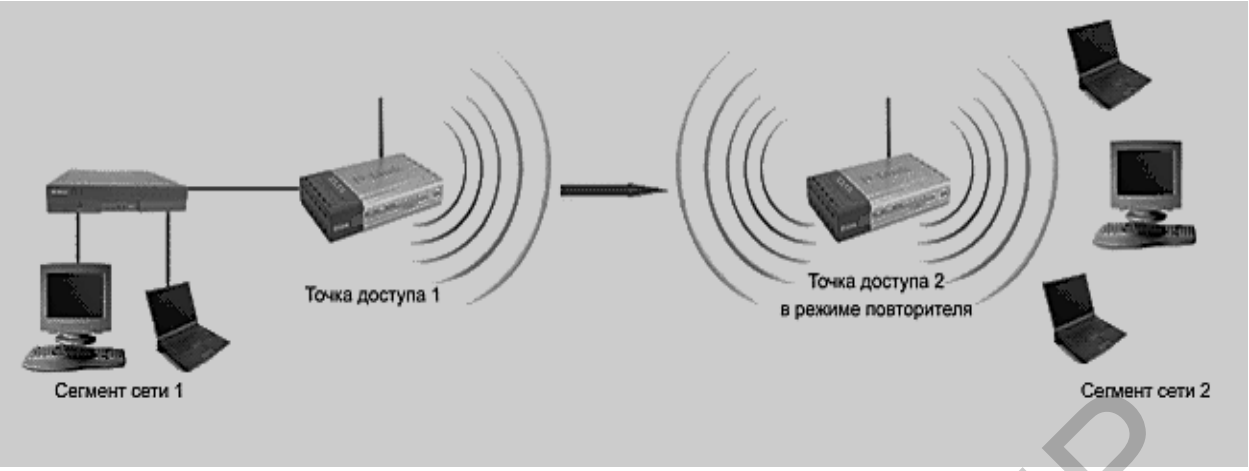


Рисунок 1.10 – Схема организации и функционирования беспроводной сети в режиме «Повторитель»

При данном способе организации беспроводной сети беспроводной повторитель работает, как и проводной повторитель, который ретранслирует все пакеты данных на его беспроводной интерфейс. Эта ретрансляция осуществляется через тот же канал связи, по которому они были получены. При использовании точки доступа как повторителя, следует знать, что наложение широковещательных доменов может привести к сокращению пропускной способности радиоканала вдвое, так как начальная точка доступа также «слышит» ретранслированный радиосигнал.

Следует отметить, что режим «Повторитель» не включен в стандарт IEEE 802.11, поэтому для его реализации рекомендуется использовать однотипное оборудование (вплоть до версии «прошивки») от одного производителя. С появлением беспроводных распределительных систем (WDS) данный режим утратил свою актуальность, однако его можно встретить в старых версиях «прошивок».

1.3.2.4 Режим «Клиент»

При переходе от проводной сети к беспроводной может обнаружиться ситуация, 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 на основе протокола «Клиент» (рисунок 1.11).

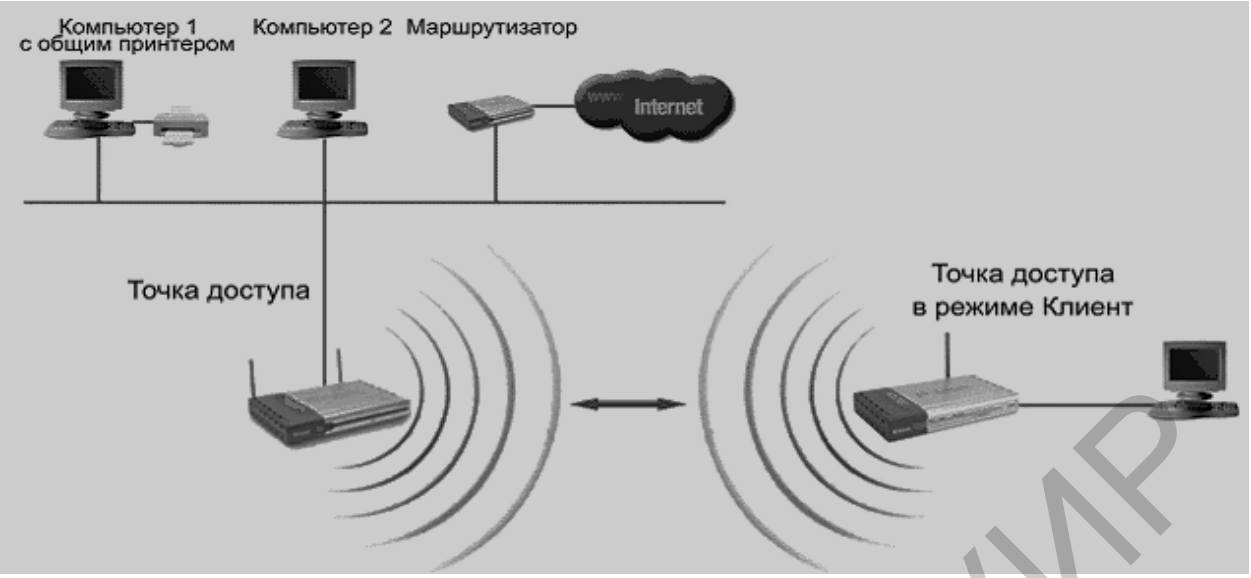


Рисунок 1.11 – Схема организации и функционирования беспроводной сети в режиме «Клиент»

При помощи точки доступа, функционирующей в режиме «Клиент», к беспроводной сети подключается только одно устройство (ПК, ПВМ, ноутбук). Следует отметить, что данный режим ПД не включен в стандарт IEEE 802.11 и поддерживается не всеми производителями оборудования Wi-Fi.

1.3.2.5 Режим WDS (распределенная беспроводная система), или мостовой режим

В данном режиме точки доступа соединяются только между собой, образуя мостовое соединение. Обобщенная структурная схема мостового соединения представлена на рисунке 1.12. Видно, что каждая точка доступа может соединяться с несколькими другими точками доступа. Все точки доступа в этом режиме должны использовать одинаковый радиоканал, поэтому количество точек доступа, участвующих в образовании моста, не должно быть большим. Подключение абонентов осуществляется по проводной сети через up-Link – порты точек доступа.

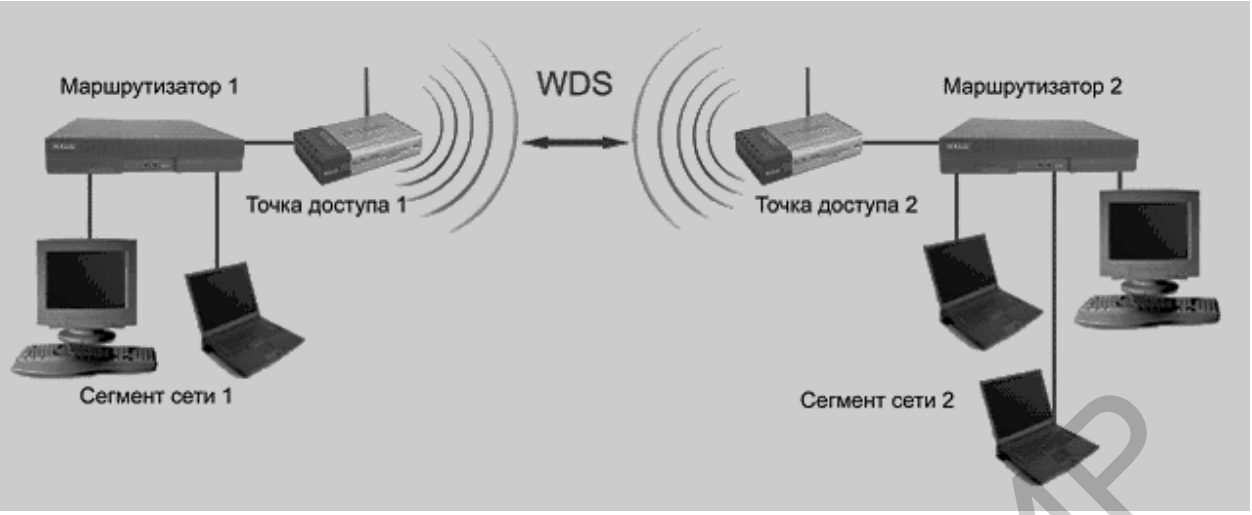


Рисунок 1.12 – Режим WDS, или мостовой режим

Беспроводной мост может использоваться там, где прокладка кабеля связи между зданиями нежелательна или невозможна. На рисунке 1.13 представлена структурная схема, реализующая мостовой режим установления соединения и ПД между двумя зданиями.

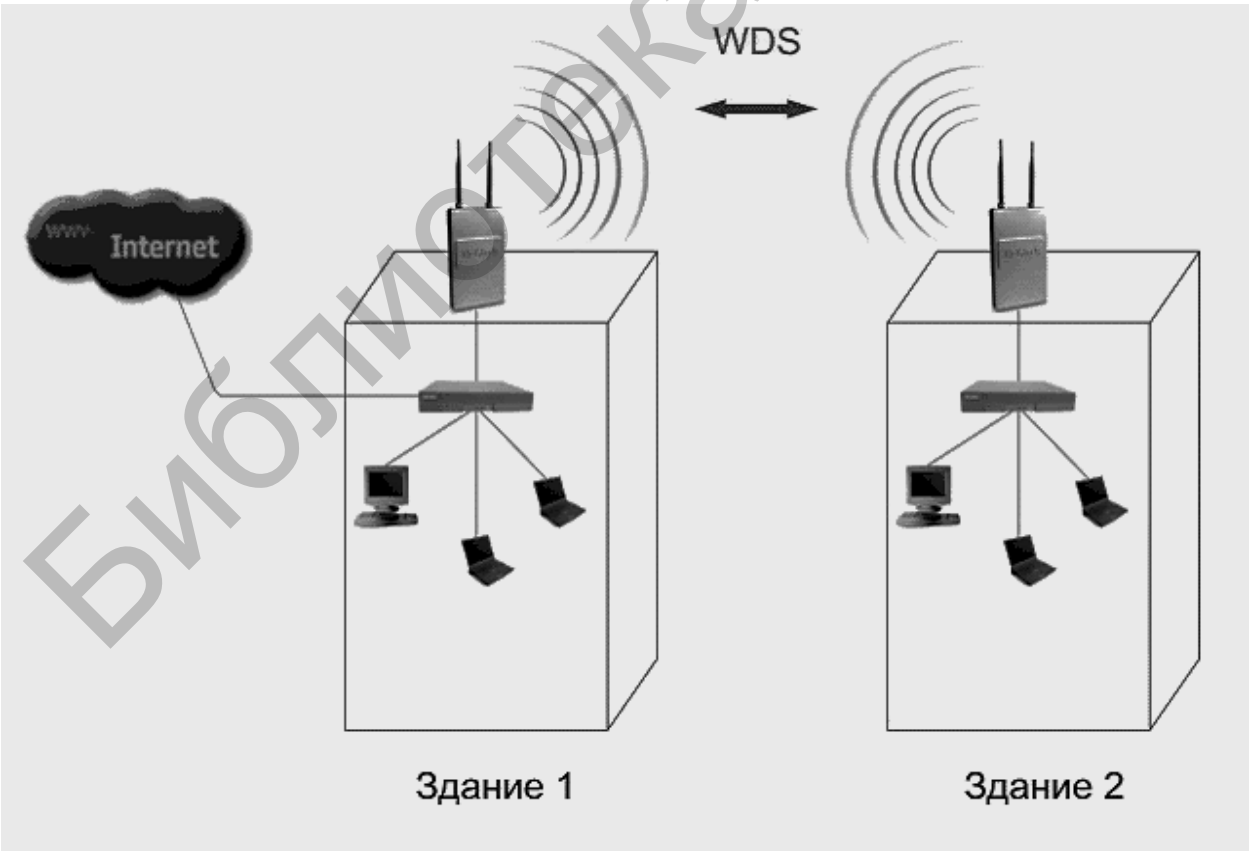


Рисунок 1.13 – Мостовой режим между двумя зданиями

Данное решение организации Wi-Fi сети позволяет получить значительную экономию средств, обеспечить простоту настройки и гибкость изменения топологии сети при перемещении мест расположения офисов.

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

1.3.2.6 Режим WDS with Access Point (распределенная беспроводная система, включающая точку доступа)

Данный режим установления соединения и ПД может быть реализован в общем случае в виде следующей структурной схемы (рисунок 1.14).

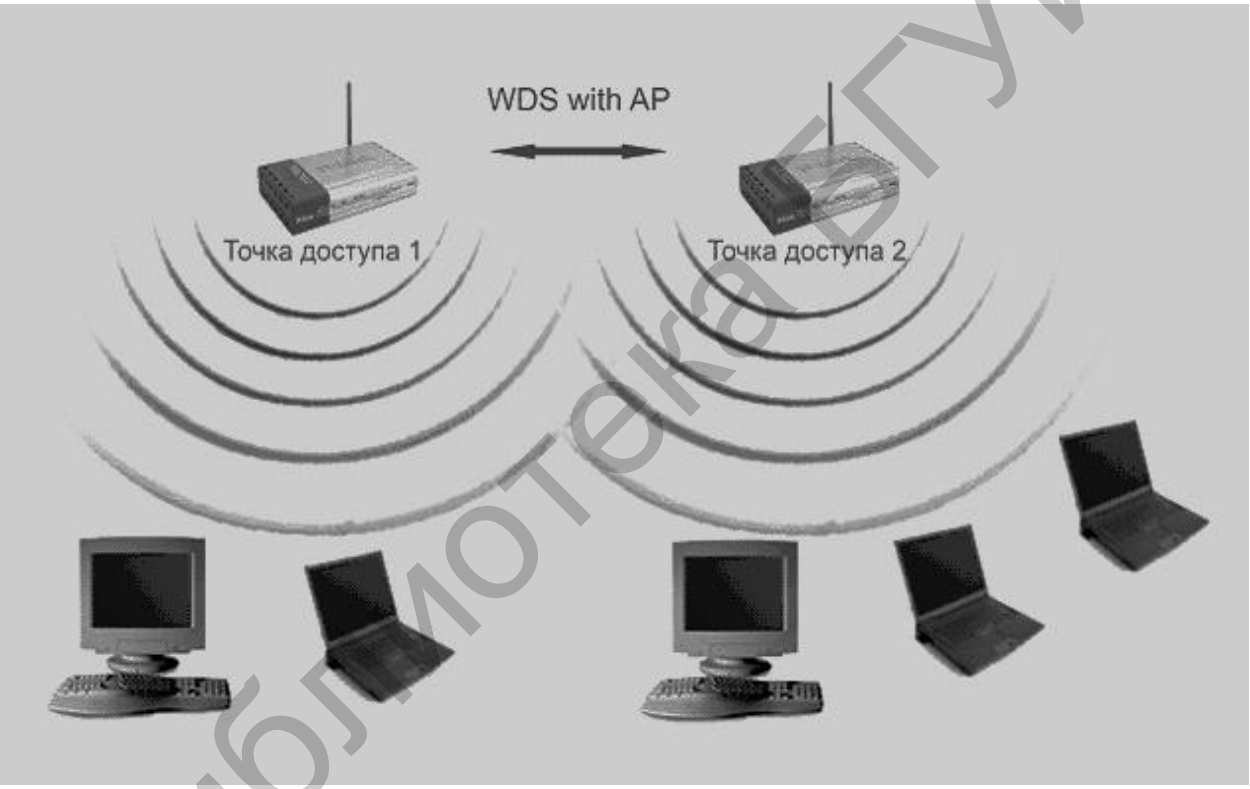


Рисунок 1.14 – Обобщенная структурная схема режима передачи данных WDS with AP

При реализации данного режима ПД можно организовать не только через мостовую связь между точками доступа, но и одновременно подключить абонентские компьютеры. Это позволяет достичь существенной экономии оборудования и упростить топологию Wi-Fi сети. Данная технология организации Wi-Fi сетей поддерживается большинством современных точек доступа.

Однако следует отметить, что все устройства в составе одной WDS with AP работают на одной радиочастоте и создают взаимные помехи, а это ограничивает количество абонентов до 15–20. Для увеличения количества обслуживаемых абонентов можно использовать несколько WDS-сетей, настроенных на разные радиочастоты (радиоканалы), соединенные проводными линиями связи через uplink-порты.

В общем случае технологии организации беспроводных сетей, функционирующих в режиме WDS, аналогичны стандартным технологиям проводных сетей.

1.4 Оформление отчета по выполненной работе

Отчет по лабораторной работе должен содержать:

- титульный лист, форма которого установлена кафедрой;
- результаты выполнения домашнего задания;
- описание основных топологий Wi-Fi сетей;
- перечень оборудования Wi-Fi сетей.

1.5 Контрольные вопросы

1 Дайте определение термину «топология», приведите классификацию топологий.

2 Поясните сущность топологий iBSS, BSS и ESS, а также их достоинства и недостатки.

3 Опишите порядок включения дополнительных абонентов в Wi-Fi сеть с топологией:

- «кольцо»;
- «звезда»;
- «шина».

4 Поясните принцип организации Wi-Fi сетей с топологиями «точка – точка» и «точка – много точек».

5 Поясните принцип организации Wi-Fi сети с топологией «звезда, точка – много точек».

6 Поясните принципы передачи данных в режимах Ad-Hoc, «Инфраструктура» и «Расширенная инфраструктура».

7 Поясните принцип передачи данных в режимах функционирования «Клиент» и «Повторитель» Wi-Fi сети.

Литература

1 Беспроводные сети Wi-Fi : учеб. пособие / А. В. Пролетарский [и др.]. – М. : Интернет-университет информационных технологий : БИНОМ. Лаборатория знаний, 2007.

2 Роман, П. Основы построения беспроводных локальных сетей стандарта 802.11 / П. Роман, Дж. Лиэри. – М. : Издательский дом «Вильямс», 2004.

3 Столлингс, В. Беспроводные линии связи и сети / В. Столлингс. – М. : Издательский дом «Вильямс», 2003.

4 Феер, К. Беспроводная цифровая связь. Методы модуляции и расширения спектра / К. Феер. – М. : Радио и связь, 2001.

5 Широкополосные беспроводные сети передачи информации / В. Вишневский [и др.]. – М. : Эко-Трендз, 2005.

6 Григорьев, В. А. Сети и системы радиодоступа / В. А. Григорьев, О. Н. Лагутенко, Ю. А. Распаев. – М. : Эко-Трендз, 2005.

ЛАБОРАТОРНАЯ РАБОТА №2

Проектирование и расчет антенно-фидерных трактов Wi-Fi сетей

2.1 Цель работы

Получить навыки расчета и проектирования антенно-фидерных трактов радиосистем Wi-Fi сетей.

2.2 Домашнее задание к лабораторной работе

1 По приведенным ниже методическим указаниям и рекомендованной литературе подготовиться к выполнению лабораторной работы.

2 Изучить состав и назначение функциональных элементов антенно-фидерных трактов Wi-Fi сетей.

3 По заданным параметрам радиотракта рассчитать состав элементов простого и расширенного антенно-фидерного трактов.

2.3 Классификация и основные технические характеристики беспроводного оборудования D-Link

2.3.1 Классификация беспроводного оборудования компании D-Link

Компания D-Link разрабатывает и производит ряд серий беспроводного оборудования, обеспечивающего построение Wi-Fi сетей с различными техническими характеристиками, а именно:

1) серия *Air PlusG* предназначена для создания экономичных беспроводных сетей стандарта 802.11q, использующих диапазон с несущей частотой f_H = 2,4 ГГц;

2) серия *Air Plus XtremeG* предназначена для создания высокоскоростных беспроводных сетей стандарта 802.11q, использующих частотный диапазон f_H = 2,4 ГГц;

3) серия *Air Plus XtremeG* с поддержкой технологии MIMO предназначена для создания высокоскоростных беспроводных сетей стандарта 802.11q с увеличенным радиусом действия, использующих диапазон радиочастот f_H = 2,4 ГГц;

4) серия *Air Plus Xtreme AG* предназначена для создания беспроводных сетей масштаба предприятия стандартов 802.11a/b/q, функционирующих в диапазоне радиочастот 2,4/5 ГГц;

5) серия *Air Premier* предназначена для создания беспроводных сетей масштаба предприятия и внешних сетей 802.11e/q, функционирующих в диапазоне радиочастот с f_H = 2,4 ГГц.

2.3.2 Элементы беспроводных сетей: назначение, основные технические характеристики и функциональные возможности

Для построения беспроводных сетей типа LAN, WLAN и Wi-MAX в целом необходимы следующие функциональные элементы: усилители мощности радиопередатчиков, фильтры, антенны, кабели связи, разъемы, устройства грозозащиты и соответствующее программное обеспечение для радиотехнических устройств.

Адаптер представляет собой устройство, выполняющее такую же функцию, как и сетевая карта компьютера, включенного в проводную сеть, т. е. он используется для подключения компьютера к беспроводной сети. Адаптеры выполняются в виде локальных блоков (рисунок 2.1, *а*, *в*) и электронных плат с внешней антенной (рисунок 2.1, *б*). Первый тип адаптеров подключается к компьютерам через порт USB 2.0, а второй тип адаптеров подключается к компьютеру через слот расширения PCI, PCMCI и Compact Flach (см. рисунок 2.1).

а *б* *в*

а – DWL-G650 (порт USB 2.0, порт RJ-11); *б* – DWL-G520 (порт USB 2.0);
в – DWL-G620

Рисунок 2.1 – Общий вид сетевых адаптеров

Для доступа к беспроводной сети адаптер может устанавливать связь непосредственно с другими адаптерами. Такая сеть называется беспроводной одноранговой сетью, или Ad-Hoc (в переводе «к случаю»), она может устанав-

ливать связь через специальное устройство, называемое *точкой доступа*. Такой режим работы адаптера называется *инфраструктурный*.

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

В качестве примера рассмотрим основные технические характеристики двух типов адаптеров, а именно DWL-G520+ фирмы D-Link и ZyAIR G-300 фирмы ZyXEL (таблица 2.1).

Таблица 2.1 – Основные технические характеристики адаптеров

DWL-G520+	*ZyAIR G-300*
Шифрование-64/128/256-бит WEP	Шифрование 64/128-бит WEP
поддержка WPA	поддержка WPA
поддержка стандартов 802.11, в/в+	скорость ПД B < 54 Мбит/с
скорость ПД B < 54 Мбит/с	поддержка стандартов 802.11q
аутентификация 802.1x	аутентификация 802.1x
антенна типа «Штырь» с G = 5 дБі	антенна типа «Штырь» с G = 5 дБі

Точка радиодоступа (далее точка доступа) представляет собой автономный модуль со встроенным микрокомпьютером и приемно-передающим устройством и обеспечивает взаимодействие и обмен информацией между беспроводными адаптерами, а также связь с проводным сегментом сети (рисунок 2.2). Таким образом, точка радиодоступа выполняет функции коммутатора. Для связи с проводным сегментом сети точка доступа имеет сетевой интерфейс (uplink port). Кроме того, через этот интерфейс может осуществляться настройка точки радиодоступа.

Рисунок 2.2 – Общий вид точки доступа

Точка доступа может работать (использоваться) в следующих режимах:

- *базовый режим* – точка доступа используется для подключения к ней беспроводных адаптеров;

- *режим WDS* (Wireless Distributed System – распределенная беспроводная сеть) – точка доступа используется для построения распределенной беспроводной сети на основе взаимодействия с другими точками доступа.

Возможны следующие подрежимы использования точек доступа:

- беспроводной мост «точка – точка»;
- «точка – много точек»;
- «беспроводной клиент»;
- «повторитель сигналов».

Точки доступа функционируют на основе передачи широковещательных радиосигналов. Радиоприемник точки доступа может получать радиосигналы в диапазоне работы нескольких радиопередатчиков точек доступа. Приемная радиостанция (радиоприемник точки доступа) выделяет нужную точку радиодоступа на основе использования «идентификатора зоны обслуживания» – SSID (Service Set Indentiver). Почти все беспроводное оборудование, выпускаемое компанией D-Link, комплектуется съемными штатными антеннами с коэффициентом усиления G = 2–5 дБi (например, DWL-2100 AP, DWL-2700 AP, DWL-520, DWL-3520 AP и др.). Это позволяет штатную антенну легко снять и подключить вместо нее антенну с большим коэффициентом усиления и необходимой диаграммой направленности (в технических характеристиках беспроводного оборудования всегда указывается, 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 расчета антенно-фидерного тракта и энергетических характеристик как системы, так и беспроводной сети в целом. К таким характеристикам относятся:

- *мощность радиопередатчика*, которая измеряется либо в милливаттах (мВт), либо в децибел-милливаттах (дБмВт);

- *чувствительность радиоприемника*, используемая для определения скорости передачи информации. Чем выше чувствительность приемника, тем больше скорость передачи информации.

В таблице 2.2 приведены основные технические характеристики двух точек доступа, а именно DWL-6700 AP (DLink) и ZyAIR G-1000 (ZyXEL).

Таблица 2.2 – Основные технические характеристики точек доступа

Параметры точек доступа	*Тип точки доступа*	
	DWL-G700	*ZyAIR G-1000*
Скорость ПД, Мбит/с	54	54
Режим работы	Точка доступа, беспроводной повторитель	Точка доступа, беспроводной повторитель
Методы шифрования	WEP, WPA и WPA2	64/128 бит WEP/WPA
Поддержка протокола	802.1x, 802.11b/q	802.1x RADIUS
Фильтрация MAC-адресов	Есть	Сведений нет
Протокол SSID	Есть	Сведений нет
Протокол DHCP	Есть	Сведений нет
Порты	10/1000 Base-TX	10/1000 BASE-TX
Тип антенны	«Штырь», *G* = 5 дБi	Две антенны типа «Штырь», *G* = 5 дБi

Маршрутизатор представляет собой автономное устройство со встроенным микрокомпьютером и приемно-передающим устройством и предназначен для организации распределенных беспроводных сетей. Маршрутизаторы выпускаются с одной или двумя антеннами (рисунки 2.3 и 2.4 соответственно).

Рисунок 2.3 – Беспроводной маршрутизатор DI-624S

Рисунок 2.4 – Беспроводной MIMO-маршрутизатор DI-634M

В таблице 2.3 приведены основные технические характеристики трех типов маршрутизаторов: DI-624s и DI-634M фирмы D-Link, а также ZyAIR G-2000 фирмы ZyXEL.

Таблица 2.3 – Основные технические характеристики беспроводных маршрутизаторов

Параметры маршрутизаторов	*Тип маршрутизаторов*		
	DI-624S	*DI-643M*	*ZyAIR G-2000*
Скорость соединения и передачи данных	До 108	До 108	До 54
Количество и тип портов	4 типа 10/1000 Base TX LAN	4 типа 10/1000 Base TX LAN	4 типа 10/1000 LAN
	2 типа USB 2.0	1 типа 10/1000 Base TX WAN	1 типа USB 2.0
Радиус действия, м	До 150	До 150	До 100
Методы шифрования	WEP, WPA, WPA2	WPA, WPA2	WEP, WPA
Способ маршрутизации	IP-маршрутизация	IP-маршрутизация VPN	IP-маршрутизация VPN
Количество встроенных серверов	6	5	4
Тип управления	web-интерфейс	web-интерфейс	На основе MAC-адресов 802.1x, RADIUS

Следует отметить, что компаниями Intel, ZyXEL и др. выпускаются точки радиодоступа, которые могут выполнять также функции моста и маршрутизатора (например, УАI1О-5 100).

Усилитель мощности – автономное устройство (например, С24ХХ), предназначенное для увеличения мощности передаваемого радиосигнала и повышения чувствительности канала приема, а также компенсации потерь в антенно-фидерном тракте между радиомодемом и антенной. Усилитель мощности может быть установлен непосредственно на антенне. При включении усилителя мощности в радиосистему существенно увеличивается радиус зоны покрытия радиосигналом. Однако при использовании усилительной мощности необходимо учитывать следующие факторы:

- если мощность радиопередатчика точки доступа очень большая и не попадает в диапазон допустимой интенсивности радиосигнала на входе порта усилителя, то использовать точку доступа все же можно с усилителем мощности, но в этом случае необходимо включить в тракт между усилителем мощности и точкой доступа кабельную сборку или какой-либо специальный элемент, затухание на котором обеспечит необходимое ослабление сигнала;

- ослабляя переданный радиосигнал, необходимо установить такой уровень сигнала, который бы обеспечивал надежную радиосвязь между абонентами, т. е. радиоустройствами.

Полосовой фильтр – автономное устройство, включаемое в антенно-фидерный тракт и предназначенное для обеспечения электромагнитной совместимости с другими электро- и радиосистемами. Полосовые фильтры бывают настраиваемыми и с фиксированной центральной частотой (f_H = 2,4 ГГц), которая настраивается в процессе производства фильтра, поэтому при заказе фильтра необходимо указывать тип его настройки. Полосовые фильтры отличаются шириной полосы пропускания и величиной затухания (ослабления) радиосигнала, которая может достигать до 1,5 дБ.

Устройство (модуль) грозовой защиты является автономным устройством и в оборудовании D-Link входит в комплект всех внешних антенн. Устройства грозовой защиты имеют разъемы N-type (female) <-> N-type (male).

Инжектор питания – автономное устройство, которое включается в тракт приема-передачи радиосигнала между активным оборудованием (точкой доступа) и входным портом усилителя мощности. Инжектор имеет два порта – оба типа M-type, одним из которых подключается к блоку питания, а второй подключается к розетке с напряжением 220 В. Вносимое инжектором затухание в тракт приема-передачи радиосигнала составляет не более 0,5 дБ. Инжектор питания и блок питания входит в комплект поставки усилителей мощности.

Кабельная сборка SMA-RP-pluq<->N-type (male), которую часто называют piqtale, представляет собой небольшой переходник с антенного вывода (indoor) точки доступа (данный переходник называется сокращенно SMA-RP – реверс SMA) на широко используемый в антенно-фидерном тракте высокочастотный разъем N-type. На рисунке 2.5 представлена в общем виде кабельная сборка типа piqtale.

Данная кабельная сборка входит в комплект поставки всех внешних (outdoor) антенн компании D-Link. Кабельная сборка piqtale вносит затухание порядка 0,5 дБ (антенны для внутреннего использования также комплектуются необходимыми коаксиальными кабелями связи и высокочастотными разъемами).

Рисунок 2.5 – Общий вид кабельной сборки типа piqtale

Переходник TLK-N-type-MM используется для изменения конфигурации (конструкции) порта с female (гнезда) на male (штекер). Общий вид переходника TLK-N-type-male-male представлен на рисунке 2.6.

Рисунок 2.6 – Общий вид переходника TLK-N-type-MM

Общепринятым является то, что коаксиальный разъем, устанавливаемый стационарно, например, на входы или выходы усилителей, фильтров, генераторов сигналов, а также 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 антенно-фидерного тракта на элементах от различных производителей. Данную проблему позволяет легко разрешить использование переходника (кабельной сборки) N-type (female) <-> M-type (male), общий вид которой представлен на рисунке 2.7. Кабельная сборка имеет обозначение HQNf-Nm 1.5.

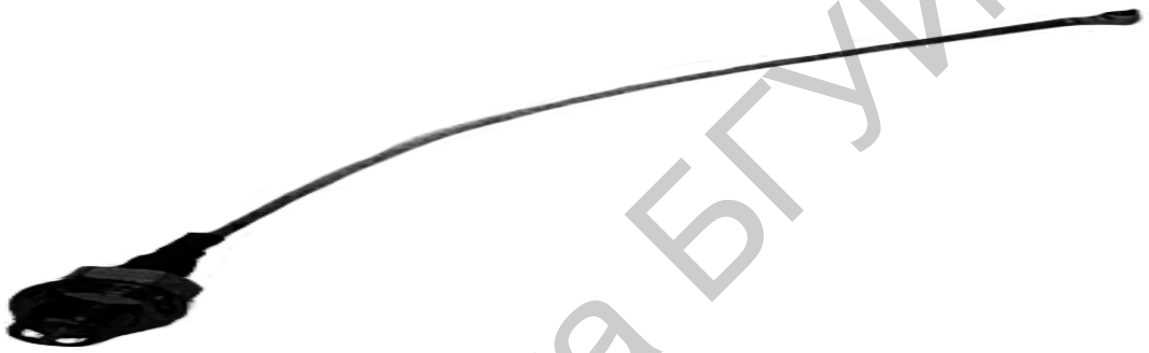


Рисунок 2.7 – Общий вид переходника (кабельной сборки)
N-type (female) <-> M-type (male)

Данная кабельная сборка имеет стандартную длину 15 м. Можно использовать кабельные сборки большей длины, например, соединив две 15-метровые сборки. Однако в этом случае необходимо соблюдать следующие условия:

- уровень радиосигнала на входном порту усилителя мощности должен соответствовать динамическому диапазону, который указан в его характеристиках;
- уровень радиосигнала должен быть допустимым для обработки сигнала тракта.

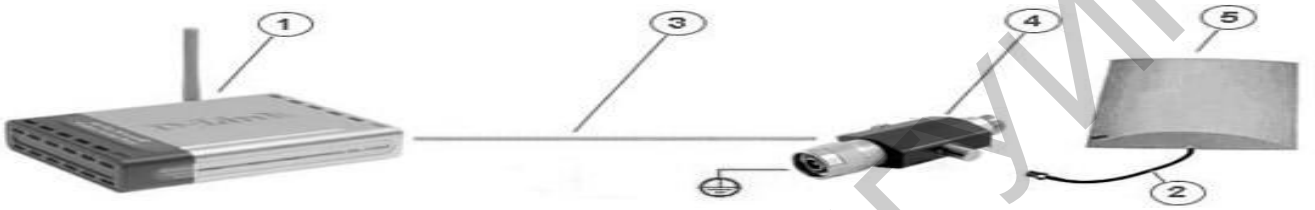
Внешние антенны – автономные устройства, предназначенные для увеличения радиуса зоны покрытия радиосигналом или дальности передачи информации. Антенны, используемые внутри помещений, имеют коэффициент усиления G = 7 дБi, а внешние антенны – G = 25 дБi. Так, например, внешняя антенна типа ANT24-2100 имеет G = 21 дБi. Все антенны имеют разъемы типа N-Type (female).

2.4 Построение антенно-фидерных трактов Wi-Fi сетей

2.4.1 Принцип построения простого антенно-фидерного тракта точки радиодоступа

Антенно-фидерный тракт считается простым, если в нем отсутствуют активные элементы. Возможны два варианта построения антенно-фидерного тракта, которые практически будет отличаться длиной кабельной сборки, а именно NQNf-Nm1,5 длиной 1,5 м и NQNf-Nm15 длиной 15 м.

На рисунке 2.8 представлен простой антенно-фидерный тракт.



1 – точка доступа типа DWL-2100 AP;
2 – кабельная сборка piqtale (в комплекте с антенной);
3 – кабельная сборка N-type (female) <-> N-type (male);
4 – модуль грозовой защиты (в комплекте с антенной);
5 – внешняя антенна типа ANT24-1400
Рисунок 2.8 – Простой антенно-фидерный тракт точки доступа

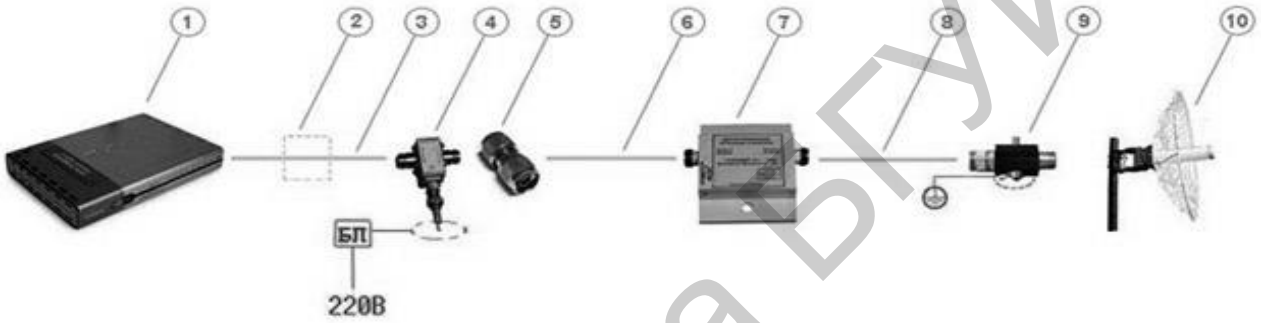
Расстояние, на которое возможно вынести антенну в данном случае, сильно ограничивается мощностью радиопередатчика точки доступа и затуханием, вносимым пассивными элементами. При выносе антенны на большее расстояние мощность как принятого, так и переданного радиосигнала может полностью поглотиться кабельными сборками и переходниками.

При использовании даже самой короткой кабельной сборки (NQNf-Nm1,5) к антенне подводится мощность радиопередатчика значительно меньшей, чем на активном порту точки доступа, что может существенно отразиться на дальности передачи радиосигнала.

Для увеличения дальности передачи радиосигнала можно исключить из антенно-фидерного тракта модуль грозовой защиты, чего, однако, следует избегать. Разработчики беспроводного оборудования компании D-Link рекомендуют использовать кабельные сборки не длиннее 6 м и по возможности антенны с максимальным коэффициентом усиления.

2.4.2 Принцип построения расширенного антенно-фидерного тракта точки доступа

Расширенным антенно-фидерным трактом считается тракт, который содержит как пассивные, так и активные элементы. На рисунке 2.9 представлен один из вариантов построения расширенного антенно-фидерного тракта. Данный антенно-фидерный тракт содержит все вышеперечисленные элементы (см. рисунок 2.9). Назначение данных элементов антенно-фидерного тракта рассмотрено выше. Наличие большого количества элементов в рассматриваемом антенно-фидерном тракте позволяет использовать на практике различные методы их построения.



1 – полосовой фильтр; 2 – кабельная сборка типа N-Type (female) <-> N-Type (male); 3 – инжектор питания; 4 – переходник типа TLK-N-Type-MM; 5 – кабельная сборка типа <piqtale>; 6 – усилитель мощности; 7 – кабельный переходник (кабельная сборка) NQNf-Nm1,5; 8 – кабель; 9 – модуль грозозащиты; 10 – параболическая антенна

Рисунок 2.9 – Расширенный антенно-фидерный тракт

2.5 Расчет параметров антенно-фидерного тракта Wi-Fi сетей

Методику расчета параметров антенно-фидерного тракта рассмотрим на основе следующих примеров.

Пример 1. Требуется определить длину кабельной сборки на основе использования коаксиального кабеля с затуханием 0,1 дБ/м на частоте 2,4 ГГц, если организуется антенно-фидерный тракт с усилителем типа NCS24O5 с выходной мощностью $P_{ВЫХ}$ = 500 мВт при допустимом уровне входного радиосигнала $P_{ВХ}$ = 10–100 мВт и при выходной мощности радиопередатчика точки доступа $P_{Т.Д}$ = 200 мВт.

Решение. Из условий поставленной задачи следует, что необходимо ослабить мощность радиопередатчика точки доступа на 100 мВт, или в 2 раза (на 3 дБ). Следовательно, для того чтобы использовать в тракте усилитель

мощности с $P_{ВЫХ}$ = 500 мВт, необходимо включить в тракт кабельную сборку длиной L = 3/0,1 = 30 м, т. е. включить две типовые сборки NQNf-Nm15.

Пример 2. Определить максимальное расстояние от активного порта точки радиодоступа с мощностью радиосигнала 16 дБмВт до входного порта усилителя типа NCS2401 для расширенного антенно-фидерного тракта (см. рисунок 2.9) затухание радиосигнала на коаксиальном кабеле принимаем равным 0,1 дБ/м.

Решение

1 Определяем суммарное затухание радиосигнала на тракте до порта усиления мощности без учета потерь мощности в полосовом фильтре: $У_{общ}$ = 0,5 дБ (piqtale) + 0,5 дБ (инжектор) + 3,75 дБ (15 метровая сборка + + 3 разъема по 0,75 дБ) = 4,75 дБ.

2 Следовательно, мощность, которая поступает на вход усилителя мощности, равна $У_{мм} = P_{т.д} – У_{общ}$ = 16 – 4,75 = 11,25 дБВт.

3 Для усиления мощности NCS2401 нижняя граница допустимой интенсивности радиосигнала на входном порту составляет 4 мВт (6 дБмВт). Следовательно, можно увеличить длину кабельной сборки на $\ell' = У_{ум} – У_{вх}/0,1$ = = 11,25 – 6/0,1 = 5,25/0,1 = 52,5 м. Таким образом, максимальная длина кабельной сборки будет равна $\ell'' = \ell' + \ell_{ст}$ = 52,5 + 15 = 67,5 м.

4 Далее необходимо определить полное затухание радиосигнала. Предположим, что от удаленного радиопередатчика на усилитель мощности поступает радиосигнал мощностью $P_{рс}$ = –98 дБмВт; в режиме приема коэффициент усиления усилителя мощности равен 30 дБ. Затухание тракта до порта радиоприемника точки доступа составляет 16 дБ (4,75 дБ + 11,25 дБ).

5 Определяем интенсивность радиосигнала, поступившего на радиоприемник точки доступа: $P''_{рс} = P_{сс}$ + 30 – 16 = – 98 + 30 – 16 = – 82 дБмВт.

6 По данным таблицы 2.4 определяем скорость передачи данных точки доступа при рассчитанной интенсивности радиосигнала.

Таблица 2.4 – Зависимость чувствительности приемника от скорости передачи данных

Скорость передачи данных, Мбит/с	Чувствительность приемника, дБмВт
54	–66
48	–71
36	–76
24	–80
18	–83
12	–85
9	–86
6	–87
4	–88
2	–89

Так как мощность (–82 дБВт) расчетной величины равняется примерно табличной величине (–83 дБВт), то при такой длине кабельной сборки точка доступа может работать на скорости 18 Мбит/с. Для увеличения скорости передачи информации необходимо либо уменьшить длину кабельной сборки, либо выбрать усилитель мощности с большим коэффициентом усиления.

В таблице 2.5 приведены величины затухания радиосигнала на частоте 2,4 ГГц в зависимости от типа среды распространения радиосигнала.

Таблица 2.5 – Затухание радиосигнала на частоте 2,4 ГГц в зависимости от типа среды распространения

Наименование	*Единица измерения*	*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 piqtale	дБ	0,5
Полосовой фильтр NSC F24XXX	дБ	1,5
Коаксиальный кабель	дБ/м	0,3
Разъем N-type	дБ	0,75
Инжектор питания	дБ	0,5

2.6 Экспериментальная часть лабораторной работы

Экспериментальная часть лабораторной работы предусматривает выполнение следующих расчетов.

1 По заданным параметрам антенно-фидерного тракта (таблица 2.6), состоящего из кабельной сборки с затуханием радиосигнала $У_{кб}$ и усилителя мощности с коэффициентом усиления $G_{ум}$, рассчитать мощность радиосигнала на его выходе, если входная мощность радиосигнала равна $P_{вх}$.

Таблица 2.6 – Исходные данные антенно-фидерного тракта, состоящего из одной кабельной сборки

1	2	3	4	5	6	7	8
$У_{кб}$, дБ	4	5	12	14	16	18	20
$G_{ум}$, дБ	20	20	22	25	29	33	35
$P_{вх}$, дБ	2,5	2,5	2,7	3,0	3,3	3,5	3,7

2 По заданным параметрам антенно-фидерного тракта (таблица 2.7), состоящего из двух кабельных сборок с затуханием радиосигнала соответственно $У_{кб1}$ и $У_{кб2}$ и усилителя мощности с коэффициентом усиления $G_{ум}$, рассчитать мощность радиосигнала на его входе, если входная мощность радиосигнала равна $P_{вх}$.

Таблица 2.7 – Исходные данные антенно-фидерного тракта, состоящего из двух кабельных сборок

1	2	3	4	5	6	7	8
$У_{кб1}$, дБ	9	11	13	15	17	19	21
$У_{кб2}$, дБ	6	7	7,5	7	8	8,5	8
$G_{ум}$, дБ	26	28	30	33	36	38	41
$P_{вх}$, дБ	3,1	3,3	3,7	4,0	4,3	4,5	4,7

3 По заданной мощности радиосигнала на входе антенно-фидерного тракта ($P_{вых/тракта}$), допустимой мощности радиосигнала на входе адаптера ($P_{вх/тракта}$) абонента определить ослабление радиосигнала (таблица 2.8).

Таблица 2.8 – Мощностные параметры радиосигнала

1	2	3	4	5	6	7	8
$P_{вх/тракта}$	80	85	90	100	105	112	117
$P_{вых/тракта}$	35	41	43	47	49	52	57

2.7 Оформление отчета по выполненной работе

Отчет должен содержать:

- титульный лист, форма которого установлена кафедрой;
- результаты домашних расчетов;
- основные параметры функциональных элементов радиотракта Wi-Fi сети;
- результаты выполнения пунктов 1–3 подраздела 2.6.

2.8 Контрольные вопросы

1 Определение, назначение и основные параметры радиотракта.

2 Основные функциональные элементы простого и расширенного антенно-фидерного трактов.

3 Классификация комплекса технических средств Wi-Fi сети.

4 Основные технические характеристики:

- сетевых адаптеров;
- точек доступа;
- маршрутизаторов.

5 Пояснение результатов выполнения пунктов 1–3 подраздела 2.6.

Литература

1 Беспроводные сети Wi-Fi : учеб. пособие / А. В. Пролетарский [и др.]. – М. : Интернет-университет информационных технологий : БИНОМ. Лаборатория знаний, 2007.

2 Роман, П. Основы построения беспроводных локальных сетей стандарта 802.11 / П. Роман, Дж. Лиэри. – М. : Издательский дом «Вильямс», 2004.

3 Столлингс, В. Беспроводные линии связи и сети / В. Столлингс. – М. : Издательский дом «Вильямс», 2003.

4 Феер, К. Беспроводная цифровая связь. Методы модуляции и расширения спектра / К. Феер. – М. : Радио и связь, 2001.

5 Широкополосные беспроводные сети передачи информации / В. Вишневский [и др.]. – М. : Эко-Трендз, 2005.

6 Григорьев, В. А. Сети и системы радиодоступа / В. А. Григорьев, О. Н. Лагутенко, Ю. А. Распаев. – М. : Эко-Трендз, 2005.

ЛАБОРАТОРНАЯ РАБОТА №3

Организация и настройка Wi-Fi сети в режиме передачи данных Ad-Hoc

3.1 Цель работы

Изучить принципы организации, настройки и технической эксплуатации Wi-Fi сети в режиме передачи данных с Ad-Hoc.

3.2 Домашнее задание к лабораторной работе

1 Изучить технические характеристики сетевых адаптеров, используемых в лабораторной работе.

2 Изучить принцип организации и функционирования Wi-Fi сети в режиме Ad-Hoc.

3 По заданным параметрам рассчитать энергетические характеристики радиоканала между двумя сетевыми адаптерами (рабочими станциями).

4 По заданным параметрам сетевого оборудования рассчитать максимально возможное число абонентов Wi-Fi сети.

3.3 Состав лабораторной работы

В состав лабораторной работы входят четыре персональных компьютера (ПК) с сетевыми адаптерами типа TWL-541P. Структурная схема лабораторной Wi-Fi сети, реализующая режим передачи данных Ad-Hoc, приведена на рисунке 3.1. Программное обеспечение на ПК лабораторной работы предустановлено и не нуждается в модернизации.

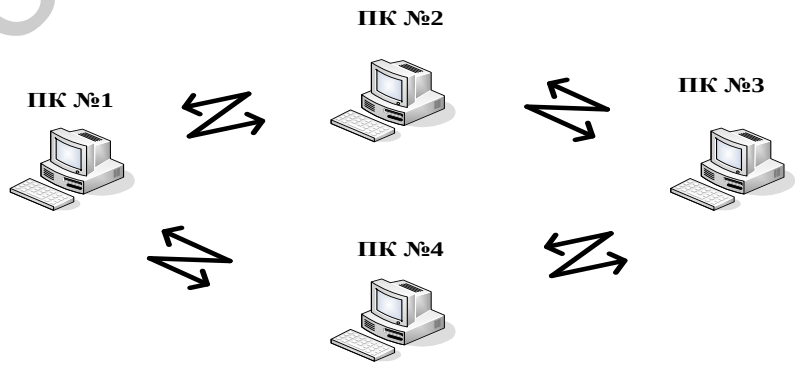


Рисунок 3.1 – Структурная схема лабораторной Wi-Fi сети, реализующая режим передачи данных Ad-Hoc

3.4 Экспериментальная часть лабораторной работы

3.4.1 Основные этапы настройки сетевого оборудования лабораторной Wi-Fi сети

К основным этапам настройки сетевого оборудования лабораторной Wi-Fi сети в режиме ПД Ad-Hoc относятся:

1) установка программного обеспечения сетевых адаптеров TWL-541P;

2) настройка адресации сетевых адаптеров TWL-541P;

3) настройка режимов шифрования сетевых адаптеров TWL-541P;

4) организация и настройка сетевого подключения адаптеров TWL-541P.

3.4.2 Установка программного обеспечения сетевых адаптеров TWL-541P

Установка программного обеспечения сетевых адаптеров TWL-541P, включенных в PCI–слот ПК, выполняется в следующей последовательности.

1 Включите электропитание ПК №1−4 и дождитесь загрузки ОС, используя программное обеспечение ПК, которое не требует дополнительной предустановки.

2 Вставьте компакт-диск с мастером установки (Setup Wizard) TWL-541P в привод CD-ROM ПК − запуск мастера установки выполняется автоматически.

3.4.3 Настройка адресации сетевых адаптеров TWL-541P

Настройка адресации сетевых адаптеров и организация WI-FI сети в режиме ПД Ad-Hoc может быть выполнена двумя способами, а именно:

- с использованием встроенной службы Windows XP;

- с использованием программы Tenda Wireless Adapter Configuration Utility, записанной на компакт-диске (мастер установки Setup Wizard).

Настройка сетевого адаптера TWL-541P ПК с использованием встроенной службы Windows выполняется в следующей последовательности.

1 В главном меню ПК навести указатель на раздел «Сетевое окружение» и нажать кнопку мыши, затем войти в раздел «Свойства».

2 В появившемся меню ПК «Сетевые подключения» войти в раздел «Беспроводное сетевое соединение» (рисунок 3.2).

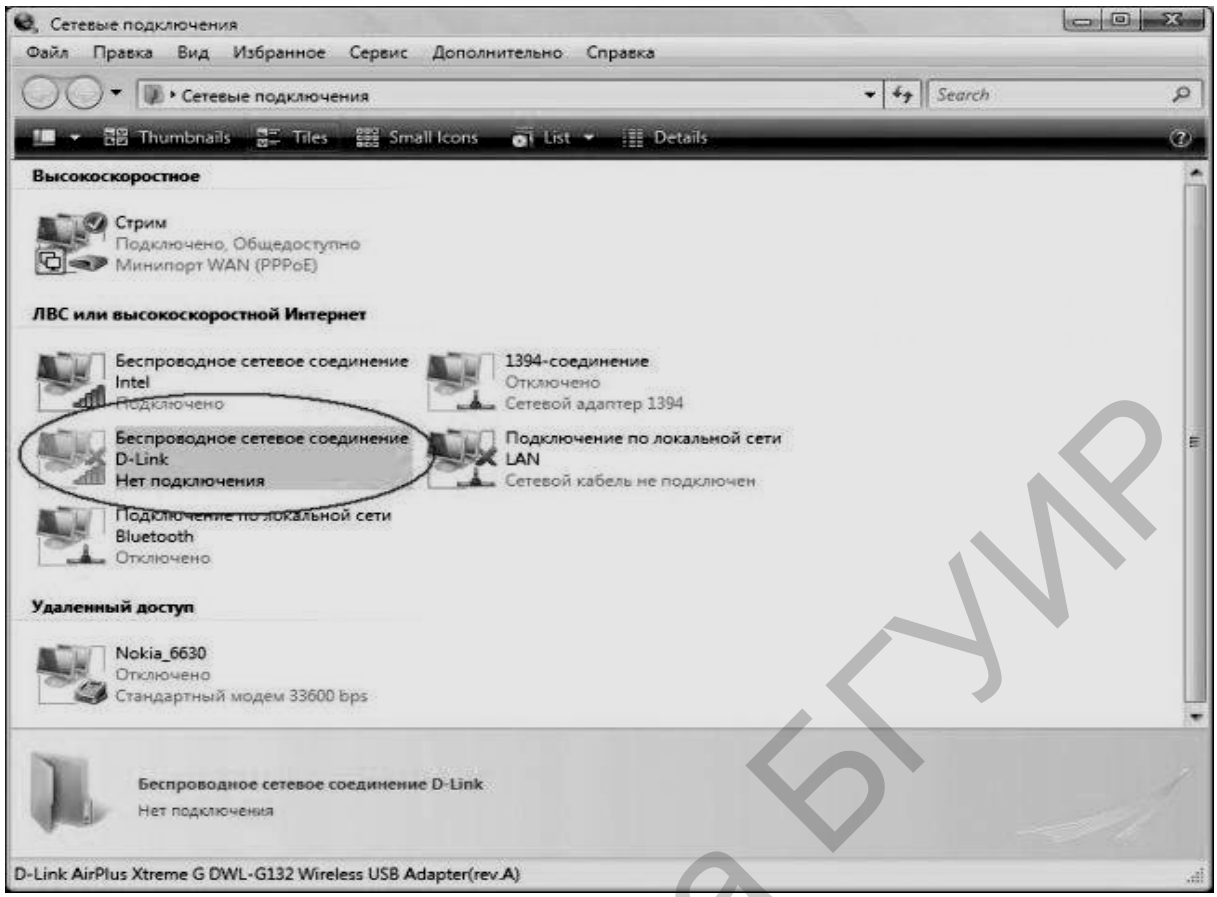


Рисунок 3.2 – Структура текста окна ПК в настройке
«Беспроводное сетевое соединение»

3 В появившейся таблице войти в раздел «Свойства» и нажать кнопку мышки.

4 В появившемся меню ПК «Беспроводное сетевое соединение − свойства» (рисунок 3.3) войти последовательно в разделы «Ответчик обновления топологии уровня связи» и «Протокол интернета (TCP/IP)». Далее войти в раздел «Свойства».

5 В появившемся меню ПК «Общие свойства: Протокол интернета (TCP/IP)» (рисунок 3.4) установить IP-адрес ПК №1 192.168.0.3, ПК №2 192.168.0.4, ПК №3 192.168.0.5 и ПК №4 192.168.0.6, маску подсети 255.255.255.0 и основной шлюз 192.168.1.254.

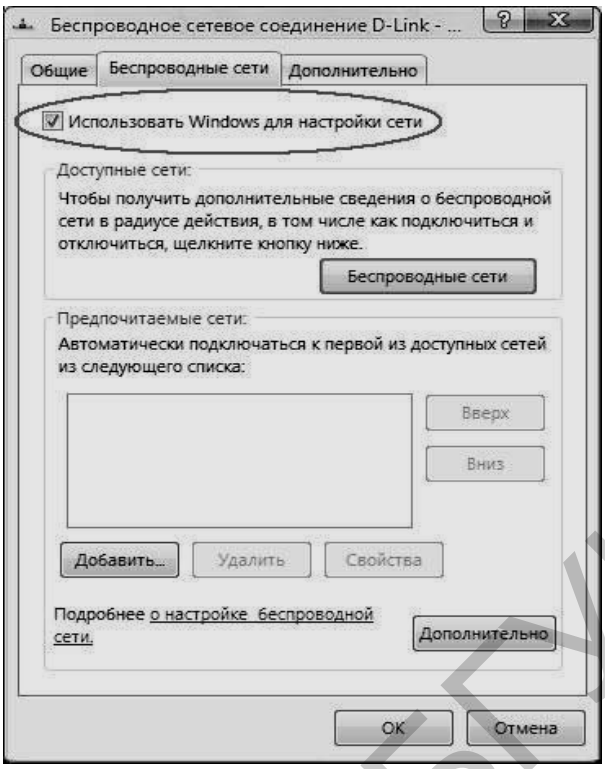


Рисунок 3.3 – Структура текста вкладки ПК
в настройке «Беспроводные сети»

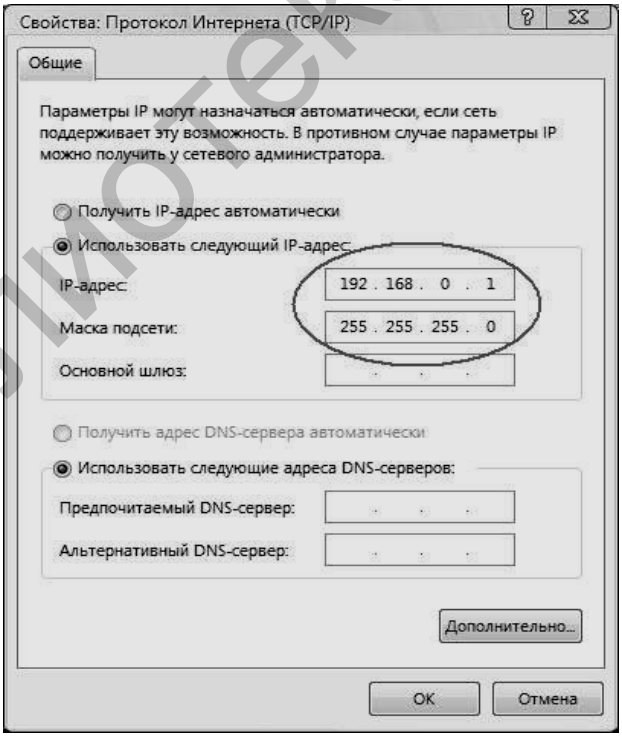


Рисунок 3.4 – Структура текста вкладки ПК в настройке
«Общие свойства: Протокол интернета (TCP/IP)»

6 Ввести команду «ОК» и в появившемся меню «Беспроводное сетевое соединение» (см. рисунок 3.3) войти в раздел «Беспроводные сети» и нажать кнопку мышки.

7 В появившемся меню окна ПК войти в раздел «Добавить» и в новом меню окна ПК (рисунок 3.5) «Свойства беспроводной сети» («Связи», «Проверка подлинности», «Подключение») ввести:

- сетевое имя (SSID) lab3;
- проверка подлинности «Открытая»;
- шифрование данных WEP (в пункте 3.4.4 приводится методика настройки четырех ключей шифрования);

Поставить галочку напротив «Ключ представлен автоматически» и ввести:

- ключ сети 50301;
- подтверждение 50301;
- индекс ключа (расширенный) [1].

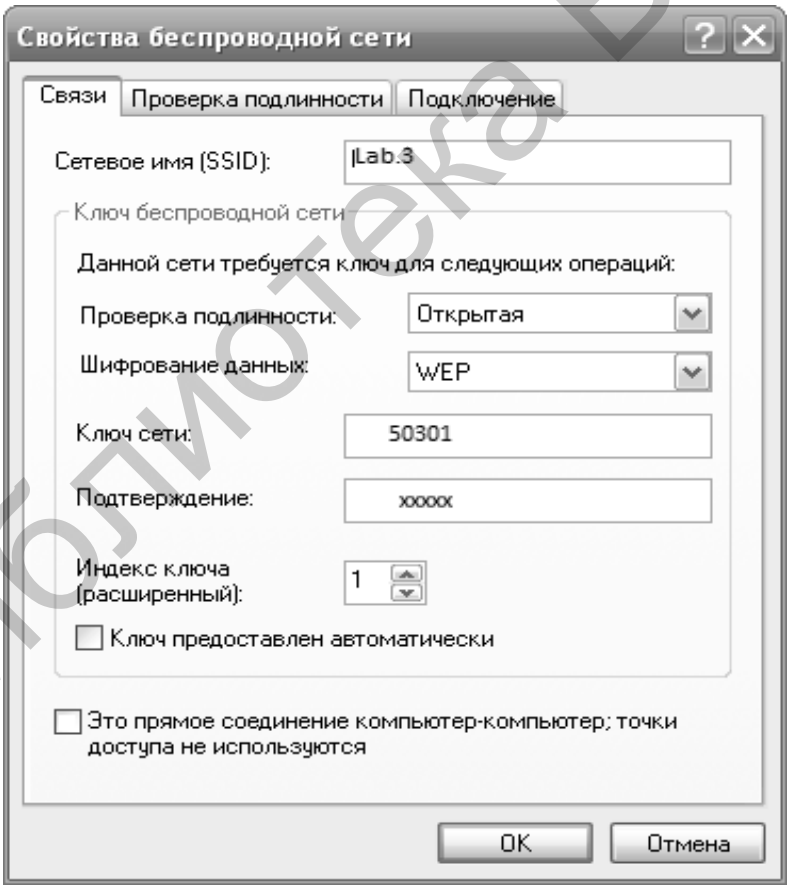


Рисунок 3.5 – Структура окна вкладки
в режиме настройки шифрования

8 Войти в раздел (опцию) «Это прямое соединение компьютер − компьютер» (точки доступа не используются) (см. рисунок 3.5) и ввести команду «ОК».

9 В появившемся окне ПК «Общие», «Беспроводные сети», «Дополнительно» (см. рисунок 3.3) ввести команду ОК.

3.4.4 Настройка (четырех ключей) шифрования сетевых адаптеров TWL-541P

Выполненные в предыдущем пункте настройки не обеспечивают безопасность беспроводного подключения. Беспроводной адаптер Tenda TWL541P рассчитан на работу с установкой режимов шифрования WEP и WPA2-PSK.

Поскольку в сети с данным режимом передачи данных отсутствует точка доступа, а сетевой адаптер Tenda TWL541P не поддерживает режим шифрования WPA/WPA2 в режиме ПД Ad-Hoc, то необходимо выполнить настройку только WEP-шифрования.

Для запуска этого режима шифрования необходимо выполнить следующие настройки.

1 Запустите программу Tenda Wireless Adapter Configuration Utility и создайте в ней соединение типа Ad-Hoc на ПК №1 согласно подпункту 7 пункта 3.4.3.

2 В программе Tenda Wireless Adapter Configuration Utility на вкладке Profile Manager в разделе Profile Settings установить следующие настройки безопасности (рисунок 3.6):

- Encryption Method – WEP;
- Authentication Mode – Shared Key.

3 Далее необходимо настроить WEP-ключи. Для этого нажмите Configure WEP Keys и в появившемся окне (рисунок 3.7) установите следующие значения:

- Key Format – ASCII, что соответствует символьному представлению ключа;
- Key size – 40-Bit (5 chars), ключ длиной 5 символов с учетом регистра (например, bsuir);
- Key 1 – Key 4 – ввести значение ключей;
- Нажать «ОК» и затем Save.

4 Описанные настройки должны быть выполнены на ПК №2–4.

Рисунок 3.6 – Вкладка окна настройки
режимов шифрования

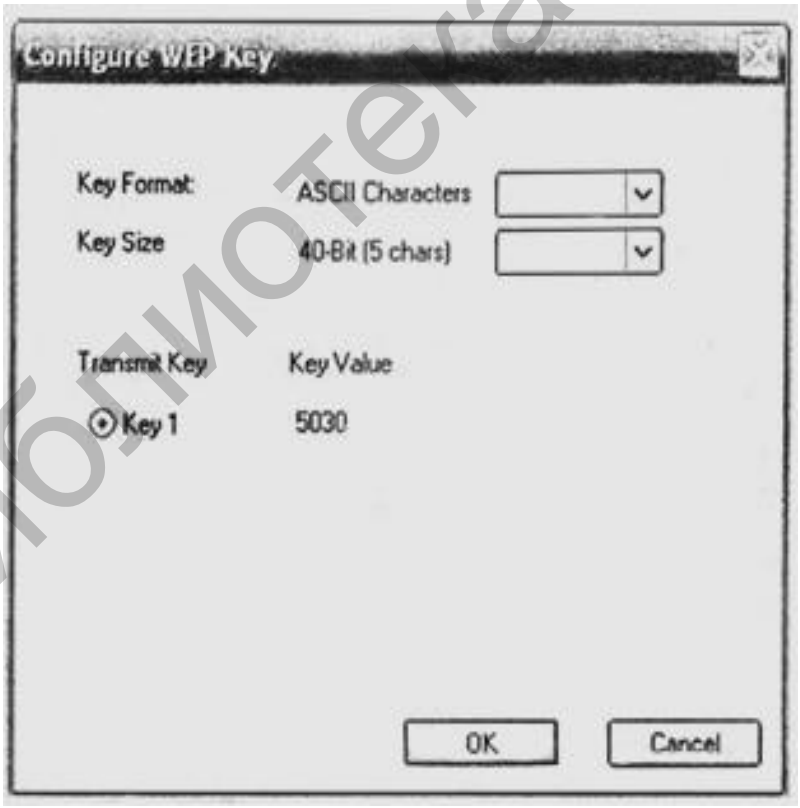


Рисунок 3.7 – Вкладка окна настройки
WEP ключей

3.4.5 Организация и настройка сетевого подключения адаптеров TWL-541P

Организация и настройка сетевого подключения адаптеров TWL-541P выполняется в следующей последовательности:

1 На ПК №2 необходимо запустить службу Windows XP в соответствии с подпунктом 7 пункта 3.4.3 (см. рисунок 3.5) и в основном окне ПК выбрать появившуюся сеть SSID lab3. При совпадении ключей доступа ПК №2 подключиться к ПК №1 и таким образом будет организован беспроводной канал связи между ПК №1 и 2. Для организации лабораторной Wi-Fi сети в режиме ПД Ad-Hoc, состоящей из четырех рабочих станций, необходимо выполнить все те же действия с ПК №3 и 4, что и с ПК №2.

2 Далее выполните обмен сообщениями между ПК №1 и 2, ПК №2 и 3, ПК №3 и 4. Текст сообщения «Группа ххххх. Режим ПД Ad-Hoc, Windows XP».

3 Для обмена сообщениями необходимо создать папку с указанным текстом и сделать ее доступной для сетевого окружения, для чего создайте на ПК №1–4 папки с указанным текстом сообщения: на ПК №1 для ПК №2, на ПК №2 для ПК №3 и на ПК №3 для ПК №4.

Для выполнения предыдущего пункта необходимо на ПК №1:

1) нажать правую кнопку мыши, вызвать на рабочем столе ПК меню «Упорядочить знаки» и войти в раздел «Создать»;

2) указать «Создать папку» и нажать кнопку мыши;

3) в появившемся меню «Новая папка» нажать правую кнопку мыши, войти в раздел «Открыть» и щелкнуть кнопкой мыши;

4) в появившемся окне ПК «Новая папка» навести указатель на любое пустое место и нажать правую кнопку мыши;

5) войти в раздел «Создать» → «Текстовый документ» и щелкнуть кнопкой мыши;

6) в появившемся документе «Текстовый документ» ввести текст сообщения «Группа хххххх. Режим ПД Ad-Hoc, Windows XP» (рисунок 3.8);

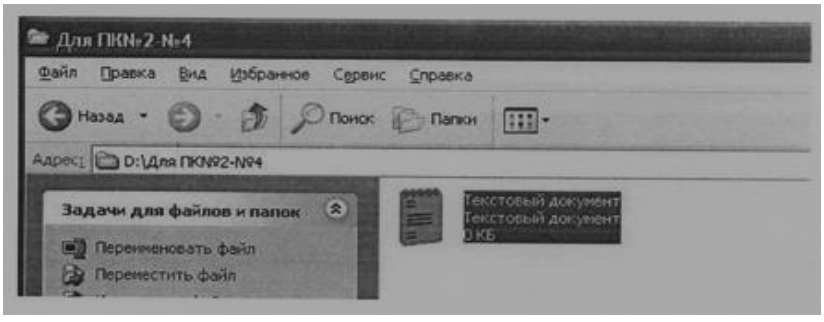


Рисунок 3.8 – Окно ПК с текстом сообщения

7) для сохранения текста щелкнуть кнопкой мыши на разделе «Файл» → «Сохранить»;

8) закрыть программу;

9) для доступа к этой папке через Wi-Fi сеть нажать правой кнопкой мыши на ярлык папки и в контекстном меню выбрать раздел «Общий доступ и безопасность», во вкладке «Доступ» поставить стрелку на пункт «Открыть общий доступ к этой папке» (рисунок 3.9), выбрать «Применить» и нажать «ОК»;

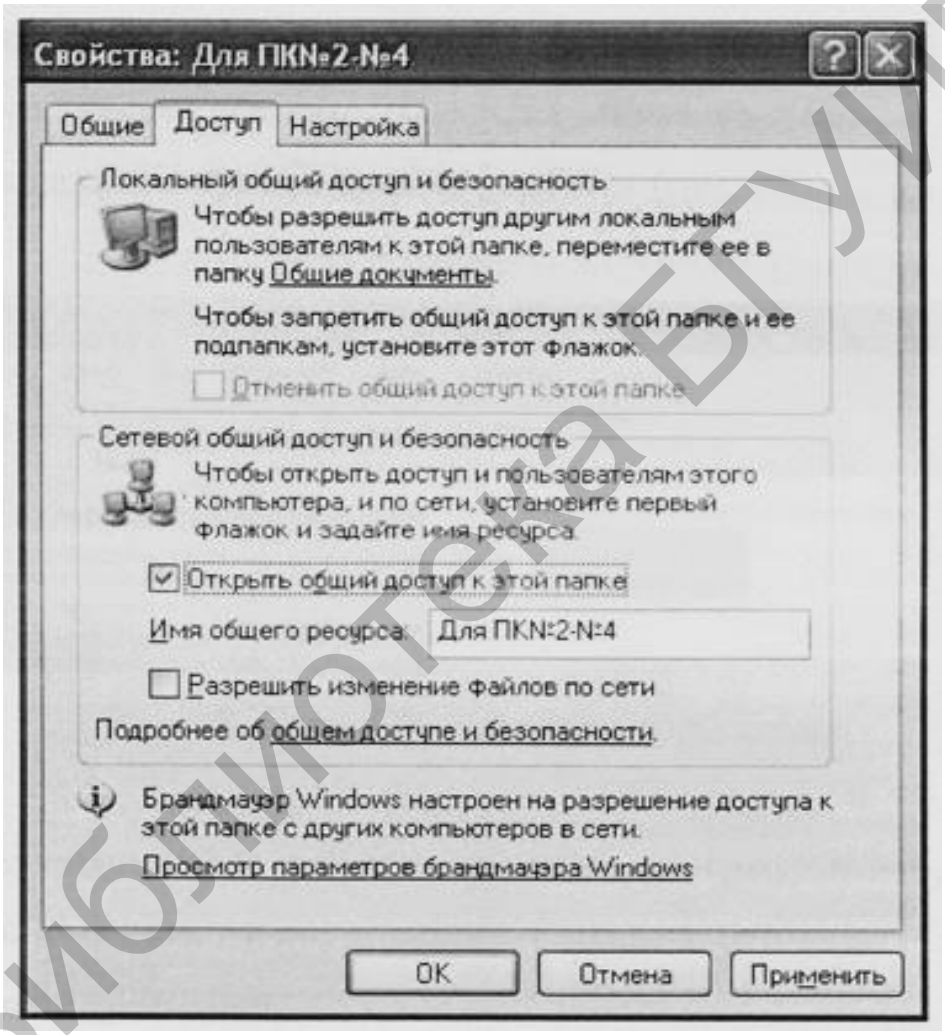


Рисунок 3.9 – Окно общего доступа и безопасности папки

10) на ПК №2 (№3 или №4) открыть «Мой компьютер» → «Сетевое окружение» → «Вся сеть» → WORKGROUP → «ПК №2 (№3, №4)» (рисунок 3.10), копировать этот файл на ПК №2.

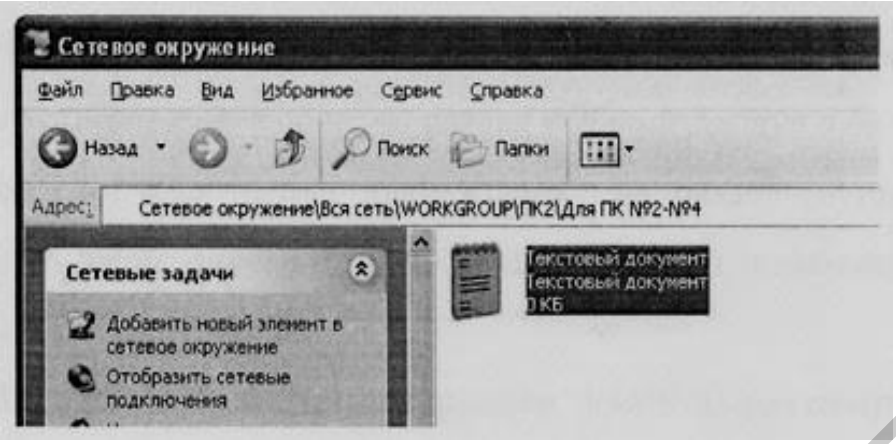


Рисунок 3.10 – Окно «Сетевое окружение»

Выполненные действия должны показать, что лабораторная Wi-Fi сеть полностью работоспособна.

3.5 Оформление отчета по выполненной работе

Отчет по лабораторной работе должен содержать:

- титульный лист, форма которого установлена кафедрой;
- результаты выполнения домашнего задания;
- результаты экспериментальной части выполнения лабораторной работы.

3.6 Контрольные вопросы

1 Основные этапы настройки сетевого оборудования и лабораторной работы в режиме ПД Ad-Hoc.

2 Порядок установки программного обеспечения сетевых адаптеров TWL-541P.

3 Порядок установки драйвера сетевого адаптера TWL-541P вручную.

4 Методика настройки адресации сетевых адаптеров TWL-541P.

5 Методика установки технологии шифрования WEP на сетевых адаптерах TWL-541P.

6 Методика настройки четырех ключей шифрования на сетевых адаптерах TWL-541P.

7 Принцип организации и настройки сетевого подключения адаптеров TWL-541P.

Литература

1 Беспроводные сети Wi-Fi : учеб. пособие / А. В. Пролетарский [и др.]. – М. : Интернет-университет информационных технологий : БИНОМ. Лаборатория знаний, 2007.

2 Роман, П. Основы построения беспроводных локальных сетей стандарта 802.11 / П. Роман, Дж. Лиэри. – М. : Издательский дом «Вильямс», 2004.

3 Столлингс, В. Беспроводные линии связи и сети / В. Столлингс. – М. : Издательский дом «Вильямс», 2003.

4 Феер, К. Беспроводная цифровая связь. Методы модуляции и расширения спектра / К. Феер. – М. : Радио и связь, 2001.

5 Широкополосные беспроводные сети передачи информации / В. Вишневский [и др.]. – М. : Эко-Трендз, 2005.

6 Григорьев, В. А. Сети и системы радиодоступа / В. А. Григорьев, О. Н. Лагутенко, Ю. А. Распаев. – М. : Эко-Трендз, 2005.

ЛАБОРАТОРНАЯ РАБОТА №4

Организация и настройка Wi-Fi сети в режиме передачи данных «Инфраструктура» (BSS)

4.1 Цель работы

Изучить принципы организации, настройки и технической эксплуатации Wi-Fi сети в режиме передачи данных «Инфраструктура».

4.2 Домашнее задание

1 Изучить технические характеристики сетевых адаптеров и точки доступа, используемые в лабораторной работе.

2 Изучить принцип организации и функционирования Wi-Fi сети в режиме «Инфраструктура».

3 По заданным параметрам рассчитать энергетические характеристики радиотракта между максимально удаленным сетевым адаптером (рабочей станции) и точкой доступа.

4 По заданной скорости обмена информацией и объему передаваемой информации рассчитать максимально возможное число рабочих станций сети.

5 По заданной чувствительности приемника точки доступа определить максимально возможную скорость обмена данных.

4.3 Состав лабораторной установки

В состав лабораторной установки входят точка доступа типа DAP-1150 и четыре персональных компьютера (ПК) с сетевыми адаптерами типа TWL-541P.

Структурная схема лабораторной Wi-Fi сети, реализующая режим передачи данных «Инфраструктура», приведена на рисунке 4.1. Программное обеспечение на ПК лабораторной работы предустановлено и не нуждается в модификации.

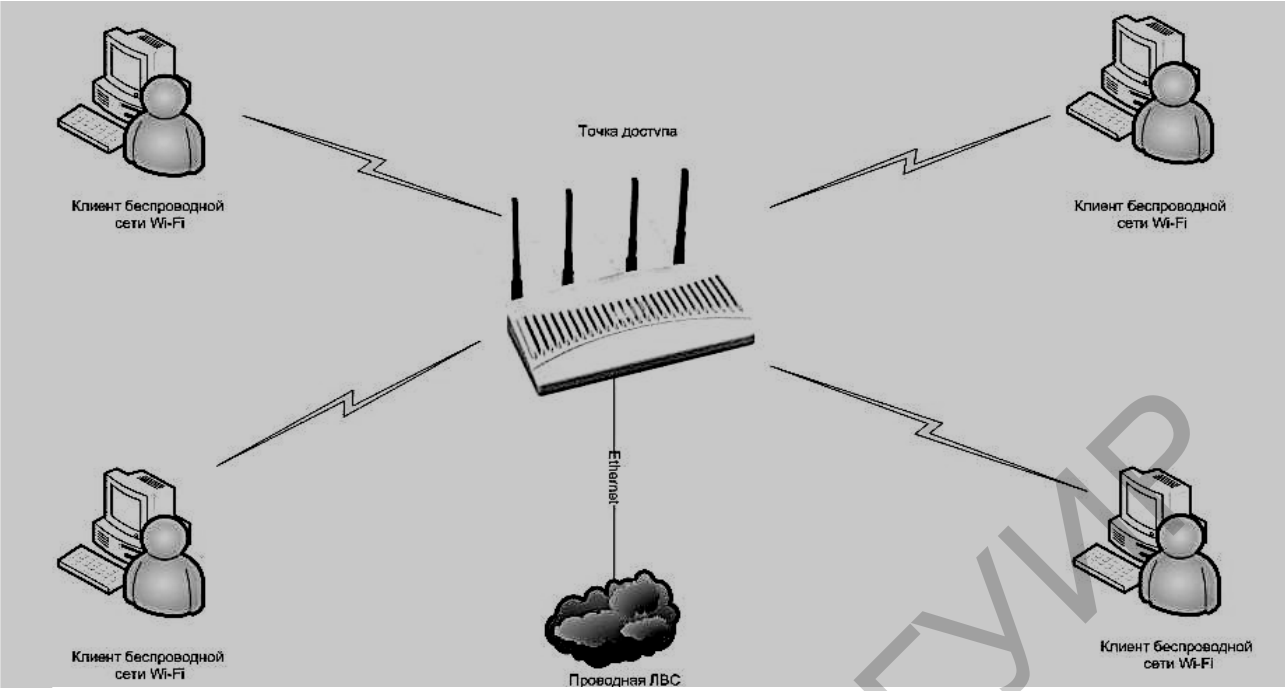


Рисунок 4.1 – Структурная схема лабораторной Wi-Fi сети, реализующая режим «Инфраструктура»

4.4 Экспериментальная часть лабораторной работы

4.4.1 Основные этапы настройки сетевого оборудования лабораторной сети

К основным этапам настройки сетевого оборудования лабораторной Wi-Fi сети в режиме передачи данных «Инфраструктура» относятся:

1) настройка параметров точки доступа DAP-1150;
2) настройка адресации на сетевых интерфейсах (адаптерах);
3) настройка сетевого подключения;
4) настройка режимов шифрования и передачи данных.

4.4.2 Установка программного обеспечения и настройка параметров точки доступа DAP-1150

Настройка параметров точки доступа может быть выполнена с использованием как проводного Ethernet-соединения, так и беспроводного интерфейса.

При большом количестве рабочих станций (ПК с беспроводными сетевыми интерфейсами) не рекомендуется использовать беспроводной интерфейс,

т. к. в этом случае может возникнуть путаница в настройках абонентских сетевых адаптеров.

Установка программного обеспечения и настройка параметров точки доступа D-Link DAP-1150 в инфраструктурном режиме выполняется в следующей последовательности.

1 В окне вкладки ПК «Сетевые подключения» (см. рисунок 3.1) отключите сетевые и бессетевые адаптеры. В контекстном меню выберите «Отключить» для каждого адаптера. В результате ПК №1–4 будут изолированы друг от друга. Сетевых подключений нет.

2 Настройте сетевые адаптеры ПК №1–4 для связи с точкой доступа, для чего перейдите во вкладку «Подключения по локальной сети» → «Свойства» → «Протокол TCP/IP» → «Свойства» (см. рисунок 3.4):

- установите следующие параметры: 192.168.0.50 для точки доступа и 192.169.0.3–192.168.0.6 для беспроводных адаптеров соответственно ПК №1–4;
- укажите маску 255.255.255.0;
- включите кабельное соединение точки доступа с ПК №1.

3 Выполните подключение к точке доступа:

а) подключите адаптер питания точки доступа к сети переменного тока: индикатор питания Power должен быть включен;

б) проверьте подключение антенны типа штырь к антенному разъему точки доступа и соединение точки доступа кабелем Ethernet с соответствующим портом персонального компьютера: один из концов кабеля должен быть подключен к порту LAN точки доступа, а второй конец кабеля связи − к порту Ethernet ПК;

в) сбросьте настройки точки доступа, записанные ранее. Для этого в течении 5 с нажмите и удерживайте кнопку Reset, при этом категорически запрещается отключать электропитание. Время перезагрузки точки доступа составляет примерно 20 с. По окончании загрузки на точке доступа включаются индикаторы Power и LAN;

г) загрузите браузер, после чего на экране дисплея ПК появится окно входа в систему (рисунок 4.2). В адресной строке введите IP-адрес точки доступа по умолчанию http://192.168.0.50;

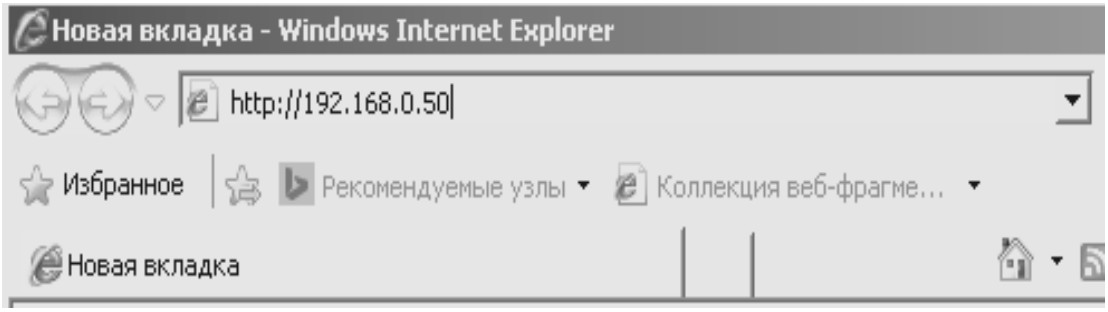


Рисунок 4.2 – Окно входа в систему

д) на экране дисплея ПК появится окно для ввода имени и пароля точки доступа (рисунок 4.3).

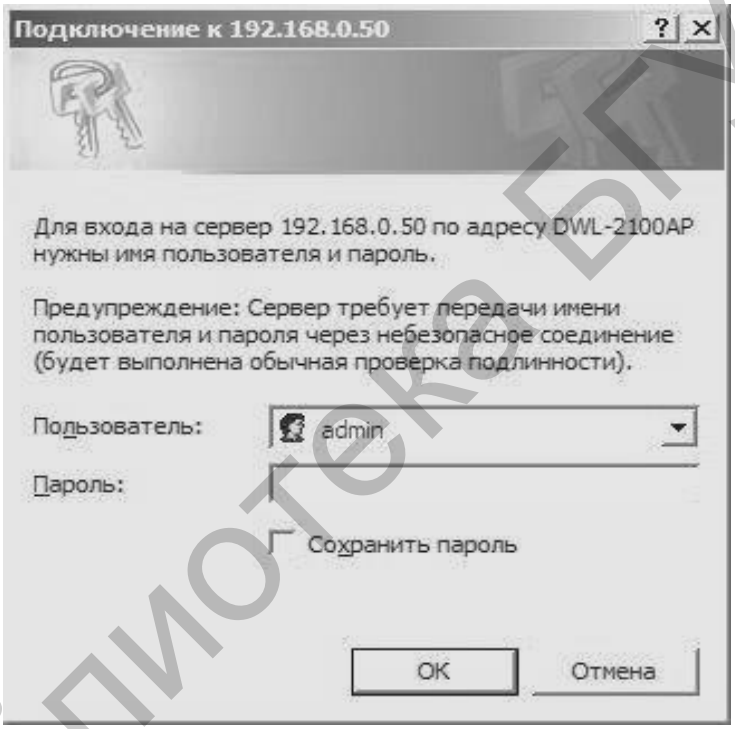


Рисунок 4.3 – Структура текста окна компьютера в режиме набора http:// (IP-адреса)

4 Настройка точки доступа включает выполнение двух режимов: предварительного и основного.

Предварительный режим предполагает выполнение следующих операций:

1) введите в качестве имени пользователя admin с пустым паролем;

2) настройте IP-адрес точки доступа (это нужно в том случае, когда сеть имеет много точек доступа);

3) на вкладке SETUP нажмите кнопку LAN SETUP (слева);

4) установите IP-адрес точки доступа в беспроводном режиме 192.168.0.1;

5) установите маску 255.255.255.0;

6) по завершении настройки нажмите Save setting (сохранить), чтобы перезагрузить точку доступа с новыми настройками.

Основой режим настройки точки доступа включает выполнение следующих операций:

1) дождитесь загрузки точки доступа и введите в браузере новый адрес: http://192.168.0.1;

2) на вкладке Setup нажмите кнопку Wireless Setup (рисунок 4.4);

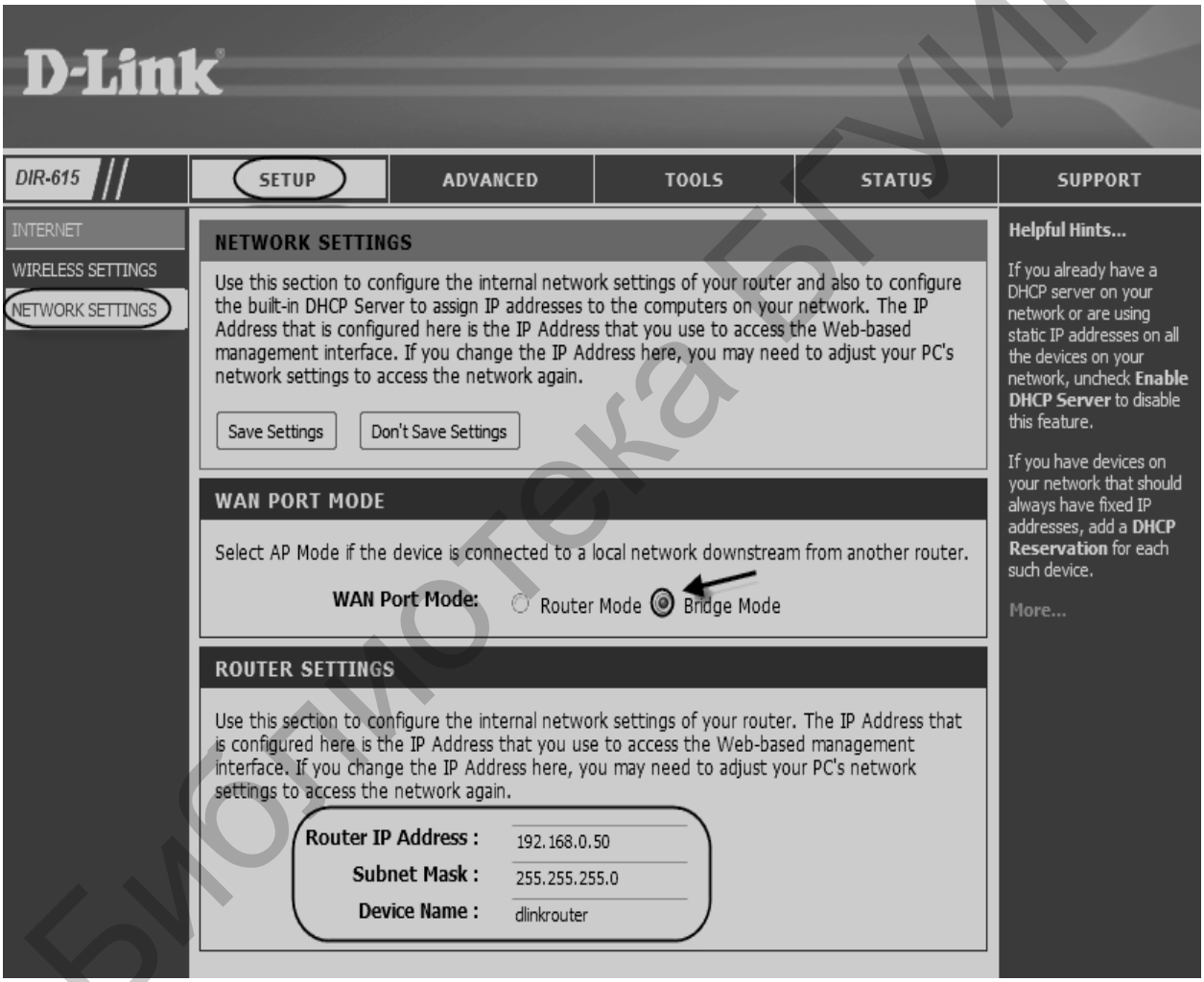


Рисунок 4.4 – Структура текста окна компьютера в режиме Wireless при выполнении основного режима настройки точки доступа

3) установите (см. рисунок 4.4):

- Wireless Mode: Router Mode;
- SSID: Network;

- SSID Broadcast: Enable (выключить);

- Channel: 6.

Выполненные настройки не обеспечивают безопасность беспроводного подключения.

При организации работы Wi-Fi сети без защиты данных от несанкционированного доступа необходимо:

1) нажать Setup и Save Setting, чтобы перезагрузить точку доступа с новыми настройками;

2) отключить точку доступа от сетевого интерфейса (отключить желтый кабель от порта LAN точки доступа и порта Ethernet ПК).

Теперь точка доступа настроена на подключение беспроводных абонентов. Для того чтобы предоставить абонентам доступ в сеть Интернет, нужно к точке доступа подключить широкополосный канал или ADSL-модем. Данный пункт в лабораторной работе не выполняется.

В лабораторной работе предусматривается использование точки доступа с установкой режима шифрования WEP.

Для запуска режима WEP-шифрования необходимо выполнить следующие шаги настройки точки доступа (рисунок 4.5):

1) подключить желтый кабель и ввести режим SSID для канала, как было описано выше. Далее в поле Security Mode в настройке защиты выбрать WEP и Open;

2) так как аутентификация с общим ключом предполагает также шифрование данных по WEP, то в поле Encryption (Шифрование) активно только будет Enable;

3) выбирать тип ключа (Key Type) и размер ключа (Key Size);

4) при 64-битном ключе с типом ключа ASCII ввести пятизначную последовательность – ключ доступа 50301;

5) выполнить настройку сетевых адаптеров TWL-541P ПК №1–4 в соответствии с введенными параметрами точки доступа. Настройка сетевых адаптеров TWL-541P выполняется по методике, приведенной в лабораторной работе №3 (см. подраздел 3.4.2).

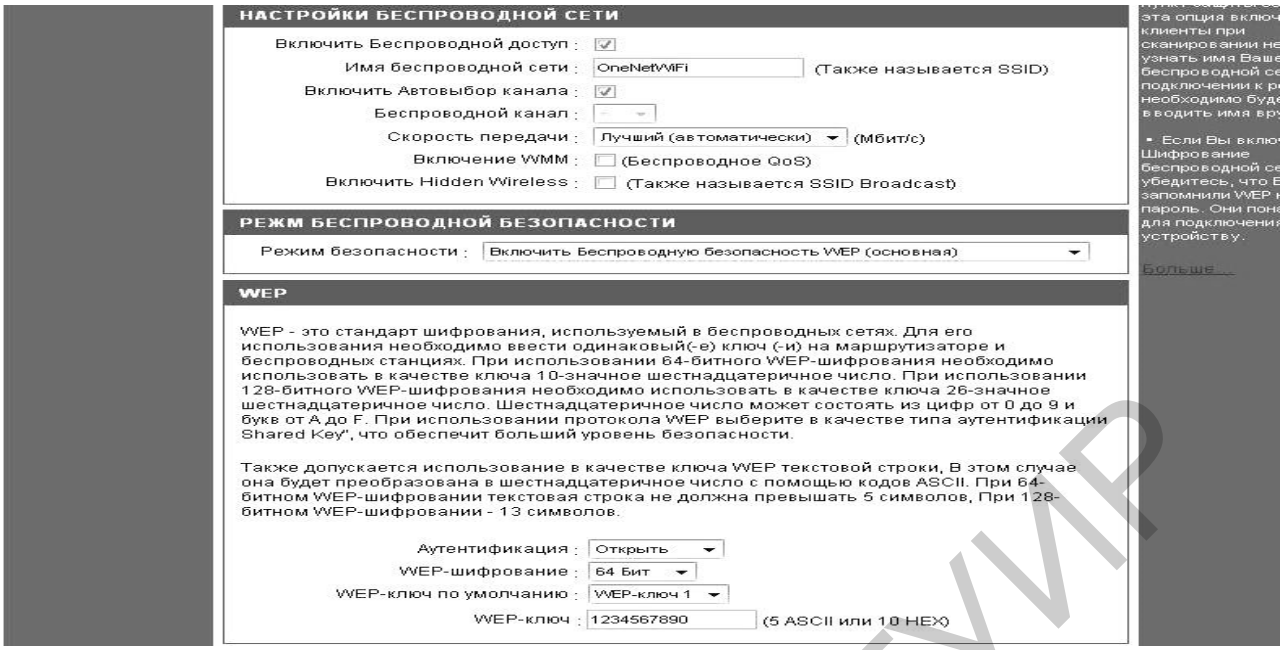


Рисунок 4.5 – Структура текста окна компьютера в режиме Wireless при настройке режима WEP-шифрования

После этого Wi-Fi сеть, реализующая режим ПД «Инфраструктура», будет сконфигурирована.

При помощи команды Ping проверьте возможность взаимодействия ПК №1 с ПК №2 и ПК №3 с ПК №4.

Для проверки работоспособности Wi-Fi сети необходимо передать файл с текстом «Лабораторная работа №4» в режиме ПД «Инфраструктура» с ПК №1 на ПК №2. Данный этап организации Wi-Fi сети выполняется в соответствии с подразделом 3.4.5 лабораторной работы №3.

4.4.3 Ограничение количества беспроводных абонентов

Ограничение количества беспроводных абонентов Wi-Fi сети выполняется следующим образом.

1 Сбросьте настройки точки доступа до заводских.

2 ПК №1–4 должны быть ассоциированы с точкой доступа.

3 Перейдите в меню Advanced Settings – Performance веб-интерфейса точки доступа.

4 Включите контроль количества беспроводных абонентов (Connection Limit-Enable) и ограничьте количество обслуживаемых абонентов (User Limit) одним (например, ПК №1). Сохраните и активируйте настройки точки доступа (рисунок 4.6).

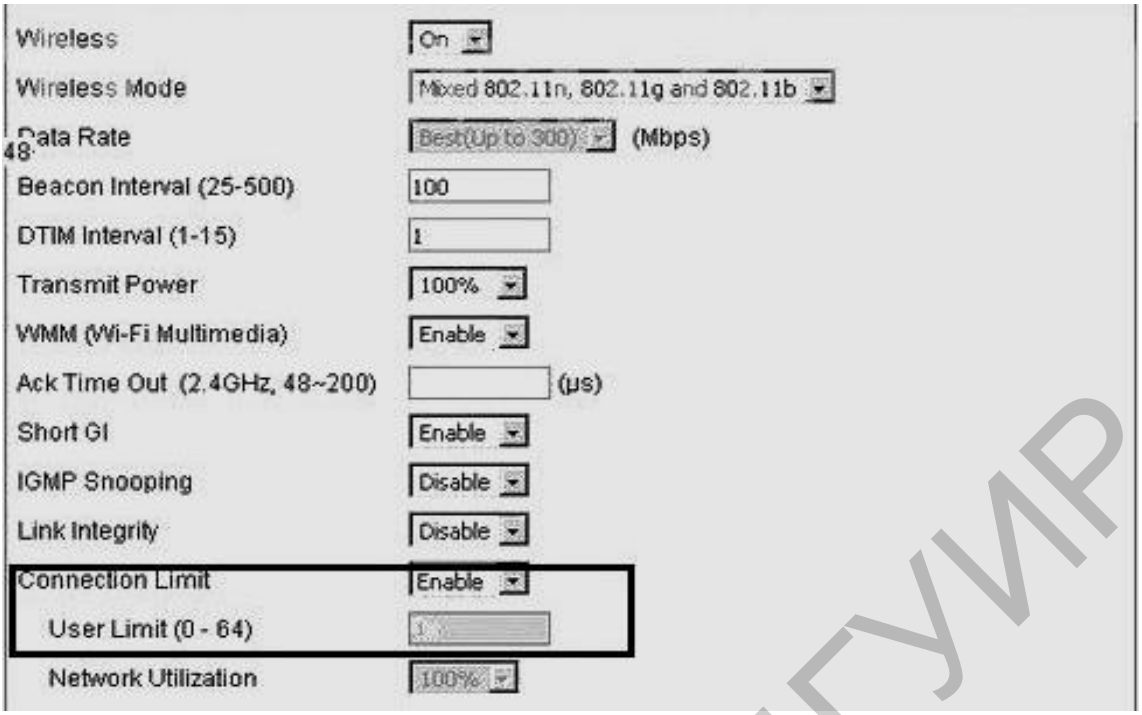


Рисунок 4.6 – Вкладка меню с контролем количества беспроводных абонентов

5 Протестируйте возможность ассоциирования с точкой доступа всех четырех ПК лабораторной работы. Ассоциироваться с точкой доступа должен только ПК №1.

6 Отключите контроль количества беспроводных абонентов (Connection-Limit-Disable). Сохраните и активируйте настройки.

7 На точке доступа включите интегрирование беспроводного и проводного каналов связи (Link Integrate).

8 Отключите от сети Ethernet-порт точки доступа.

9 Протестируйте возможность ассоциирования ПК с точкой доступа в этом случае. Сделайте соответствующий вывод в лабораторной работе.

4.4.4 Метод запрета беспроводным абонентам Wi-Fi сети взаимодействовать друг с другом

Запрет беспроводным абонентам Wi-Fi сети взаимодействовать друг с другом выполняется следующим образом.

1 Ассоциируйте с точкой доступа ПК: ПК №1 и ПК №2 в SSID Sales, а ПК №3 и №4 в SSID guest;

2 Настройте IP-адреса сетевых адаптеров ПК следующим образом:

- IP-адрес ПК №1: 192.168.0.1/24;
- IP-адрес ПК №2: 192.168.0.10/24;
- IP-адрес ПК №3: 192.168.0.11/24;
- IP-адрес ПК №4: 192.168.0.20/24.

3 Перейдите в меню Advanced Setting-Filters – WLAN Partition (см. рисунок 4.6). По умолчанию установлено значение Internal Station Connection-Enable (включено). Это означает, что беспроводным абонентам разрешено взаимодействовать друг с другом в своем и других SSID на точке доступа:

- *Disable*: беспроводные абоненты не могут взаимодействовать друг с другом, будучи подключенными в один и тот же SSID, но могут взаимодействовать с абонентами в других SSID точки доступа;

- *Guest mode*: беспроводные абоненты не могут взаимодействовать с абонентами в том же имени других SSID.

Использованием настроек по умолчанию для Internal Station Connection при помощи команды ping проверьте возможность ПК №1 и 2 (SSID sales) взаимодействовать друг с другом и с ПК №3 и 4.

Для Multi-SSID2 sales установите значение Internal Station Connection – Disable. Сохраните и активируйте настройки.

При помощи команды ping проверьте возможность ПК №1 и 2 (SSID sales) взаимодействовать друг с другом и с ПК №3 и 4 (SSID guest). Обмен ICMP-пакетами между ПК №1 и 2 должен быть успешным, а с ПК №3 и 4 – нет.

Для Multi-SSID2 установите значение Internal Station Connection – Guest mode. Сохраните и активируйте настройки.

При помощи команды ping проверьте возможность ПК №1 и 2 (SSID sales) взаимодействовать друг с другом и с ПК №3 и 4 (SSID guest). Обмен ICMP-пакетами между ПК в обоих случаях должен быть неуспешным.

Верните заводские настройки опции Internal Station Connection.

4.5 Оформление отчета по выполненной лабораторной работе

Отчет по лабораторной работе должен содержать:

- титульный лист, форма которого установлена кафедрой;
- результаты выполнения домашнего задания;
- результаты экспериментальной части лабораторной работы.

4.6 Контрольные вопросы

1 Основные этапы настройки сетевого оборудования лабораторной работы в режиме ПД «Инфраструктура».

2 Методика настройки точки доступа.

3 Методика настройки сетевых адаптеров в режиме ПД «Инфраструктура».

4 Методика установки режимов шифрования WEP и WPA на сетевом оборудовании Wi-Fi сети в режиме ПД «Инфраструктура».

5 Методика проверки функционирования Wi-Fi сети в режиме ПД «Инфраструктура».

6 Методика настройки сети в режиме ограничения количества абонентов сети.

7 Методика настройки сети в режиме запрета беспроводным абонентам взаимодействовать друг с другом.

8 Методика подключения новых (дополнительных) рабочих станций (ПК) в точке доступа в режиме ПД «Инфраструктура».

9 Методика расширения (увеличения) функциональных возможностей точки доступа в режиме ПД «Инфраструктура».

Литература

1 Беспроводные сети Wi-Fi : учеб. пособие / А. В. Пролетарский [и др.]. – М. : Интернет-университет информационных технологий : БИНОМ. Лаборатория знаний, 2007.

2 Роман, П. Основы построения беспроводных локальных сетей стандарта 802.11 / П. Роман, Дж. Лиэри. – М. : Издательский дом «Вильямс», 2004.

3 Столлингс, В. Беспроводные линии связи и сети / В. Столлингс. – М. : Издательский дом «Вильямс», 2003.

4 Феер, К. Беспроводная цифровая связь. Методы модуляции и расширения спектра / К. Феер. – М. : Радио и связь, 2001.

5 Широкополосные беспроводные сети передачи информации / В. Вишневский [и др.]. – М. : Эко-Трендз, 2005.

6 Григорьев, В. А. Сети и системы радиодоступа / В. А. Григорьев, О. Н. Лагутенко, Ю. А. Распаев. – М. : Эко-Трендз, 2005.

ЛАБОРАТОРНАЯ РАБОТА №5

Организация и настройка Wi-Fi сети в режиме передачи данных «Расширенная инфраструктура» (EBSS)

5.1 Цель работы

Изучить принципы организации, настройки и технической эксплуатации Wi-Fi сети в режиме передачи данных «Расширенная инфраструктура», или WDS with AP (Wireless Distribution System with Access Point).

5.2 Домашнее задание

1 Изучить технические характеристики сетевых адаптеров и точек доступа, используемых в лабораторной работе.

2 Изучить принцип организации и функционирования Wi-Fi сети в режиме «Расширенная инфраструктура».

3 По заданным параметрам рассчитать энергетические характеристики радиоканала между точками доступа сети.

4 По заданной канальной скорости передачи данных рассчитать допустимую чувствительность приемника точки доступа.

5.3 Состав лабораторной установки

В состав лабораторной установки входят точка доступа типа DAP-1150 и четыре ПК с сетевыми адаптерами типа TWL-541P (рисунок 5.1). Программное обеспечение на ПК лабораторной работы предустановлено и не нуждается в модификации.

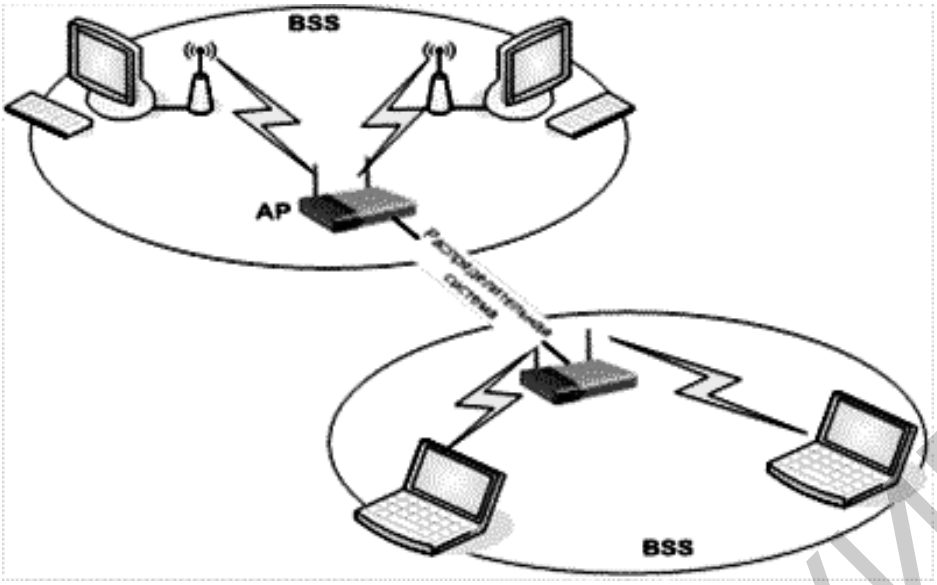


Рисунок 5.1 – Структурная схема Wi-Fi сети,
функционирующая в режиме ПД «Расширенная инфраструктура»

5.4 Экспериментальная часть лабораторной работы

5.4.1 Основные этапы настройки сетевого оборудования лабораторной сети

К основным этапам настройки сетевого оборудования лабораторной Wi-Fi сети в режиме передачи данных «Расширенная инфраструктура» относятся:

1) настройка параметров двух точек доступа;

2) настройка адресации на сетевых интерфейсах (адаптерах);

3) настройка радиомоста и сетевого подключения рабочих станций (персональных компьютеров);

4) настройка режимов шифрования и передачи данных.

5.4.2 Настройка параметров двух точек доступа лабораторной Wi-Fi сети

Процесс настройки Wi-Fi сети заключается в настройке двух отдельных Wi-Fi сетей или двух отдельных точек доступа с двумя ПК, включенных в каждую сеть (см. рисунок 5.1).

Настройка параметров оборудования Wi-Fi сети может выполняться как в проводном, так и в беспроводном режимах.

Настройка параметров оборудования Wi-Fi сети в *проводном режиме* выполняется в следующей последовательности.

1 Проверьте включение электропитания точек доступа и всех ПК, а также подключение ПК №1 и 3 соответственно к точкам доступа №1 и 2.

2 Сбросьте настройки точек доступа и дождитесь включения ОС точек доступа и ПК.

3 В структуре окна «Сетевые подключения» (см. рисунок 3.2) отключите беспроводные интерфейсы.

4 Запустите браузер Internet Explorer и в адресной строке (см. рисунок 4.2) введите 192.168.0.50 и по умолчанию логин admin, пароль – пустой.

5 Откройте вкладку ПК Home → LAN (рисунок 4.4) и в поле IP-address введите номера точек доступа: 192.168.0.51 первой точки доступа и 192.168.0.52 второй точки доступа.

6 Откройте вкладку ПК Home → Wireless и установите для точек доступа режим (Mode): WDS with AP (рисунок 5.2).

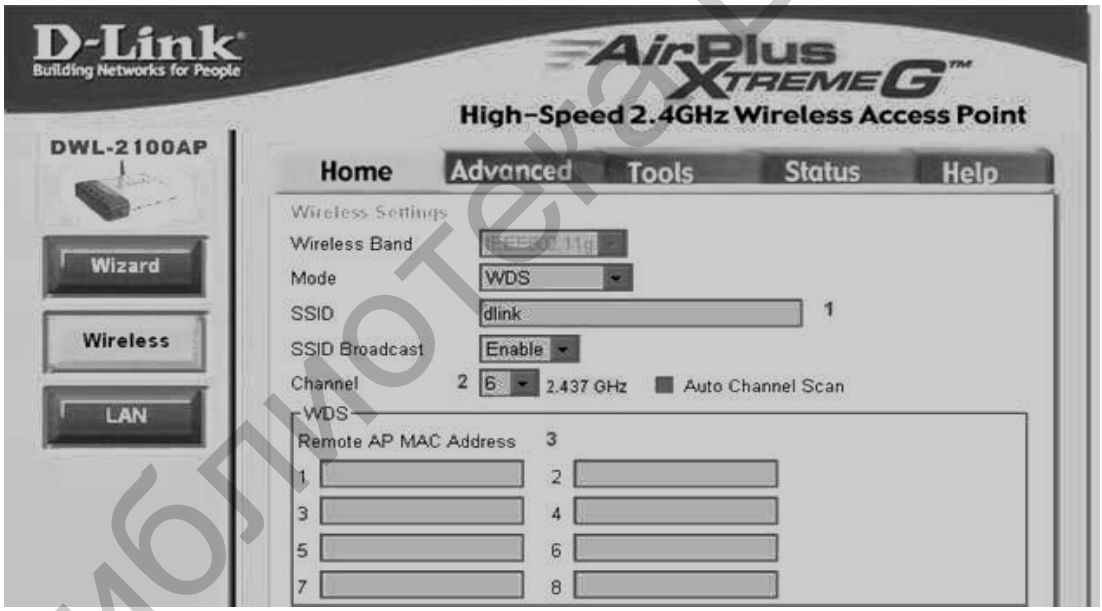


Рисунок 5.2 – Настройка точек доступа в режиме WDS with AP

7 Укажите SSID: SSID Network 1 для первой точки доступа и SSID Network 2 для второй точки доступа.

8 Укажите SSID Broadcast: Enable.

9 Установите один и тот же номер ПК – 6 (1;6;11).

10 В первой точке доступа в поле Remote AP MAC Address укажите MAC-адрес второй точки доступа (00:13:46:75:85:64), MAC-адрес первой точки доступа (00:15:48:79:87:65).

11 Укажите IP-адреса точки доступа №1 и ПК №1.1 и 1.2 соответственно 192.168.0.51, 192.168.0.3, 192.168.0.4; в точке доступа №2 и ПК №2.1 и 2.2 соответственно 192.168.0.52, 192.168.0.5 и 192.168.0.6.

12 Выполните перезагрузку точек доступа и ПК.

13 Отключите точки доступа от сетевых интерфейсов. Точки доступа настроены на беспроводное подключение ПК и на взаимодействие друг с другом.

14 Далее выполните тестирование (функционирование) распределенной Wi-Fi сети путем передачи сообщения «Расширенная Wi-Fi сеть» с ПК №1.1 точки доступа №1 на ПК №2.1 точки доступа №2 и в обратном направлении.

15 Для проверки работоспособности Wi-Fi сети необходимо выполнить следующие действия:

- создать на ПК №1.1 папку с txt-файлом (см. лабораторную работу №3) и назвать ее «Для ПК №2.1» (рисунок 5.3);

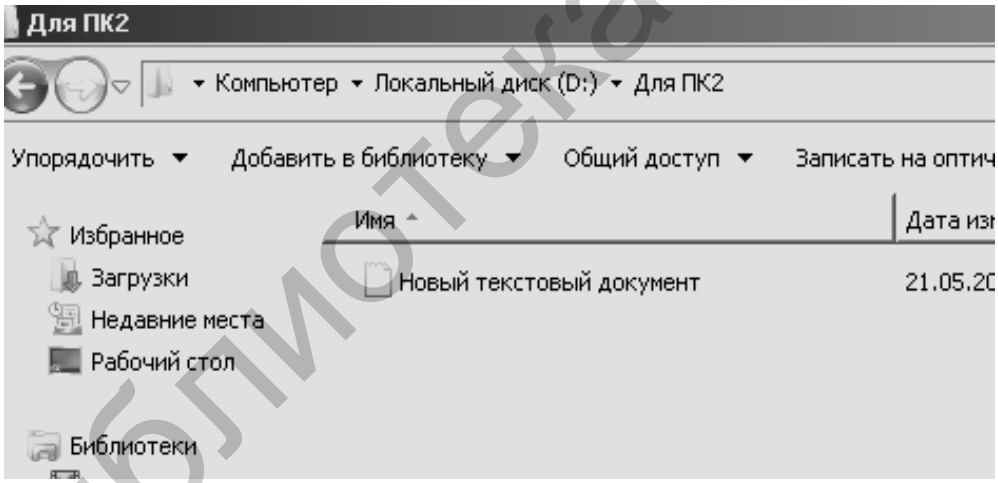


Рисунок 5.3 – Вкладка окна с txt-файлом

- открыть доступ к этой папке, чтобы ее можно было «увидеть» через Wi-Fi сеть. Для этого необходимо щелкнуть правой кнопкой мыши на ярлыке папки и в контекстном меню выбрать пункт «Общий доступ и безопасность», а во вкладке «Доступ» поставить галочку на пункт «Открыть общий доступ к этой папке» (рисунок 5.4);

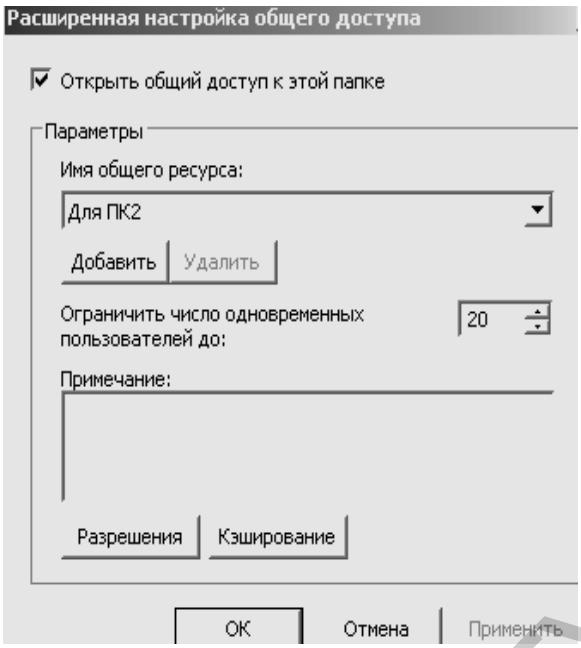


Рисунок 5.4 – Вкладка окна общего доступа и безопасности папки

- ввести команды «Применить» и «ОК»;

- на ПК №2.1 открыть «Мой компьютер» → «Сетевое окружение» → «Вся сеть» → WORKGOUP → «ПК №2.1» → «Для ПК №2.1» (рисунок 5.5). Скопировать этот файл на ПК №2.1.

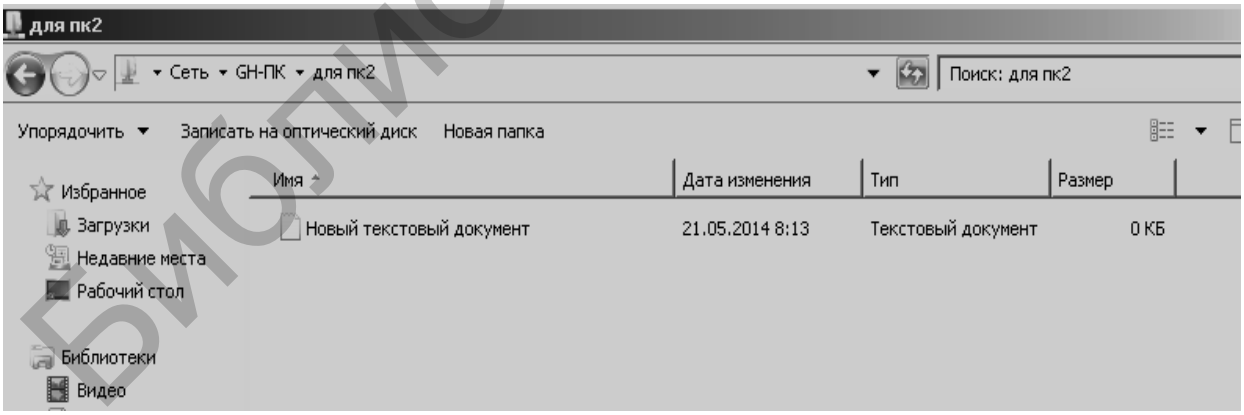


Рисунок 5.5 – Вкладка окна «Сетевое окружение»

Эти же действия выполните с ПК №2.4 точки доступа №2.

Выполненные ранее действия должны подтвердить работоспособность Wi-Fi сети в режиме ПД «Расширенная инфраструктура».

5.4.3 Включение режимов шифрования данных

Точки доступа DAP-1150 обеспечивают защиту данных от несанкционированного доступа на основе использования механизмов шифрования WEP и WPA-PSK.

Для включения механизма шифрования WEP необходимо выполнить следующие действия:

1) подключить ПК №1.1 и 2.1 к точкам доступа №1 и 2 соответственно с использованием проводных интерфейсов;

2) ввести режим WDS with AP;

3) указать SSID Broadcast: Enable;

4) указать номер канала (6);

5) в поле Authentication ввести Shared Key (общий ключ) (рисунок 5.6);

Рисунок 5.6 – Структура текста окна ПК в режиме WDS with AP при установке шифрования WEP

6) ввести тип ключа ASCII в поле Key Type;

7) ввести размер ключа 64 бит в поле Key Type;

8) ввести ключ доступа 50301.

Для включения механизма шифрования WPA2-PSK необходимо выполнить следующие действия:

1) в поле Authentication ввести WPA2-PSK (рисунок 5.7);

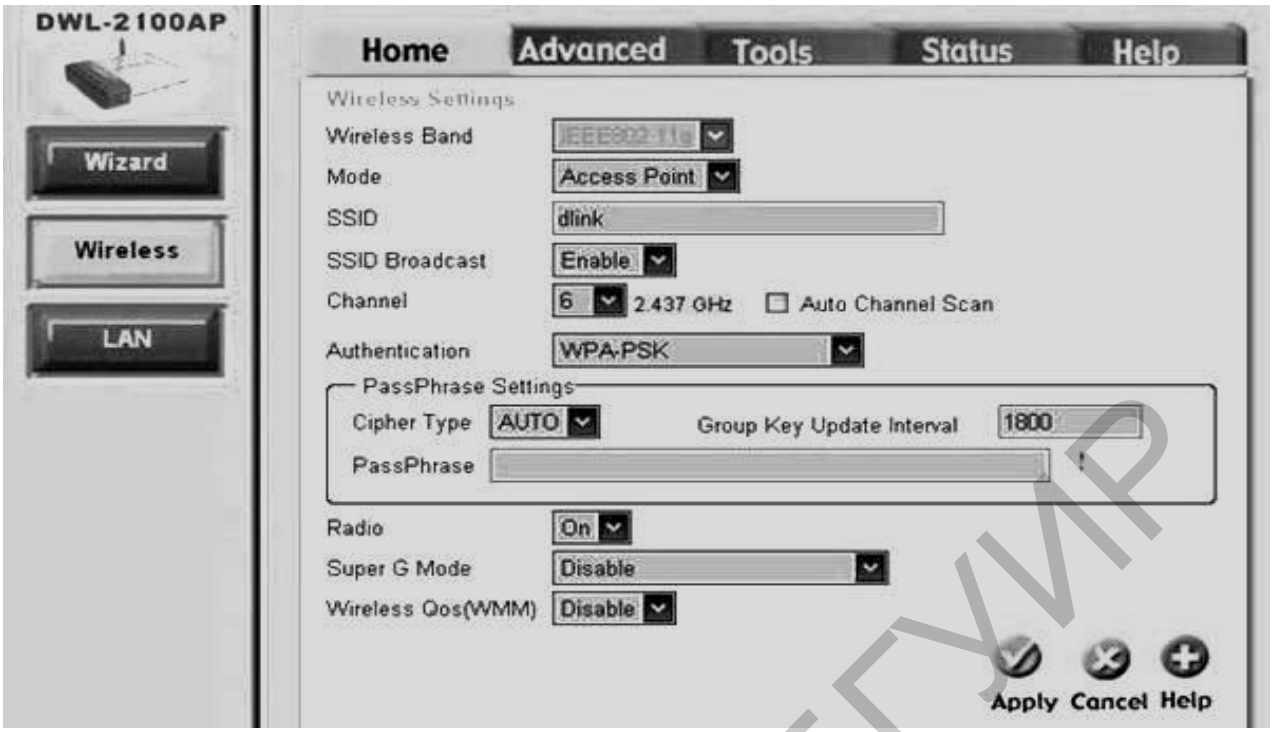


Рисунок 5.7 – Структура текста окна ПК в режиме WDS with AP при установке шифрования WPA2-PSK

2) выбрать тип шифрования (Cipher Type). Возможные варианты: AUTO, TKIP, AES. Если будет выставлено AUTO, то точка доступа будет подстраивать тип шифрования под первую рабочую станцию (ПК) подключившегося абонента;

3) выставить интервал обновления группового ключа (Group Key Update Interval), равный 1800 с;

4) ввести в поле Pass Phrase ключ secret pass.

После этого необходимо выполнить аналогичные настройки на сетевых адаптерах ПК №1.1, 1.2, 2.1 и 2.2.

Выполняются эти настройки с помощью утилиты управления Intel PRO-Set / Wireless в следующей последовательности:

1) отройте главное окно утилиты, выберите профиль соединения и нажмите кнопку (команду «Свойства»);

2) в открывшемся диалоговом окне перейдите к закладке «Настройка защиты» и выберите тип сетевой аутентификации «Общая» (Shared Key);

3) выберите механизм шифрования WEP или WPA2-PSK, задайте длину ключа 64 бита, ключи шифрования 50301 или secret pass соответственно;

4) выполните тестирование как с использованием правильно установленных ключей шифрования, так и измененного в одном знаке ключа шифрования одного из сетевых адаптеров ПК сети.

5.4.4. Организация и настройка Wi-Fi сети в режиме фильтрации ассоциаций беспроводных абонентов с точкой доступа на основе MAC-адресов

Лабораторная Wi-Fi сеть организуется по топологии «Звезда» и функционирует в режиме ПД «Инфраструктура» (см. рисунок 1.9).

Цель работы – научиться настраивать MAC-фильтры.

Настройка Wi-Fi сети в режиме фильтрации ассоциаций беспроводных абонентов с точкой доступа выполняется в следующей последовательности.

Введите IP-адреса беспроводных сетевых адаптеров ПК №1–4 в следующей нумерации:

- ПК №1: 192.168.0.1/24;
- ПК №2: 192.168.0.2/24;
- ПК №3: 192.168.0.3/24;
- ПК №4: 192.168.0.4/24.

Настройка точки доступа выполняется с ПК №1 следующим образом:

1) сбросьте настройки точки доступа до заводских;

2) откройте web-интерфейс точки доступа и, используя вкладку Basic-Settings-Wireless, укажите:

- режим работы – Access Point;
- SSID Network;
- SSID Broadcast: Enable;
- Channel: 6;
- Authentication: Open System;
- в меню Filters – Wireless MACACL включите фильтрацию подключений к точке доступа по MAC-адресам: Access Control List-Accept.

В этом случае фильтр будет действовать по типу «белого списка»: ассоциироваться с точкой доступа будет разрешено только ПК, MAC-адреса которых будут содержаться в списке (рисунок 5.8).

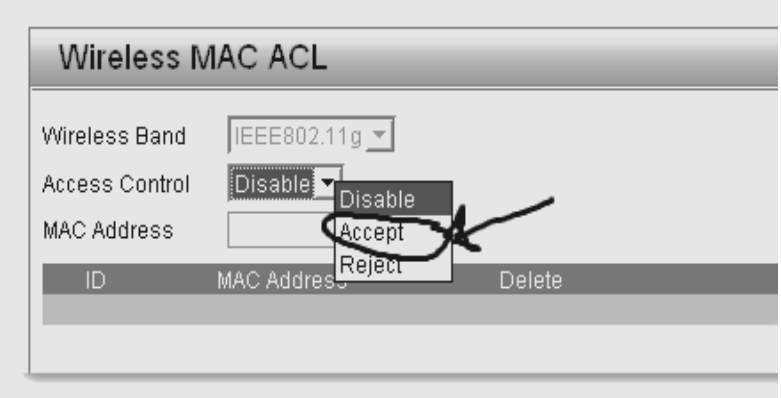


Рисунок 5.8 – Вкладка окна фильтра MAC-адресов в режиме «белого списка»

Далее необходимо:

1) в поле MAC-Address указать MAC-адрес беспроводного сетевого адаптера ПК №1;

2) протестировать возможность ассоциирования с точкой доступа ПК №1;

3) повторить действие с ПК №2;

4) на точке доступа изменить фильтр на запрещающий:

Access Control List-Reject (рисунок 5.9).

Рисунок 5.9 – Вкладка окна с изменением фильтра
на запрещающий сигнал Reject

В этом случае фильтр будет действовать по типу «черного списка»: ассоциироваться с точкой доступа будет разрешено всем ПК, кроме тех, чьи

MAC-адреса будут содержаться в списке. Далее выполните следующие действия:

1) сохраните и активируйте настройки;

2) протестируйте возможность ассоциирования с точкой доступа ПК №1;

3) повторите действие с ПК №2–4;

4) отключите на точке доступа фильтрацию подключений к точке доступа по MAC-адресам;

5) протестируйте ассоциирование с точкой доступа ПК №1–4;

6) выключите точку доступа и ПК.

5.5 Оформление отчета по выполненной лабораторной работе

Отчет должен содержать:

- титульный лист, форма которого установлена кафедрой;
- результаты выполнения домашнего задания;
- основные характеристики Wi-Fi сети лабораторной установки;
- результаты выполнения экспериментальной части лабораторной работы.

5.6 Контрольные вопросы

1 Принцип организации Wi-Fi сети в режиме ПД «Расширенная инфраструктура».

2 Методика настройки точек доступа Wi-Fi сети в режиме WDS with AP.

3 Методика настройки сетевых адаптеров ПК в режиме ПД WDS with AP.

4 Методика настройки точки доступа при использовании механизма шифрования данных WEP и WPA2-PSK.

5 Принцип организации Wi-Fi сети при реализации режима фильтрации абонентов сети.

6 Принцип настройки точки доступа при реализации режима фильтрации абонентов сети.

7 Принцип организации защиты данных от несанкционированного доступа при реализации режима фильтрации абонентов сети.

Литература

1 Беспроводные сети Wi-Fi : учеб. пособие / А. В. Пролетарский [и др.]. – М. : Интернет-университет информационных технологий : БИНОМ. Лаборатория знаний, 2007.

2 Роман, П. Основы построения беспроводных локальных сетей стандарта 802.11 / П. Роман, Дж. Лиэри. – М. : Издательский дом «Вильямс», 2004.

3 Столлингс, В. Беспроводные линии связи и сети / В. Столлингс. – М. : Издательский дом «Вильямс», 2003.

4 Феер, К. Беспроводная цифровая связь. Методы модуляции и расширения спектра / К. Феер. – М. : Радио и связь, 2001.

5 Широкополосные беспроводные сети передачи информации / В. Вишневский [и др.]. – М. : Эко-Трендз, 2005.

6 Григорьев, В. А. Сети и системы радиодоступа / В. А. Григорьев, О. Н. Лагутенко, Ю. А. Распаев. – М. : Эко-Трендз, 2005.

ЛАБОРАТОРНАЯ РАБОТА №6

Методы защиты данных Wi-Fi сетей от несанкционированного доступа, используемые в Wi-Fi сетях

6.1 Цель работы

Изучить используемые в Wi-Fi сетях методы и технологии защиты данных от несанкционированного доступа.

6.2 Домашнее задание

1 Изучить типы угроз (атак) безопасности передачи данных, возможных в Wi-Fi сетях.

2 Изучить используемые в Wi-Fi сетях методы и технологии защиты данных от несанкционированного доступа.

3 Изучить используемые в Wi-Fi сетях аппаратурные и программные средства защиты данных от несанкционированного доступа.

4 Изучить административные методы организации безопасности в Wi-Fi сетях.

6.3 Общие сведения о методах организации защиты данных в Wi-Fi сетях

6.3.1 Классификация угроз (атак) безопасности передачи данных, возможных в Wi-Fi сетях

Беспроводные сети связи типа WAN, WLAN и Wi-MAX относятся к сетям повышенного риска несанкционированного доступа к передаваемым данным. Принципиальное отличие между проводными и беспроводными сетями связи в плане организации безопасности передачи информации (ПИ) состоит в том, что в беспроводных сетях связи имеются совершенно неконтролируемые области пространств между конечными точками сети. Это позволяет противникам значительно проще проникнуть в беспроводную сеть, чем в проводную: нет необходимости подключаться к проводам, достаточно остаться в зоне приема радиосигнала и выполнять различные методы нападений, которые невозможно проводить в проводных сетях.

Наиболее важными угрозами безопасности в проводных Wi-Fi сетях связи являются:

а) подслушивание;

б) отказ в обслуживании;

в) глушение абонентской станции;

г) глушение базовой станции;

д) разрушение некачественного выполнения криптозащиты информации;

е) искажение проходящей в сети информации;

ж) контроль трафика и извлечение из него конфиденциальной информации;

з) атака ПК пользователей и серверов сети;

и) внедрение поддельных точек доступа;

к) рассылка спама, совершение других противоправных действий от имени атакуемой сети и др.

В настоящее время для организации ПИ в Wi-Fi сетях применяются сложные алгоритмические математические модели аутентификации, шифрования данных и контроля целостности их передачи, но тем не менее вероятность доступа к информации Wi-Fi сетей связи является очень существенной. В связи с этим повышению безопасности ПИ в Wi-Fi сетях связи уделяется большое внимание.

6.3.2 Классификация и краткая характеристика методов организации безопасности передачи данных, используемых в Wi-Fi сетях

На начальном этапе внедрения Wi-Fi сетей для обеспечения безопасности ПД или ПИ использовали пароль SSID (Server Set Identifier – сеансовый идентификатор сервера). Однако с широким развитием Wi-Fi сетей было установлено, что данный механизм (пароль) не может обеспечить надежную защиту информации от несанкционированного доступа.

В настоящее время безопасность ПИ в Wi-Fi сетях организуется на основе следующих основных методов (механизмов), являющихся элементами теории криптографической защиты: *аутентификация*, *целостность* и *конфиденциальность*.

Криптографические механизмы существуют в виде алгоритмов (математических функций) и секретных ключей. Аутентификация, целостность данных и их конфиденциальность поддерживаются тремя типами криптографический функций, а именно:

- симметричным шифрованием;

- асимметричным шифрованием;

- хэш-функциями.

Симметричное шифрование, которое часто называют шифрованием с помощью секретных ключей, чаще всего используется для обеспечения передачи данных. Для того чтобы обеспечить секретность ПД, абоненты должны совместно выбрать единый математический алгоритм, который будет использоваться для шифрования и дешифрования данных. Кроме того, абонентам нужно выбрать общий секретный ключ, который будет использоваться ими для шифрования и дешифрования данных.

Алгоритм симметричного шифрования данных приведен на рисунке 6.1.

Рисунок 6.1 – Алгоритм симметричного шифрования данных

Для шифрования данных в настоящее время используются следующие алгоритмы секретных ключей:

- DES (Data Encryption Standard – стандарт блочного шифрования);

- 3 DES (тройной DES);

- IDEA (International Data Encryption Algorithm – международный блочный алгоритм шифрования).

Алгоритм шифрования **DES** был разработан корпорацией IBM в 1947 году. Использует для шифрования данных 56-битный код и оперирует блоками данных по 64 бита. Отличается высокой быстротой шифрования и дешифрования данных и часто используется для одновременного шифрования большого количества данных.

Алгоритм шифрования **3 DES**, или TDES, функционирует на основе механизма DES и предусматривает шифрование данных три раза и тремя различными ключами.

Алгоритм шифрования **IDEA**, разработанный в 1991 году, использует ключ длиной 128 бит и отличается высокой стойкостью к несанкционированной дешифрование данных.

Следует отметить, что все три алгоритма шифрования шифруют сообщение блоками по 64 бита. Если объем сообщения превышает 64 бита, что чаще

всего происходит на практике, то сообщение разбивается на блоки по 64 бита, а затем сводится воедино. Чаще всего для этого используется один из следующих четырех методов:

а) ECB (Electronic Code Book – электронная кодовая книга);

б) CBC (Cipher Block Changing – цепочка зашифрованных данных);

в) CFB-x (Cipher Feed Back-x – битовая зашифрованная обратная связь);

г) OFB (Output Feed Back – выходная обратная связь).

Шифрование с помощью секретного ключа чаще всего используется для поддержки секретных данных и очень эффективно реализуется с помощью неизменяемых и «вшитых» программ (firmware).

Этот метод можно использовать и для реализации функции аутентификации и поддержки целостности данных. Однако метод цифровой подписи в этом случае является более эффективным.

Как отмечается специалистами шифрования данных, метод использования секретных ключей имеет следующие недостатки:

а) необходимость часто менять секретные ключи, так как всегда существует риск их случайного раскрытия;

б) затруднительность обеспечения безопасного генерирования и распространения секретных ключей.

От данных недостатков свободен в некоторой степени метод асимметричного шифрования данных.

Метод асимметричного шифрования данных часто называется шифрованием с помощью общего ключа, при котором используются разные, но взаимно дополняющие друг друга ключи и алгоритмы шифрования и дешифрования.

Для того чтобы установить абонентам связь друг с другом с использованием шифрования данных при помощи общего ключа, обеим сторонам (абонентам) нужно иметь два ключа: общий и частный. Таким образом, обе стороны сети (абоненты) для шифрования и дешифрования будут использовать разные ключи.

Алгоритм асимметричного шифрования данных приведен на рисунке 6.2.

Рисунок 6.2 – Алгоритм асимметричного шифрования данных

Общий ключ используется для следующих типовых задач:

- обеспечение секретности данных;
- аутентификация отправителя данных;
- безопасное получение и применение общих ключей.

К широко используемым общим ключам относятся:

- RSA (Rivest-Shamir-Adleman) – Ривест-Шамир-Адлеман;
- EL-Gamal – Эль-Гамаль.

Следует отметить две важные особенности алгоритма асимметричного шифрования данных, а именно:

а) алгоритм генерирования пар общих/частных ключей отличается высокой сложностью, требует больших процессорных мощностей, но в результате получаются пары очень больших случайных чисел, одно из которых становится общим ключом, а другое – частным. Высокая сложность генерирования таких чисел абсолютно необходима для обеспечения уникальности каждой пары общих/частных ключей;

б) алгоритм шифрования данных с помощью общих ключей редко используется для поддержки секретности данных из-за ограниченной производительности процессоров. Вместо этого их часто используют в приложениях, где аутентификация производится с помощью цифровой подписи и управления ключами.

Алгоритм шифрования данных «*Безопасная хэш-функция*» базируется на формировании специальной функции, которую легко рассчитать, но обратное восстановление практически невозможно, так как это требует больших процессорных мощностей.

Передаваемое сообщение пропускают через математическую функцию (хэш-функцию), и на выходе получается некая последовательность битов, которая называется «хэш», или «результат обработки сообщения». Хэш-функция принимает сообщение (данные) любой длины и выдает на выходе хэш фиксированной длины. Алгоритм шифрования хэш-функции представлен в виде следующей схемы (рисунок 6.3)

Рисунок 6.3 – Алгоритм вычисления хэш-функций

Обычные хэш-функции включают в себя следующие алгоритмы:

- MD4 (Message Digest 4) – дайджест сообщения версии 4;
- MD5 (Message Digest 5) – дайджест сообщения версии 5;
- SHA (Secure Hash Algorithm) – безопасный хэш-алгоритм.

Высокую криптостойкость ПД обеспечивает организация безопасности Wi-Fi сетей с использованием алгоритмов, таких как *цифровая подпись* и *цифровой сертификат*.

Алгоритм шифрования данных «*Цифровая подпись*» представляет собой зашифрованный хэш, который добавляется к сообщению (документу). Алгоритм шифрования данных с использованием цифровой подписи реализуется по следующей схеме (рисунок 6.4).

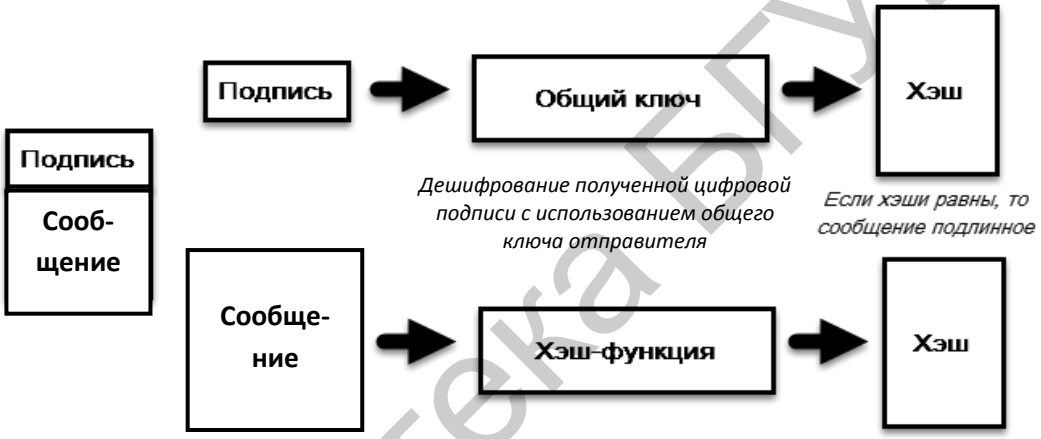


Рисунок 6.4 – Алгоритм шифрования
и дешифрования данных с цифровой подписью

Цифровая подпись может использоваться для аутентификации отправителя и целостности документа и создаваться с помощью сочетания хэш-функций и криптографических общих ключей.

Алгоритм шифрования данных «*Цифровой сертификат*» реализуется как сообщение с «*цифровой подписью №*» и используется для подтверждения действительности общего ключа.

В настоящее время широко распространен сертификат X.509, важным элементом которого является эмитирующая организация, или центр сертификации CA (Certification Authority).

Передача общего ключа производится по следующей схеме (рисунок 6.5).

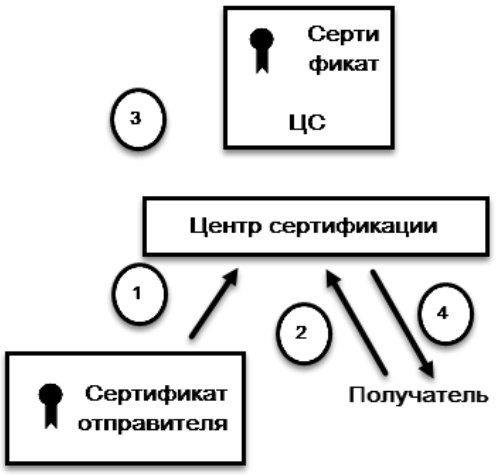


Рисунок 6.5 – Схема передачи общего
ключа с цифровым сертификатом

Передача общего ключа осуществляется в следующей последовательности.

1 Отправитель создает сертификат, в который включает общий ключ: сертификат представляет собой определенную структуру данных, связывающую общий ключ с его обладателем, и набор элементов и функций, используемых абонентами сети при установлении защищенных соединений.

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 этого механизма необходима надежная система распространения общего ключа центра сертификации среди абонентов сети. Для этого создана инфраструктура (система) открытых ключей (PKI – Public Key Infrastructure). Система открытых ключей (PKI) представляет собой иерархическую структуру управления функциями организации безопасности ПД абонентов, участвующих в защищенном обмене информации. В общем PKI представляет собой совокупность сотрудников и технических средств сети: межсетевые экраны, маршрутизаторы, защищенные средства приложений и другие программно-аппаратные комплексы, которые нуждаются в проверке подлинности информации.

6.3.3 Общие сведения о методах шифрования WEP, WPA и WPA2

6.3.3.1 Шифрование данных WEP: определение и способы шифрования

Механизм шифрования данных WEP (Wired Equivalent Privacy – секретность на уровне проводной связи) в беспроводных сетях реализуется на основе алгоритма шифрования RC4 (Rivest's Cipher v4 – код Ривеста, версия 4) и представляет собой *симметричное потоковое шифрование* с переменной длиной ключа, работающее почти в 10 раз быстрее, чем алгоритм шифрования DES, и используется для шифрования больших объемов данных. Для нормального обмена информацией ключи шифрования у абонента и точки радиодоступа должны быть одинаковы.

Ядро алгоритма WEP состоит из функции генерации ключевого потока. Эта функция (операция) генерирует последовательность битов, которая затем объединяется с открытым текстом путем суммирования по модулю два. Дешифрование сообщения состоит из генерации этого ключевого потока и суммирования его с полученной шифрограммой по модулю два и с восстановлением исходного сообщения.

Вторая главная часть алгоритма шифрования данных состоит в реализации функций (операций) *инициализации*, которая использует ключ переменной длины для создания начального состояния генератора ключевого потока. Алгоритм WEP-шифрования может быть выполнен двумя способами: *потоковым* и *блочным*.

Способ *потокового WEP-шифрования данных* выполняется по следующей схеме (рисунок 6.6).

Рисунок 6.6 – Схема потокового WEP-шифрования данных

Шифрованное сообщение получается путем суммирования по модулю два исходного сообщения и ключевой последовательности, сформированной на основе заранее заданного ключа и исходного сообщения. Ключевая последовательность имеет длину, соответствующую длине передаваемого сообщения и подлежащую шифрованию.

Способ *блочного WEP-шифрования данных* реализуется по следующей схеме (рисунок 6.7).

Рисунок 6.7 – Схема способа блочного WEP-шифрования данных

При реализации данного способа шифрования используются информационные блоки определенной длины, которые не меняются в процессе шифрования. Передаваемое сообщение делится на блоки, и функция суммирования по модулю два выполняется над ключевой последовательностью и каждым блоком. Размер блока фиксирован, а последний фрагмент исходного сообщения дополняется «0» до длины нормального блока. Например, при блочном шифровании с 16-байтовыми блоками исходное сообщение длиной 38 байт делится на два блока длиной 16 байт и один блок длиной 6 байт, который затем дополняется 10 байтами из нулевых двоичных символов до длины 16 байт.

Следует отметить, что при потоковом и блочном шифровании используется метод *электронной кодовой книги (ECB)*. Метод ECB характеризуется тем, что одно и то же исходное сообщение на входе порождает одно и то же зашифрованное сообщение на выходе. Это является недостатком системы безопасности, так как злоумышленник может легко обнаружить повторяющиеся последовательности в зашифрованном сообщении и, соответственно, раскрыть содержание сообщения. Для устранения указанного недостатка используются следующие операции:

- векторы инициализации (IVs – Initialization Vector’s);

- обратная связь (FM – Feed back Modes).

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

Сущность способа WEP-шифрования с использованием вектора инициализации (IVs) состоит в том, что данный вектор используется для модификации ключевой последовательности. При изменении IVs ключевая последовательность также меняется. Стандарт IEEE 802.1x рекомендует использование нового значения IVs для каждого нового фрейма, передаваемого в эфир. 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-битным базовым ключом шифрования WEP таким образом, что на вход алгоритма шифрования подается 64- или 128-битный ключ. Вектор инициализации присутствует в нешифрованном виде в заголовке фрейма радиоканала, что позволяет приемной станции успешно декодировать принятый фрейм.

Несмотря на то, что обычно говорят об использовании WEP-шифрования с длиной 64 или 128 бит, эффективная (рабочая) длина ключа составляет лишь 40 или 104 бита по причине передачи IVs в нешифрованном виде. При настройках системы шифрования в оборудовании при 40-битном эффективном ключе вводятся 5 байтовых ASCII-символов ($10 \times 4 = 40$), при 104-битном эффективном ключе вводятся 13 байтовых ASCII-символов ($13 \times 8 = 104$) или 26 шестнадцатеричных чисел ($26 \times 4 = 104$). Некоторое оборудование может работать со 128-битным ключом.

WEP-шифрование с использованием обратной связи применяется обычно при блочном шифровании и позволяет исключить формирование одним и тем же исходным сообщением одного и того же шифрованного сообщения. Наиболее часто применяется тип обратной связи, известный как цепочка шифрованных блоков (CBC). Условно данный способ шифрования реализуется по данной схеме (рисунок 6.8).

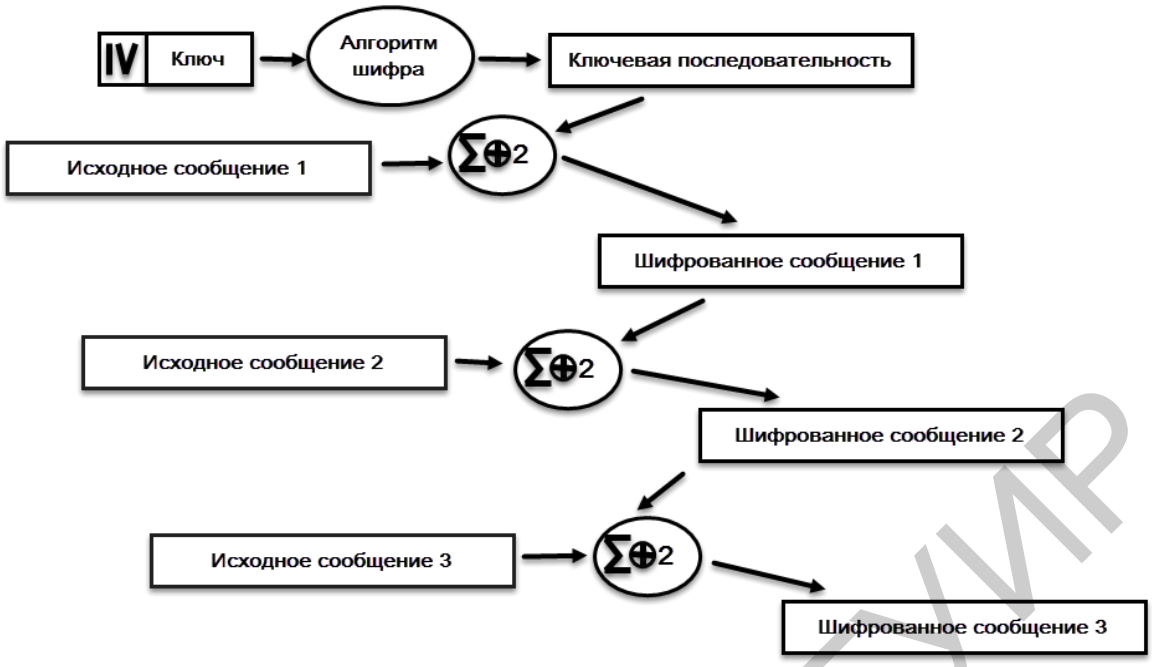


Рисунок 6.8 – Схема способа шифрования WEP
с использованием обратной связи

В основе цепочки шифрованных блоков лежит идея вычисления двоичной функции суммирования по модулю два между блоком исходного сообщения и предшествующим ему блоком шифрованного сообщения. Поскольку самый первый блок не имеет предшественника, для модификации ключевой последовательности, используется вектор инициализации.

6.3.3.2. Методы шифрования данных WPA и WPA2

Метод шифрования WPA (Wi-Fi Protected Access – защищенный доступ к Wi-Fi, т. е. к беспроводным сетям) был разработан в 2002 году организацией WECA (Wireless Ethernet Compatibility Aliance – альянс производительности оборудования Wi-Fi сетей) – основным производителем оборудования Wi-Fi в то время во всем мире. В связи с этим такой метод шифрования данных обеспечивает совместимость оборудования Wi-Fi сетей различных производителей. Механизм шифрования WPA обеспечивает более высокий уровень безопасности ПД, чем метод шифрования WEP, а также позволяет перепрограммировать защиту старого оборудования без внесения аппаратных изменений. Метод шифрования WPA базируется на использовании следующих протоколов защиты данных Wi-Fi сетей:

1) протокол динамического обновления ключей стандарта IEEE 802.1x (метод аутентификации и контроля доступа на канальном уровне);

2) протокол EAP (Extensible Authentication Protocol) расширенной аутентификации;

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

4) технология MIC (Message Integrity Check) проверки целостности сообщений.

К основным усовершенствованиям протокола TKIP относятся следующие процедуры:

- пофреймовое изменение ключей шифрования: 128-битные WEP-ключи изменяются быстро, а их количество может достигать более 500 млрд, что делает сети максимально защищенными;

- контроль целостности сообщения защищает сети от внешнего проникновения и изменения данных;

- усовершенствованный метод управления ключами.

Метод (алгоритм) шифрования WPA может работать в двух режимах:

1) корпоративный (Enterprise);

2) персональный (Pre-shared Key).

В первом случае хранение базы данных и проверка аутентификации в больших сетях согласно стандарту 802.1x обычно осуществляется специальным сервером, чаще всего сервером RADIUS (Remote Authentication Dial-In User Interface – служба удаленной аутентификации пользователя по коммутируемым линиям), в котором используется как протокол расширенной аутентификации EAP (Extensible Authentication Protocol), так и протокол защиты транспортного уровня TLS.

Во втором случае подразумевается применение алгоритма WPA всеми категориями абонентов сети, т. е. реализуется упрощенный режим защиты ПД, не требующий сложных механизмов (протоколов). Этот режим называется WPA-PSK (WPA – Pre Shared Key) и предлагает введение одного пароля на каждый узел беспроводной сети (точки доступа, маршрутизатора, адаптера и моста). В этом случае, пока пароли совпадают, абоненту будет разрешен доступ в сеть.

Следует заметить, что использование пароля для защиты данных делает WPA-PSK доступным для атак сети и ПД методом подбора. Однако этот механизм исключает путаницу с ключами WEP, заменяя их целостной четкой системой на основе цифро-буквенного пароля. Методы шифрования данных, используемые в Wi-Fi сетях, постоянно совершенствуются.

В 2004 году был утвержден стандарт IEEE 802.11i, разработанный корпорацией Wi-Fi Alliance, известный как *метод (алгоритм) шифрования WPA2*. Данный метод шифрования базируется на основе протоколов

стандарта 802.1x и TKIP//CCMP. CCMP (Counter Mode with CBCMAC) – протокол шифрования на основе алгоритма AES (Advanced Encryption Standard – расширенный стандарт шифрования).

Метод шифрования WPA2 – это абсолютно новая система безопасности, целиком лишенная слабых мест метода шифрования WEP. Так как метод WPA2 использует дополнительные меры обеспечения безопасности Wi-Fi сетей (RST – Robust Security Network), то его применение в Wi-Fi сетях требует обязательного изменения как в аппаратурной, так и в программной частях соответствующего оборудования данных сетей связи. Следовательно, Wi-Fi сеть, соответствующая RSN, является несовместимой с Wi-Fi сетью, использующей метод WEP. В переходный период внедрения WPA2 предусматривается поддержка оборудования Wi-Fi сетей с WEP. Метод WAP2 применяется к различным сетевым реализациям Wi-Fi сетей и может задействовать протокол TKIP, но по умолчанию RSN использует AES и CCMP, которые должны заменить WEP и TKIP.

В реализации RSN используется алгоритм AES в качестве системы шифрования подобно тому, как алгоритм RC4 используется в методе WPA. Однако механизм шифрования в AES более сложный, чем в RC4: AES – это блочный шифр, использующий блоки данных длиной 128 бит.

CCMP – это протокол безопасности, используемый AES и являющийся аналогичным TKIP в методе WPA. Протокол CCMP вычисляет MIC (код целостности сообщения), используя метод CBC-MAC (Cipher Block Chaining Massage Authentication Code – цепочки зашифрованных блоков кода аутентификации сообщений). Изменение даже одного бита в сообщении приводит к совершенно другому результату.

Одним из важнейших недостатков метода WEP была высокая сложность управления секретными ключами, в результате чего ключи метода WEP не менялись длительное время (или никогда), что облегчало работу хакерам. Система RSN определяет структуру ключей с ограниченным сроком действия, сходную с алгоритмом TKIP.

В системе AES/CCMP, чтобы вместить все ключи, требуется 512 бит памяти, что значительно меньше, чем для алгоритма TKIP. В обоих случаях мастер-ключи используются не прямо, а для ввода других ключей. В этом случае администратору сети для выполнения данной операции требуется один мастер-ключ. Сообщения составляются из 128-битного блока данных, дешифрованного секретным ключом длины 128 бит. В результате получается шифр значительно сложнее, чем WPA.

Метод шифрования WPA2, так же как метод WPA, может работать в двух режимах, а именно в *корпоративном* и *персональном*. Данный метод шифрования целесообразно использовать для защиты ПД больших Wi-Fi сетей связи, так как он обеспечивает высокую защиту данных и оперативное управление секретным ключом.

6.3.4. Общие рекомендации по организации безопасности передачи данных в Wi-Fi сетях

Для организации высокого уровня безопасности ПД в Wi-Fi сетях необходимо руководствоваться следующими правилами:

а) использовать метод шифрования WAP2 (стандарт 802.11i), а также несколько (два и более) разных алгоритмов шифрования данных;

б) запретить трансляцию в эфир идентификатора SSID;

в) использовать максимально длинные ключи;

г) изменять статические ключи и пароли;

д) пользоваться сложным паролем для доступа к настройкам точки доступа;

е) по возможности не использовать в Wi-Fi сетях протокол TCP/IP для организации папок и принтеров общего доступа;

ж) не разрешать гостевой доступ к ресурсам общего доступа и использовать длинные и сложные пароли;

з) управлять доступом абонентов по MAC-адресам;

и) использовать специальные сетевые операционные системы (Windows NT, Windows XP и др.);

к) располагать антенны как можно дальше от окон, внешних стен здания, а также ограничивать мощность радиоизлучения и др.

Выполнение данных рекомендаций может существенно повысить безопасность передачи данных в Wi-Fi сетях.

6.4 Оформление отчета по выполненной работе

Отчет по лабораторной работе должен содержать:

- титульный лист, форма которого установлена кафедрой;
- результаты выполнения домашнего задания;
- основные методы шифрования данных, используемые в Wi-Fi сетях;
- основные методы и технологии аутентификации абонентских устройств.

6.5 Контрольные вопросы

1 Типы угроз безопасности ПД, возможных в Wi-Fi сетях.

2 Определения терминов теории криптографической защиты информации: аутентификация, целостность данных и конфиденциальность данных.

3 Механизм симметричного шифрования данных.

4 Механизм асимметричного шифрования данных.

5 Механизм шифрования и дешифрования данных с цифровой подписью.

6 Механизм шифрования и дешифрования данных с передачей общего ключа с цифровым сертификатом.

7 Механизмы шифрования данных WEP, WPA, WPA2, их достоинства и недостатки.

Литература

1 Беспроводные сети Wi-Fi : учеб. пособие / А. В. Пролетарский [и др.]. – М. : Интернет-университет информационных технологий : БИНОМ. Лаборатория знаний, 2007.

2 Роман, П. Основы построения беспроводных локальных сетей стандарта 802.11 / П. Роман, Дж. Лиэри. – М. : Издательский дом «Вильямс», 2004.

3 Столлингс, В. Беспроводные линии связи и сети / В. Столлингс. – М. : Издательский дом «Вильямс», 2003.

4 Феер, К. Беспроводная цифровая связь. Методы модуляции и расширения спектра / К. Феер. – М. : Радио и связь, 2001.

5 Широкополосные беспроводные сети передачи информации / В. Вишневский [и др.]. – М. : Эко-Трендз, 2005.

6 Григорьев, В. А. Сети и системы радиодоступа / В. А. Григорьев, О. Н. Лагутенко, Ю. А. Распаев. – М. : Эко-Трендз, 2005.

ЛАБОРАТОРНАЯ РАБОТА №7

Методы организации Wi-Fi сетей на основе многофункционального телекоммуникационного шлюза 2Wire1701HG

7.1 Цель работы

Изучить принцип построения, функционирования универсального шлюза. Получить практические навыки в настройке и технической эксплуатации универсального шлюза типа 2Wire1701HG.

7.2 Домашнее задание

1 Изучить основные технические характеристики, принципы построения и функционирования шлюза 2Wire1701 HG, основные принципы и этапы его технической эксплуатации.

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

7.3 Состав лабораторной установки

В состав лабораторной установки входят шлюз 2Wire1701HG, четыре компьютера с сетевыми адаптерами TWL-541P, поддерживающие протокол Wi-Fi, локальная сеть лаборатории 501, являющаяся составной частью мультисервисной сети кафедры ИКТ.

Обобщенная структурная схема лабораторной работы представлена на рисунке 7.1

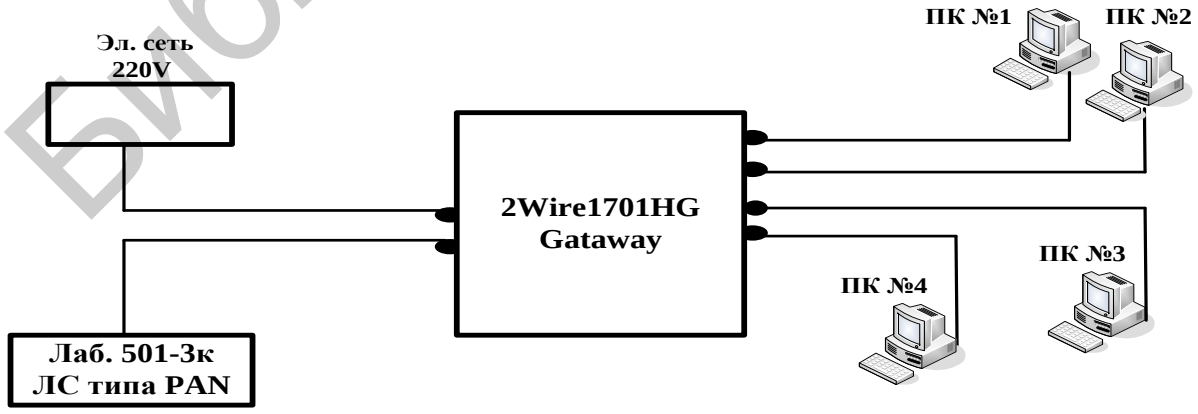


Рисунок 7.1 – Обобщенная структурная схема лабораторной работы

Кроме организации сети данной структуры, 2Wire1701HG может обеспечивать следующие варианты связей.

1 Соединение по топологии Ad-Hoc «точка – точка». Данное соединение абонентов или ПК можно представить в виде следующей схемы (рисунок 7.2).

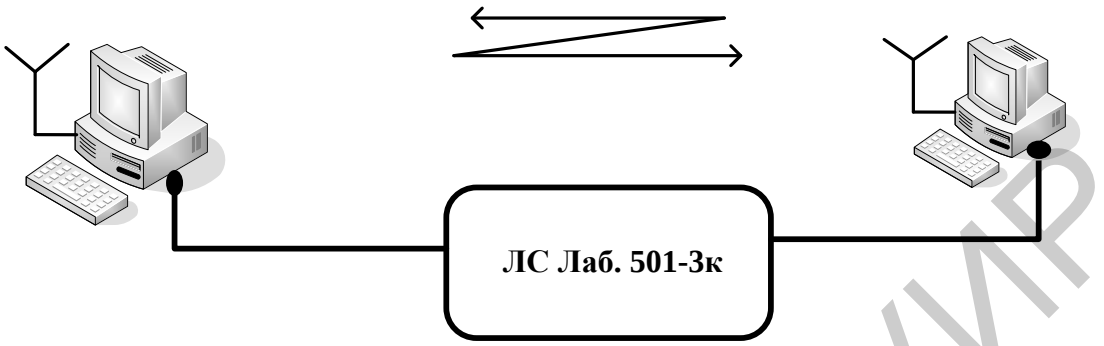


Рисунок 7.2 – Структурная схема беспроводной
сети по топологии Ad-Hoc

2 Соединение с использованием роутера (маршрутизатора) и модема, что условно можно представить в виде схемы (рисунок 7.3).

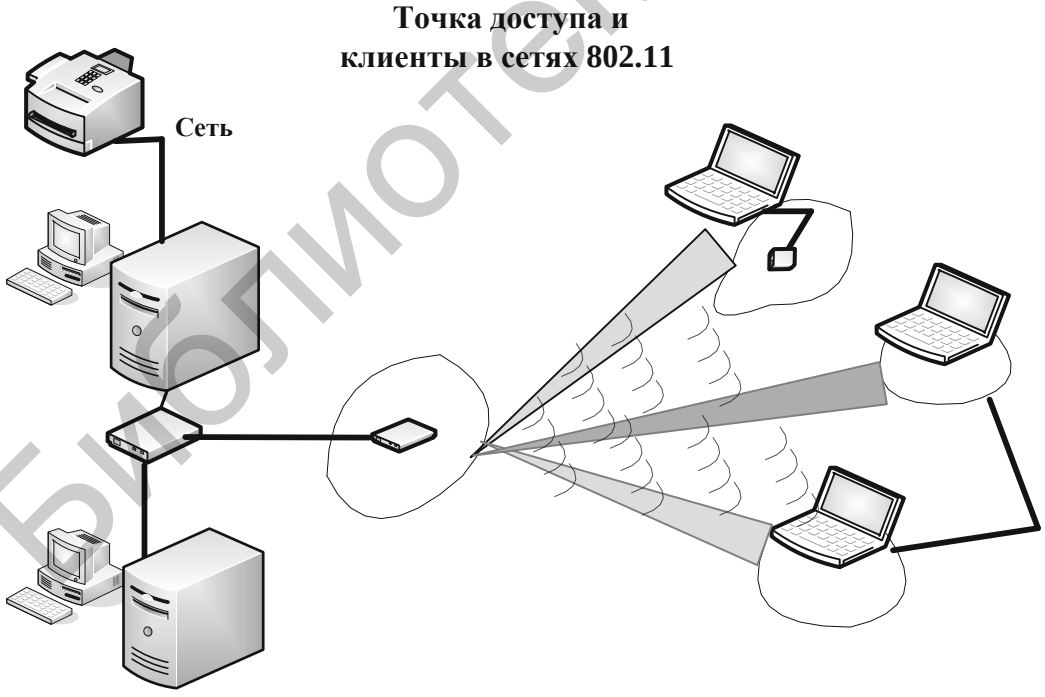


Рисунок 7.3 – Структурная схема беспроводной сети по топологии
«Распределенная инфраструктура»

Данное соединение – это соединение по топологии организации «клиентской точки». В этом режиме точка доступа работает как клиент и может соединяться с точной 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 топологии «Мост», которое условно можно представить в виде следующей схемы (рисунок 7.4).

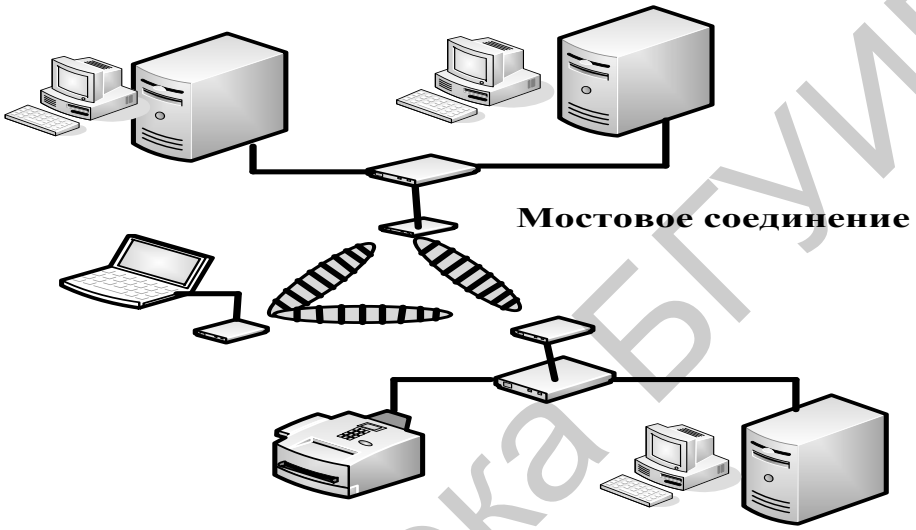


Рисунок 7.4 – Структурная схема беспроводной сети по топологии «Мост»

4 Использование 2Wire1701HG в качестве репитера (повторителя) по следующей схеме (рисунок 7.5).

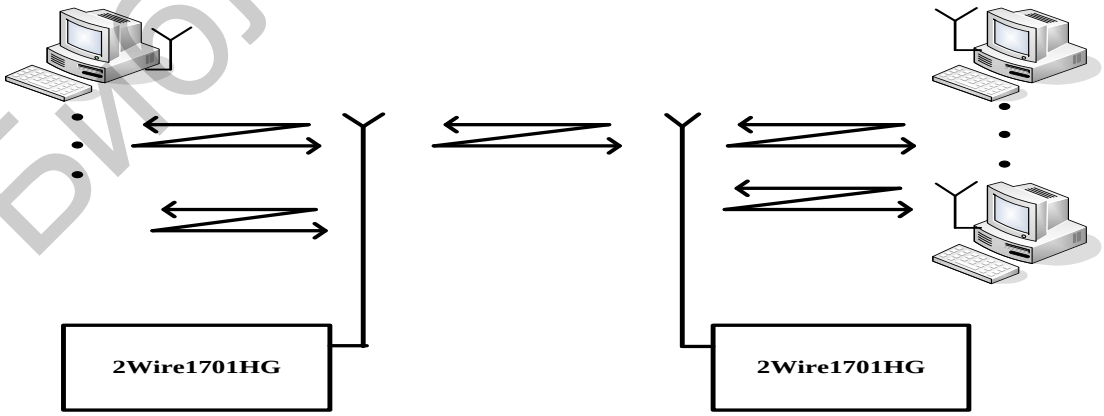


Рисунок 7.5 – Структурная схема беспроводной сети
по топологии «Повторитель»

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

7.4 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 1990-х гг. Аналогично проводному Ethernet 802.3 стандарт IEEE 802.11 определяет протокол использования единой среды передачи, получивший название Carrier Sense Access 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 определить, свободна ли среда и готов ли приемный узел к приему.

После получения пакета данных приемный узел должен передать сигнал подтверждения (ACK) факта безошибочного приема. Если ACK не получен, попытка передачи данных будет повторена.

В стандарте предусмотрено обеспечение безопасности данных, которое включает аутентификацию для проверки, авторизован ли входящий в сеть узел, 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 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, 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:

- IEEE 802.11a;
- IEEE 802.11x.

На практике наибольшее применение получили три стандарта, а именно: IEEE 802.11a, 802.11b, 802.11g. В таблице 7.1 приведены основные характеристики данных стандартов.

Таблица 7.1 – Основные характеристики стандартов беспроводной связи (IEEE 802.11a, 802.11b, 802.11g)

Основные технические параметры стандартов	*Стандарт IEE*		
	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, 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*) 2Wire1701HG функционирует на основе реализации протоколов двух нижних уровней семиуровневой модели взаимодействия открытых систем связи, 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 рисунке 7.6.

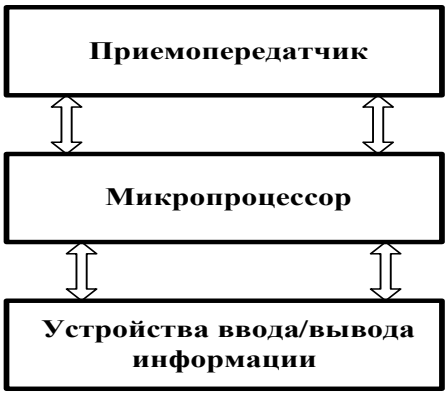


Рисунок 7.6 – Обобщенная структурная схема шлюза 2Wire1701HG

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 наоборот 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. Поддерживание 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 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 ча-

стот 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 2Wire1701HG один и тот же LLC, что значительно упрощает объединение проводных и беспроводных сетей. Подуровни MAC данных сетей имеют тонкие различия, которые 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, 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/CD. Работает он следующим образом. Станция, которая собирается передавать информацию, сначала «слушает эфир» и, если среда передачи данных свободна, осуществляет передачу через некоторое время. Наличие случайной задержки необходимо для того, чтобы сеть не «зависала», если несколько станций одновременно попытаются 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 выслать на точку доступ запрос на очистку эфира. Затем 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 не во всех моделях оборудования стандарта IEEE 802.11, включается лишь в крайних случаях. В Ethernet при передаче потоковых данных используется управление с точки доступа к каналу связи, распределенное между всеми станциями. В стандарте IEEE 802.11, напротив, 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 802.1lb будет ниже, чем у проводного Ethernet. Таким образом, если сетям Ethernet 10 Мбит/с 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», в то время как Ethernet 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.

7.5 Экспериментальная часть лабораторной работы

7.5.1 Порядок включения и проверки работоспособности шлюза 2Wire1701HG

Для включения и проверки работоспособности шлюза необходимо:

а) наличие у всех устройств, которые подключены к шлюзу, сетевого интерфейса, совместимого с моделью используемого шлюза 2Wire1701HG;

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

в) проверить подключение четырех ПК к шлюзу;

г) включить электропитание шлюза и ПК. Далее проверка функционирования шлюза выполняется в режимах POWER (электропитание), Local Network (локальная сеть) и Broad Link (широкополосная линия связи) по методике, приведенной в таблицах 7.2–7.4. соответственно.

Таблица 7.2 – Индикатор Power (электропитание шлюза)

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

Таблица 7.3 – Индикатор LocalNetwork (локальная сеть)

Цвет индикатора Local Network	*Состояние шлюза*
OFF (выключено) – индикатор не включен	Шлюз не подключен к розетке питания или главному компьютеру путем HomePNA, USB, Ethernet или Wireless
ON (включено) – зеленый цвет индикатора	Шлюз подключен через Ethernet, USB или Wireless

Таблица 7.4 – Индикатор BroadbankLink (широкополосная линия связи)

Цвет индикатора Broadbank Link	*Состояние шлюза*
OFF (выключено) – индикатор не включен	Нет сигнала. Шлюз не подключен
Мигающий оранжевый	Шлюз устанавливает соединение
Красный	Шлюз не обнаружил сигнал
Оранжевый	Шлюз обнаружил сигнал, но не смог подключиться к провайдеру сети (не установлено соединение)
Мигающий зеленый	Шлюз подключает доступные сервисы
Зеленый	Шлюз полностью подключил доступные сервисы

7.5.2 Порядок проверки работоспособности шлюза 2Wire1701HG 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 необходимо 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 в свойствах соединения: «Состояние» → «Поддержка».

5 Еще одним способом проверки правильности соединения является проверка свойств локальной сети в самом шлюзе. В браузере (например, Internet Explorer) наберите адрес шлюза 192.168.1.254. Во внутренних настройках шлюза выберите пункт Home Network, и на панели Local Devices отобразятся компьютеры, включенные в локальную сеть, а также способ соединения – проводной или беспроводной. Также можно не устанавливать IP-адреса вручную, а оставить функцию «Получить IP-адрес автоматически».

В этом случае по технологии DHCP шлюз сам раздаст IP-адреса по порядку, начиная с 192.168.1.64.

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. Следовательно, будет проверена работоспособность всей сети.

7.5.3 Порядок проверки работоспособности шлюза 2Wire1701HG 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 подпункты 2–5 (см. пункт 7.5.2) для беспроводных сетей.

2 Проверить работоспособность беспроводной сети:

а) вручную вытащить кабель из соответствующего порта шлюза 2Wire1701HG. В «Сетевых подключениях» проводное соединение станет недо-

ступно, 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.

7.5.4 Настройка и соединение шлюза 2Wire1701HG, подключенного к ПК, с сетью Интернет

Зайдите в настройки широкополосного соединения, набрав адрес шлюза 192.168.1.254. Выберите 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 = 0, VCI = 33). Эти параметры уникальны для каждого провайдера;

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

3) в разделе Broadband Connection установить тип соединения Connection Type. Для ADSL-соединения использовать тип соединения PPP, Username – имя пользователя, Password – пароль, Confirm password – подтверждение пароля. Эти параметры также выдаются провайдером. Остальные параметры являются необязательными, их можно не изменять.

После окончания настроек нажать кнопку Save (Сохранить настройки).

7.5.5 Настройка параметров безопасности шлюза 2Wire1701HG

Настройки параметров безопасности выполняются по следующей методике.

В устройство 2Wire1701HG 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 без-

опасности наберите в браузере адрес шлюза 192.168.1.254. Выберите 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 2Wire1701HG 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.

Через Inbaundarid Outbound Control – управление входящим и исходящим трафиком – можно запрещать/разрешать входящий (Inbound) или исходящий (Outbound) трафик для определенного типа протокола (например, FTP, HTTP, NetBIOS). Протоколы, отмеченные галочкой, будут разрешены.

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

1) выбрать Firewall → Firewall Settings;

2) выбрать пункт Allow Individual Applications → Add a new defined Application;

3) Application name – можно ввести любое имя приложения (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 (приложения). Эта функция очень полезна, если нужно ограничить время пользования сетью;

7) Map to Host Port – переназначение порта. Эта функция используется, когда нужно скрыть порты, по которым работает приложение во внешней сети. Применяется с той целью, чтобы злоумышленник не мог однозначно определить, какое именно приложение работает в сети, и не мог остановить 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 400–4010;

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, нажать Add Definition;

10) возвратиться к пункту Firewall Settings. В списке приложений найти приложение test, выделить его и нажать Add, после чего оно появится в списке Hosted Application. Следовательно, подобным образом можно настроить несколько приложений и использовать их одновременно;

11) удалить приложения можно кнопкой Remove.

7.6 Оформление отчета по выполненной лабораторной работе

Отчет должен содержать:

- титульный лист, форма которого установлена кафедрой;
- результаты выполнения домашнего задания;
- основные технические характеристики аппаратуры шлюза 2Wire1701HG;
- обобщенную структурную схему шлюза 2Wire1701HG;
- результаты выполнения лабораторной работы.

7.7. Контрольные вопросы

1 Основные качественные и количественные характеристики шлюза 2Wire1701HG.

2 Принцип построения и функционирования шлюза 2Wire1701HG.

3 Варианты построения сетей связи на основе шлюза 2Wire1701HG.

4 Основные методы защиты информации, используемые в шлюзе 2Wire1701HG, и их свойства.

5 Порядок выполнения следующих процедур:

- включение и проверка работоспособности шлюза;
- проверки работоспособности в режиме проводного соединения;
- проверка работоспособности в режиме беспроводного соединения;

- настройка и соединение шлюза и подключение к нему ПК с сетью Интернет;

- настройка 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 2Wire1701HG: техническое описание, 4.1.

3 Универсальный телекоммуникационный шлюз 2Wire1701HG: руководство пользователя, 4.2.

ЛАБОРАТОРНАЯ РАБОТА №8

Техническая диагностика многофункционального телекоммуникационного шлюза 2Wire1701HG

8.1 Цель работы

Научиться открывать консоль управления и диагностики телекоммуникационного шлюза, анализировать техническое состояние шлюза и оборудования офисной локальной сети.

8.2 Домашнее задание к лабораторной работе

1 По данному методическому руководству и рекомендованной литературе подготовиться к выполнению лабораторной работы.

2 Изучить состав и технические характеристики оборудования лабораторной работы.

3 Изучить методику выполнения технической диагностики и контроля телекоммуникационного шлюза 2Wire1701HG.

4 Изучить принцип построения офисной локальной сети на основе телекоммуникационного шлюза 2Wire1701HG.

5 Подготовить отчет по лабораторной работе с результатами практического выполнения задания.

8.3 Состав лабораторной установки

В состав лабораторной установки входят: телекоммуникационный шлюз 2Wire1701HG, четыре компьютера и проводное оборудование мультимедийной сети кафедры.

8.4 Методы технической диагностики оборудования беспроводных офисных сетей типа LAN

8.4.1 Общая характеристика телекоммуникационного шлюза 2Wire1701HG

Телекоммуникационный шлюз 2Wire1701HG позволяет создавать эффективные локальные как проводные, так и беспроводные сети связи. Встроенный

высокоэффективный маршрутизатор обеспечивает равномерное распределение данных между всеми ПК сети без снижения скорости ПД: шлюз 2Wire1701HG поддерживает несколько технологий, а именно: Ethernet, прямой USB и HyperG Wireless. У шлюза имеется четыре порта Ethernet для подключения к ПК с возможностью ПД со скоростью 10 или 100 Мбит/с. Порт USB 1.1 позволяет напрямую подключать ПК или другие сетевые устройства.

При организации беспроводной сети 2Wire1701HG поддерживает интегрированную точку радиодоступа между проводной и беспроводной сетями. Мощная беспроводная технология 2Wire1701HG практически устраняет радиопомехи при организации ПД. Шлюз имеет радиопередатчик с выходной мощностью 400 мВт. Кроме того, шлюз имеет специальную тройную антенну: антенна используется только для передачи пакетов, таким образом смягчая потери мощности, связанные с переключением антенны назад и вперед между передачей и приемом. Это приводит к большей чувствительности точки радиодоступа, поскольку размещение антенны может быть оптимизировано с помощью специализированного набора приемных антенн.

Для защиты данных от несанкционированного доступа используется профессиональная сетевая защита: стандартная NAT/PAT-безопасность и функция Stateful Packet Inspection (SPI), которая выполняет две функции, а именно:

- контроль пакетов *с учетом состояния*. Производится блокировка Denialg of Service attacks (DOS-атаки, направленные на отказ обслуживания, или, например, флуд SYN/FIN или Smurf), и обнаруживает и записывает в файл отчета обнаруженные сканирования портов TCP и UPD;

- контроль пакетов *без учета состояния*. В этом случае осуществляется фильтрация спецтрафика NetBios (проверяется наличие подозрительных пакетов и фрагментов IP-адреса).

Функция безопасности NAT переводит IP-адрес местной сети во внешний адрес, поддерживаемый шлюзом 2Wire1701HG, эффективно скрывая существование офисной (домашней) сети для сети Интернет. Шлюз использует этот внешний адрес, чтобы связаться с сетью Интернет от имени устройств локальной сети.

Функция безопасности PAT поддерживается некоторыми маршрутизаторами и позволяет хостам в локальной сети связываться с остальной частью сети, в том числе с абонентами сети Интернет, не раскрывая их собственный IP-адрес. Все внешние IP-адреса маршрутизаторов транслируются на IP-адреса исходящих пакетов. Ответы возвращаются маршрутизатору, который переводит их назад в частный IP-адрес оригинального, или выделенного, хоста для конеч-

ного принятия. Во время трансляции адреса порта каждый ПК в локальной сети переводится к тому же самому IP, но с присвоением разного номера порта.

Функция безопасности I&OPB осуществляет блокировку входящих и исходящих пакетов при взаимодействии с сетью Интернет.

Уровень безопасности беспроводной сети, используемый по умолчанию, в общем соответствует способу (технологии), обозначаемому как WEP (Wired Equivalent Privacy – проводная эквивалентная защита) и реализуемому на основе использования 40- или 64-битного кодирования данных. По умолчанию шлюз 2Wire1701HG работает с включенным WEP-шифрованием и сконфигурированным сетевым именем 2Wire910.

8.4.2 Основные технические характеристики шлюза 2Wire1701HG

Среди технических характеристик шлюза 2Wire1701HG можно выделить следующие:

- количество проводных портов: 4;
- количество беспроводных абонентов: 254;
- радиус зоны обслуживания беспроводных абонентов: 100 м;
- интерфейсы местной сети: Ethernet, HomePNA1, USB2;
- интерфейсы беспроводной сети: 802.11 b/g;
- совместимость стандартов: ADSLG.dmt (F.992.1 1JU) – внутренняя или внешняя пара; Home PNA 2.0; USB 1.1; TCP/IP; DHCP; и YPN передача с PPTP; L2TP; PPPoE и PPPoA; Ethernet 802.3 и Wi-Fi 802.11 b/g;
- серийный номер шлюза: sno1234567S910;
- номер шифровального ключа: 987654321;
- поддерживаемые операционные системы: Windows 98, 98 Second Edition, ME, XP, MAC 10.1 или выше;
- web-браузер: Netscape 7.1, Microsoft Internet Explorer 5.5 и выше;
- максимальная скорость передачи данных в беспроводном режиме: 54 Мбит/с;
- скорость передачи данных в проводном режиме с использованием сети Ethernet: от 10 до 100 Мбит/с;
- скорость передачи данных по каналам связи на основе технологии ADSL 2: 8 Мбит/с;
- методы расширения спектра частот радиосигнала: DSSS и FHSS;
- диапазон частот: 2,4–2,4835 ГГц;
- источник электропитания: сеть с напряжением 220 В и с автономным выпрямителем.

8.4.3 Основные сведения о канале управления и диагностики шлюза 2Wire1701HG

MDC (Management/Diagnostic Console) – консоль управления и диагностики шлюза 2Wire1701HG, отображающая информацию о состоянии шлюза, его подключениях по широкополосной линии (сети) к сетевым устройствам, входящим в состав лабораторной установки, общую информацию о системе (сетевых системных особенностях шлюза) и безопасности шлюза и сети, а также файл отчета об ошибках сети.

MDC позволяет использовать следующие опции:

- просмотр информации о конфигурации и доступных сервисах;
- просмотр файлов отчета о совершенных действиях;
- тестирование и диагностика;
- настройка шлюза.

Следует отметить, что доступные страницы настроек MDC зависят от версии программного обеспечения. Для данного шлюза используется ПО версии 4.21.x. Панель навигации MDC формирует следующие разделы и соответствующие им пункты контроля технического состояния шлюза (таблица 8.1).

Таблица 8.1 – Панель навигации MDC

Разделы	*Пункты контроля*
System Summary (Общая информация о системе)	**System** (Система), **Configuration** (Конфигурация), **Components** (Компоненты)
Broad Link (Широкополосная линия связи)	**Statistics** (Статистика), **Detailed DSL Statistics** (Подробная статистика DSL), **Configure** (Конфигурация), **Configure Multiple Link** (Конфигурация нескольких линий)
Local Network (Локальная сеть)	**Status** (Статус сети), **Statistics** (Статистика), **Device List** (Список устройств), **Wireless Settings** (Установки для настройки беспроводной сети), **Configure** (Конфигурация), **Address Allocation** (Адрес назначения)
FireWall (Сетевой экран или сетевая защита)	**Settings** (Установки для настройки сетевого экрана), **Detailed Information** (Подробная информация), **Advanced Settings** (Дополнительные настройки)
Troubleshooting (Устранение неполадок)	**DSL Diagnostics** (Диагностика DSL), **Event Log** (Журнал событий/Файл отчета), **Network Test** (Тестирование сети), **Upgrade History** (История обновления), **Reset** (Сброс системы)
Advanced (Расширенные настройки)	**Syslog Settings** (Параметры настройки журнала системных событий), **Provision Information** (Предоставление информации), **Configure Time Service** (Конфигурация службы времени на сервере), **Configure Services** (Конфигурация служб на сервере), **Static Routes** (Статические маршруты), **DNS Resolve** (Разрешения DNS)

8.5 Порядок выполнения лабораторной работы

По рисунку 8.1 проверьте подключение к портам Local Ethernet шлюзов ПК №1–4 (порты Ethernet ПК) и шлюза к мультимедийной сети кафедры, а также всех устройств лабораторной установки к электросети.

Включите электропитание всех ПК и шлюза. По индикаторам шлюза проконтролируйте начальную загрузку шлюза. Шлюз 2Wire1701HG имеет три индикатора состояния, которые позволяют диагностировать техническое состояние шлюза и контролировать работу сети в целом (таблица 8.2).

Таблица 8.2 – Индикатор шлюза Power (Электропитание)

Цвет индикатора POWER (электропитание)	*Состояние шлюза*
Индикатор не включен	Не подключено питание
Мигающий зеленый	Шлюз загружается
Зеленый	Шлюз включен
Красный	Системная ошибка
Мигающий зеленый	Шлюз обновляет программное обеспечение

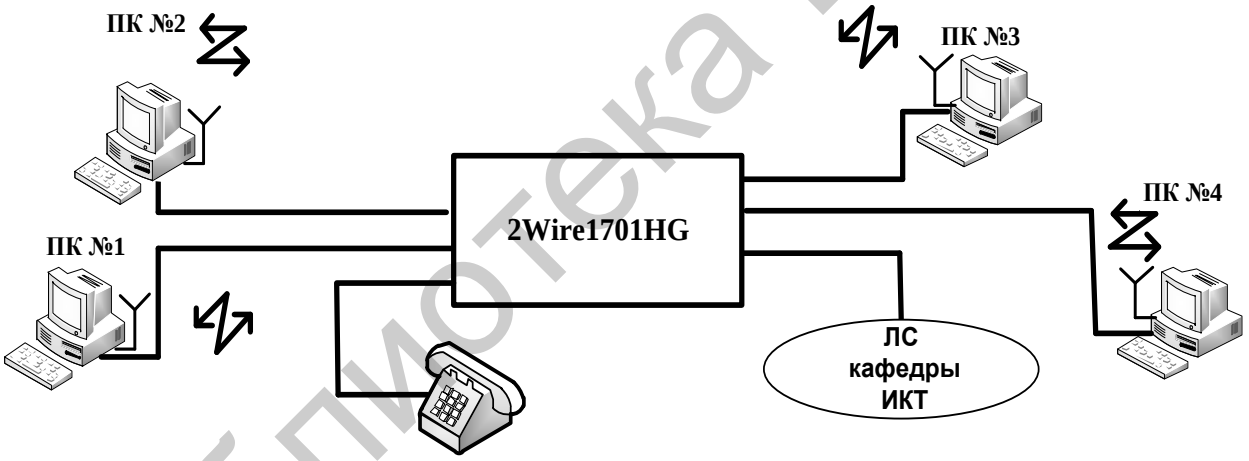


Рисунок 8.1 – Структурная схема офисной сети лабораторной работы на основе телекоммуникационного шлюза 2Wire1701HG

Индикатор Broadbank Link (Широкополосная линия связи) отображает шесть состояний шлюза, которые приведены в таблице 8.3.

Таблица 8.3 – Индикатор Broadbank Link (Широкополосная линия связи)

Цвет индикатора Broadbank Link	*Состояние шлюза*
1	2
Индикатор не включен	Нет широкополосного сигнала. Шлюз не подключен или нет подключения к нужному сервису. Шлюз не может определить сигнал DSL

1	2
Мигающий оранжевый	Шлюз устанавливает соединение
Красный	Шлюз не обнаружил сигнал
Зеленый	Шлюз обнаружил сигнал, но не смог подключиться к поставщику услуг сети Интернет либо не было настроено соединение
Мигающий зеленый	Шлюз подключает доступные сервисы
Оранжевый или зеленый	Шлюз полностью подключил доступные сервисы

Индикатор Local Network (Локальная сеть) отображает два состояния шлюза, которые приведены в таблице 8.4.

Таблица 8.4 – Индикатор Local Network (Локальная сеть)

Цвет индикатора Local Network	*Состояние шлюза*
Индикатор не включен	Шлюз не подключен к розетке питания, компьютеру путем Home PNA, USB, Ethernet или Wireless
Зеленый	Шлюз подключен через Ethernet, USB или Wireless

Откройте доступ к MDC шлюза 2Wire1701HG с ПК №1, включенного в проводном режиме, для чего необходимо:

а) зайти в меню Internet Explorer ПК;

б) в строке со знаками -><- ввести адрес http://gateway.2Wize.net/-management и щелкнуть кнопкой мыши;

в) в новом меню со строкой http://gateway.2Wize.net/management подвести курсор под данную строку и щелкнуть кнопкой мыши;

г) в появившемся меню System Password ввести пароль admin и команду Save.

После открытия панель навигации MDC должна выдать таблицу 8.1, которая позволяет выбрать нужную страницу на сайте или ссылки для выполнения технической диагностики шлюза и сети связи в целом.

Примечания

1 В отчет лабораторной работы записывается информация по опциям всех шести разделов и пунктов контроля таблицы 8.1.

2 В лабораторной установке отсутствует подключение к провайдеру сети Интернет по DSL Diagnostics.

Выполните техническую диагностику шлюза и офисной сети в режиме «Инфраструктура» (см. таблицу 8.1) в следующей последовательности.

8.5.1 Раздел System Summary (Общая информация о системе)

Запишите в отчет лабораторной работы информацию по следующим пунктам контроля:

- System (Система);
- Configuration (Конфигурация);
- Components (Компоненты).

Информация здесь и далее записывается по опциям соответствующих пунктов и соответствующих разделов.

8.5.2 Раздел Broadband Link (Широкополосная линия)

Запишите в отчет лабораторной работы информацию с каждой страницы по следующим пунктам контроля:

- Summary (Общий обзор);
- Statistics (Статистика);
- Detailed DSL Statistics (Подробная статистика линии DSL);
- Configure (Конфигурация, или настройка линии DSL);
- Configure Multiplex Links (Конфигурация нескольких линий DSL).

8.5.3 Раздел Local Network (Локальная сеть)

Запишите в отчет лабораторной работы информацию по следующим пунктам контроля:

- Status (Статус сети);
- Statistics (Статистика);
- Device List (Список устройств);
- Wireless Settings (Установки настройки беспроводной сети);
- Configure (Конфигурация сети);
- Adress Allocation (Адрес назначения).

8.5.4 Раздел Firewall (Сетевой экран или сетевая защита)

Запишите в отчет лабораторной работы информацию по следующим пунктам:

- Settings (Установки для настройки сетевого экрана);
- Ditailed İnformation (Подробная информация);
- Advanced Settings (Дополнительные настройки).

8.5.5 Раздел Troubleshooting (Устранение неполадок)

Запишите в отчет лабораторной работы информацию по следующим пунктам:

- DSL Diagnostics (Диагностика DSL);
- Event Log (Журнал событий/Файл отчета);
- Network Tests (Тестирование сети);
- Upgrade History (История обновления);
- Reset (Сброс системы).

8.5.6 Раздел Advanced (Дополнительные настройки)

Запишите в отчет лабораторной работы информацию по следующим пунктам контроля:

- Syslog Settings (Система параметров настройки);
- Provisioning Information (Предоставление информации);
- Configure Time Service (Настройка службы времени на сервере);
- Configure Services (Настройка служб на сервере);
- Static Routes (Статические маршруты);
- DNS Resolve (Разрешения DNS);
- Traffic Shaping (Формирование трафика);
- Link Manager (Менеджер ссылок);
- Detailed Log (Подробный отчет).

8.6 Оформление отчета по выполненной лабораторной работе

Отчет должен содержать:

- титульный лист, форма которого установлена кафедрой;
- результаты выполнения домашнего задания;
- структурную схему офисной сети (лабораторной установки);
- результаты выполнения лабораторной работы по пунктам 8.5.1–8.5.6.

8.7 Контрольные вопросы

1 Количественные характеристики шлюза 2Wire1701HG.

2 Варианты построения сетей связи на основе шлюза 2Wire1701HG.

3 Порядок функционирования шлюза в следующих режимах диагностики:

- Summary (Общий вид);

- Broadbank Link (Широкополосная линия связи) в подрежимах: общий обзор, статистика, статистика DSL;

- Local network (Локальная сеть) в подрежимах: статус, статистика, список устройств;

- Wireless LAN (Беспроводная локальная сеть);

- Troubleshooting (Устранение неполадок): анализ общей информации, просмотр истории подключений, файл отчета о событиях, тестирование сети и статические маршруты.

Литература

1 2Wire1701HG – Техническое описание шлюза / Automation, CA, 2007.

2 2Wire1701HG Руководство пользователя / 1704. Automation Parkway, San Jose, CA, 2007.

3 Столлингс, В. Беспроводные линии связи и сети / В. Столлингс. – М. : Издательский дом «Вильямс», 2003.

4 Григорьев, В. А. Сети и системы радиодоступа / В. А. Григорьев, О. Н. Лагутенко, Ю. А. Распаев. – М. : Эко-Трендз, 2005.

Св. план 2017, поз. 42

Учебное издание

Королёв Алексей Иванович
Конопелько Валерий Константинович
Цветков Виктор Юрьевич

ПЕРЕДАЧА И ЗАЩИТА ДАННЫХ В СЕТЯХ ИНФОКОММУНИКАЦИЙ. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Редактор *А. К. Петрашкевич*
Корректор *Е. Н. Батурчик*
Компьютерная правка, оригинал-макет *В. М. Задоля*

Подписано в печать **.**.2017. Формат 60×84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 6,5. Уч.-изд. л. . Тираж 30 экз. Заказ 124.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
ЛП №02330/264 от 14.04.2014.
220013, Минск, П. Бровки, 6