Министерство науки и высшего образования
Российской Федерации
Федеральное государственное автономное образовательное
учреждение высшего образования
«Севастопольский государственный университет»

ИССЛЕДОВАНИЕ СПОСОБОВ ОРГАНИЗАЦИИ И КОНФИГУРАЦИИ БЕСПРОВОДНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению лабораторной работы по дисциплине
«Инфокоммуникационные системы и сети»
для студентов дневного и заочного отделения по направлению
09.03.02 «Информационные системы и технологи»,
09.03.03 «Прикладная информатика»

Севастополь
2019

УДК 681.326

Исследование способов организации и конфигурации беспроводных компьютерных сетей. Методические указания / Сост. В.С.Чернега. - Севастополь: Изд-во СевГУ, 2019.- 24 с.

Цель указаний: Помочь студентам в изучении принципов построения, способов передачи и модуляции сигналов, методов доступа и защиты в беспроводных компьютерных сетях, а также способов их конфигурации.

Методические указания предназначены для выполнения лабораторной работы по дисциплине "Компьютерные сети" для студентов дневной и заочной формы обучения

Методические указания рассмотрены и утверждены на методическом семинаре и заседании кафедры информационных систем
(протокол № 2 от 24 февраля 2019 г)

Допущено учебно-методическим центром СевГУ в качестве методических указаний.

Рецензент:
Кротов К.В.., канд. техн. наук, доцент кафедры ИС;

СОДЕРЖАНИЕ

1. ЦЕЛЬ РАБОТЫ

Исследование способов задания режимов работы и параметров конфигурации точек доступа и сетевых интерфейсных карт беспроводных компьютерных сетей, а также влияния этих параметров на работу сети. Приобретение практических навыков разворачивания и настройки беспроводных сетей.

2. ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ ПОЛОЖЕНИЯ

2.1. Способы построения беспроводных сетей

В зависимости от количества компьютеров в сети и расстояния между ними, беспроводные сети WLAN (*Wireless Local Area Network*) могут быть созданы двумя различными способами:

1) сеть без базовой станции (*Ad Hoc*);
2) сеть с точкой доступа (*Infrastructure Network*).

В сети, использующей способ **Ad HOC,** базовая станция отсутствует. Этот способ получил также обозначение IBSS (*Independent Basic Service Set*), передача данных в котором осуществляется в режиме «точка-точка». Компьютеры в такой сети непосредственно взаимодействуют друг с другом, пока они находятся в пределах устойчивой радиосвязи. В режиме Ad HOC требуется минимум оборудования: каждый компьютер должен быть оснащен только беспроводным адаптером. При такой конфигурации нет необходимости создания сетевой инфраструктуры. Основными недостатками режима Ad Hoc являются ограниченный диапазон действия компьютерной сети и невозможность подключения к внешней сети (например, к Интернету). На практике режим рекомендуется использовать при наличии в сети 3…4-х компьютеров и расстояния между ними не более 30 м.

При втором способе построения – ***Infrastructure Network***, компьютеры взаимодействуют друг с другом не напрямую, а через базовую станцию – **точку доступа AP** (*Access Point*), которая выполняет в беспроводной сети роль своеобразного концентратора (аналогично тому, как это происходит в традиционных кабельных сетях). Через точку доступа возможен выход во внешние проводные сети. В компьютерной сети может быть несколько AP, объединенных проводной сетью Ethernet. Фактически такая сеть представляет собой набор базовых станций с перекрывающимися зонами охвата. Стандартом IEEE 802.11 предусматривается возможность перемещения рабочих станций из зоны одной AP в зону другой (роуминг).

Существует два режима взаимодействия с точками доступа: **BSS** *(Basic Service Set*) и **ESS** (*Extended Service Set*). В режиме BSS все станции связываются между собой только через точку доступа, которая может выполнять также роль моста к внешней сети (рисунок 1). Как видно из рисунка, расстояние между компьютерными станциями увеличивается, как минимум, вдвое. Одна точка доступа обеспечивает обслуживание от 15 до 250 абонентов, в зависимости от конфигурации сети и технологии доступа. Увеличить емкость сети можно просто, добавив

новые точки доступа, при этом не только расширяется зона обслуживания, но и снижается вероятность перегрузки.

В **расширенном режиме** ESS существует инфраструктура нескольких базовых сетей BSS, причем сами точки доступа взаимодействуют друг с другом через некоторую систему, называемую **системой распространения** (DS, *Distribution System*), позволяющую передавать трафик от одной BSS к другой (рисунок 2). Связь базовых сетей с DS осуществляется посредством точек доступа. Между собой точки доступа соединяются с помощью сегментов кабельной сети, либо радиомостов, т.е. система распространения представляет собой либо совокупность устройств AP либо сегмент локальной сети.

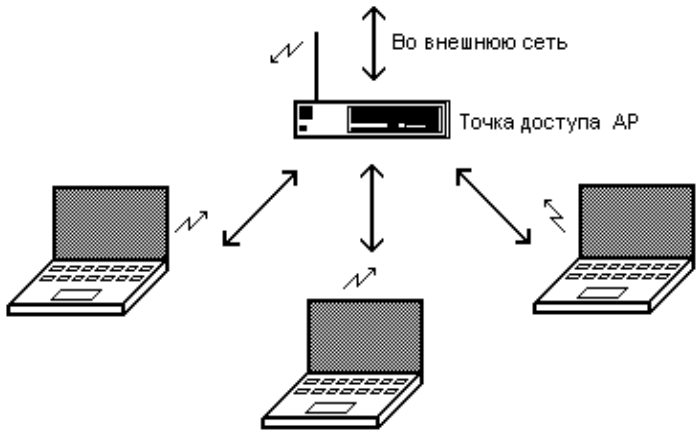

Рисунок 1 – Беспроводная сеть с точкой доступа

Кроме двух различных режимов функционирования беспроводных сетей на MAC-уровне определяются правила коллективного доступа к среде.

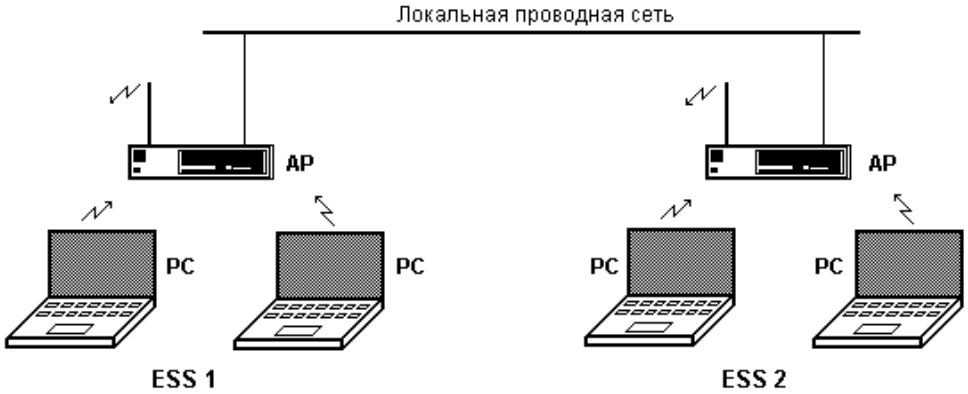

Рисунок 2 – Объединение беспроводных сетей

Существуют жесткие правила, регламентирующие коллективный доступ к среде передачи сигналов. Это вызвано тем, что при одновременной передаче сигналов в эфир двух и более станций одновременно выделить отдельные пакеты весьма затруднительно, а в ряде случаев и невозможно.

В беспроводных сетях при организации доступа используется два способа обслуживания: **асинхронный** (*Asynchronous Data Service*) и **обслуживание с ограниченным временем** (*Time Bounded Service*).

При асинхронном обслуживании каждая из станций может получить доступ к разделяемой среде, но при этом возможны коллизии, которые станции пытаются предотвратить. Этот способ не гарантирует номинальную пропускную способность сети. Служба используется как в сетях без базовой станции, так и в сетях с точкой доступа. Способ ограниченного времени обслуживания гарантирует максимально допустимое время доступа станции к среде. Он применяется только в сетях с промежуточной станцией (точкой доступа). В процессе реализации способа формируются так называемые суперкадры с двумя временными интервалами:

1) *бесконкурентного доступа*, в течение которого точка доступа поочередно опрашивает станции и при их готовности осуществляет обмен кадрами, при этом гарантируется номинальная производительность сети;

2) состязательного доступа.

Основными компонентами беспроводных компьютерных сетей являются базовая станция и компьютеры, снабженные беспроводными сетевыми картами.

2.2. Точка доступа и беспроводная сетевая карта

Основным узлом любой беспроводной сети является базовая станция – **точка доступа**, через которую рабочие станции по радио связываются друг с другом и с корпоративной сетью. Она определяет не только радиус действия и скорость передачи данных, но и решает элементарные задачи управления и обеспечения безопасности.

Высококачественные точки доступа оснащаются приемо-передатчиками с двумя антеннами, причем в каждый момент времени работает антенна с лучшим качеством приема. Переключение антенн уже на удалении в несколько метров дает повышение качества и, соответственно, скорости передачи по сравнению с одноантенными точками доступа. Обычно используемые ненаправленные антенны жестко крепятся к корпусу.

Многие точки доступа выполняют также функции маршрутизатора, имеют встроенный Ethernet-коммутатор и аппаратный брандмауэр. Большинство точек доступа-маршрутизаторов для малых офисов обычно имеет 4 LAN-порта и один WAN-порт. LAN-порты – обычно типа Ethernet, WAN-порт может быть портом Ethernet или ADSL.

Управление отдельными точками доступа, как правило, осуществляется через последовательный или USB интерфейс. Это позволяет непосредственно подключать их к консоли управления (рабочей станции). В большинстве точек доступа реализована поддержка протоколов HTTP и telnet, чем обеспечивается удобное администрирование через Internet и интерфейс браузера. Защита удаленного управления осуществляется при помощи протоколов SSL и SSH. Нередко точки доступа поставляются вместе со вспомогательными программными инструментами для измерения мощности излучения или скорости передачи данных. Для авто-

матической раздачи всем клиентам сети IP-адресов в точке доступа функционирует сервер **DHCP**. Если точка доступа соединена с компьютерной сетью, то необходимо правильное взаимодействие DHCP-сервера сети с имеющимся в точке сервером DHCP. Для сервера сети точка доступа должна быть клиентом и получать свой IP-адрес от этого сервера, а ее собственные клиенты - обращаться к ней посредством функции ретрансляции сервера имен доменов **DNS** (*Domain Name Server*).

2.3. Форматы кадров и способы доступа в беспроводных сетях

Кадры в беспроводных сетях формируется на MAC-уровне, а на физическом уровне к ним прибавляется только заголовок физического уровня. Кадры MAC-уровня могут быть трех типов: данных, управляющие (ACK, RTS, CTS и др.) и сигнальные (*Beacon*). На MAC-уровень от верхнего уровня поступают пакеты приложений. Если размер пакетов превышает предельно допустимую длину кадра, то осуществляется его фрагментация. Формат кадра и структура заголовка показаны на рисунке 3.

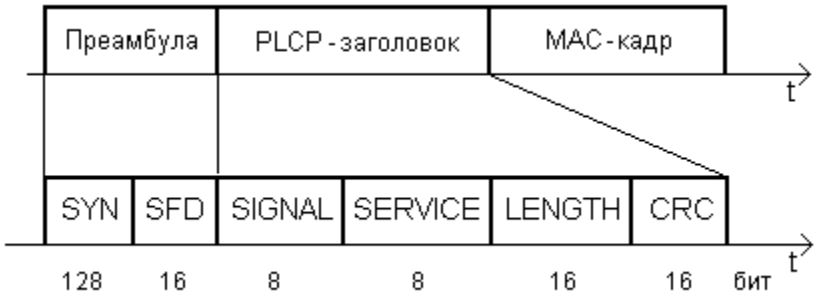

Рисунок 3 – Формат кадра физического уровня

Перед передачей кадра в канал к нему добавляется заголовок физического уровня, состоящий из преамбулы длиною 144 бита и собственно заголовка **PLCP** (*Physical Layer Convergence Protocol*) размером 48 бит. Преамбула служит для обеспечения тактовой и цикловой синхронизации. Она состоит из синхронизирующей битовой последовательности SYN вида 1010…, которая завершается маркерной кодовой комбинацией **SFD** (*Start Frame Delimiter*) F3A0h, сигнализирующей о начале кадра. PLCP-заголовок содержит поле SIGNAL с информацией о скорости передачи и способе модуляции, поле SERVICE, включающее дополнительную информацию о наличии вариантов расширений и поле LENGTH, в котором указано время в микросекундах, необходимое для передачи следующей за заголовком части кадра. Все поля заголовка кодируются циклическим кодом с образующим полиномом 16-й степени. Результат кодирования помещается в поле контрольной последовательности CRC. Все поля заголовка передаются со скоростью 1 Мбит/с. Остальная часть кадра может передаваться с другой допустимой данным стандартом скоростью, которая указывается в полях SIGNAL и SERVICE.

Кроме рассмотренного формата кадра IEEE 802.11b дополнительно предусмотрен укороченный заголовок (рисунок 4). Поле синхронизации в нем сокращено до 56 бит, символ SFD передается в обратном порядке.

Рисунок 4 – Укороченный формат заголовка кадров сети IEEE 802.11b

При таком формате преамбула передается со скоростью 1 Мбит/с, а поля PLCP-заголовка - со скоростью 2 Мбит/с. Остальная часть кадра может передаваться с любой допустимой скоростью, установленной для стандарта IEEE 802.11b.

Для обеспечения передачи данных в конкретный интервал времени только одной рабочей станции в компьютерных беспроводных сетях принят механизм множественного доступа с контролем несущей и предотвращением коллизий **CSMA/CA** (*Carrier Sense Multiple Acsses with Collision Avoidance*). Перед началом передачи станция слушает эфир и дожидается, когда канал освободится. Канал считается свободным при условии, что не обнаружено активности в течение определенного промежутка времени – межкадрового интервала (IFS) определенного типа. Если в течение этого промежутка канал оставался свободным, станция ожидает еще в течение случайного промежутка времени и, если канал еще не занят, передает свой кадр. Если кадр предназначен конкретному устройству (не широковещательная или многоадресная передача), то приемник, успешно приняв этот блок, посылает передатчику короткий кадр подтверждения получения АСК (*ACKnowledge*). Если передатчик не принял АСК, он считает посланный кадр утерянным и повторяет процедуру его передачи сначала.

Примечательно, что если станция повторно передает кадр, для определения незанятости канала она должна использовать увеличенный межкадрный интервал (EIFS). Кроме того, время ожидания выбирается случайным образом на некотором интервале. При первой попытке передачи этот интервал минимален. При каждой последующей он удваивается до тех пор, пока не достигнет заданного предельного значения. Эти меры приводят к тому, что станция, успешно передавшая кадр, имеет преимущества в захвате канала (кто ошибается, тот дольше ждет).

Перед первой попыткой получить доступ к каналу станция загружает длительность случайного интервала ожидания в специальный счетчик. Его значение декрементируется с заданной частотой, пока канал свободен. Как только счетчик обнулится, станция может занимать канал. Если до обнуления счетчика канал занимает другая станция, счет останавливается, сохраняя достигнутое значение сче-

та. При следующей попытке отсчет начинается с сохраненной величины. В результате не успевшая в прошлый раз станция получает больше шансов занять канал в следующий интервал. В проводных сетях Ethernet подобного механизма нет.

Однако описанные процедуры доступа не избавляют от проблемы "скрытой точки". Для ее преодоления используются два дополнительных кадра – **RTS** (*Request to Send* – запрос на передачу) и **CTS** (*Clear to Send* – подтверждение готовности). Станция, желающая отправить блок данных, передает адресату короткий кадр RTS, в котом указывается время, требуемое для передачи, включая время ожидания квитанции. Если приемное устройство готово к приему, оно выставляет передающему ответный кадр – CTS, в котором содержится скорректированное время. Это время передается в поле **NAV** (*Network Allocation Vector*). Станции устремятся установить минимально возможным данный интервал времени. Затем в соответствии с описанной выше процедурой передающее устройство отправляет кадр с данными и дожидается подтверждения ACK.

Стандартом IEEE 802.11 предусмотрено два механизма контроля за активностью в канале (обнаружения несущей) – физический и виртуальный. Первый механизм реализован на физическом уровне и сводится к определению уровня сигнала в антенне и сравнению его с пороговой величиной. Виртуальный механизм обнаружения несущей основан на том, что в передаваемых кадрах данных, а также в управляющих кадрах ACK и RTS/CTS содержится информация о времени, необходимом для передачи кадра (или группы кадров) и получения подтверждения. Все станции сети получают информацию о текущей передаче и могут определить, сколько времени канал будет занят, – т.е. устройство при установлении связи всем сообщает, на какое время оно резервирует канал.

Все описанные механизмы относятся к сети с распределенным управлением DCF. Однако в сети могут присутствовать и AP, наделенные полномочиями узурпировать управление, – тогда их называют точками координации (PC). Когда сеть переходит в режим PCF, в трафике появляются интервалы, в которых конкурентный доступ отменен, и весь обмен происходит под управлением PC. По завершении такого интервала сеть возвращается в режим DCF. Интервалы под управлением PC следуют через строго определенный период, в начале каждого интервала PC выставляет особый сигнальный кадр (*Beacon*). PC не может передать очередной сигнальный кадр до тех пор, пока канал не освободится, т.е. очередной "свободный от конкуренции" интервал может начаться с задержкой.

Фактически режим PCF – это режим синхронной передачи, под который в асинхронной сети резервируются определенные интервалы. Этот режим позволяет использовать технологию IEEE 802.11 для таких приложений, как передача аудио/видео и других синхронных по своей природе данных.

2.4. Обеспечение безопасности передачи данных

Важнейшим требованием, предъявляемым к беспроводной связи, является обеспечение безопасности передачи данных. По этой причине разработчики на MAC-уровне предусмотрели механизм защиты данных, включающий аутентификацию станций и собственно шифрование передаваемых данных. Этот механизм должен обеспечивать такой же уровень защиты, как и в обычных сетях Ethernet, поэтому его назвали **WEP** (*Wired Equivalent Privacy* – эквивалент проводной конфиденциальности).

Алгоритм WEP основан на использовании четырех общих для одной сети секретных ключей длиной по 40 бит. Само шифрование происходит по алгоритму RC4 компании RSA Security. Алгоритм использует перемножение блоков исходных данных на псевдослучайную последовательность такой же длины, что и блок шифруемых данных. Генератор псевдослучайной последовательности инициализируется 64-разрядным числом, состоящим из 24-разрядного вектора инициализации *IV* (*Initialization Vector*) и 40-разрядного секретного ключа. Существенно, что если секретный ключ известен устройствам сети и неизменен, то вектор *IV* может изменяться от пакета к пакету. Для защиты от несанкционированного изменения передаваемой информации каждый шифрованный пакет защищается 32-разрядной контрольной суммой *ICV* (*Integrity Check Value*). Таким образом, при шифровании к передаваемым данным добавляется 8 байт – 4 для ICV, 3 для IV и еще 1 байт содержит информацию о номере используемого секретного ключа (одного из четырех). В принципе, секретный ключ может быть гораздо длиннее – 64, 128 и т.д. бит. Ключ представляет собой набор ASCII-символов длиной 5 (для 40-битного) или 13 (для 104-битного ключа) символов.

Алгоритм WEP показал на практике невысокую криптостойкость. На смену ему пришел сначала улучшенный алгоритм шифрования **WPA** (Wi-Fi *Protected Access*) а затем **WPA2**. WPA включает в себя протоколы 802.1x, EAP, TKIP и MIC.

Протокол 802.1x обеспечивает аутентификацию удаленных клиентов и выдачу им временных ключей для шифрования данных. Ключи (в зашифрованном виде) высылаются клиенту на незначительный промежуток времени, после которого генерируется и высылается новый ключ.

В протоколе **TKIP** (*Temporal Key Integrity Protocol*) реализованы динамические ключи шифрования, кроме того, каждая станция в сети также получает свой Master-ключ (который тоже время от времени меняется). Ключи шифрования имеют длину 128 бит и генерируются по сложному алгоритму, а общее количество возможных вариантов ключей достигает сотни миллиардов, а меняются они очень часто. Тем не менее, используемый алгоритм шифрования – по-прежнему RC4.

По протоколу **MIC** (*Message Integrity Check*) выполняется проверка целостности пакетов. Протокол позволяет отбрасывать пакеты, которые были «вставлены» в канал третьим лицом, т.е. ушли не от действительного отправителя.

В беспроводных сетях также широко применяется стандарт шифрования **AES** (*Advanced Encryption Standard*), основанный на симметричном алгоритме блочного шифрования. Пришёл на смену устаревшему стандарту 3DES. Размер блока при шифровании AES составляет 128 бит, длина ключа может составлять 128, 192 или 256 бит.

Для обеспечения аутентификации (проверки подлинности) удаленных клиентов беспроводных сетей разработан стандарт 802.1x, базирующийся на группе протоколов, в частности:

- **EAP** (*Extensible Authentication Protocol*) – протокол расширенной аутентификации пользователей или удаленных устройств;
- **TLS** (*Transport Layer Security*) – протокол защиты транспортного уровня, он обеспечивает целостность передачи данных между сервером и клиентом, а так же их взаимную аутентификацию;
- **RADIUS** (*Remote Authentication Dial-In User Server*) – сервер аутентификации удаленных клиентов. Он и обеспечивает аутентификацию пользователей.

2.5. Настройка параметров беспроводных сетей

2.5.1. Конфигурация сетевого адаптера

Просматривать и настраивать параметры сетевой карты можно средствами Windows (Wireless Network Connection), либо использовать специальную утилиту, поставляемую совместно с сетевой картой.

В процессе задания и настройки параметров сетевого адаптера устанавливаются или проверяются следующие параметры.

1. Идентификатор (имя) беспроводной сети **SSID** (*Service Set IDentifier*). По умолчанию (заводская установка) SSID – **default**. Имя может состоять из любой комбинации латинских букв и цифр. Рекомендуется использовать короткие имена без пробелов (5-8 символов). Следует иметь в виду, что SSID-имя беспроводной сети должно совпадать у всех адаптеров данной сети. Имя сети обычно передаётся в эфир для реализации возможности обнаружения точки доступа беспроводными клиентами, находящимися в зоне её обслуживания. Настройки большинства точек доступа позволяют отключить широковещание SSID, что позволяет скрыть беспроводную сеть от посторонних, однако, возможность подключения клиентов, знающих SSID, сохранится.
2. Частота несущей **(Frequency)**, используемой адаптером. Она определяется соответствующим стандартом, по которому реализован данная сетевая карта (802.11a – 5 ГГц, 802.11b и g – 2,4 ГГц).
3. Используемый канал передачи (**Channal**). Частотный диапазон в полосе 2,4 ГГц делится на несколько полос – каналов (всего их 13). Пользователь может выбрать канал с номером от 1 до 13. Заводской настройкой (по умолчанию) обычно устанавливается канал с номером 6. Следует помнить, что номер канала, в котором будут работать адаптеры, должен совпадать у всех адаптеров данной сети.
4. Скорость передачи данных (**Tx Rate**) в Мбит/с. Она может быть установлена в диапазоне 11…54 Мбит/с. По умолчанию данный параметр задается **Auto**. Это означает, что скорость будет устанавливаться автоматически, в зависимости от качества связи (уровня принимаемого сигнала). Однако бывают ситуации, ко-

гда в режиме Auto (особенно при неустойчивой связи) адаптер постоянно «скачет» по скоростям. В этом случае лучше принудительно задать ему скорость работы.

5. Режим (тип) работы сети (**Wireless Mode**). Пользователь может задать работу сети в режиме **Infrastructure** – с базовой станцией (точкой доступа), либо **Ad Hoc** – в сети находятся только рабочие станции.
6. Способ шифрования передаваемых данных (**Encryption**). В процессе настройки шифрование может быть отключено (**Disabled**) либо разрешено (**Enabled**). Во время первичной настройки беспроводной сети шифрование лучше отключить. После проверки функционирования сети целесообразно включить режим шифрования. При этом обычно можно выбирать протокол защиты из ряда протоколов WEP, WPA, WPA-PSK, WPA2 или WPA2-PSK. Последний из них является наиболее надежным.
7. Режим аутентификации (**Authentication**). При этом аутентификация может быть отключена (**Open Authentication**) или включена.
8. Уровень и формат ключа шифрования (**Key Length**). Обычно изготовителем предусмотрено использование нескольких видов ключа. В этом случае пользователю следует выбрать индекс ключа и ввести с клавиатуры указанное количество ASCII-символов или 16-ричных цифр в соответствующее поле диалогового окна (ключ должен совпадать на всех беспроводных устройствах). В связи с тем, что алгоритм перевода ключа из символьного вида в шестнадцатеричной может отличаться у Microsoft и других производителей собственных интерфейсов, рекомендуется вводить ключ в шестнадцатеричном коде.
9. Стек сетевых протоколов. Обычно задается стек TCP/IP-протоколов.
10. IP-адрес. Он может устанавливаться автоматически, если точка доступа имеет DHCP-сервер, либо вручную оператором. В первом случае нужно выбрать опцию **Obtain an IP address automatically**, а во втором – **Use the following IP address**. При ручной установке необходимо задать следующие параметры:
    - IP-адрес - IP Address;
    - Маска подсети - Subnet Mask;
    - Шлюз по-умолчанию - Default Gateway;
    - Адрес DNS сервера - DNS Server 1;
    - Адрес альтернативного DNS сервера (может отсутствовать).

Эти параметры для реальной сети обычно получают у провайдера сетевых услуг.

При правильной настройке сетевой карты, рабочие станции получат адреса из диапазона 192.168.0.2…254 с маской 255.255.255.0. В качестве шлюза по умолчанию (default gw) и DNS сервера будет установлен адрес 192.168.0.1 (адрес маршрутизатора).

Пользователь может также проконтролировать ряд технических параметров беспроводной связи. Такими параметрами могут быть:

1) качество сигнала (**Signal Quality**). Для количественной оценки качества используется мощность (уровень) принимаемого сигнала, отображаемые в % или в виде некоторой пиктограммки;

2) количество переданных и принятых пакетов, что свидетельствует о наличии передачи вообще и о ее качестве;
3) другие параметры.

Следует заметить, что у разных производителей сетевого оборудования названия параметров настройки могут отличаться. Однако смысл их понятен по виду и количественному значению устанавливаемых параметров.

2.5.2. Конфигурация точки доступа

Для настройки точки доступа (маршрутизатора) нужно использовать Web-интерфейс, доступ к которому производится по адресу http://192.168.1.1. Обратите внимание, что адрес компьютера, с которого происходит обращение, должен находиться в этой же сети, то есть в диапазоне от 192.168.1.2 до 192.168.1.254, при маске 255.255.255.0. Для этого можно либо установить его вручную, либо настроить автоматическое получение параметров IP от сервера DHCP, встроенного в маршрутизатор и включенного по умолчанию.

При входе в Web-интерфейс перед Вами появляется страница-меню со структурой интерфейса настройки точки доступа (в нашем случае Linksys WRT54GL). Меню содержит 8 разделов.

1. Раздел **System Information.** Это меню позволяет администратору наблюдать за работой системы.
2. Раздел **Setup, который состоит из ряда подразделов:**

2.1. **Basic Setup.** На данной странице производится настройка соединения с Интернет и конфигурирование локальной сети.

2.2. **DDHCP.** В этом подразделе осуществляется конфигурация DHCP-сервера, в частности, начальный сетевой адрес для клиентов, максимальное количество клиентов, время аренды адреса и ряд других.

2.3. **MAC Address Clone.** Позволяет задать произвольный аппаратный адрес сетевому интерфейсу. Данная функция полезна, когда произведена замена сетевого оборудования. В случае использования аутентификации по MAC адресу, нет необходимости обращаться за перерегистрацией, достаточно сменить адрес на предыдущий. Позволяет изменять адрес глобального и беспроводного сетевых интерфейсов.

2.4. **Advanced Routing.** На данной странице производится настройка маршрутизации сетевого трафика. В зависимости от способа подключения к Интернет выбирается режим работы (**Operating Mode**) маршрутизатора. Если маршрутизатор используется для предоставления доступа в «Интернет», то выбирается режим **Gateway**, иначе **Router** (BGP, RIP2, OSPF). Маршрутизатор поддерживает таблицу из 20 правил, которые указывают маршрут прохождения трафика.

2.5. **Virtual Local Area Network (VLANs). Позволяет выполнить** настройку виртуальных LAN, для чего необходимо связать порты маршрутизатора с соответствующими VLAN.

3. **Раздел Wireless.** Этот раздел состоит из следующих подразделов.

3.1. **Basic Settings.** Здесь производится установка основных параметров, в частности, режима работы устройства (с точкой доступа или без нее, работа в статусе клиента или сетевого моста); используемого стандарта передачи сигналов; идентификатора сети; номер канала; временного интервала ожидания подтверждения и др.

3.2. **RADIUS** (Remote Authentication Dial-In User Service). Служба RADIUS обеспечивает надежную аутентификацию пользователей беспроводной сети. Для идентификации станции используется MAC адрес. Для успешной авторизации необходимо указание секретного ключа (RADIUS Shared Secret).

3.3. **Wireless Security**. Данная группа настроек позволяет установить тип шифрования и аутентификации беспроводного трафика. Маршрутизатор поддерживает следующие протоколы защиты: WPA Pre-Shared Key; WPA RADIUS; WAP2; RADIUS и WEP (в порядке убывания стойкости). Для настройки защиты указывается протокол защиты, номер ключа по умолчанию, длина ключа шифрования и др.

3.4. **Wireless MAC Filter**. Механизм защиты основан на фильтрации аппаратных адресов устройств. Для активизации данной функции необходимо установить параметр **Use Filter в Enable**. Настройка списка фильтра производится командой Edit MAC Filter List. Параметр **Filter Mode** задает режим обработки списка. При выборе *Prevent PCs listed from accessing the wireless network* пользователи указанные в списке не будут допущены в сеть. При выборе *Permit only PCs listed to access the wireless network* доступ в сеть будет разрешен только адресам, указанным в списке.

3.5. **Advanced Wireless Settings.** Выполняются дополнительные настройки, в частности, указывается пропускная способность в базовом режиме и при передаче; тип аутентификации – автоматический или с разделяемым ключом; интервал отправки сигнальных пакетов; размер преамбулы и пр.

3.6. **WDS.**

4. Раздел **Security.** Состоит из двух подразделов Firewall и VPN.

4.1. **Firewall.** Межсетевой экран (Firewall) поддерживает функции фильтрации содержимого пакетов. Для активизации функций Firewall необходимо установить параметр SPI Firewall в состояние Enabled. Путем установок определенных опций можно запретить рабочим станциям доступ в Интернет и подключение анонимных клиентов, запретить загрузку приложений Java и активного содержимого ActiveX, блокировать широковещательный трафик и некоторые другие функции.

4.2. **VPN.** В данном подразделе устанавливаются механизмы аутентификации в вирутальной частной сети (Virtual Private Network). Маршрутизатор поддерживает аутентификацию в соответствии с протоколами тунелирования IPSec, PPTP и L2TP.

5. Раздел **Access Restrictions.** Предоставлена возможность задания политики доступа к Internet (Internet Access). Создается политика доступа, которая распространяется на рабочие станции, указанные в списке List of PCs. Политика мо-

жет разрешать или запрещать доступ к Интернет. Устанавливаются дни недели и временные интервалы, в которые действует политика. Также можно создавать ограничения на доступ к некоторым службам в Интернет, например Peer2Peer. Кроме того, поддерживается блокировка доступа к Web-сайтам по адресам и ключевым словам.

6. Раздел **Applications & Games**. Состоит из ряда подразделов, в которых задаются функции портов.

6.1. **Port Range Forwarding**. Обеспечивает перенаправление пакетов идущих на порты маршрутизатора на определенные порты сервера сети. Некоторые приложения для нормального функционирования требуют, чтобы определенные порты были открыты. К таким приложениям относятся серверы и некоторые сетевые игры. Когда запрос приходит на маршрутизатор, он перенаправляется указанному в таблице компьютеру. Для обеспечения безопасности можно ограничить количество портов, а также отключать эту функцию, когда в ней нет необходимости. Для добавления перенаправления порта необходимо указать приложение, начальный и конечный порт, имя протокола и сетевой адрес компьютера.

6.2. **Port Forwarding**. Назначение данной функции совпадает с Port Range Forwarding, отличие заключается в том, что она поддерживает перенаправление одного порта, а не диапазона.

6.3. **Port Triggering**. Позволяет переназначать номера портов для определенного приложения. Необходимо указать программный диапазон и назначенный диапазон. Данные, поступающие на порты в назначенном диапазоне, будут перенаправлены на порты, на которых функционирует приложение.

6.4. **De-militarized Zone (DMZ).** Позволяет подключать указанный хост к Интернет. Все порты данной станции будут доступны из вне. Суть DMZ заключается в том, что она не входит непосредственно ни во внутреннюю, ни во внешнюю сеть, и доступ к ней может осуществляться только по заранее заданным правилам межсетевого экрана. На практике DMZ выполняется как отдельная IP-подсеть, вынесенная в отдельный сегмент сети, который физически либо с помощью технологии VLAN отделен от внутренний локальной сети предприятия.

6.5. **Quality of Service (QoS).** Настраивается качество обслуживания в сети за счет установления приоритетов для трафика определенного типа и происхождения. Позволяет задать уровень приоритета для типа приложения, например Skype (VoIP). Устанавливает приоритет для трафика определенной подсети, приоритет для устройства с определенным MAC адресом, приоритет и пропускную способность каждого из четырех портов проводного сегмента Ethernet.

7. Раздел **Administration.** Включает ряд подразделов, в которых выполняются настройки логина и пароля (**Management / Router Management**); удаленного доступа (**Remote Access**); доступа через Web-интерфейс (**Web Access**); настройки служб (**Services**); занесения событий в журнал (**Log** Management) и ряд других опций.

8. Раздел **Status.** В данном разделе расположены информационные страни-

цы, отражающие состояние маршрутизатора, сетей и приложений, работающих на точке доступа. Включает следующие подразделы.

8.1. **Router**. Отображает информацию о состоянии и настройках системы, процессора, памяти и сети. Также отображаются параметры настройки Интернет-соединения.

8.2. **LAN**. Отображает состояние локальной сети и список клиентов DHCP сервера. Данный список показывает список клиентов DHCP сервера, которые подключены к сети, либо же были подключены ранее, но их адрес сохранился. В таблице приводится соответствие символьного, сетевого и физического адресов, а также время, на которое выдается клиенту адрес. Для удаления записей из DHCP таблице имеется соответствующая ссылка в столбце Delete.

8.3. **Wireless.** Отображается состояние беспроводной сети и статистика передачи пакетов.

8.4. **System Information**. Показывает краткое содержание рассмотренных выше разделов, отображает сводную информацию о сети и точке доступа.

UPnP (Universal Plug and Play) – это архитектура одноранговых соединений между персональными компьютерами и интеллектуальными устройствами, установленными, например, дома. UPnP строится на основе стандартов и технологий Интернета, таких, как TCP/IP, HTTP и XML, и обеспечивает автоматическое подключение подобных устройств друг к другу и их совместную работу в сетевой среде, в результате чего сеть (например, домашняя) становится доступной большему числу людей.

Сетевые продукты, использующие технологию Universal Plug and Play, заработают сразу, как только будут физически подключены к сети. UPnP поддерживает практически все технологии сетевых инфраструктур, как проводные, так и беспроводные. В их число, в частности, входят: кабельный Ethernet, беспроводные сети Wi-Fi (802.11b), порт IEEE 1394 ("Fire-wire"), сети на основе телефонных линий и сети на основе линий электропитания. Подключение всех этих устройств и персонального компьютера друг к другу упростит пользователям доступ к новейшим службам и приложениям.

При необходимости Вы можете задать самостоятельно имя маршрутизатора – **Router Name**. Его желательно выбирать таким, чтобы по имени можно было определить тип маршрутизатора, его месторасположение и пр. В нашей работе его можно назвать, например, WRT-54.

Максимальная длина передаваемого блока **MTU** может задаваться автоматически (опция **–Auto**), либо вручную (**Manuel**). При ручной установке она не должна превышать значение 1500 байтов.

Передаются ли (а точнее – принимаются ли) данные в сети можно узнать, щелкнув правой кнопкой мыши по иконке **Сетевое окружение** на рабочем столе и выбрать в появившемся меню пункт **Свойства**. В окне свойств сетевого подключения нужно обратить внимание на счетчик принятых пакетов. Если там стоит число, отличное от нуля, значит беспроводный адаптер принимает пакеты, т.е. слышит другие адаптеры в той же беспроводной сети. Счетчик же отправленных

пакетов показателем работоспособности сети не является. Адаптер (точнее его драйвер) может отправлять пакеты «в никуда», даже в случае неработоспособности беспроводной сети.

У многих производителей сетевого оборудования, в том числе и в Windows-интерфейсе Zero Wireless Configuration, предусмотрена возможность сохранения профилей настроек в профайлах. Эта возможность позволяет избежать рутинной работы при частой смене настроек одной и той же сети.

Если в сконфигурированной Вами сети не все компьютеры видят друг друга, то убедитесь в правильности настройки адаптеров, после которой у всех адаптеров сети должны быть одинаковыми:

- алгоритмы аутентификации (Shared Keys или WPA);
- алгоритм шифрования (WEP-128bit, WPA-TKIP или WPA-AES);
- длина ключа, в случае WEP-шифрования, (обычная длина – 128bit);
- ключ шифрования. Если используется WEP, то возможная причина неполадки – использование ASCII-ключа, и в сети используется разнородное оборудование (от разных производителей). Попробуйте ввести ключ в шестнадцатеричном представлении.
- порядковый номер, индекс, номер ключа (в случае WEP шифрования).

3. ОПИСАНИЕ ЛАБОРАТОРНОЙ УСТАНОВКИ

Лабораторная установка состоит из трех компьютеров, оснащенных интерфейсными картами беспроводных сетей типа и двух точек доступа типа Linksys WRT54GL. Аббревиатура устройства WRT-54GL означает: *Wireless RouTer* с предельной скоростью передачи 54 Мбит/с и поддержкой стандартов IEEE 802.11 b/g.

На передней панели расположены два логотипа – с правой стороны Linksys, с левой – Cisco Systems. Здесь же размещены индикаторы питания, активности портов DMZ и WAN, четырех портов LAN 10/100Base-TX и WAN 10/100 Base-TX (последний промаркирован на корпусе как Internet-порт). Индикатор питания при перезагрузке мигает.

На задней панели находятся кнопка Reset (сброс пользовательских настроек), порт WAN, четыре LAN-порта, разъем для подключения питания и две антенны, крепящиеся с помощью резьбового соединения к разъемам на корпусе. Внутренняя операционная система устройства выполнена на ядре Linux и позволяет легко менять прошивки устройства, изменяя его базовую функциональность и добавляя те функции, которые необходимы конкретному заказчику. При этом прошивки доступны совершенно бесплатно. Начальный IP-адрес WRT54GL по умолчанию — **192.168.1.1.**

WRT54GL функционально представляет собой высокоскоростной маршрутизатор фирмы *Linksys* стандарта Wireless-G и объединяет в себе возможности трех устройств:

1) встроенной точки беспроводного доступа, обеспечивающей высокоскоростное подключение к сети устройств стандартов Wireless-G (802.11g на скорости 54 Мбит/с) и Wireless-B (802.11b на скорости 11 Мбит/с);

2) коммутатора стандарта 10/100 Ethernet на 4 порта, работающего в полнодуплексном режиме, для соединения устройств Ethernet через проводную сеть. Для создания сети нужных размеров можно подсоединять компьютер напрямую или подключить дополнительные концентраторы и коммутаторы;

3) маршрутизатора, обеспечивающего работу сети и дает возможность организовать доступ к высокоскоростному Интернет-подключению (кабельному или реализованному по технологии DSL) со всех подключенных к сети рабочих станций.

Благодаря применению технологий TKIP и AES, в которых используется 128-битное шифрование промышленного уровня, обеспечивается защита данных и конфиденциальность. Маршрутизатор может работать в качестве DHCP-сервера, обладает мощным межсетевым экраном SPI для защиты сетевых компьютеров от несанкционированного доступа и большинства известных видов атак через Интернет. Устройство поддерживает режим виртуальных сетей и может обеспечивать фильтрацию доступа в Интернет пользователей сети.

4. ПРОГРАММА РАБОТЫ

4.1. Ознакомиться с техническими характеристиками сетевого адаптера и точки доступа и пояснить суть выводимых сведений и системных параметров.

4.2. Провести настройку и контроль параметров сетевого адаптера беспроводной компьютерной сети на рабочих станциях.

4.2.1. Установить драйвер сетевого адаптера.

4.2.2. Настроить сетевые адаптеры учебной сети.

4.3. Проверить функционирование сети различными способами.

4.3.1. Подсоединиться к сети и проверить ее функционирование путём зондирования удаленных станций (пингования).

4.3.2. Проверить функционирование сети путем копирования файлов с удалённой станции на свой компьютер.

4.3.3. Настроить сетевые адаптеры учебной сети в режим работы с помощью точки доступа.

4.3.4. Проверить функционирование сети с базовой станцией путем копирования файлов с удалённой станции на свой компьютер.

4.4. Выполнить исследование Web-интерфейса точки доступа.

4.4.1. Подключиться к точке доступа.

4.4.2. Исследовать процедуры фильтрации клиентов по MAC-адресам.

4.5. Провести полную настройку беспроводной сети с начала, используя вместо специализированной утилиты средства Windows.

5. ПОРЯДОК ВЫПОЛНЕНИЯ ИССЛЕДОВАНИЙ

5.1. Установка и настройка сети на рабочих станциях

5.1.1. **Установить драйвер сетевого адаптера** D-Link DWL G520 (510) и сетевой адаптер D-Link DWL G520 на системную плату, если эти операции еще не проделаны. После загрузки компьютер автоматически обнаружит новое устройство.
5.1.2. Запустить, находящуюся на рабочем столе утилиту D-Link AirPlus XtremeG Wireless Utility, ознакомится с полученным интерфейсом.
5.1.3. **Выписать поля настройки** в рабочую тетрадь, указать возможные значения их параметров и пояснить влияние этих установок на работу сети.
5.1.4. **Настроить сетевые адаптеры** учебной сети в режим работы без базовой станции (Ad Hoc) и провести сеансы связи без шифрования трафика со всеми рабочими станциями сети. Для конфигурирования адаптера в режиме Ad Hoc – без базовой станции – необходимо выполнить следующие установки на первом компьютере в разделе «Настройка»:

а) Имя сети **SSID**, например **net1**;
б) Беспроводной режим – **Ad Hoc**;
в) Аутентификация –**открытая**;
г) Шифрование – **отключить**;
Нажать на кнопку «Применить».

В разделе "Расширенные настройки" установить:

а) Частота – 802.11b –2.4 Ггц;
б) Номер канала связи (канала AdHoc)– 6;
в) Профиль установок IP – Отключить;
г) Режим питания – Отключить;
д) Автозапуск – Включить;
г) Скорость работы беспроводного адаптера – Data Rate – Авто.
Нажать на кнопку «Применить».

В разделе "Обзор сетей" появится неподключённый профиль net1. В этом же разделе нажать на кнопку «Расширенные настройки» и выбрать "только AdHoc сеть".

На второй машине необходимо выполнить те же самые настройки. Если в «Обзоре сетей» в профиле будет net1, то его следует удалить, так как активный профиль должен быть только на одной машине. После подключения появятся значок «Подключение к беспроводной сети» в правом нижнем углу (в трее).

5.2. Проверка функционирования сети различными способами

5.2.1. **Подсоединиться к сети и проверить ее функционирование** путём зондирования удаленных станций (пингования). Выполнить пингование всех компьютеров, входящих в беспроводную сеть. Убедиться, что удаленные компьютеры отвечают на ping-запросы, а счетчики переданных и полученных пакетов – увеличиваются. Удаленный компьютер должен отвечать на ping-запросы, а счет-

чик полученных пакетов – увеличиваться. Зафиксировать в отчете численные параметры результатов зондирования удалённой станции.

Примечание: IP-адрес своей и удалённой станций можно узнать, если выполнить следующие действия: Пуск->**Выполнить**, написать команду **cmd** (для того, чтобы командная консоль не исчезала). Затем выполнить команду **ipconfig**. Пингование выполняется командой «**ping** IP-адрес удалённого компьютера».

5.2.2. **Проверить функционирование сети путем копирования файлов с удалённой станции на свой компьютер**.

Зайти в «Сетевое окружение», находящееся на рабочем столе. Найдите созданную Вами беспроводную сеть и компьютеры, входящие в ее состав. (Номер компьютера можно узнать у преподавателя, либо прочитать его на системном корпусе).

Для того, чтобы осуществить копирование одного или нескольких файлов из каждой рабочей станции сети в свой компьютер, следует выполнить следующие действия:

а) Открыть доступ к папкам на удаленной станции. Чтобы это сделать, следует выбрать необходимую папку, кликнув по ней правой клавишей мыши, открыть закладку «Доступ» и поставить галочку «Открыть общий доступ».

б) В «Сетевом окружении» найти нужный компьютер или папку, к которой открыт доступ. Скопировать её в свой компьютер.

в) Закрыть доступ к «открытым» папкам. Убедиться в невозможности их копирования. Сделать выводы по результатам и отметить их в отчете.

Обратить внимание, что происходит изменение счетчиков переданных и принятых пакетов, что свидетельствует о работоспособности сети.

***Примечание*:** Если этого не происходит, то беспроводная сеть не функционирует. Возможные причины: разные каналы, SSID, ключи/типы шифрования, или на одном компьютере оно включено, на втором – нет. Возможно, что на каком-то из компьютеров установлен 802.11b адаптер, а на другом – 802.11g, а также на втором отключена работа в режиме совместимости с 802.11b (возможно, также вместо 54G Auto нужно поставить 54G LRS или даже перевести все адаптеры в режим 802.11b Only).

5.2.3. **Настроить сетевые адаптеры учебной сети в режим работы с помощью точки доступа**.

Сначала необходимо подать питание на одну из точек, затем настроить параметры беспроводной сети в утилите D-Link Airplus Utility следующим образом:

а) Имя сети – **linksys**;

б) Беспроводной режим – **Infrastructure**;

в) Аутентификация –**открытая**;

г) Шифрование – **отключить**.

В разделе «Расширенные настройки»

а) Частота – 802.11b –**2.4 Ггц**:

б) Номер канала связи (канала AdHoc) – **6**;

в) Профиль установок IP – **Отключить**;

г) Режим питания – **Отключить**;

д) Автозапуск – **Включить**;

е) Скорость работы беспроводного адаптера – Data Rate – **Авто**.

Убедиться, что в разделе «Обзор сетей» в окне «Доступная сеть» появится соответствующий значок подключения к точке доступа, что свидетельствует об установленном соединении. Следует отметить, что данная точка доступа позволяет организовать беспроводную сеть между компьютерами, работающими под управлением различных ОС, например Windows 98/XP.

5.3. Повторить исследования, указанные в пунктах 5.2.1 – 5.2.3, для компьютерной сети, работающей с базовой станцией (рабочей точкой).

5.4. Исследование Web-интерфейса точки доступа

Чтобы загрузить Web-интерфейс точки доступа следует выполнить следующие пункты:

5.4.1. **Подключиться к точке доступа**.

В "Internet Explorer", в строке URL-адреса ввести IP-адрес данной точки доступа "192.168.1.3" (или указанный преподавателем). Произойдёт загрузка Web-интерфейса устройства и система попросит ввести имя пользователя и пароль. По умолчанию имя пользователя – **root**, пароль – **admin**. После ввода имени пользователя и пароля происходит загрузка окна интерфейса точки доступа.

Примечание: если загрузка произошла в автономном режиме, следует выбрать «Сервис» и убрать галочку «Работать автономно»

Ознакомиться с интерфейсом и параметрами настройки точки доступа, пояснить назначение всех установок и их влияние на функционирование сети. Перевод английских терминов имеется в приложении к лабораторной работе (Файл "Параметры настройки БКС" в папке лабораторных работ по КС).

5.4.2. **Исследовать процедуры фильтрации клиентов по MAC-адресам**.

Установить параметр настройки так, чтобы Ваша сеть не была видна другими компьютерами и после этого убедиться, что это так. Используя средства фильтрации клиентов по MAC-адресам (Закладка «Wireless»->Wireless MAC Filter), запретить одному из компьютеров сети доступ. Для этого необходимо в окне «Wireless MAC Filter» поставить галочку «Enable/Включено» и на опции «Prevent PCs listed from accessing the wireless», т.е. указать список компьютеров, которым будет запрещен доступ к удалённому компьютеру. Затем нажать кнопку «Edit MAC Filter List». В открывшемся окне указать MAC-адрес сетевого адаптера «запрещённого» компьютера. Сохранить нажатием кнопки «Save Settings». Убедиться в правильности функционировании процедуры фильтрации, согласно пункту 5.2.

Примечание: Физический адрес сетевой карты можно узнать так:

1) Дважды кликнуть по значку беспроводного соединения в трее;
2) Выбрать закладку «Поддержка», затем «Подробности».

После чего, опять разрешить доступ и проверить возможность работы этого компьютера в сети.

5.5. Настройка беспроводной сети средствами Windows

5.5.1. Для настройки беспроводной сети средствами Windows (на Windows 98 только утилитой) следует дважды кликнуть по значку беспроводного соединения в трее. В окне выбрать «Свойства», затем закладку «Беспроводные сети». Поставить галочку «Использовать Windows для настройки сети». В этой же закладке с помощью кнопки «Добавить» можно настроить соединение (задать сетевое имя, настройка шифрования, также определить режим подключения – автоматически/по требованию).

С помощью кнопки «Дополнительно» можно определить беспроводной режим работы (точка доступа, либо сеть компьютер-компьютер).

Обзор доступных сетей осуществляется двойным щелчком на значке беспроводного соединения в трее, затем нажать на кнопку «Беспроводные сети». Для подключения к уже существующей или созданной сетям, следует выбрать нужную сеть в списке и нажать «Подключить». Проверить доступность ресурсов удалённого компьютера через «Сетевое окружение» или пингованием.

5.5.2. Для настройки беспроводной сети средствами Windows с заданием вручную IP-адресов следует выполнить следующие действия:

а) дважды щелкнуть по значку беспроводного соединения в трее;

б) в закладке «Общие» нажать на кнопку «Свойства»;

в) в закладке «Общие», в окне со списком компонентов, выбрать «Протокол Интернета (TCP/IP)» и нажать «Свойства».

г) Поставить галочку в окне «Использовать следующий IP-адрес». Например, 192.168.1.101, маска 255.255.255.0, на другом компьютере – 192.168.1.102. Нажать «Ок».

д) Нажать кнопку «Беспроводные сети» и подключиться к нужной сети. На компьютерах, в трее, должны появиться соответствующие значки подключения.

Проверить доступность ресурсов удалённого компьютера через «Сетевое окружение» или пингованием. Сделать выводы по полученным результатам.

6. СОДЕРЖАНИЕ ОТЧЕТА

6.1. Цель и программа работа.
6.2. Названия полей настройки сетевого адаптера и точки доступа с возможными значениями установок.
6.3. Письменные пояснения и обоснования режимов и параметров конфигурации.
6.4. Выводы по результатам экспериментов.

7. КОНТРОЛЬНЫЕ ВОПРОСЫ

7.1. В каких случаях целесообразно использовать беспроводные компьютерные сети?

7.2. Что представляет собой точка доступа в беспроводных сетях и каковы ее функции?
7.3. Расскажите о способах передачи и модуляции сигналов в беспроводных сетях.
7.4. С какой целью в беспроводных цепях применяются при модуляции ССК-последовательности или многочастотная модуляция ортогональных сигналов OFDM?
7.5. Назовите параметры беспроводных компьютерных сетей, которые регламентируются международными стандартами.
7.6. Как в беспроводных сетях регулируется доступ станций к среде?
7.7. Какие процессы происходят в сети во время установления соединения?
7.8. По какому принципу рабочая станция выбирает точку доступа. если их несколько в зоне достижимости?
7.9. Начертите диаграммы обмена кадрами между станциями при различных режимах доступа к сети и раскройте целесообразность применения каждого из способов.
7.10. Поясните необходимость и значения каждого из полей параметров настройки и какое влияние оказывают эти параметры на передачу данных в беспроводных сетях.
7.11. Расскажите о способах и протоколах защиты передачи данных в беспроводных сетях.
7.12. Как задаются IP-адреса для адаптера и точки доступа?
7.13. С какой целью применяется DHCP-сервер и где он располагается?

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Создание простой сети с помощью Packet Tracer. https://itmarathon.educom.ru/pdf/admin/%D0%A1%D0%B5%D1%82%D0%B8(%D1%82%D1%80%D0%B5% D0%BD%D0%B8%D1%80%D0%BE%D0%B2%D0%BA%D0%B02.pdf (дата обращения: 26.07.2020).
2. Дибров М.В. Сети и телекоммуникации. Маршрутизация в IP–сетях. В 2 ч. Часть 2: учебник и практикум для академического бакалавриата / М.В. Дибров. – М.: Изд-во Юрайт, 2019. – 351 с. https://biblio-online.ru/book/seti-i-telekommunikacii-marshrutizaciya-v-ip-setyah-v-2-ch-chast-2-437865
3. Сети и телекоммуникации: учебник и практикум для академического бакалавриата / Под ред. К.Е. Самуйлова, И.А. Шалимова, Д.С. Кулябова. – М.: Изд-во Юрайт, 2016. – 363 с. https://biblio-online.ru/book/seti-i-telekommunikacii-432824
4. Чернега В.С. Компьютерные сети / В.С. Чернега, Б. Платтнер. — Севастополь: Изд-во СевНТУ, 2006. — 500 с.