ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ им. проф. М. А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)

С. С. Владимиров

БЕСПРОВОДНЫЕ СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ

Лабораторный практикум

СПб ГУТ)))

Санкт-Петербург
2021

УДК ХХХ.ХХХ.Х (ХХХ)
ББК ХХ.ХХ хХХ
В 57

Рецензенты
— —

Утверждено редакционно-издательским советом СПбГУТ
в качестве учебного пособия

Владимиров, С. С.
В 57 Беспроводные системы передачи данных : лабораторный практикум / С. С. Владимиров ; СПбГУТ. — СПб, 2021. — 29 с.

Учебное пособие призвано ознакомить студентов старших курсов с технологиями беспроводных систем передачи данных. Представленный материал служит справочным и методическим пособием при выполнении курса практических работ по дисциплинам «Беспроводные системы передачи данных» и «Передача данных в беспроводных сетях».

Предназначено для студентов, обучающихся по направлениям 11.03.02 «Инфокоммуникационные технологии и системы связи» и 09.03.01 «Информатика и вычислительная техника».

УДК ХХХ.ХХХ.Х (ХХХ)
ББК ХХ.ХХ хХХ

Содержание

Лабораторная работа 1
Настройка Wi-Fi 802.11 в ОС семейства GNU/Linux

1.1. Цель работы

Ознакомиться с принципами настройки соединений Wi-Fi (802.11) в ОС семейства GNU/Linux на примере операционной системы Debian Linux с использованием различных программных средств с интерфейсом командной строки.

1.2. Теоретические сведения

Для работы с оборудованием Wi-Fi (сетевыми картами 802.11) в ОС семейства GNU/Linux как правило используюся следующие программы:

1. Программный пакет **wireless-tools**. Базовый набор утилит для управления беспроводными соединениями. На сегодня считается устаревшим, но все еще широко используется.

2. Программа **iw**. Современный пакет, использующий библиотеку nl80211, и ставший стандартом для современных дистрибутивов. В настоящее время находится в процессе разработки, и поддерживается не всеми модулями беспроводных чипов.

3. Программный пакет **WPA supplicant**. Обеспечивает поддержку стандарта IEEE 802.11i-2004/RSN (Robust Secure Network, надежная защищенная сеть). Позоляет использовать протоколы аутентификации/шифрования WEP, WPA, WPA2. Без этого пакета возможна работа лишь с протоколом WEP.

1.2.1. Программный пакет wireless-tools

Программный пакет wireless-tools является традиционным средством настройки беспроводного Wi-Fi соединения в ОС GNU/Linux. Он состоит из следующих программ, использующих интерфейс командной строки:

- iwconfig — управление основными параметрами беспроводного интерфейса;
- iwlist — запускает сканирование эфира и выводит доступные частоты, скорости, ключи шифрования и прочее;
- iwspy — определяет статистику и качество беспроводного соединения до заданного узла (работает не со всеми сетевыми картами);
- iwpriv — управляет настройками, специфичными для конкретной сетевой карты;
- ifrename — позволяет переименовать интерфейс, основываясь на различных критериях;
- iwevent — отображает события, вызванные драйвером беспроводной карты и соответствующими модулями ядра ОС;

- iwgetid — выводит идентификатор беспроводной сети (ESSID), к которой подключен компьютер, и некоторые другие параметры (обычно используется в скриптах для автоматизации задач).

Как и большинство программ, работающих с сетевыми интерфейсами, утилиты пакета wireless-tools требуют прав суперпользователя для выполнения любых операций, приводящих к изменению настроек. Операции просмотра прав суперпользователя как правило не требуют.

Важно: Здесь и далее при указании команд будут использоваться следующие обозначения:

- `$ команда` — запуск команды с правами обычного пользователя;
- `# команда` — запуск команды с правами суперпользователя root;
- `$ sudo команда` — запуск команды с правами суперпользователя root от имени обычного пользователя с использованием утилиты sudo.

В лабораториях кафедры для запуска команд с правами суперпользователя root необходимо использовать третий вариант с утилитой sudo.

Как правило для работы с беспроводным интерфейсом его требуется активировать с помощью утилиты ifconfig или утилиты ip. Например, для активации («поднятия») интерфейса wlan0 необходимо использовать команды:

```
$ sudo ifconfig wlan0 up
```

или

```
$ sudo ip link set wlan0 up
```

1.2.1.1. Утилита iwconfig

При запуске без параметров утилита iwconfig выводит на экран список имеющихся в системе сетевых интерфейсов с указанием поддерживаемых интерфейсом беспроводных технологий и основных параметров соединения.

```
$ sudo iwconfig
wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=0 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off

eth0      no wireless extensions.

lo        no wireless extensions.
```

В данном случае на компьютере всего три интерфейса: беспроводной Wi-Fi интерфейс wlan0 (не подключенный к сети), проводной интерфейс eth0 и loopback-интерфейс lo.

Для того, чтобы посмотреть параметры конкретного интерфейса, необходимо указать его имя сразу после названия утилиты.

```
$ sudo iwconfig wlan0
wlan0 IEEE 802.11  ESSID:"WIFINET"
      Mode:Managed  Frequency:2.437 GHz  Access Point: 34:28:14:AC:21:5E
      Bit Rate=58.5 Mb/s   Tx-Power=15 dBm
      Retry short limit:7   RTS thr:off   Fragment thr:off
      Encryption key:off
      Power Management:off
      Link Quality=60/70  Signal level=-50 dBm
      Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
      Tx excessive retries:0  Invalid misc:8   Missed beacon:0
```

Приведен пример для сетевого интерфейса wlan0, подключенного к беспроводной сети с идентификатором WIFINET, работающей в частотном диапазоне 2,4 ГГц в 6 канале (2,437 ГГц).

Формат запуска утилиты iwconfig для настройки сетевого интерфейса имеет следующий вид:

```
iwconfig interface [essid X] [nwid N] [mode M] [freq F]
                   [channel C] [sens S] [ap A] [nick NN]
                   [rate R] [rts RT] [frag FT] [txpower T]
                   [enc E] [key K] [power P] [retry R]
                   [modu M] [commit]
```

Краткое описание параметров приведено в табл. 1.1. Более подробно про параметры и возможные их значения можно прочесть в справке программы (команда: `man iwconfig`).

Таблица 1.1

Параметры, задаваемые утилитой iwconfig

Параметр	Описание
essid	Задает ESSID (Extended Service Set Identification), т. е. имя сети, к которой необходимо подключиться.
nwid	Задает идентификатор сети. Используется только для устаревшего (так называемого pre-802.11) оборудования. В 802.11 используются параметры ESSID или AP в зависимости от типа сети.
mode	Задает режим работы устройства, определяющий топологию сети. Доступны несколько значений параметра: • Ad-Hoc — одноранговая сеть без точек доступа; • Managed — присоединение к сети из нескольких точек доступа с использованием роуминга; • Master — узел будет являться источником пакетов синхронизации или играть роль точки доступа; • Repeater — узел ретранслирует пакеты между другими устройствами в сети (режим повторителя); • Secondary — узел играет роль запасной точки доступа или запасного повторителя; • Monitor — узел не подключается к какой-либо сети и просто перехватывает пакеты в заданном канале (на заданной частоте); • Auto — автоматический режим.

Продолжение табл. 1.1

Параметры, задаваемые утилитой iwconfig

Параметр	Описание
freq	Задает рабочую частоту в герцах. Для удобства можно использовать суффиксы k (кГц), M (МГц) и G (ГГц). Задать можно только определенные частоты, соответствующие центральным частотам каналов 802.11. Доступные для сетевой карты частоты можно посмотреть, использовав утилиту iwlist. Параметр freq фактически дублирует параметр channel. При подключении к существующей сети игнорируется (поскольку рабочая частота/канал задается точкой доступа или задающим узлом Ad-Hoc сети).
channel	Задает номер канала. Задать можно только определенные каналы, соответствующие используемой технологии 802.11. Доступные для сетевой карты каналы можно посмотреть, использовав утилиту iwlist. Параметр channel фактически дублирует параметр freq. При подключении к существующей сети игнорируется (поскольку рабочая частота/канал задается точкой доступа или задающим узлом Ad-Hoc сети).
sens	Задает порог чувствительности приемника в децибелах по мощности (дБм). Как правило используется в качестве порогового значения при роуминге и «хэндовере», определяющего когда переподключаться к другой точке доступа.
ap	Заставляет сетевую карту присоединиться к точке доступа, определяемой по MAC-адресу, получаемому при сканировании эфира. Используется, если необходимо подключиться к конкретной точке доступа (или узлу одноранговой сети) из работающих в данной сети. Если сигнал от заданной точки доступа низкий, то устройство может самостоятельно переключиться в автоматический режим. Кроме MAC-адреса можно указать значения параметра off (перейти в автоматический режим, оставшись подключенным к точке доступа) или any (сразу искать точку доступа с лучшим уровнем сигнала).
nick	Задает имя станции в сети. С точки зрения практического применения параметр малополезен и используется лишь несколькими диагностическими программами.
rate	Задает скорость передачи данных в бит/с. Для удобства можно использовать суффиксы k (кбит/с), M (Мбит/с) и G (Гбит/с). Значения меньше 1000 программа пытается искать в списке скоростей, заданных в драйвере сетевой карты (можно посмотреть утилитой iwlist).
rts	Проверка свободности канала перед передачей каждого пакета. Увеличивает объем служебного трафика, но при этом улучшает работу сети в случае наличия скрытых узлов или большого количества активных узлов.
frag	Включает фрагментацию IP-пакетов. Задается максимальный размер пакета в байтах.
txpower	Задает мощность передатчика в децибелах по мощности (дБм). Также можно указать значение в милливаттах (мВт), которое будет автоматически пересчитано в дБм по формуле $P = 30 + 10\log(W)$, где W — это уровень мощности в ваттах (Вт). Для этого используется суффикс mW. Также доступны значения on и off, включающие и выключающие передатчик, соответственно; а также значение auto и fixed, включающие и выключающие автоматическое управление мощностью передатчика.

Окончание табл. 1.1

Параметры, задаваемые утилитой iwconfig

Параметр	Описание
key/enc	Позволяет управлять видами шифрования, ключами скремблирования и режимом безопасности. Используется для подключения к сети с WEP шифрованием.
power	Управление режимами энергосбережения.
retry	Указывает как часто транслировать MAC-адрес.
modu	Позволяет указать используемый вид модуляции. Список доступных для сетевой карты видов модуляции можно посмотреть утилитой iwlist.
commit	Дополнительная опциональная команда, принуждающая сетевую карту немедленно принять заданные изменения. Как правило не требуется.

1.2.1.2. Утилита iwlist

Утилита iwlist является эффективным инструментом, позволяющим просмотреть возможности беспроводной сетевой карты, а также просканировать эфир для определения активных беспроводных сетей.

Формат запуска утилиты iwlist имеет следующий вид:

```
iwlist [interface] команда
```

Возможные команды и их краткое описание приведены в табл. 1.2. Через знак «/» указаны возможные варианты написания команд. Их полное описание можно прочесть в справке программы (команда: `man iwlist`).

Таблица 1.2

Команды утилиты iwlist

Команда	Описание
scan/scanning	Определяет и выводит список точек доступа и одноранговых Ad-Hoc сетей, доступных сетевой карте. Указывает параметры этих сетей.
freq/frequency/channel	Выводит список доступных каналов Wi-Fi и соответствующих им несущих частот.
rate/bit/bitrate	Выводит список скоростей передачи, поддерживаемых сетевой картой.
keys/enc/encryption	Выводит поддерживаемые размеры ключей шифрования и сами ключи, прописанные на устройстве.
power	Выводит свойства энергосбережения и режимы работы устройства.
txpower	Выводит возможные значения мощности передатчика.
retry	Выводит ограничения на повторную передачу.
ap/accesspoint/peers	Выводит список доступных точек доступа и/или узлов Ad-Hoc сети.
event	Выводит системные события, относящиеся к работе интерфейса.
auth	Выводит установленные параметры WPA-аутентификации.

Окончание табл. 1.2

Команды утилиты iwlist

Команда	Описание
wpa/wpakeys	Выводит записанные ключи шифрования WPA.
genie	Выводит основные параметры, записанные в устройстве. Требуется для работы WPA.
modu/modulation	Выводит поддерживаемые устройством методы модуляции.

1.2.2. Программа iw

В отличие от пакета wireless-tools все операции над беспроводной сетевой картой выполняются одной программой iw с использованием библиотеки nl80211. Синтаксис программы iw также сделан более приближенным к обычному языку.

Как и команды пакета wireless-tools, программу iw необходимо запускать с правами суперпользователя.

Общий формат запуска программы iw имеет следующий вид:

```
iw command [option]
```

Список основных команд с кратким описанием приведен в табл. 1.3. Более подробно про работу с утилитой можно почитать во встроенной справке (команда: `iw help`). Для более удобного чтения справки можно передать ее в утилиту-просмотрщик less командой

```
$ sudo iw help | less
```

После этого можно использовать возможности less для навигации по справке.

Таблица 1.3

Команды и параметры утилиты iw

Команда	Описание
event	Выводит события ядра, относящиеся к беспроводным интерфейсам. Аналог утилиты iwevent.
phy/list	Выводит все беспроводные устройства и их параметры.
phy *имя-устр* info	Выводит параметры указанного беспроводного устройства.
dev	Выводит все беспроводные интерфейсы.
dev *интерфейс*	Указывает программе работать с конкретным интерфейсом.
Следующие команды вводятся после «dev интерфейс»	
scan	Определяет и выводит список точек доступа и одноранговых Ad-Hoc сетей, доступных сетевой карте. Указывает параметры этих сетей. Аналог команды scan утилиты iwlist.
link	Выводит статус соединения.
connect ESSID	Подключение к сети с идентификатором ESSID.
key 0:ключ	Подключение к сети с WEP шифрованием с использованием ключа. Используется с предыдущей командой. Тип ключа (шестнадцатеричный или ASCII) определяется автоматически.

1.2.3. Программа WPA supplicant

WPA supplicant реализует согласование ключей шифрования с аутентификатором WPA (WPA Authenticator), аутентификацию EAP с сервером аутентификации (Authentication Server), а также управляет роумингом и выполняет сопряжение адаптера с беспроводной сетью. Также он может быть использован для настройки аутентификации в проводных сетях.

При использовании WPA supplicant возможны два варианта настройки. Первый вариант предполагает написание специального конфигурационного файла и указание его при запуске программы. Этот способ чаще всего применяется на практике. Второй вариант основан на использовании интерактивной командной утилиты wpa_cli, используемой для настройки ранее запущенного WPA supplicant. Этот вариант может быть удобнее при тестировании сетей.

Как правило для запуска WPA supplicant используется команда

```
$ sudo wpa_supplicant -B -i интерфейс -c конфигурационный файл
```

Для примера приведем конфигурационный файл для подключения к сети WIFINET с паролем «Password» при использовании аутентификации WPA2-PSK (Pre-shared key).

```
network={
        ssid="WIFINET"
        scan_ssid=1
        key_mgmt=WPA-PSK
        pairwise=CCMP TKIP
        group=CCMP TKIP
        psk="Password"
        }
```

Некоторые параметры, указываемые в конфигурационном файле, и их краткое поисание приведены в табл. 1.4. Более подробное описание и примеры конфигураций для схем аутентификации, отличных от WPA-PSK приведены в руководстве по написанию комфигурационного файла (команда: `man wpa_supplicant.conf`.

Таблица 1.4

Параметры, указываемые в конфигурационном файле wpa_supplicant.conf

Параметр	Описание
ssid	Идентификатор сети
scan_ssid	Позволяет соединиться с беспроводной сетью со скрытым SSID.
key_mgmt	Способ аутентификации.
pairwise	Способ шифрования для unicast соединений. Допускаются три варианта: 1. CCMP — AES/CBC-MAC. 2. TKIP — протокол целостности временного ключа (Temporal Key Integrity Protocol). 3. NONE — использовать ключи для групповых (multicast) соединений.

Окончание табл. 1.4

Параметры, указываемые в конфигурационном файле wpa_supplicant.conf

Параметр	Описание
group	Способ шифрования для групповых (multicast) соединений. Допускаются варианты: 1. CCMP — AES/CBC-MAC. 2. TKIP — протокол целостности временного ключа (Temporal Key Integrity Protocol). 3. WEP104 — WEP (Wired Equivalent Privacy) с 104-битным ключом. 4. WEP40 — WEP (Wired Equivalent Privacy) с 40-битным ключом.
psk	Ключ доступа к сети (256-битный). Может представлять собой строку ASCII длиной от 8 до 63 символов, из которых формируется ключ, либо сам ключ в виде строки из 64 16-теричных цифр.

Список использованных источников

1. Tourrilhes J. Wireless Tools for Linux // Материал с сайта Hewlett Packard GitHub Pages. URL: https://hewlettpackard.github.io/wireless-tools/Tools.html.

2. Wireless tools for Linux // Материал с сайта Wikipedia.org. URL: https://en.wikipedia.org/wiki/Wireless_tools_for_Linux.

3. Wireless network configuration // Материал с сайта ArchWiki. URL: https://wiki.archlinux.org/index.php/Wireless_network_configuration.

4. WPA supplicant // Материал с сайта ArchWiki. URL: https://wiki.archlinux.org/index.php/WPA_supplicant.

5. Григорян М. Linux WiFi из командной строки с wpa_supplicant // Материал с сайта Хабр. URL: https://habr.com/post/315960/.

6. iwconfig(8) - Linux man page // Материал с сайта Linux Documentation. URL: https://linux.die.net/man/8/iwconfig.

7. iwlist(8) - Linux man page // Материал с сайта Linux Documentation. URL: https://linux.die.net/man/8/iwlist.

8. iw(8) - Linux man page // Материал с сайта Linux Documentation. URL: https://linux.die.net/man/8/iw.

9. wpa_supplicant.conf(5) - Linux man page // Материал с сайта Linux Documentation. URL: https://linux.die.net/man/5/wpa_supplicant.conf.

10. Example wpa_supplicant configuration file // Материал с сайта Computer Science Department of the Universitat Politecnica de Catalunya. URL: http://www.lsi.upc.edu/lclsi/Manuales/wireless/files/wpa_supplicant.conf.

1.3. Порядок выполнения задания

Лабораторная работа предназначена для выполнения бригадой студентов не более двух человек. Допускается выполнение на личных компьютерах/ноутбуках, работающих под управлением ОС семейства GNU/Linux. По

согласованию с преподавателем допускается выполнение работы на личном компьютере под управлением ОС семейства BSD Unix (кроме Mac OS X).

По результатам работы должен быть сделан отчет. Отчет оформляется согласно примеру, приведенному в разделе **XXX**. По каждому пункту должны быть указаны: команда и результат выполнения команды (в текстовом формате). По каждому подразделу должны быть сделаны и написаны выводы. Отчет должен быть оформлен в электронном виде в формате PDF и выслан на электронную почту преподавателя. Допускается также сдача печатного экземпляра отчета (в этом случае листы отчета не должны быть сшиты, допускается только скрепление листов на канцелярскую скрепку).

1.3.1. Настройка беспроводного интерфейса при помощи пакета wireless-tools

1.3.1.1. Ознакомление со свойствами интерфейса

1. Определить тип беспроводной сетевой карты с помощью утилит lspci или lsusb в зависимости от типа карты.
2. Определить название беспроводного интерфейса с помощью утилиты iwconfig.
3. Активировать беспроводной интерфейс с помощью утилиты ifconfig или утилиты ip.
4. Вывести на экран список доступных каналов Wi-Fi и соответствующих им несущих частот.
5. Просканировать диапазон и определить доступные сетевой карте точки доступа. Определить какой тип шифрования/аутентификации используется каждой из точек доступа. В отчете привести список доступных точек доступа с указанием протокола шифрования/аутентификации и подробные параметры одной из точек. Для вывода только идентификаторов точек доступа удобно использовать утилиту grep совместно с утилитой iwlist (пример использования приведен ниже).

```
$ sudo iwlist wlan0 scan | grep SSID
```

1.3.1.2. Подключение к сети с аутентификацией/шифрованием по протоколу WEP

1. Найти и определить параметры беспроводной сети (точки доступа) «OPDSLABWEP».
2. Подключиться к точке доступа. Ключ WEP: $(1100110011)_{16}$. Проверить факт подключения.
3. Получить от точки доступа адрес по протоколу DHCP. Проверить факт получения адреса утилитой ifconfig или утилитой ip.

Для получения адреса по DHCP необходимо использовать утилиту dhclient, запускающуюся командой:

```
$ sudo dhclient -v интерфейс
```

4. Проверить доступность контрольного узла при помощи утилиты ping. IP-адрес узла: 10.1.1.2.

1.3.2. Настройка беспроводного интерфейса посредством программы iw

1.3.2.1. Ознакомление со свойствами интерфейса

1. Определить название беспроводного интерфейса с помощью утилиты iw.

2. Активировать беспроводной интерфейс с помощью утилиты ifconfig или утилиты ip.

3. Вывести на экран подробные параметры беспроводного устройства, соответствующего используемому интерфейсу.

4. Просканировать диапазон и определить доступные сетевой карте точки доступа. Определить какой тип шифрования/аутентификации используется каждой из точек доступа. В отчете привести список доступных точек доступа с указанием протокола шифрования/аутентификации и подробные параметры одной из точек. Для вывода только идентификаторов точек доступа удобно использовать утилиту grep совместно с утилитой iw.

1.3.3. Подключение к сети с аутентификацией/шифрованием по протоколу WPA2-PSK

1. Найти и определить параметры беспроводной сети (точки доступа) «OPDSLABWPA».

2. Написать конфигурационный файл WPA supplicant для подключения к сети «OPDSLABWPA». Пароль: opdslabwpa. Тип шифрования CCMP (AES).

3. Подключиться к сети, использовав программу WPA supplicant и написанный конфигурационный файл. Проверить факт подключения.

4. Получить от точки доступа адрес по протоколу DHCP. Проверить факт получения адреса утилитой ifconfig или утилитой ip.

5. Проверить доступность контрольного узла при помощи утилиты ping. IP-адрес узла: 10.1.1.2.

1.4. Контрольные вопросы

1. Что такое технология Wi-Fi?

2. Какие частотные диапазоны и частотные каналы используются в сетях Wi-Fi?

3. Защита сетей Wi-Fi с использованием WEP и WPA2.

Лабораторная работа 2
Изучение основ работы с программой D-Link Wi-Fi Planner Pro

2.1. Цель работы

Ознакомиться с основами работы с программой D-Link Wi-Fi Planner Pro.

2.2. Теоретические сведения

Программа D-Link Wi-Fi Planner Pro предназначена для первичного анализа плана помещения с целью размещения на нем точек доступа Wi-Fi. Программа ориентирована на использование оборудования D-Link.

Список использованных источников

1. В. Лаврухин «Как правильно проектировать WiFi-сеть». Материал с сайта http://wireless.sut.ru.
2. Проект сети стандарта WiFi для Кампуса. Материал с сайта http://wi-life.ru.
3. Ошибки при развертывании сетей Wi-Fi. Материал с сайта http://wi-life.ru.
4. Ю. Ревич «Беспроводная точность. Подробно о Wi-Fi». Материал с сайта http://www.dgl.ru.
5. Общие рекомендации по построению беспроводных сетей. Материал с сайта http://zyxel.ru.
6. Andrew von Nagy «High Capacity WLAN Requirements Gathering».

2.3. Порядок выполнения задания

1. **Задание**. Расчет размещения точек для плана двухкомнатной квартиты.
2. Зарегистрироваться на сайте D-Link (http://tools.dlink.com/ru/signform.asp).
3. После подтверждения регистрации (письмо придёт на указанную электронную почту) зайти на сайт под указанными при регистрации электронной почтой и паролем. Выбрать программу Wi-Fi Planner Pro.
4. Ознакомиться с появившейся в окне краткой последовательностью действий.
5. Создать новый проект (кнопка «Create project») с названием согласно фамилии студента, выполняющего работу.
6. Добавить план этажа. В качестве плана задать файл с рисунком плана двухкомнатной квартиты. План нарисовать самостоятельно или взять из сети Интернет.

7. Указать масштаб, пользуясь кнопкой «Scale floor plan». Масштаб взять с плана квартиры или указать, согласуясь со средними размерами типовых комнат.

8. Задать зону покрытия («Define Wi-Fi zone»—«Coverage zone»).

9. Нарисовать на схеме перегородки/стены. Тип перегородок взять, как в собственной квартире. Внешние стены несущие бетонные («Concrete wall»).

10. Нарисовать область типа помещения. Выбрать тип помещения «Closed Office Area».

11. Рассчитать размещение точек автоматически, нажав на кнопку «Advisor». Настройки точек доступа оставить по умолчанию (диапазон 2,4 ГГц). Сравнить с результатом выполнения предыдущей практической работы.

12. Сохранить результат для отчета в виде изображения, использовав соответствующую кнопку «Export as image».

13. Сгенерировать отчет программы, использовав кнопку «Generate Report. . . ». Сгенерированный отчёт в формате PDF приложить к отчету по лабораторной.

14. Разместить точки вручную так, чтобы по всей рабочей зоне обеспечить уровень сигнала не хуже, чем -55 дБ. Сравнить с результатом выполнения предыдущей практической работы и автоматическим размещением.

15. Сохранить результат для отчёта в виде изображения, использовав соответствующую кнопку «Export as image».

16. Сгенерировать отчет программы, использовав кнопку «Generate Report. . . ». Сгенерированный отчёт в формате PDF приложить к отчету по лабораторной.

17. Составить отчет, в котором указать последовательность действий, полученные результаты работы и выводы по ним. К отчету по лабораторной приложить сгенерированные в программе отчеты (всего 2).

2.4. Контрольные вопросы

1. Этапы проектирования сети 802.11.
2. Оценка количества точек доступа 802.11.
3. Оценка зоны покрытия сети 802.11.
4. Влияние препятствий и несущих конструкций на радиосигнал.

Лабораторная работа 3
Настройка сетевого оборудования Wi-Fi

3.1. Цель работы

Ознакомиться с принципами настройки сетевого оборудования Wi-Fi на примере развертывания точки доступа Wi-Fi с шифрованным доступом.

3.2. Порядок выполнения задания

В рамках работы возможны варианты реализации точки доступа:

1. Реализация/настройка точки доступа на базе стандартного беспроводного маршрутизатора 802.11.
2. Развертывание точки доступа на основе персонального компьютера (ноутбука) с встроенной сетевой картой 802.11 Wi-Fi под управлением ОС MS Windows или GNU/Linux.
3. Развертывание точки доступа на основе персонального мобильного компьютера (планшет/смартфон) под управлением ОС Android или iOS.

Работу выполнять по следующим шагам:

1. Выбрать вариант реализации точки доступа.
2. Настроить точку доступа с SSID «IKVT-71-номер по журналу» и шифрованием WPA2-PSK (если оборудование не поддерживает данный режим, то возможен иной вариант шифрования, например WEP).
3. Продемонстрировать работоспособность точки доступа, подключившись к развернутой сети с клиентского устройства.
4. Составить отчет, в котором указать:
   а) выбранный вариант реализации точки доступа;
   б) ход настройки ТД (текст + скриншоты);
   в) подключение клиентского устройства к ТД (текст + скриншоты).
   г) выводы по работе.

3.3. Контрольные вопросы

1. Способы подключения к сети Wi-Fi.

Лабораторная работа 4
Оценка степени защищенности сети Wi-Fi

4.1. Цель работы

Ознакомиться с принципами подбора (взлома) ключа для сети Wi-Fi на примере сети с шифрованием по методу WEP.

4.2. Теоретические сведения

4.2.1. Программный пакет aircrack-ng

Будет добавлено позднее.

Список использованных источников

1. Aircrack-ng. URL: https://www.aircrack-ng.org/.
2. iwconfig(8) - Linux man page // Материал с сайта Linux Documentation. URL: https://linux.die.net/man/8/iwconfig.

4.3. Порядок выполнения задания

Лабораторная работа предназначена для выполнения бригадой студентов. Допускается выполнение на личных компьютерах/ноутбуках, работающих под управлением ОС семейства GNU/Linux. По согласованию с преподавателем допускается выполнение работы на личном компьютере под управлением ОС семейства BSD Unix (кроме Mac OS X).

По результатам работы должен быть сделан отчет. Отчет оформляется согласно примеру, приведенному в разделе **XXX**. По каждому пункту должны быть указаны: команда и результат выполнения команды (в текстовом формате). По каждому подразделу должны быть сделаны и написаны выводы. Отчет должен быть оформлен в электронном виде в формате PDF и выслан на электронную почту преподавателя. Допускается также сдача печатного экземпляра отчета (в этом случае листы отчета не должны быть сшиты, допускается только скрепление листов на канцелярскую скрепку).

4.3.1. Атака на сеть с шифрованием WEP

1. Определить название беспроводного интерфейса с помощью утилиты iwconfig. В дальнейшем в примерах команд будем считать, что интерфейс называется wlan0.

```
$ sudo iwconfig
lo        no wireless extensions.

enp3s0    no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
```

```
          Mode:Managed  Access Point: Not-Associated   Tx-Power=0 dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

Важно: Вывод команд на лабораторных и личных компьютерах может отличаться.

2. Активировать беспроводной интерфейс с помощью утилиты ifconfig или утилиты ip.

3. Перевести беспроводной адаптер в режим мониторинга при помощи утилиты airmon-ng.

```
$ sudo airmon-ng start wlan0

Found 1 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    442 wpa_supplicant

PHY    Interface  Driver      Chipset

phy0   wlan0      rt2800pci   Ralink corp. RT3290 Wireless
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)
```

4. При помощи утилиты iwconfig убедиться, что интерфейс перешел в режим монитора.

```
$ sudo iwconfig

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.422 GHz  Tx-Power=20
   dBm
          Retry short  long limit:2   RTS thr:off   Fragment thr:off
          Power Management:off
```

5. Завершить все процессы, которые могут помешать выполнению работы.

```
$ sudo airmon-ng check kill
Killing these processes:

    PID Name
    442 wpa_supplicant
```

6. Просканировать трафик Wi-Fi программой airodump-ng, чтобы определить все работающие точки доступа и их пользователей в пределах зоны действия. В выведенном списке сетей найти сеть OPDSLABWEP с методом шифрования WEP. Из информации о точке доступа запомнить её BSSID (MAC-адрес) и канал (CH).

Для прекращения раобты airodump-ng нажать Ctrl + C .

```
$ sudo airodump-ng wlan0mon
 CH  4 ][ Elapsed: 0 s ][ 2021-03-10 10:39

 BSSID              PWR  Beacons   ...  CH  ENC CIPHER  AUTH ESSID

 00:21:91:86:35:29  -64        4   ...  8   WPA2 CCMP   PSK  OPDSLABWPA
 1C:AF:F7:B3:38:3D  -48        2   ...  3   WEP  WEP         OPDSLABWEP
 00:22:BE:92:98:74  -75        2   ...  1   WPA2 CCMP   PSK  <length: 1>
 00:22:BE:92:98:72  -75        2   ...  1   WPA2 CCMP   PSK  testingNet
 00:22:BE:92:98:71  -75        2   ...  1   WPA2 CCMP   PSK  StudNet

 BSSID              STATION            PWR   Rate  ...

 00:22:BE:92:98:70  8E:A3:79:95:37:08   -1   36e-  ...
```

7. Подключиться к сети OPDSLABWEP с одного-двух сторонних устройств (смартфон, ноутбук, ПК). Это необходимо для того, чтобы в дальнейшем генерировать в сети трафик, имитирующий работу пользовательских устройств.

8. Начать захват трафика Wi-Fi сети OPDSLABWEP указанной ниже командой. В качестве BSSID указать идентификатор (MAC-адрес) точки доступа OPDSLABWEP, полученный ранее. Параллельно имитировать работу пользователей, обращаясь с других устройств к ресурсам сети).

```
$ sudo airodump-ng --bssid 1C:AF:F7:B3:38:3D -c 3 -w WEPcrack wlan0mon

CH  3 ][ Elapsed: 5 mins ][ 2021-03-10 13:18

 BSSID              PWR RXQ  Beacons    #Data, ... ESSID

 1C:AF:F7:B3:38:3D  -44  96     3047     3999  ... OPDSLABWEP

 BSSID              STATION            PWR   Rate  ...

 1C:AF:F7:B3:38:3D  C0:4A:00:2B:56:1D  -32   54    ...
```

Для генерации трафика на лабораторном ПК (играющем роль стороннего пользовательского устройства) удобно подключиться к нему с помощью SSH и запустить tcpdump на беспроводном интерфейсе, подключенном к сети OPDSLABWEP.

```
$ sudo tcpdump -i wlan0
```

Когда будет перехвачено порядка 20 тысяч пакетов (колонка Data), прервать захват нажатием Ctrl + C .

В результате перехвата трафика в рабочем каталоге (на лабораторных ПК это скорее всего домашний каталог /home/student/) появятся файлы с перехваченным трафиком и логи перехвата:

```
-rw-r--r--  1 root root 3746133 мар 10 13:20  WEPcrack-01.cap
-rw-r--r--  1 root root     482 мар 10 13:20  WEPcrack-01.csv
-rw-r--r--  1 root root     591 мар 10 13:20  WEPcrack-01.kismet.csv
-rw-r--r--  1 root root    2713 мар 10 13:20  WEPcrack-01.kismet.netxml
-rw-r--r--  1 root root 3669701 мар 10 13:20  WEPcrack-01.log.csv
```

Постфикс «-01» в конце имени файла указывает на номер попытки захвата трафика.

9. Провести обработку перехваченного трафика, проанализировав векторы инициализации пакетов.

```
$ aircrack-ng WEPcrack-01.cap
```

Убедиться, что ключ был найден верно.

Если попытка поиска ключа не удалась, повторить захват трафика, захватив на 5000 пакетов больше (контролировать по столбцу Data).

10. Перевести беспроводной адаптер в обычный режим работы (Managed) при помощи утилиты airmon-ng. При помощи утилиты iwconfig убедиться, что интерфейс перешел в режим Managed.

```
$ sudo airmon-ng stop wlan0mon
$ sudo iwconfig
```

11. Сделать выводы по результатам работы

4.4. Контрольные вопросы

1. Защита сетей Wi-Fi с использованием WEP и WPA2.

Лабораторная работа 5
Использование программного комплекса SPLAT! для расчета зон радиопокрытия

5.1. Цель работы

Ознакомиться с принципами расчета трактов радиопередачи и зон покрытия радиопередатчиков с использованием программного комплекса Splat.

5.2. Теоретические сведения

5.2.1. Программный пакет SPLAT!

Программный пакет SPLAT! (Signal Propagation, Loss, And Terrain) предназначен для расчета потерь на трассе радиосигнала и определения зон радиопокрытия радиопередающего оборудования. Он позволяет моделировать передачу в частотном диапазоне от 20 МГц до 20 ГГц. Учитывает информацию о инженерных сооружениях, углах наклона антенн, высотах антенн над уровнем моря или средним рельефом.

В результате работы SPLAT! формирует отчеты, графики и топографические карты, отображающие пути передачи сигнала, потери на трассе, напряженность поля и ожидаемые зоны покрытия передатчиков и ретрансляторных систем.

Программа основывается на алгоритме модели нерегулярной местности Лонгли–Райса (Longley–Rice, Irregular terrain model, ITM).

SPLAT! предназначен для использования в ОС Linux и Unix. Тем не менее существуют и версии, портированные под MS Windows и Mac OS X.

SPLAT! является консольным приложением и запускается в терминале. По умолчанию в нем используется английская система мер, соответственно, для проведения расчетов следует запускать SPLAT! с флагом метрической системы:

```
$ splat -metric
```

5.2.2. Цифровые топографические модели рельефа (файлы SDF)

SPLAT! импортирует топографические данные в виде SPLAT Data Files (SDFs) с расширением «`*.sdf`».

Они могут быть сгенерированы из нескольких источников информации. К примеру SDF файлы могут быть сгенерированы с помощью моделей цифровой геометрии геодезических измерений (DEM), использующих утилиты postdownload и usgs2sdf, включенные в SPLAT! по умолчанию. Для улучшения разрешения и точности можно использовать цифровые модели SRTM Version

2, особенно если они дополнены данными SDF, полученными USGS. Эти модели являются продуктом радарной миссии Space Shuttle STS-99 и доступны для большинства населенных районов Земли.

Еще большее разрешение и точность можно получить, используя топографические данные 1 arc-second SRTM-1 версии 2.1.

На лабораторных ПК файлы SDF для Санкт-Петербурга и окрестностей размещены в каталоге `/home/student/sdf/`. Скачать архив с ними можно с сайта opds.spbsut.ru.

Для того, чтобы указать SPLAT! каталог с файлами SDF, необходимо использовать флаг «`-d`»:

```
$ splat -d /home/student/sdf/
```

5.2.3. Координаты приемопередатчика (файлы QTH)

Для моделирования линии связи или зоны покрытия необходимо задать координаты размещения приемопередатчиков узлов связи. Для этого используются текстовые файлы с расширением «`*.qth`».

Файл QTH должен состоять из 4 строк:

1. Название узла (приемопередатчика).
2. Угловая координата широты размещения узла. По умолчанию используется северная широта. Для задания координаты южной широты используются отрицательные координаты. Информация о широте и долготе может быть выражена как в десятичном формате, например 74.6864, так и в градусах/минутах/секундах, например 74 41 11.0.
3. Угловая координата долготы размещения узла. По умолчанию используется западная долгота. Для пересчета координаты восточной долготы в западную необходимо вычесть ее из 360°.
4. Высота размещения антенны. По умолчанию используются футы. Если SPLAT! запускается с флагом метрической системы, то можно указывать высоту в метрах.

Для примера приведем файл координат приемопередатчика на здании СПбГУТ (листинг 5.1). Корпус СПбГУТ по адресу пр. Большевиков д. 22 имеет географические координаты (59,902607° с. ш., 30,488135° в. д.). Долготу необходимо пересчитать в западную: $360° - 30{,}488135° = 329{,}511865°$ з. д.

Будем считать, что антенна передатчика висит на высоте 30 м от поверхности земли.

Листинг 5.1

Файл координат spbsut.qth

```
SPbSUT
59.902607
329.511865
30
```

Для того, чтобы передать SPLAT! файлы координат передатчика и приемника, необходимо использовать флаги «`-t`» и «`-r`» соответственно:

```
$ splat -metric -t spbsut.qth -r receiver.qth
```

5.2.4. Параметры модели неровностей поверхности (файлы LRP)

Параметры модели неровностей поверхности обязательны для корректного анализа SPLAT!. Данные для параметра неровностей считываются из файлов с расширением «`.lrp`».

По умолчанию SPLAT! ищет в текущем каталоге либо файлы LRP с именем узлов сети, либо файл `splat.lrp`.

Файлы LRP имеют следующий формат:

1. Диэлектрическая постоянная Земли. Зависит от ландшафта, для которого производится моделирование (табл. 5.1).
2. Проводимость Земли (сименс на метр). Зависит от ландшафта, для которого производится моделирование (табл. XXX).
3. Постоянная изгиба атмосферы. В работе использовать значение 300.
4. Частота (от 20 МГц до 20 ГГц) в МГц.
5. Радиоклимат (табл. 5.2). В работе использовать значение 5.
6. Поляризация радиоволны (0 — горизонтальная, 1 — вертикальная).
7. Доля ситуации. В работе использовать значение 0.5.
8. Доля времени. В работе использовать значение 0.5.
9. Эффективная излучаемая мощность в ваттах (Вт).

Таблица 5.1

Диэлектрические постоянные Земли и значения проводимости

Местность	Диэлектрическая постоянная	Проводимость
Соленая вода	80	5,000
Ровная Земля	25	0,020
Чистая вода	80	0,010
Болото	12	0,007
Ферма, лес	15	0,005
Небольшая возвышенность	15	0,005
Горы, гравий	13	0,002
Город	5	0,001
Низменность	4	0,001

Таблица 5.2

Коды радиоклимата

Код	Радиоклимат (пример)
1	Экваториальный (Конго)
2	Континентальный субтропический (Судан)
3	Морской субтропический (западное побережье Африки)
4	Пустынный (Сахара)
5	Континентальный умеренный
6	Морской умеренный, над сушей (Британия, океанское побережье)
7	Морской умеренный, над морем

Пример файла модели неровностей поверхности `splat.lrp` приведен на листинге 5.2.

Листинг 5.2

Файл модели неровностей поверхности splat.lrp

```
5
0.001
300
434
5
1
0.5
0.5
0.1
```

Список использованных источников

1. Magliacane, J. SPLAT! A Terrestrial RF Path Analysis Application For Linux/Unix / J. Magliacane // QSL.net: [site]. URL: https://www.qsl.net/kd2bd/splat.html.

2. Ubuntu Manpage: splat An RF Signal Propagation, Loss, And Terrain analysis tool // Ubuntu Manpage Repository: [site]. URL: http://manpages.ubuntu.com/manpages/trusty/man1/splat.1.html.

3. Clark, J. Splat! RF Signal Propagation, Loss and Terrain Analysis Tool / J. Clark // Telecommunications, Navigation, & Electronics: [site]. URL: https://jeremyclark.ca/wp/telecom/splat-rf-signal-propagation-loss-and-terrain-analysis-tool/.

5.3. Порядок выполнения задания

Лабораторная работа предназначена для выполнения бригадой студентов. Допускается выполнение на личных компьютерах/ноутбуках, работающих под управлением ОС семейства GNU/Linux. По согласованию с преподавателем допускается выполнение работы на личном компьютере под управлением ОС семейства BSD Unix (кроме Mac OS X).

По результатам работы должен быть сделан отчет. Отчет оформляется согласно примеру, приведенному в разделе **XXX**. По каждому пункту должны

быть указаны: команда и результат выполнения команды (в текстовом формате). По каждому подразделу должны быть сделаны и написаны выводы. Отчет должен быть оформлен в электронном виде в формате PDF и выслан на электронную почту преподавателя. Допускается также сдача печатного экземпляра отчета (в этом случае листы отчета не должны быть сшиты, допускается только скрепление листов на канцелярскую скрепку).

1. Создать файлы QTH с координатами передатчика и приемника. В качестве передатчика выбрать СПбГУТ (`sut.qth`) (листинг 5.1). Координаты приемника (`rcv.qth`) выбрать самостоятельно так, чтобы он был расположен в пределах 5–10 км от СПбГУТ. Для определения координат приемника можно воспользоваться сервисом Google Maps или аналогичным. Обратите внимание, что Google Maps по умолчанию отображает координаты восточной долготы (не забудьте пересчитать их в западную долготу).

2. Создать файл `splat.lrp` с параметрами модели неровностей поверхности. Частоту выбрать в диапазоне от 700 до 1500 МГц. Мощность передатчика выбрать в диапазоне от 0.1 до 0.5 Вт. В качестве местности выбрать город или лес, в зависимости от выбранного места размещения приемника. Поляризацию антенны выбрать самим.

3. Провести анализ местности с прямой видимостью между передатчиком и приемником. После выполнения в рабочем каталоге появится текстовый файл с результатами SPbSUT-to-RCV.txt (название может быть иным в зависимости от заданных в QTH имен узлов). В результатах анализа содержится подробная информация о месте передатчика и приемника и местоположении любых препятствий, обнаруженных на пути прямой видимости. Если препятствие можно обойти, подняв приемную антенну на некоторую высоту, программа укажет минимальную высоту антенны, необходимую для пути прямой видимости. Результаты анализа изучить и вставить в отчет по лабораторной.

```
$ splat -d /home/student/sdf/ -metric -t sut.qth -r rcv.qth
```

Важно: в работе для запуска SPLAT! необходимо будет всегда указывать все эти параметры. В дальнейшем в тексте работы в примерах они приводиться не будут, но **задавать их необходимо**.

4. Сгенерировать файл KML с линией прямого пути для сервисов Google Earth, Google My Maps и аналогичных.

```
$ splat -kml
```

5. Открыть сервис Google My Maps (https://www.google.com/maps/d/). Создать новую карту. Используя кнопку-ссылку Import, импортировать ранее созданный KML файл. Убедиться, что узлы показаны верно. В качестве альтернативного варианта можно использовать сервис Конструктор карт Яндекса (https://yandex.ru/map-constructor/).

6. Построить график профиля местности между приемником и передатчиком.

```
$ splat -p terrain_profile.png
```

7. Построить график возвышений между приемником и передатчиком. График иллюстрирует углы возвышения и понижения, возникающие в результате разрыва между местоположением приемника и передатчика.

```
$ splat -e elevation_profile.png
```

8. Построить график, иллюстрирующий высоту ландшафта, относящийся к линии прямой видимости между передатчиком и приемником.

```
$ splat -h height_profile.png
```

9. Построить график для высоты ландшафта, нормализированной к высотам антенны передатчика и приемника.

```
$ splat -H height_profile_norm.png
```

10. Построить график, изображающий потери на пути согласно модели ITM.

```
$ splat -l path_loss_profile.png
```

11. Построить топографическую карту, отображающую линию прямого луча между передатчиком и приемником.

```
$ splat -o tx_rx_line_map.ppm
```

12. Построить топографическую карту, отображающую геометрическую зону покрытия прямой видимости для передатчика. Файл QTH приемника при этом не указывается, но для определения зон прямой видимости (LoS) необходимо указать высоту принимающих антенн с помощью флага «`-c`». Значение высоты выбрать из интервала 15–30 метров.

```
$ splat -t sut.qth -c 25 -o tx_coverage_map.ppm
```

13. Удалите из файла `splat.lrp` последнюю строку с мощностью передатчика.

14. Построить топографическую карту потерь по модели ITM для передатчика. Высота антенн задается с помощью флага «`-L`». Значение высоты выбрать из интервала 15–30 метров.

```
$ splat -t sut.qth -L 25 -o tx_loss_map.ppm
```

15. Построить топографическую карту напряженности поля передатчика. Для этого необходимо явно указать мощность передатчика в ваттах с помощью флага «`-erp`». Значение взять то, что было ранее указано в `splat.lrp`. Высота антенн задается с помощью флага «`-L`». Значение высоты выбрать из интервала 15–30 метров.

```
$ splat -t sut.qth -L 25 -erp 0.1 -o tx_field_map.ppm
```

16. Сделать выводы по результатам работы

5.4. Контрольные вопросы

1. Программа SPLAT!

Владимиров Сергей Сергеевич

БЕСПРОВОДНЫЕ СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ

Лабораторный практикум

Редактор *Х. Х. Хxxxxxxxxx*

План изданий 20ХХ г., п. ХХ

Подписано к печати ХХ.ХХ.20ХХ
Объем Х,ХХ усл.-печ. л. Тираж ХХ экз. Заказ ХХХ

Редакционно-издательский отдел СПбГУТ
193232 СПб., пр. Большевиков, 22
Отпечатано в СПбГУТ