Лабораторная работа №3

Тема: Настройка сети Wi-Fi

Теоретические сведения:

Wi-Fi

Wi-Fi — торговая марка Wi-Fi Alliance для беспроводных сетей на базе стандарта IEEE 802.11. Под аббревиатурой Wi-Fi (от английского словосочетания Wireless Fidelity, которое можно дословно перевести как «беспроводное качество» или «беспроводная точность») в настоящее время развивается целое семейство стандартов передачи цифровых потоков данных по радиоканалам.

Wi-Fi был создан в 1991 году NCR Corporation/AT&T (впоследствии — Lucent Technologies и Agere Systems) в Ньивегейн, Нидерланды. Создатель Wi-Fi — Вик Хейз (Vic Hayes) находился в команде, участвовавшей в разработке таких стандартов, как IEEE 802.11b, IEEE 802.11a и IEEE 802.11g.

Принцип работы Wi-Fi

Обычно схема Wi-Fi сети содержит не менее одной точки доступа и не менее одного клиента. Также возможно подключение двух клиентов в режиме точка-точка, когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров «напрямую». Точка доступа передаёт свой идентификатор сети (SSID) с помощью специальных сигнальных пакетов на скорости 0,1 Мбит/с каждые 100 мс. Поэтому 0,1 Мбит/с — наименьшая скорость передачи данных для Wi-Fi. При попадании в зону действия двух точек доступа с идентичными SSID приёмник может выбирать между ними на основании данных об уровне сигнала. Стандарт Wi-Fi даёт клиенту полную свободу при выборе критериев для соединения.

По способу объединения точек доступа в единую систему можно выделить:

- Автономные точки доступа (называются также самостоятельные, децентрализованные, умные);
- Точки доступа, работающие под управлением контроллера (называются также «легковесные», централизованные);

- Бесконтроллерные, но не автономные (управляемые без контроллера).

По способу организации и управления радиоканалами можно выделить беспроводные локальные сети:

Со статическими настройками радиоканалов;

- С динамическими (адаптивными) настройками радиоканалов;
- Со «слоистой» или многослойной структурой радиоканалов.

Преимущества Wi-Fi

- Позволяет развернуть сеть без прокладки кабеля, что может уменьшить стоимость развёртывания и/или расширения сети.
- Позволяет иметь доступ к сети мобильным устройствам.
- Wi-Fi устройства широко распространены на рынке. Гарантируется совместимость оборудования благодаря обязательной сертификации оборудования с логотипом Wi-Fi.
- Мобильность. Вы больше не привязаны к одному месту и можете пользоваться Интернетом в комфортной для вас обстановке.
- В пределах Wi-Fi зоны в сеть Интернет могут выходить несколько пользователей с компьютеров, ноутбуков, телефонов и т. д.

Недостатки Wi-Fi

- Производителями оборудования указывается скорость на L1 (OSI), в результате чего создаётся иллюзия, что производитель оборудования завышает скорость, но на самом деле в Wi-Fi весьма высоки служебные «накладные расходы». Получается, что скорость передачи данных на L2 (OSI) в Wi-Fi сети всегда ниже заявленной скорости на L1 (OSI). Реальная скорость зависит от доли служебного трафика, которая зависит уже от наличия между устройствами физических преград, наличия помех от других

беспроводных устройств или электронной аппаратуры, расположения устройств относительно друг друга и т. п.

- Частотный диапазон и эксплуатационные ограничения в различных странах не одинаковы.
- Стандарт шифрования WEP может быть относительно легко взломан даже при правильной конфигурации (из-за слабой стойкости алгоритма). Новые устройства поддерживают более совершенные протоколы шифрования данных WPA и WPA2.
- В режиме точка-точка стандарт предписывает лишь реализовать скорость 11 Мбит/сек (802.11b). Шифрование WPA2 недоступно, только легковзламываемый WEP.

SSID

SSID(англ. *Service Set Identifier*) — уникальное наименование безпроводной сети , которое отличает одну сеть Wi-Fi от другой. В настройках всех устройств, которые должны работать в одной безпроводной сети необходимо указывать один и тот же SSID. SSID выбирается администратором сети и может вместительность которого до 32 символов. Значение SSID на устройствах клиентов равно «ANY», что означает возможность подключения к любой доступной сети.

Любое взаимодействие точки доступа (сети), и беспроводного клиента, построено на:

- **Аутентификации** — как клиент и точка доступа представляются друг другу и подтверждают, что у них есть право общаться между собой;
- **Шифровании** — какой алгоритм скремблирования передаваемых данных применяется, как генерируется ключ шифрования, и когда он меняется.

Параметры беспроводной сети, в первую очередь ее имя (SSID), регулярно анонсируются точкой доступа в широковещательных beacon пакетах. Помимо ожидаемых настроек безопасности, передаются пожелания по QoS, по параметрам 802.11n, поддерживаемых скорости, сведения о других соседях и прочее.

Аутентификация определяет, как клиент представляется точке. Возможные варианты:

- **Open** — так называемая открытая сеть, в которой все подключаемые устройства авторизованы сразу
- **Shared** — подлинность подключаемого устройства должна быть проверена ключом/паролем
- **EAP** — подлинность подключаемого устройства должна быть проверена по протоколу EAP внешним сервером

Открытость сети не означает, что любой желающий сможет безнаказанно с ней работать. Чтобы передавать в такой сети данные, необходимо совпадение применяющегося алгоритма шифрования, и соответственно ему корректное установление шифрованного соединения.

Алгоритмы шифрования таковы:

- **None** — отсутствие шифрования, данные передаются в открытом виде
- **WEP** — основанный на алгоритме RC4 шифр с разной длиной статического или динамического ключа (64 или 128 бит)
- **CKIP** — проприетарная замена WEP от Cisco, ранний вариант TKIP
- **TKIP** — улучшенная замена WEP с дополнительными проверками и защитой
- **AES/CCMP** — наиболее совершенный алгоритм, основанный на AES256 с дополнительными проверками и защитой

Комбинация **Open Authentication, No Encryption** широко используется в системах гостевого доступа вроде предоставления Интернета в кафе или гостинице. Для подключения нужно знать только имя беспроводной сети. Зачастую такое подключение комбинируется с дополнительной проверкой на Captive Portal путем редиректа пользовательского HTTP-запроса на дополнительную страницу, на которой можно запросить подтверждение (логин-пароль, согласие с правилами и т.п).

Технологии защиты беспроводных сетей развивались в следующем хронологическом порядке: WEP, WPA, WPA2.

WEP

Wired Equivalent Privacy (WEP) — алгоритм для обеспечения безопасности сетей Wi-Fi. Используется для обеспечения конфиденциальности и защиты передаваемых данных авторизированных пользователей беспроводной сети от прослушивания. Существует две разновидности WEP: WEP-40 и WEP-104, различающиеся только длиной ключа. В настоящее время данная технология является устаревшей, так как ее взлом может быть осуществлен всего за несколько минут. Тем не менее, она продолжает широко использоваться. Для безопасности в сетях WI-Fi рекомендуется использовать WPA. WEP часто неправильно называют *Wireless Encryption Protocol*.

В 1997 году Институт инженеров электротехники и электроники (*IEEE*) одобрил механизм WEP. В октябре 2000-го года вышла статья Джесси Уолкера «Unsafe at any key size; An analysis of the WEP encapsulation», описывающая проблемы алгоритм WEP и атаки, которые могут быть организованы с использованием его уязвимостей. В алгоритме есть множество слабых мест:

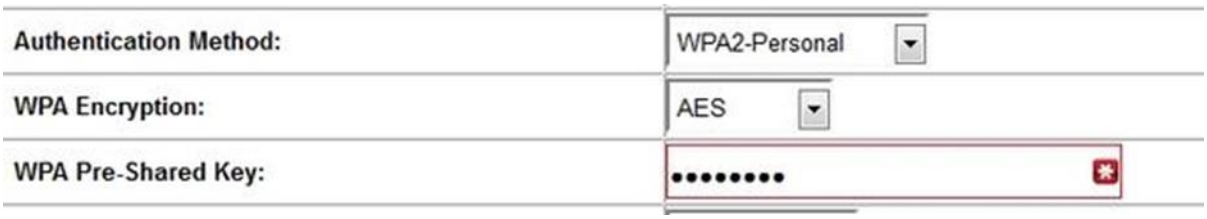
- механизмы обмена ключами и проверки целостности данных;
- малая разрядность ключа и вектора инициализации;
- способ аутентификации;
- алгоритм шифрования.

Шифрование WEP скомпрометировано, и использовать его нельзя (даже в случае динамических ключей).

WPA, WPA2

Широко встречающиеся термины WPA и WPA2 определяют, фактически, алгоритм шифрования (TKIP либо AES). В силу того, что уже довольно давно клиентские адаптеры поддерживают WPA2 (AES), применять шифрование по алгоритму TKIP нет смысла. Связка WPA2-AES является лучшей с точки зрения

безопасности на сегодняшний день. Именно так и нужно стараться настраивать Wi-Fi. Выглядеть это должно примерно так:



WPA и **WPA2** (**Wi-Fi Protected Access**) — представляет собой обновлённую программу сертификации устройств беспроводной связи. Технология WPA пришла на замену технологии защиты беспроводной Wi-Fi сети WEP. Плюсами WPA являются усиленная безопасность данных и ужесточённый контроль доступа к беспроводным сетям. Немаловажной характеристикой является совместимость между множеством беспроводных устройств как на аппаратномуровне, так и на программном. На данный момент WPA и WPA2 разрабатываются и продвигаются организацией Wi-Fi Alliance.

Стандартом WPA предусмотрен Расширяемый протокол аутентификации (EAP) как основа для механизма аутентификации пользователей. Непременным условием аутентификации является предъявление пользователем свидетельства (иначе называют мандатом), подтверждающего его право на доступ в сеть. Для этого права пользователь проходит проверку по специальной базе зарегистрированных пользователей. Без аутентификации работа в сети для пользователя будет запрещена. База зарегистрированных пользователей и система проверки в больших сетях как правило расположены на специальном сервере (чаще всего RADIUS).

WPA2 определяется стандартом IEEE 802.11i, принятым в июне 2004 года, и призван заменить WPA. В нём реализовано CCMP и шифрование AES, за счёт чего WPA2 стал более защищённым, чем свой предшественник. С 13 марта 2006 года поддержка WPA2 является обязательным условием для всех сертифицированных Wi-Fi устройств.

WPA-PSK, WPA2-PSK

Упрощённый режим Pre-Shared Key (**WPA-PSK**, **WPA2-PSK**) позволяет использовать один пароль, который хранится непосредственно в маршрутизаторе. С одной стороны все упрощается, нет необходимости создавать и сопровождать базу пользователей, с другой стороны все заходят под одним паролем.

В домашних условиях целесообразней использовать WPA2-PSK, то есть упрощенный режим стандарта WPA. Безопасность Wi-Fi от такого упрощения не страдает.

Практическое задание:

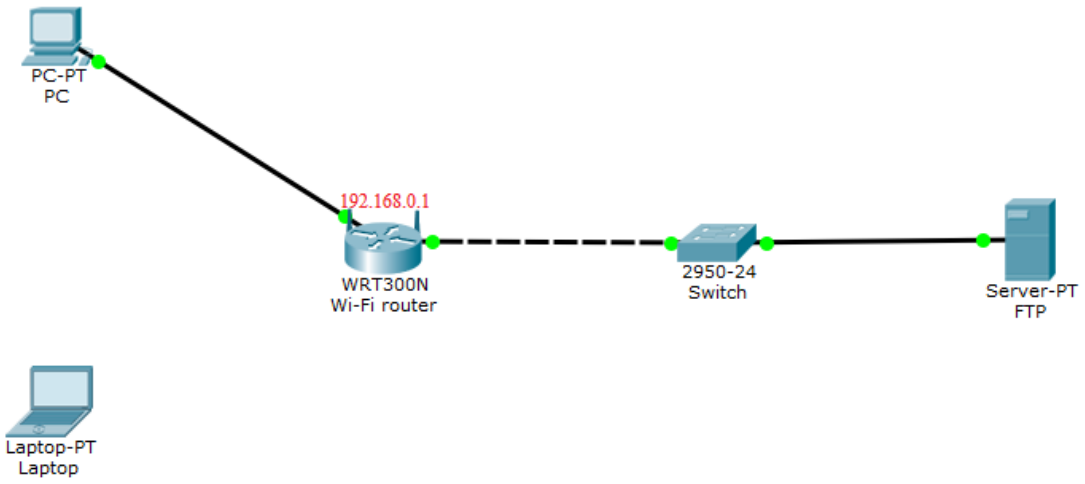


Рис. 1

Исходные данные:

x = <номер зач. кн.> mod 30

SSID = <фамилия латинницой>

passphrase = <имя латинницой>

N=<номер зач. кн.> mod 4 +1.

Исходная топология показана на Рис.1. Необходимо настроить Wi-Fi router таким образом, чтобы ноутбуксмог подсоединиться к серверу FTP. Это

необходимо сделать через GUI-интерфейс, доступ к которому можно получить с помощью браузера на PC.

Ход работы:

1. Открываем файл с названием lab3.pkt, в нем сохранена топология, изображенная на Рис.1
2. Настройки FTP-сервера производим в соответствии с данными лабораторной работы №2, с одним отличием: вместо статической IP конфигурации используем **DHCP**.
3. С помощью браузера на PC заходим на Wi-Fi маршрутизатор по адресу: http://192.168.0.1 (login **admin**, password **admin**), проводим его настройку:
    a. Setup -> DHCP Server Enabled;
    b. Setup -> Start IP Address: 192.168.1.(*x*+1);
    c. Wireless -> Network Name (SSID): *SSID*;
    d. Wireless security -> Security mode: WPA2 Personal, Encryption: AES, Passphrase: *passphrase*.
    e. Save settings;
4. Настраиваем Laptop:
    a. Wireless0 -> Port status ON;
    b. SSID: *SSID;*
    c. Authentication: WPA2-PSK, Pass phrase: *passphrase*, Encryption Type: AES;
    d. IP Configuration: DHCP.

Проверка выполнения работы:

Узнать IP-адрес ноутбука, он должен быть вида: 192.168.0.y, где:

y є [*x* + 1; x + 51].

Создать файл, в котором укажите свои ФИО и группу, и сохраните его с именем <*user*> на ноутбуке.

В окне Command Prompt вашего PC устройства введите следующую команду:

ftp 192.168.x.1

После подключения к FTP серверу необходимо загрузить созданный файл <user>.txt:

put <user>.txt

Убедитесь, загрузился ли файл на FTP сервер.

Попытайтесь просмотреть его содержимое.

Список литературы:

1. Дуглас Камер. Сети TCP/IP, том 1. Принципы, протоколы и структура = Internetworking with TCP/IP, Vol. 1: Principles, Protocols and Architecture. — М.: «Вильямс», 2003. — С. 880. — ISBN 0-13-018380-6
2. Терри Оглтри. Модернизация и ремонт сетей = Upgrading and Repairing Networks. — 4-е изд. — М.: «Вильямс», 2005. — С. 1328. — ISBN 0-7897-2817-6
3. Андрей Робачевский, Сергей Немнюгин, Ольга Стесик. Операционная система UNIX. — 2-е изд. — "БХВ-Петербург", 2007. — С. 656. — ISBN 5-94157-538-6