Практическая работа №8

ЗАЩИТА ИНФОРМАЦИИ В БЕСПРОВОДНЫХ СЕТЯХ

Цель работы. Изучить способы защиты информации в сети 802.11 путем использования шифрования и фильтрации MAC-адресов.

Краткие сведения из теории

Основной стандарт беспроводных локальных сетей – это **IEEE 802.11**.

Сети 802.11 (название дано по стандарту, иначе их называют сети **Wi-Fi** – **Wireless Fidelity**) можно использовать в двух режимах:

1) **инфраструктурный режим** (**infrastructure mode**) – подключение клиентов к другой сети, например внутренний сети компании или сети Интернет, через **точку доступа** (**Access Point**, **AP**).

2) **произвольная сеть** (**ad hoc network**) – это набор компьютеров, которые связаны таким образом, чтобы они могли напрямую отправлять кадры друг другу.

IEEE 802.11 работает на частотах ISM-организаций (для некоммерческого использования в промышленности, научных и медицинских организациях):

- 902–928 МГц;
- 2,4–2,5 ГГц;
- 5,725–5,825 ГГц.

Всем устройствам разрешается использовать эти частоты при условии, что они ограничивают свою мощность передачи до 1 мВт, чтобы не создавать помех в работе других устройств.

Стандарт 802.11 определяет сервисы, чтобы клиенты, точки доступа и соединяющие их сети могли быть согласованными беспроводными ЛВС:

- ассоциация;
- реассоциация;
- дизассоциация;
- аутентификация;
- служба распределения;
- служба интеграции;
- доставка данных;
- служба конфиденциальности;
- служба планирования трафика QoS;
- регулирование мощности передатчика;
- динамический выбор частоты.

Ассоциация. Этот сервис используется мобильными станциями для подключения к точкам доступа. Обычно он применяется сразу же после вхождения в зону действия точки доступа. По прибытии станция узнает идентификационную информацию и возможности точки доступа. Возможности точки доступа включают поддерживаемую скорость передачи данных, меры безопасности, возможности энергосбережения, поддержку качества обслуживания и т. д. Мобильная станция посылает запрос на ассоциацию с точкой доступа, которая может принять либо отвергнуть этот запрос.

Реассоциация позволяет станции сменить точку доступа.

Эта возможность полезна при перемещении станции от одной точки доступа к другой в той же расширенной 802.11 ЛВС, по аналогии с передачей в сотовой сети.

По инициативе мобильной станции или точки доступа может быть произведена **дизассоциация**, то есть разрыв отношений. Она требуется при выключении станции или ее уходе из зоны действия точки доступа.

Когда кадры достигают точки доступа, **служба распределения** определяет их маршрутизацию. Если адрес назначения является локальным для данной точки доступа, то кадры следуют напрямую по радиоканалу. В противном случае, их необходимо пересылать по проводной сети.

Служба интеграции поддерживает трансляцию, необходимую, если кадр нужно выслать за пределы сети стандарта 802.11 или если он получен из сети не этого стандарта (соединение между беспроводной ЛВС и Интернетом).

Для обработки трафика с различными приоритетами имеется служба **планирования трафика QoS.**

Регулирование мощности передатчика дает станциям информацию, которая нужна им, чтобы соответствовать установленным нормативным пределам мощности передачи, которые варьируются в зависимости от региона.

Служба **динамического выбора частоты** дает станциям информацию, необходимую, чтобы избежать передачи в частотном диапазоне 5 ГГц, который используется радарами.

Создание новой беспроводной сети в инфраструктурном режиме начинается непосредственно с конфигурации точки доступа – беспроводного маршрутизатора (роутера), подключения к ней компьютеров и другого беспроводного оборудования.

Прежде, чем подключать к беспроводной точке доступа сетевое оборудование, необходимо настроить параметры, отвечающие за безопасность беспроводной сети (тип шифрования и ключ доступа).

Ключ безопасности беспроводной сети – уникальный код (пароль), который закрывает доступ к беспроводной сети.

Вся информация, которая протекает между роутером и мобильным устройством шифруется. Это сделано для повышения безопасности сети. На сегодняшний день существует два типа шифрования Wi-Fi подключений:

– **WEP** (**Wired Equivalent Privacy**) – **приватность на уровне проводной связи;**

– **WPA** (**Wi-Fi Protected Access**) – **Wi-Fi защищенный доступ.**

В настоящее время наиболее защищенным является тип шифрования WPA второй версии (WPA2), хотя и он является скомпрометированным.

Преимуществами WPA являются усиленная безопасность данных и ужесточённый контроль доступа к беспроводным сетям, а также совместимость между множеством беспроводных устройств как на аппаратном, так и на программном уровнях. WPA2 обеспечивает безопасность в соответствии со стандартом IEEE 802.11i

Существует два обычных сценария, в которых используется WPA2.

Первый сценарий – это корпоративное использование, когда у компании есть отдельный сервер для аутентификации, хранящий имена пользователей и пароли, которые используются, чтобы определить, имеет ли право клиент получить доступ к сети.

Основные стандарты – это **802.1X**, где точка доступа позволяет клиенту вести диалог с сервером аутентификации и наблюдать результат, и **EAP** (**Extendable Authentication Protocol – расширенный протокол аутентификации**), который описывает, как взаимодействуют клиент и аутентификационный сервер.

Второй сценарий – домашнее использование в условиях, где нет аутентификационного сервера. Вместо него есть единый общий пароль, который используется клиентами для доступа в беспроводную сеть. Эта система менее сложная, чем в случае с аутентификационным сервером, но она и менее надежная.

Ключи, использующиеся для шифрования трафика, рассчитываются как часть аутентификационного опознавания.

Опознавание происходит сразу после ассоциации и аутентификации клиента на аутентификационном сервере, если он есть.

В начале опознавания у клиента есть либо пароль для аутентификационного сервера (первый сценарий), либо общий пароль сети (второй сценарий).

Пароль используется для получения основного ключа. Но основной ключ не используется прямым образом для шифрования пакетов.

Существует стандартная криптографическая практика создавать новый ключ для каждого периода использования, менять ключ для разных сеансов и держать основной ключ в секретности. При опознавании рассчитывается именно ключ сеанса.

Ключ сеанса рассчитывается при четырехпакетном опознавании.

Во-первых, **AP** (**Access Point – точка доступа**) посылает случайный номер для идентификации (рисунок 1).

Случайные номера, использующиеся только один раз в протоколах безопасности, таких как этот, называются **nonces** (**нонсы** – **временные значения**), это сокращение выражения «number used once» – «номер, использующийся только один раз».

Клиент также выбирает свой собственный временный номер. Он использует временный номер, адрес MAC и адрес AP, а также основной ключ, чтобы вычислить ключ сеанса, K_S.

Клиент посылает свой временный номер AP, AP производит тот же самый расчет, чтобы получить ключ сеанса.

Временные номера могут быть посланы открытым способом, так как на основании них невозможно рассчитать ключи без дополнительной, секретной информации.

Сообщение от клиента защищено проверкой целостности, которая называется **MIC** (**Message Integrity Check – проверка целостности сообщения**), данная проверка основывается на ключе сеанса.

В последнем из двух сообщений AP выдает клиенту общий ключ K_G, и клиент подтверждает подлинность сообщения.

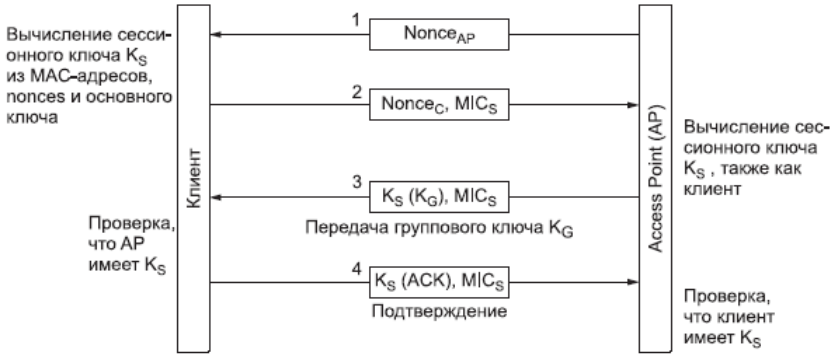

Рисунок 1 – Получение сеансового ключа

В 802.11i могут быть использованы два протокола для обеспечения конфиденциальности, цельности и аутентификации.

1 TKIP (**Temporary Key Integrity Protocol – временный протокол целостности ключа**) был временным решением.

Он был разработан для того, чтобы увеличить безопасность старых и медленных карт 802.11, так что безопасность у него, по крайней мере, выше, чем у WEP.

2 CCMP (Counter mode with Cipher block chaining message authentification code protocol) – режим счетчика с протоколом аутентификации в режиме сцепления обратной связи.

CCMP работает довольно прямым путем. Он использует шифрование AES с помощью ключа и блоков размером 128 бит.

Чтобы обеспечить конфиденциальность, сообщения зашифровываются с помощью AES в режиме счетчика.

Режим счетчика подмешивает счетчик в процесс шифрования сообщения.

Чтобы обеспечить целостность, сообщение, включая поля заголовков, кодируется шифром в режиме обратной связи, и последний блок из 128 бит сохраняется как MIC.

Затем и сообщение, и MIC высылаются. И клиент, и AP могут осуществлять данную кодировку или проверить ее при получении беспроводного пакета.

Алгоритм шифрования для WPA2 основан на **AES (Advanced Encryption Standard – улучшенный стандарт шифрования)**, американском правительственном стандарте, одобренном в 2002 году.

Ключи, которые используются для шифрования, определяются во время процедуры аутентификации.

Порядок выполнения работы

1 В программе Cisco Packet Tracer собрать сеть, представленную на рисунке 2. Для подключения ноутбуков необходимо заменить проводные сетевые платы Ethernet, которые установлены в них по умолчанию, на беспроводные.

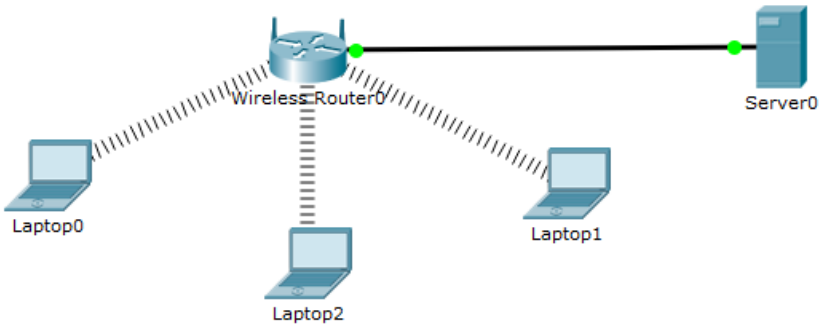

Рисунок 2 – Схема сети

2 Настроить на маршрутизаторе в закладке «Setup» IP-адрес

192.168.100.1/24 и задать в настройках DHCP-сервера стартовый IP-адрес: 192.168.100.2 и максимальное количество подключаемых устройств: 199 (рисунок 3). При этом пул IP-адресов для автоматической раздачи будет находится в диапазоне от 192.168.100.2/24 до 192.168.100.200/24. После этого необходимо нажать на кнопку «Save Settings» в нижней части экрана настроек маршрутизатора.

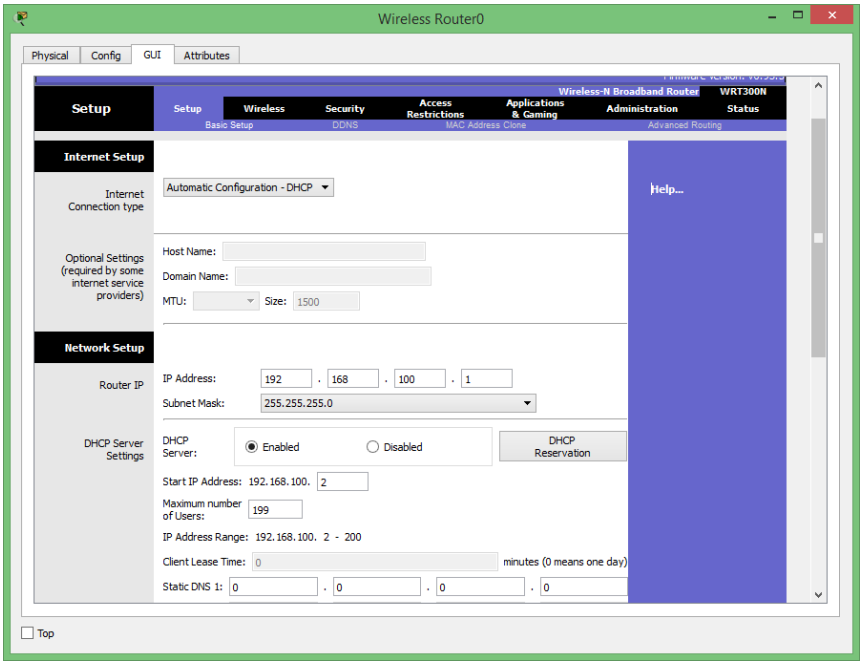

Рисунок 3 – Параметры DHCP-сервера маршрутизатора

3 Серверу, подключенному к маршрутизатору по линии Fast Ethernet необходимо задать стационарный IP-адрес 192.168.100.254/24, а в качестве шлюза по умолчанию указать IP-адрес маршрутизатора.

4 В настройках маршрутизатора в закладке «Wireless» в разделе «Basic Setup» выбрать название сети (SSID). Например, AT&T, как это показано на рисунке 4.

В настройках маршрутизатора в закладке «Wireless» в разделе «Wireless Security» выбрать следующие параметры (рисунок 5):

Security Mode – WPA2 Personal;

Encryption – AES;

Passphrase – пароль минимум из 15 символов, содержащий буквы и цифры.

После этого необходимо нажать на кнопку «Save Settings» в нижней части экрана настроек маршрутизатора.

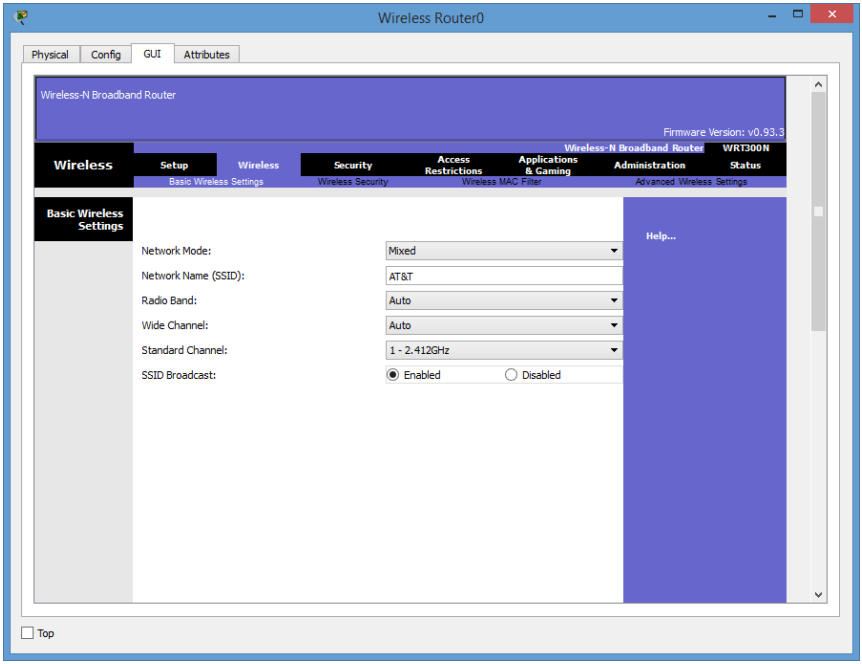

Рисунок 4 – Параметры раздела Basic Setup маршрутизатора

5 Подключить к сети AT&T два ноутбука, как это показано на рисунке 6. После этого необходимо утилитой ping проверить доступность сервера с обоих устройств.

6 Допустим, что владельце ноутбука Laptop1 так же стал известен пароль доступа к сети и он к ней подключился (необходимо выполнить подключение этого ноутбука). Теперь владельце этого ноутбука также доступны внутренние ресурсы сети.

7 Для защиты сервера необходимо определить MAC-адреса двух первых ноутбуков и в настройках маршрутизатора в закладке «Wireless» в разделе «Wireless MAC Filter» указать их в списке MAC-адресов и выбрать следующие параметры (рисунок 7). После этого все ноутбуки отключатся от сети. Повторно подключите к сети AT&T первые два ноутбука, чьи MAC-адреса указаны в параметрах маршрутизатора. Последний ноутбук подключить не получится – он не будет видеть сеть AT&T.

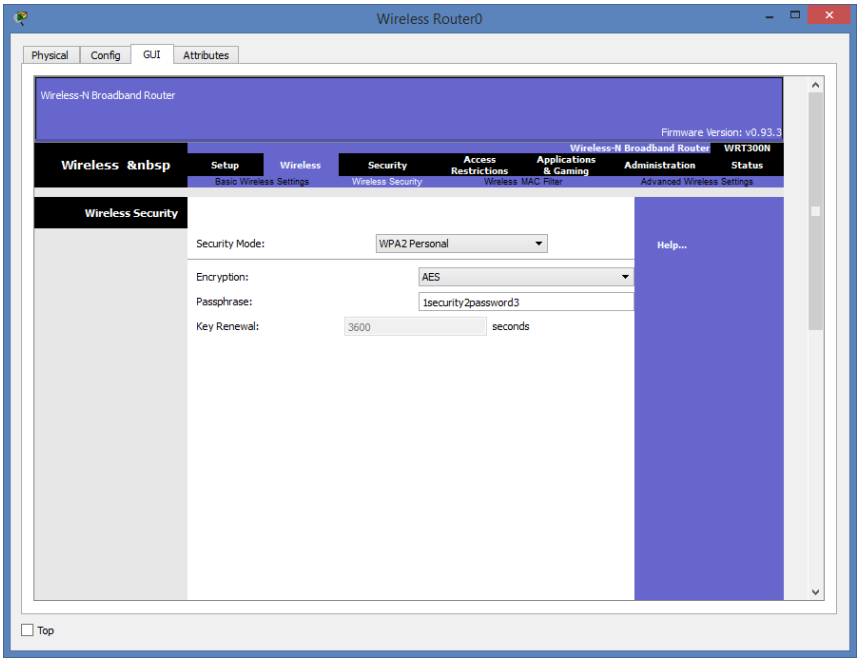

Рисунок 5 – Параметры раздела Wireless Security маршрутизатора

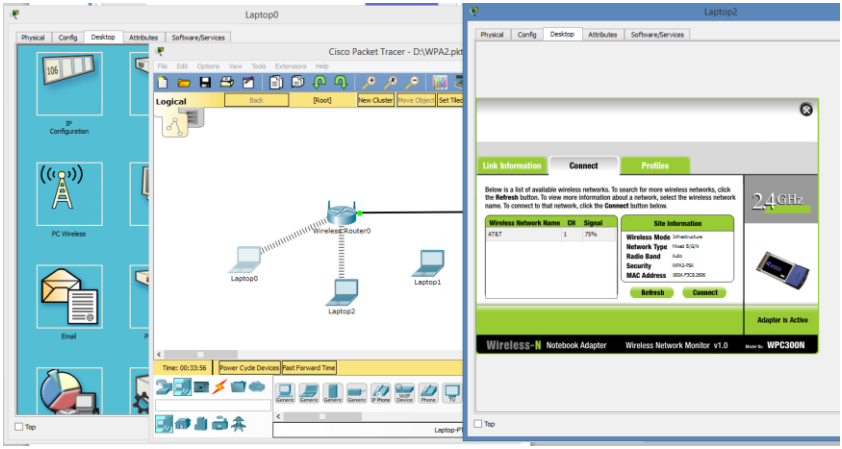

Рисунок 6 – Подключение к сети ноутбуков

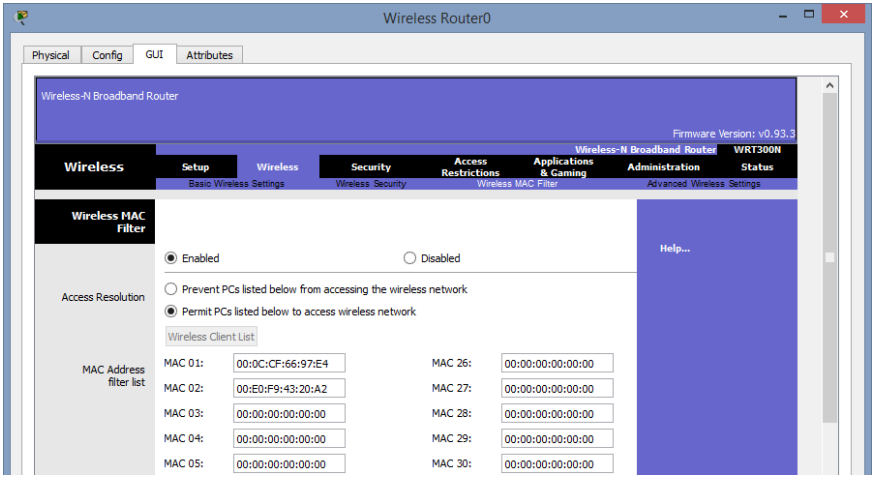

Рисунок 7 – Параметры раздела Wireless MAC Filter маршрутизатора

Содержание отчета

1 Цель работы.
2 Схема сети.
3 Настройки точки доступа.
4 Результаты выполнения утилиты ping с мобильных устройств на IP-адрес сервера.
5 Вывод по работе.

Контрольные вопросы

1 Стандарт IEEE 802.11.
2 Режимы использования беспроводной сети.
3 Частоты ISM-организаций.
4 Сервисы беспроводной сети.
5 Типы шифрования беспроводных сетей.
6 Особенности WPA2.
7 Алгоритм получения сеансового ключа.
8 Протоколы обеспечения конфиденциальности, целостности и аутентификации в Wi-Fi-сетях.