СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

Р.Р. Фаткиева

Основы построения защищенных компьютерных сетей

Беспроводные технологии

СПбГЭТУ «ЛЭТИ», 2021 г.

6. ПОСТРОЕНИЕ ЗАЩИЩЕННОГО СЕГМЕНТА БЕСПРОВОДНОЙ СЕТИ С ИСПОЛЬЗОВАНИЕМ МЕХАНИЗМОВ WPA2

Цель работы: изучение теоретического материала о технологии беспроводной передачи данных, формирование практических навыков применения методов и средств защиты беспроводной ЛВС, являющейся частью корпоративной ЛВС.

6.1 Основные понятия

WI-FI -это беспроводная технология соединения компьютеров в ЛВС с возможностью подключения к сети Internet. Использование таких сетей рекомендуется там, где развертывание кабельной системы невозможно или экономически нецелесообразно, а также имеются мобильные клиенты, которые могут легко перемещаться в рамках действующих зон сети.

Вместе с тем необходимо помнить об ограничениях беспроводных сетей. Это подверженность влиянию помех и более сложная схема обеспечения безопасности передаваемой информации. При анализе безопасности беспроводных ЛВС выделяют следующие основные угрозы [1]:

– несанкционированное подключение к устройствам и сетям;

– неконтролируемое использование инфраструктуры;

– перехват и модификация данных;

– нарушение доступности.

Основными механизмами обеспечения безопасности беспроводной ЛВС являются:

– базовые методы защиты и протоколы аутентификации IEEE 802.11i;

– управление доступом в соответствии со стандартом IEEE 802.1x;

– сегментирование сетей с помощью технологии VLAN;

– межсетевое экранирование.

Перечисленные механизмы ориентированы, как правило, на защиту канального уровня. Защита на более высоких уровнях сетевой модели реализуется механизмы защиты, предусмотренные стеком протокола TCP/IP. При построении ЛВС в защищенном исполнении целесообразно отталкиваться от категории информации, передаваемой в сети и обрабатываемой на

серверах, с учетом норм актуального на заданный момент времени законодательства. В зависимости от него формируются требования безопасности, которым должна удовлетворять ЛВС (сегмент гостевого доступа к сети Интернет, сегмент доступа к сети Интернет с мобильных устройств сотрудников, сегмент доступа к веб-ресурсам общего назначения и сегмент для соединения двух ЛВС с помощью точек доступа).

6.2. Задание

Построить защищенный беспроводной сегмент ЛВС в соответствии со схемой, представленной в практической работе 1, расширяющий инфраструктуру ЛВС и позволяющий организовать подключение пользователей с использованием механизмов WPA2.

6.3. Порядок выполнения работы

1. Подключить беспроводной маршрутизатор к ЛВС (рис 6.1), если он не был подключен в практической работе 4.

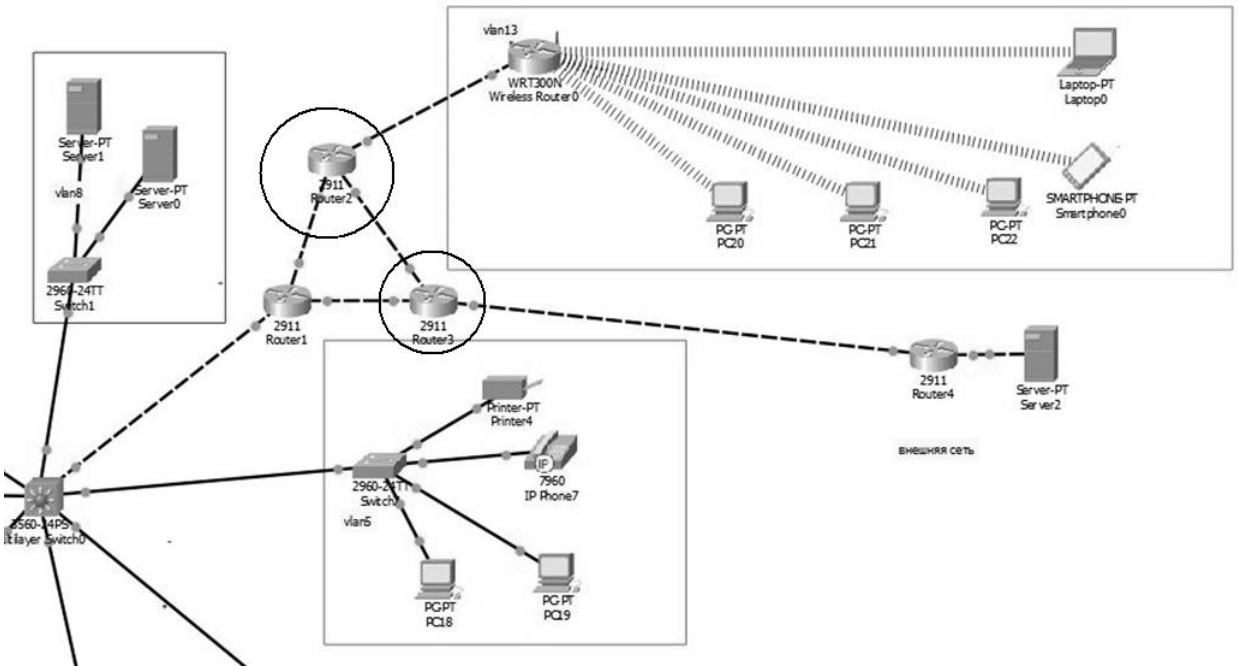

Рис. 6.1

2. Выполнить настройку маршрутизатора Wirelesss Router. Назначить устройству IP-адрес и маску сети из сети управления ЛВС (рис. 6.2).

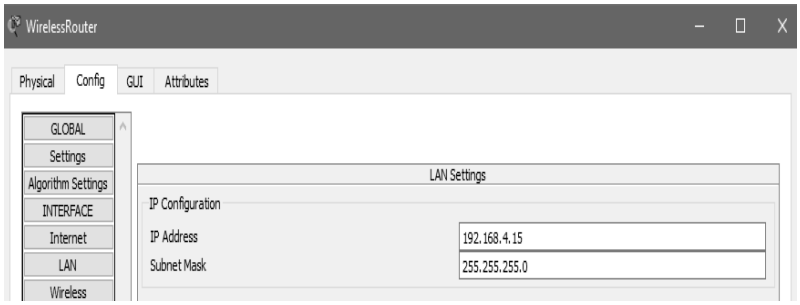

Рис. 6.2

3. К маршрутизатору подключить сервер аутентификации Server AAA.

4. в настройках маршрутизатора назначить идентификатор сети SSID, метод аутентификации – «WPA2» и параметры подключения к серверу RADIUS (IP-адрес 192.168.4.1, shared secret – «secretkey», AES) (Рис. 6.3).

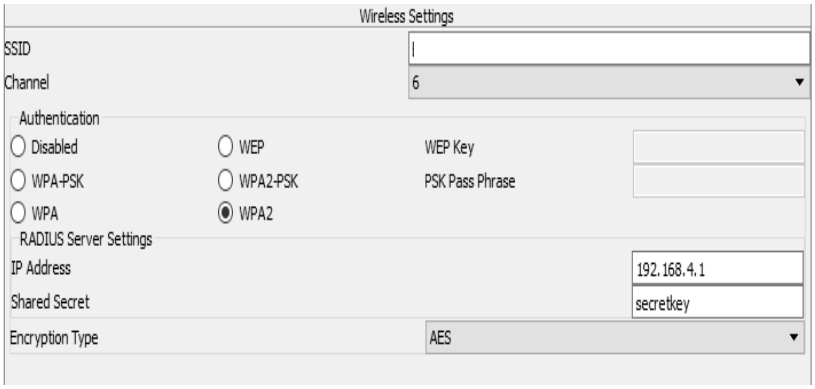

Рис. 6.3

5. На сервере Server AAA создать клиента Wireless Router, задать его сетевые параметры. Создать пользователя для подключения: UserName – «user», Password – «Password» (Рис. 6.4).

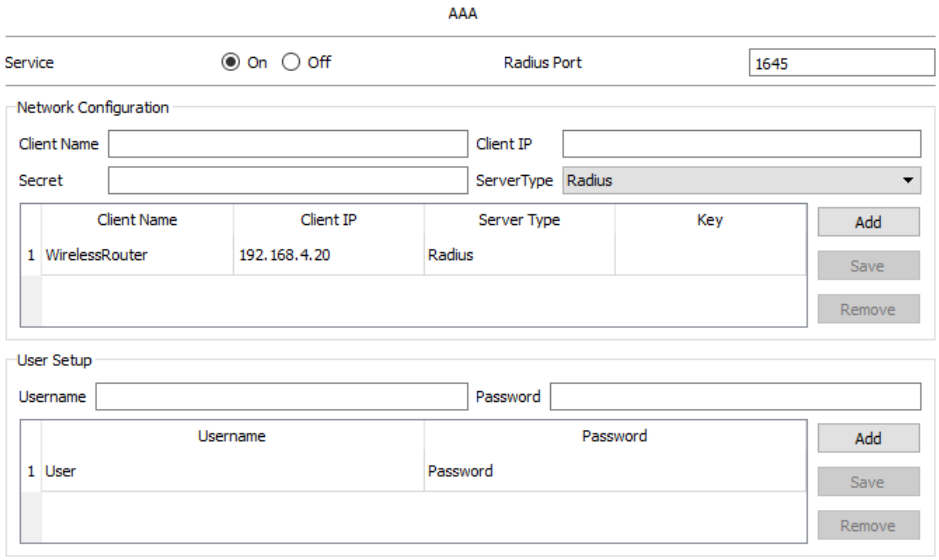

Рис. 6.4

6. На мобильной рабочей станции в параметрах беспроводного подключения указать параметры SSID, метод аутентификации, UserID и Password (Рис. 6.5).

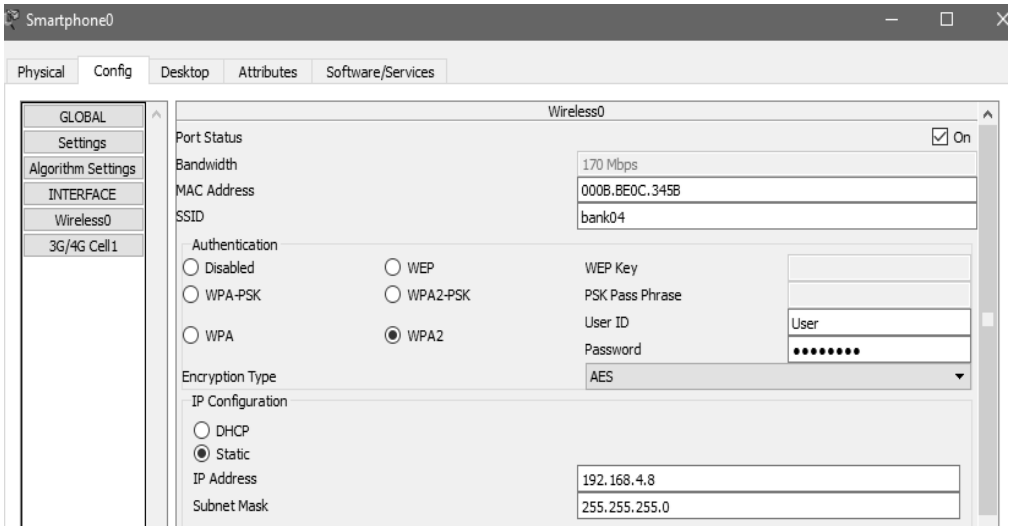

Рис. 6.5

7. Проверить возможность сетевого взаимодействия в ЛВС, например осуществить проверку возможности доступа со смартфона (Рис. 6.6), а также возможность доступа из сегмента сети (Рис. 6.7).

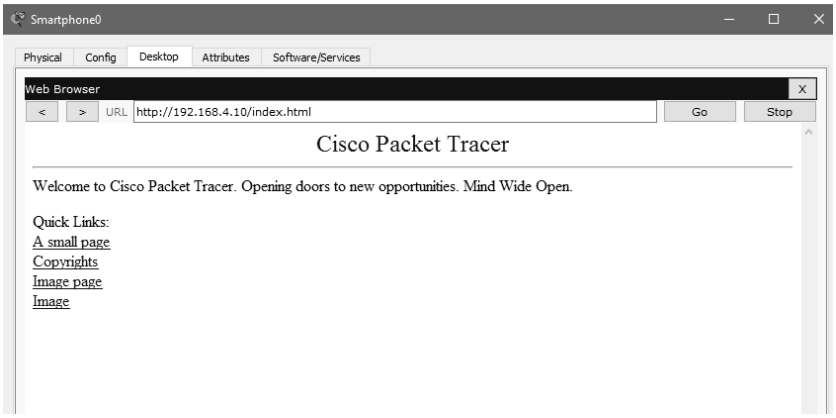

Рис. 6.6

Рис. 6.7

8. В соответствие с действующим законодательством разработать механизмы обеспечения и политику безопасности для каждого сегмента беспроводной ЛВС (для гостевого доступа к сети Интернет, для доступа к сети Интернет с мобильных устройств, доступа к веб-ресурсам общего назначения и соединения двух ЛВС с помощью точек доступа) в соответствии со схемой, представленной в практической работе 1.

3.4. Контрольные вопросы

1. Для чего требуется идентификатор SSID?
2. Как настроить ACL списки доступа на маршрутизаторе Wi-Fi?
3. Для чего необходимы диаграммы направленности антенн? Какие проблемы они выявляют?
4. Почему используется WPA2, если WPA3 обладает более широким спектром методов защиты?

5. Какие атаки возможно реализовать за счет использования атака глушения базовой станции?
6. К какой базовой станции произойдет подключение клиента при нахождении нескольких точек доступа в зоне видимости?

СПИСОК ЛИТЕРАТУРЫ

1. Колегов Д.Н. Лабораторный практикум по основам построения защищенных компьютерных сетей. Томск: Томский государственный университет, 2013. – 140 с.
2. Как настроить маршрутизатор. Электронный ресурс https://www.cisco.com/c/ru_ru/solutions/small-business/resource-center/networking/how-to-set-up-router.html
3. Настройка сопоставления SSID-VLAN на беспроводной точке доступа. Электронный ресурс. https://www.cisco.com/c/en/us/support/docs/smb/wireless/cisco-small-business-100-series-wireless-access-points/smb5172-configure-ssid-to-vlan-mapping-on-a-wireless-access-point.html.
4. Димарцио Д. Ф. Маршрутизаторы Cisco. Пособие для самостоятельного изучения. – Пер. с англ. – СПб: СимволПлюс, 2003. – 512 с., ил