МГТУ им. Н. Э. Баумана
Кафедра «Системы обработки информации и управления»

Методические указания к лабораторным работам по дисциплине Сетевые технологии в АСОиУ.

Лабораторная работа №3.

Беспроводные сети.

Для студентов 3-го курса кафедры ИУ5

Разработал: ст. преподаватель
Антонов А. И.

Москва 2024 г.

Содержание

Цель работы

Закрепление теоретических знаний и развитие практических навыков проектирования беспроводных локальных сетей. Приобретение навыков защиты беспроводной сети.

Необходимое оборудования

Персональный компьютер, система CiscoPacketTracerверсии не ниже 5.0. (Примеры выполнения работы приведены для версии CiscoPacketTracer8.0.1)

Задание

Построить сеть из двух сегментов, первый состоит из D рабочих станций и RADIUS сервера, вторая состоит из E рабочих станций соответственно.Каждый сегмент построен на базе точки доступа Linksys. Обе точки доступа подключены к маршрутизатору, к которому, в свою очередь, подключен сервер. Необходимо задать IP адреса сетевым интерфейсам маршрутизаторов, сервера и локальных компьютеров.

Первая сеть содержит D рабочих станций и сервер, подключенный с помощью витой пары. Сеть защищена по технологии WPA. Сервер является RADIUS сервером. Выдать каждой рабочей станции свой уникальный логин и пароль для подключения к точке доступа. На точке доступа включена фильтрация Telnet и FTP трафика.

Вторая сеть защищена по технологии WPA2-PSK на основе шифрования AES. Идентификатор сети скрыт. На точке доступа включена фильтрация HTTP трафика и включен белый список MAC адресов подключаемых станций. Необходимо добиться возможности пересылки данных по протоколу ICMP между устройствами внутри сетей и сервером. Продемонстрировать невозможность прохождения запрещенного трафика и невозможность подключения станций, не внесенных в белый список.

Дополнительное задание ЛР3.

В любую из беспроводных сетей добавить DNS сервер, прописать внем DNS запись для Server0 и настроить доступность Server0 по указанномуимени с сохранением ограничений которые есть в основной ЛР.

Требования

1. IP адреса первого сегмента задаются статически и находятся в диапазоне 192.16x.100+F.y, где F выбирается согласно варианту, x номер учебной группы, а y —произвольное число
2. IP адресаторогосегментатакже задаются статически и находятсявдиапазоне192.16x.200+F.y.

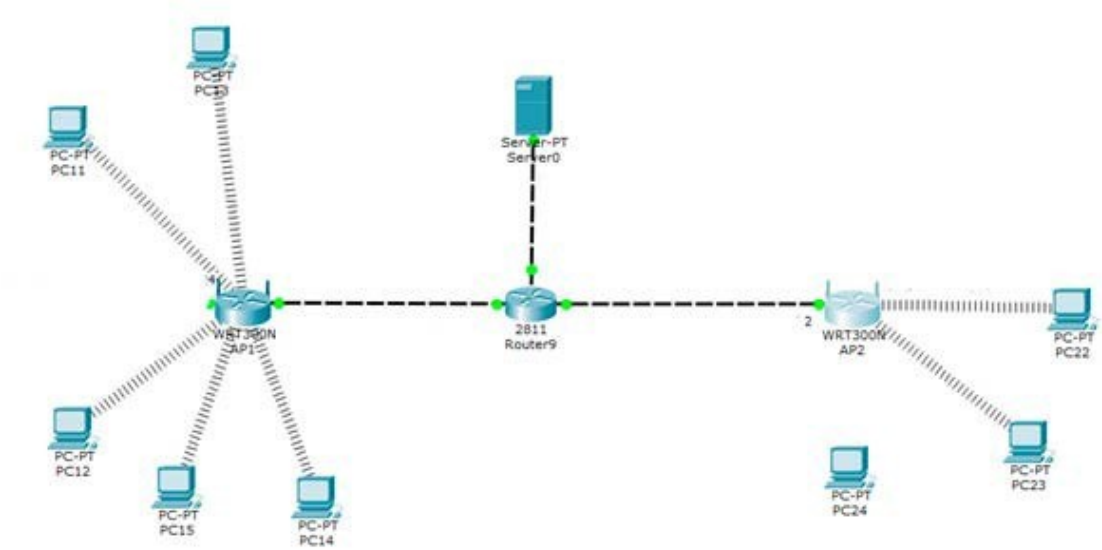

Рисунок 1. Общая схема сети

Теоретические сведения

Wi-Fi — это стандарт беспроводного подключения LAN для коммуникации разных устройств, относящийся к набору стандартов IEEE 802.11. Wi-Fi использует радиоволны (так же, как Bluetooth и сотовые сети) для коммуникации устройств в малом масштабе.Основные стандарты WiFi – 802.11a, 802.11n,802.11ac,802.11ax. Сеть WiFiопределяет её идентификатор (SSID) и канал, на котором роутер ведёт вещание. Всего для 2.4 ГГц полосы используются 11 каналов, в некоторых стандартах расширяется до 13 или 14.

Защита беспроводных технологий стала отдельной задачей – поскольку теперь 3-и лица не имеют необходимости в полном физическом доступе к сети, достаточно

относительной близости. В 1997 году технология WEP является первой попыткой защиты беспроводных сетей.WEP шифрует трафик с использованием 64 или 128-битного ключа в шестнадцатеричном формате. WPA (Wi-Fi Protected Access) – это появившийся в 2003 году протокол, которым объединение Wi-Fi Alliance заменило протокол WEP.Протокол WPA2 появился в 2004 году. Он является обновленной версией WPA. Для крупных компаний и сложных сетей становится ненадёжным использовать пароль – поэтому существуют EAPверсии протоколов – где отдельный сервер выполняет функцию надзора за сетью, и каждый пользователь имеет свой уникальный логин/пароль.

Порядок выполнения лабораторной работы

Порядок выполнения лабораторной работы

1. Собрать схему сети. Обратите внимание, что ПК соединены по беспроводной сети.Для этого на ПК должна быть возможность использования беспроводной сети. Требуется добавить модуль, содержащий данные порты.

   Добавить модуль можно сделать по следующему алгоритму:

   a. Откройте окно настройки ПК. Выберите вкладку «Physical»
   b. Выключите ПК, нажав кнопку питания (см. рисунок 2, выделено красным)
   c. Перетащите модуль, содержащий антенну (см. рисунок 2, выделено синим), в свободную ячейку маршрутизатора
   d. Включите ПК

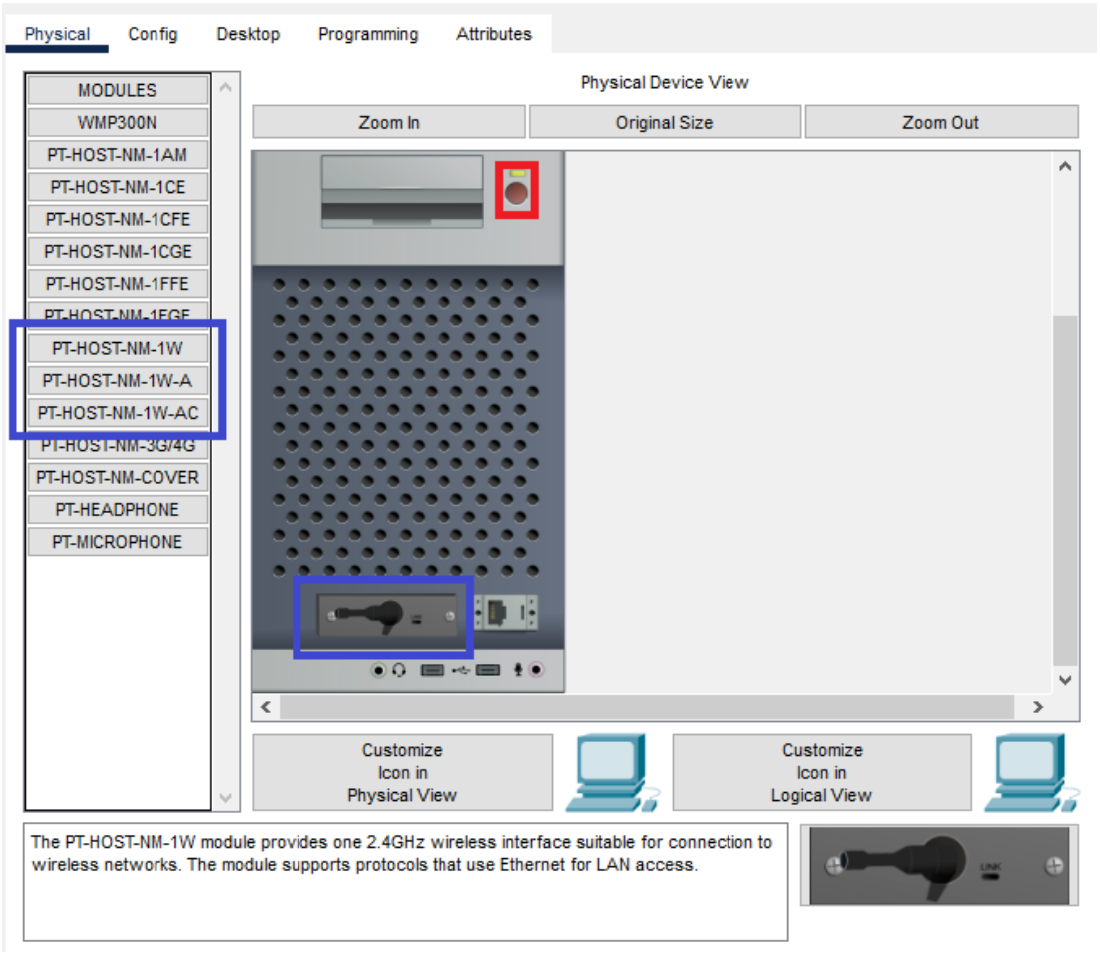

Рисунок 2. Настройка PC

2. Настройте ipадреса сети в соответствии с требованиями. Добейтесь пересылки пакетов от рабочих станций до внутренних интерфейсов роутеров.

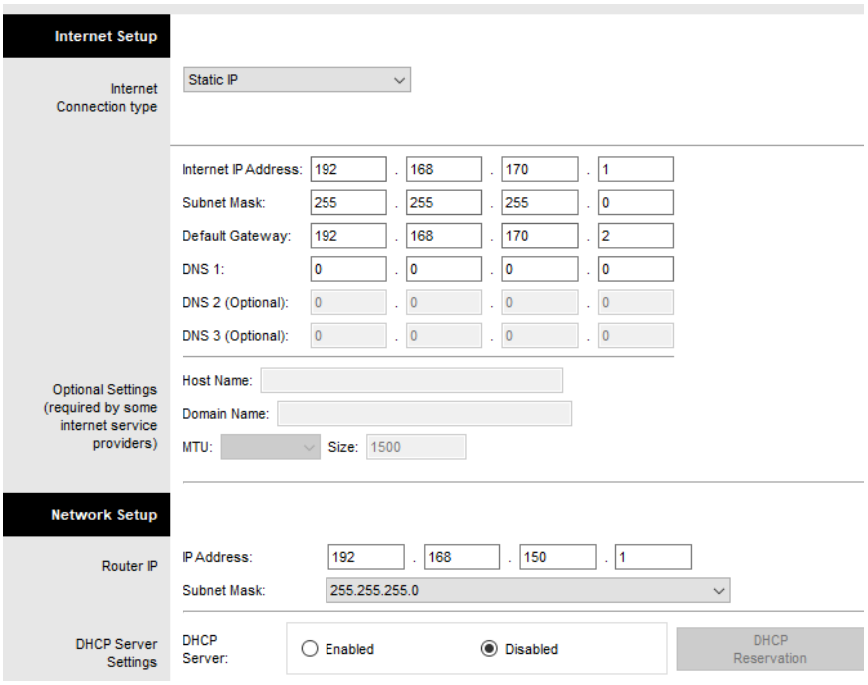

Рисунок 2. Настройка сети в wrt300n.

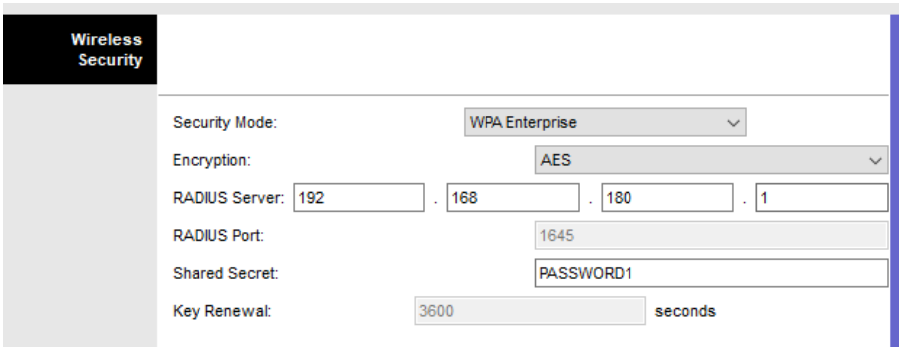

Рисунок 3. Настройка безопасности

3. Настройка RADIUS. Откройте настройки сервера. Во вкладке «Services», подразделе «AAA», введите как клиента параметры сети 1, и добавьте пользователей по количеству PC.

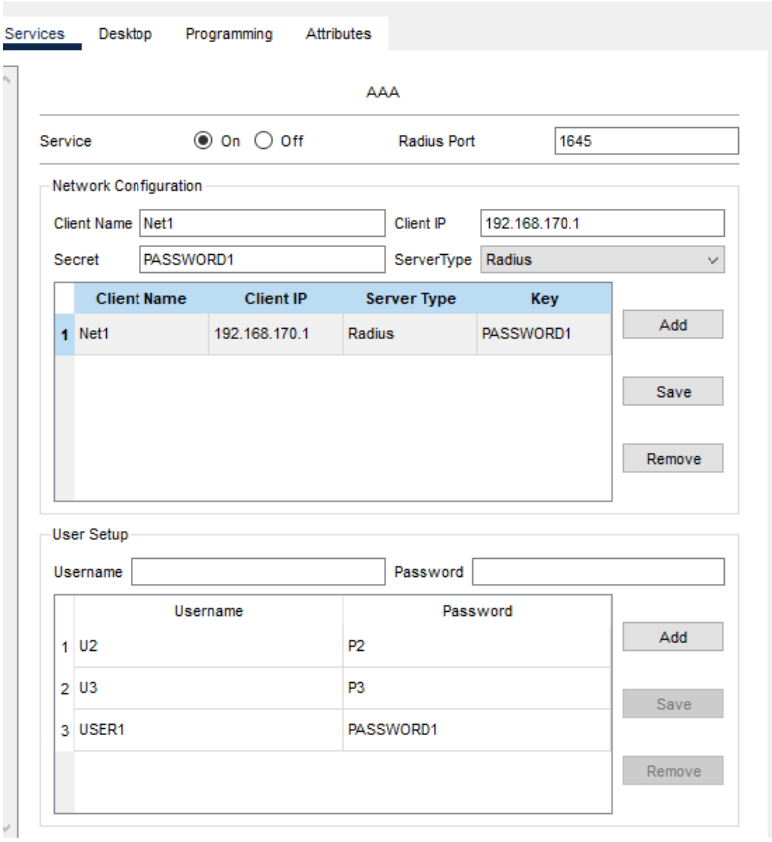

Рисунок 4. Настройка RADIUS.

4. Настройте точку доступа для сети 2. Сначала укажите название и скрытие SSIDкак на рис.5.

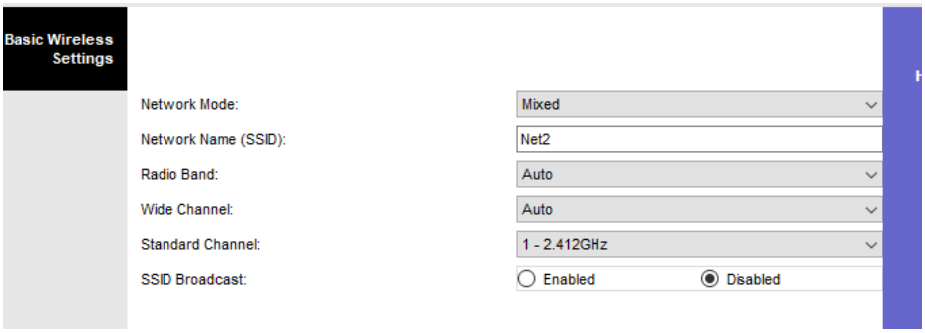

Рисунок 5. Настройка Сети 2.

ПослеукажитезащитуWPA2-Personal (pre shared key) вразделеsecurity.

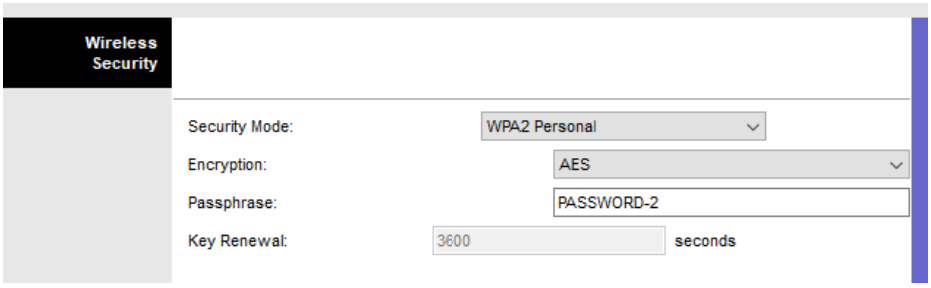

Рисунок 6. Настройка WPA2-PSK.

Настройте MAC-лист как на рисунке 7. Укажите все адреса ПК из Сети 2.

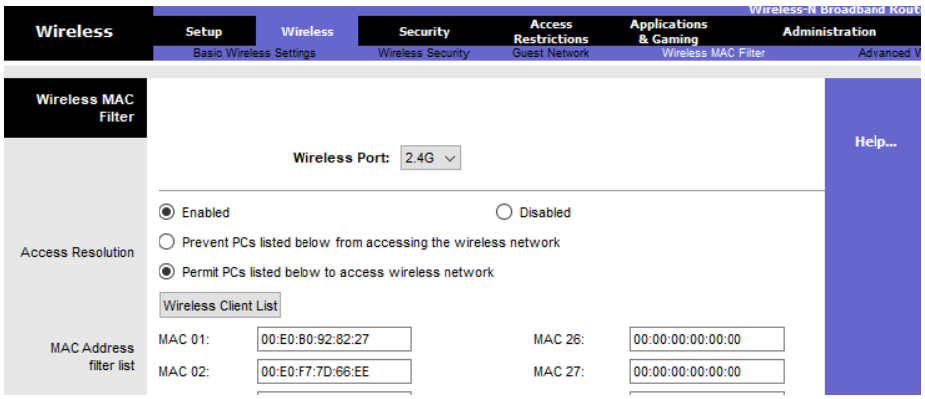

Рисунок 7. Настройка Уайт-листа.

5. Создайте политики фильтрации трафика для сетей 1 и 2 по примеру, указанному на рис. 8. В список блокированных приложений внесите соответствующие для сетей 1 и 2.

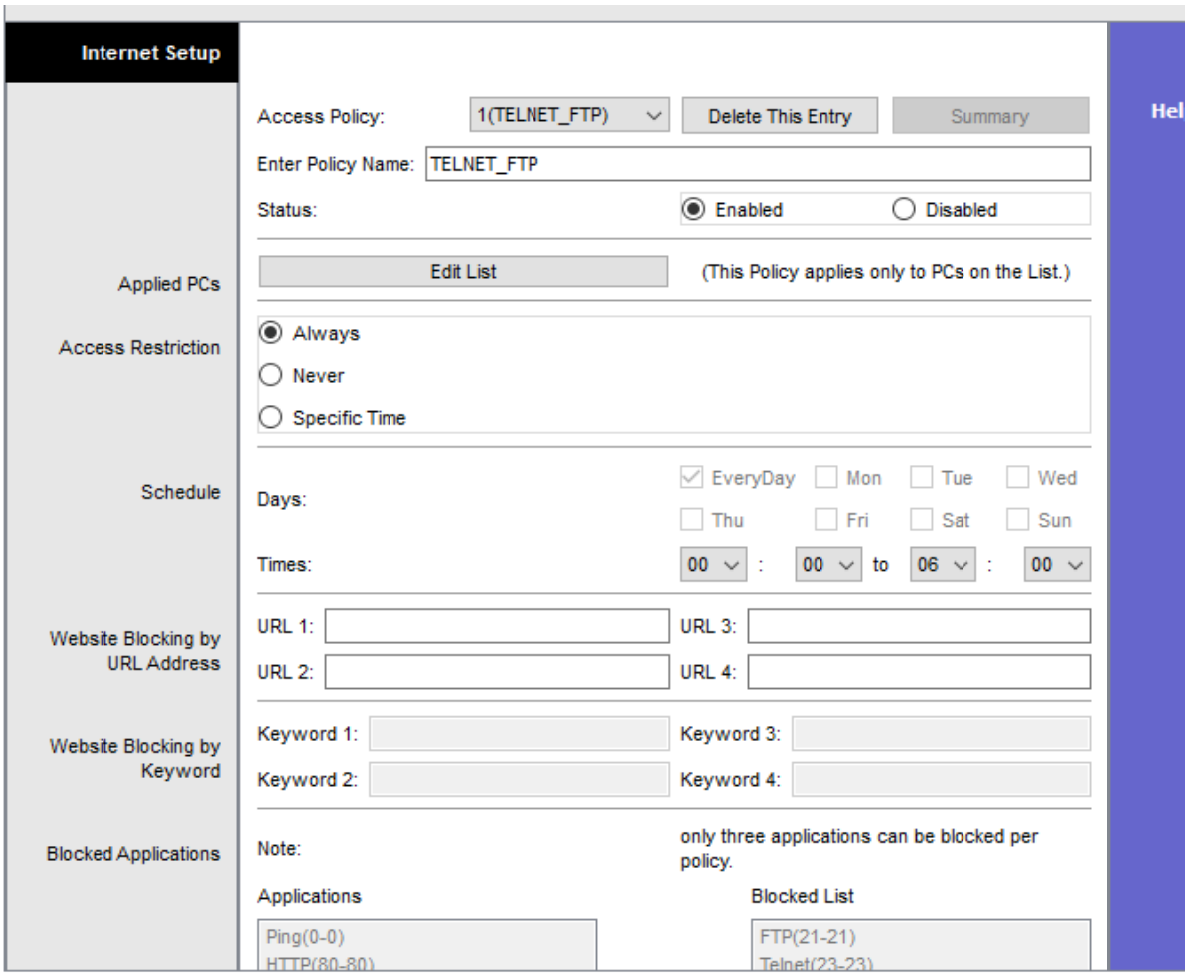

Рисунок 8. Настройка фильтрации трафика.

6. Скопируйте ПК из сети 2 и назначьте ему валидный IP-адрес. Если белый список был настроен правильно, он не сможет подключиться к сети 2.

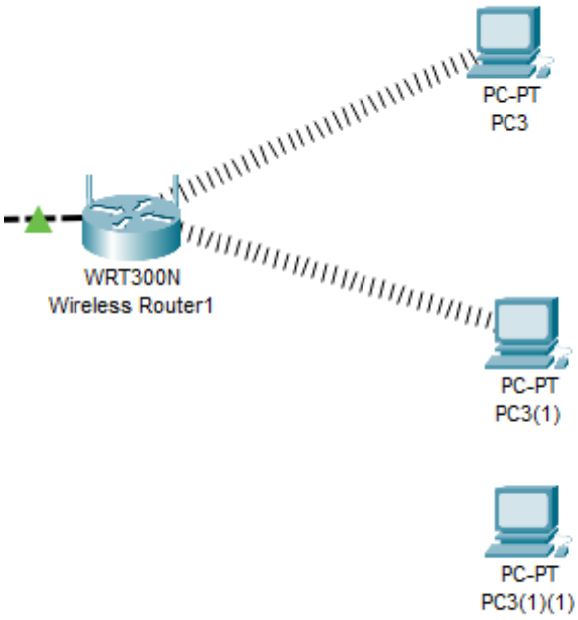

Рисунок 9. Проверка Уайт-листа.

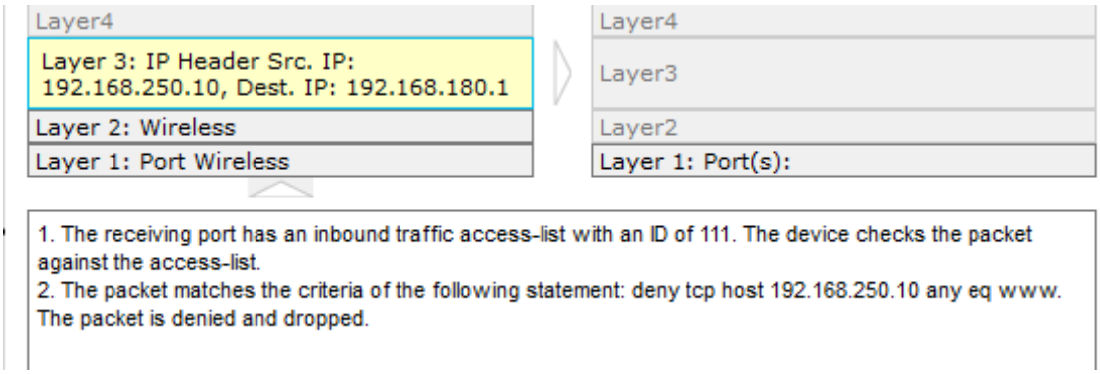

Рисунок 10. Проверка фильтрации траффика.

Контрольные вопросы

1. Что такое SSID сети?
2. Протоколы WPAи WPA-PSK – в чём различие?
3. Зачем нужна фильтрация по MAC-адресам?
4. RADIUS – принцип работы.
5. AAA – что значит аббревиатура?
6. Является ли сокрытие SSIDсети достаточной мерой безопасности?
7. Какие порты используют HTTP, TELNET, FTP?
8. Как работает DNS?