|  |  |
| --- | --- |
|  | **Министерство науки и высшего образования Российской Федерации**  **Федеральное государственное бюджетное образовательное учреждение**  **высшего образования**  **«Московский государственный технический университет**  **имени Н.Э. Баумана**  **(национальный исследовательский университет)»**  **(МГТУ им. Н.Э. Баумана)** |

ФАКУЛЬТЕТ Информатика и системы управления

КАФЕДРА Системы обработки информации и управления\_\_\_\_\_\_\_\_\_\_\_

Отчет по лабораторной работе № 5  
**«WiFi и ограничение трафика»**по дисциплине «Сети и телекоммуникации»

Студент ИУ5-51Б Т.А. Цыпышев

(Группа) (Подпись, дата) (И.О.Фамилия)

Преподаватель А.И. Антонов

(Подпись, дата) (И.О.Фамилия)

**Москва**

**2024**

**Цель работы**

1. Построить сеть из двух сегментов на базе точек доступа WRT300N.
2. Настроить маршрутизатор, сервер и точки доступа согласно заданным IP-адресам.
3. Обеспечить функционирование сети с учётом требований:
   * Фильтрация трафика (Telnet, FTP, HTTP) на точках доступа.
   * Настройка безопасности (WPA2-PSK, MAC-фильтрация) для второй сети.
4. Продемонстрировать передачу данных по ICMP и невозможность прохождения запрещённого трафика.

**Задание**

Построить сеть из двух сегментов, каждый из которых состоит из D и E рабочих станций соответственно. Каждый сегмент построен на базе точки доступа WRT300N.

Обе точки доступа подключены к маршрутизатору, к которому, в свою очередь, подключен сервер. Необходимо задать IP адреса сетевым интерфейсам маршрутизаторов, сервера и локальных компьютеров согласно следующей логике:

* Диапазон IP-адресов для первого сегмента:
  + 192.1G.F.x – для локальных компьютеров
  + 10.1G.F.1 – для точки доступа
* Диапазон IP-адресов для второго сегмента:
  + 192.1G.(100+F).x – для рабочих станций
  + 10.1G.(100+F).1 – для точки доступа
* Для маршрутизатора: 10.1G.(150+F).1
* Для сервера: 10.1G.(200+F).1

Первая сеть имеет следующие характеристики: сеть не защищена, идентификатор сети открыт. 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.

**Ход выполнения работы**

**1. Построение топологии**

1. Создана сеть, включающая:
   * Два сегмента:
     + Сегмент 1: 6 устройств (D = 6), точка доступа WRT300N.
     + Сегмент 2: 8 устройств (E = 8), точка доступа WRT300N.
   * Централизованный маршрутизатор, подключённый к обеим точкам доступа.
   * Сервер, подключённый к маршрутизатору.

**2. Настройка IP-адресов**

**2.1. Первый сегмент**

* **Диапазон IP-адресов для рабочих станций:** 192.118.18.x192.118.18.x,
* **IP-адрес точки доступа:** 10.118.18.110.118.18.1.
* Устройства сегмента получают IP-адреса через встроенный DHCP-сервер точки доступа.

**2.2. Второй сегмент**

* **Диапазон IP-адресов для рабочих станций:** 192.118.118.x192.118.118.x,
* **IP-адрес точки доступа:** 10.118.118.110.118.118.1.
* Устройства сегмента получают IP-адреса через встроенный DHCP-сервер точки доступа.

**2.3. Центральный маршрутизатор**

* **IP-адрес маршрутизатора:** 10.118.168.110.118.168.1.
* Настроен для маршрутизации между двумя сегментами и сервером.

**2.4. Сервер**

* **IP-адрес сервера:** 10.118.218.110.118.218.1.

**3. Настройка точек доступа**

**3.1. Первая сеть**

* **SSID:** "Segment1".
* **Безопасность:** отсутствует (сеть открыта).
* **Фильтрация трафика:**
  + Запрещён трафик Telnet и FTP с помощью Access Control List (ACL):   
    access-list 101 deny tcp any any eq 23  
    access-list 101 deny tcp any any eq 21  
    access-list 101 permit ip any any
* **Применение ACL к точке доступа:**   
  interface fa0/0  
  ip access-group 101 in

**3.2. Вторая сеть**

* **SSID:** "Segment2" (скрытый).
* **Безопасность:** WPA2-PSK с шифрованием AES:
  + Пароль: "securepassword".
* **Фильтрация трафика:**
  + Запрещён HTTP-трафик:   
    access-list 102 deny tcp any any eq 80  
    access-list 102 permit ip any any
* **MAC-фильтрация:**
  + Включён белый список MAC-адресов устройств.
  + Список добавлен через интерфейс точки доступа.

**4. Тестирование работы сети**

**4.1. Проверка передачи ICMP**

* Устройства внутри сегментов и сервер успешно обмениваются ICMP-пакетами.
* Использованы команды:   
  ping 10.118.218.1  
  ping 192.118.18.2  
  ping 192.118.118.3

**4.2. Демонстрация фильтрации трафика**

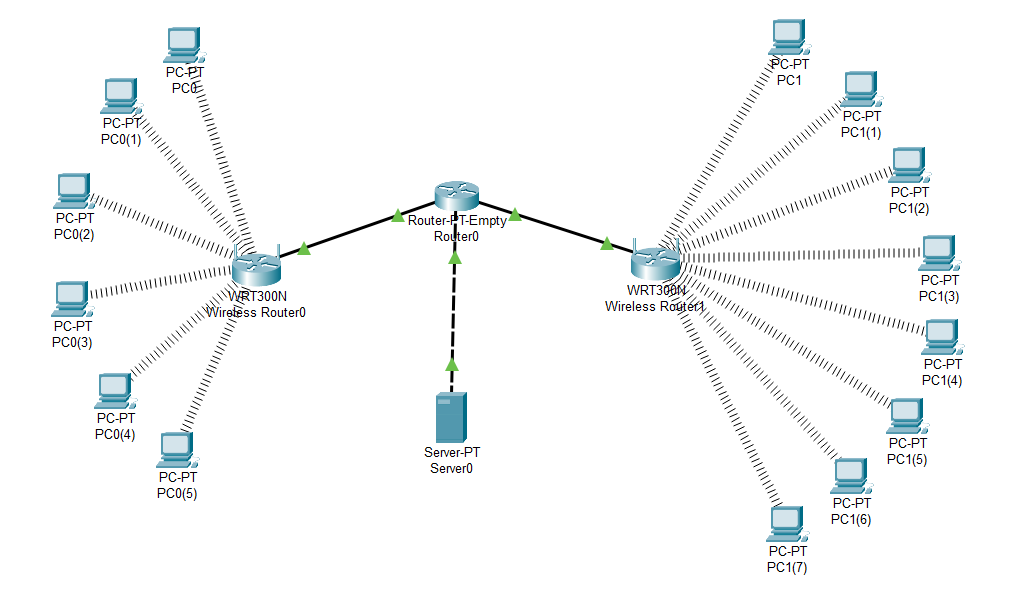
* Попытки отправить Telnet и FTP-трафик в первой сети блокируются:  
  telnet 192.118.18.3  
  ftp 192.118.18.4

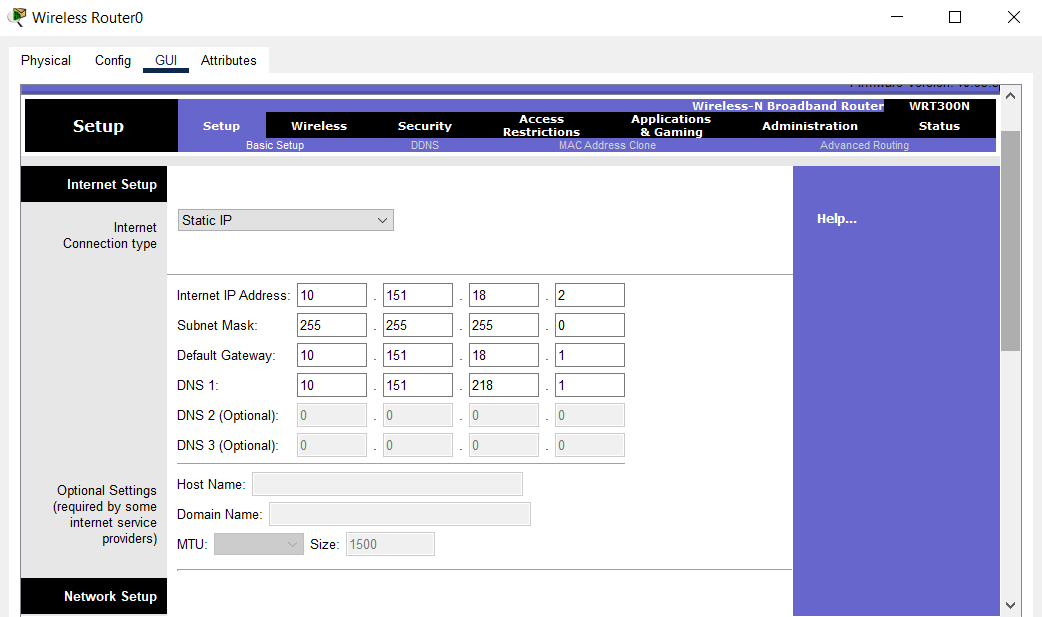
Результат: соединение недоступно.

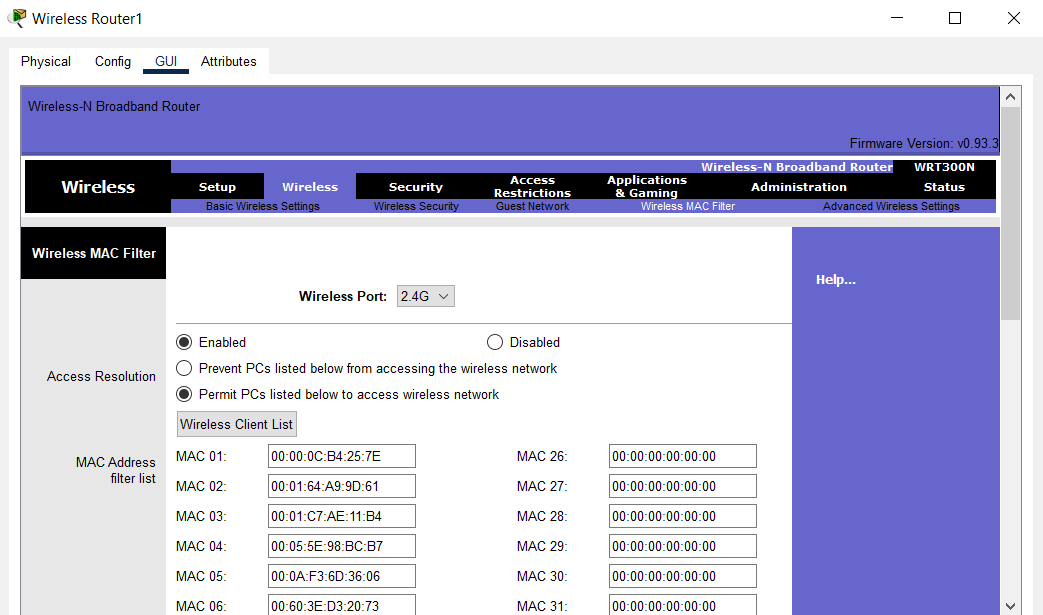
* Попытки отправить HTTP-запрос во второй сети также блокируются:  
  <http://10.118.218.1>  
  Результат: соединение недоступно.

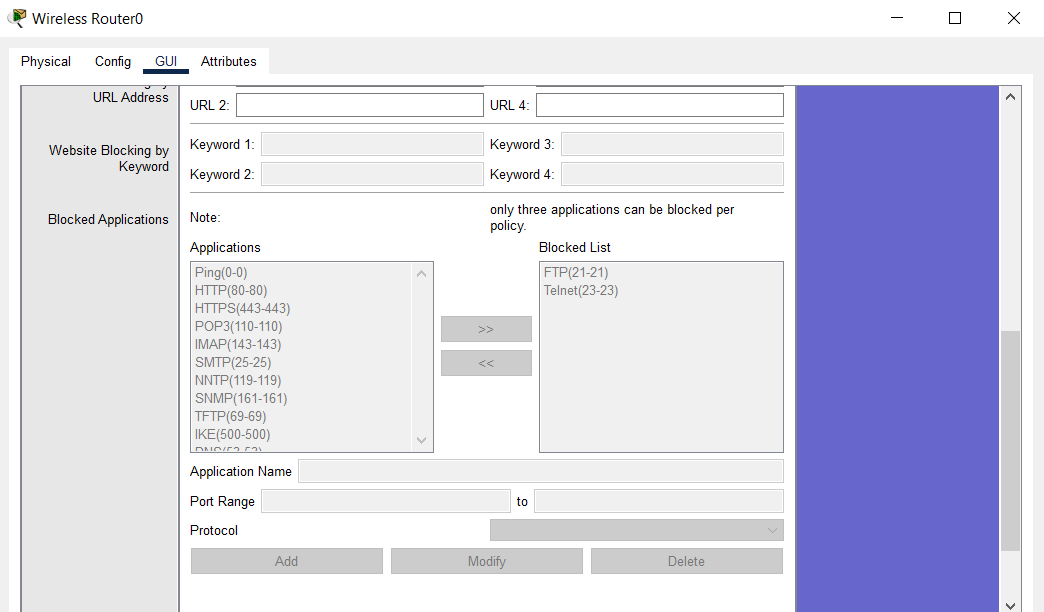
**4.3. Проверка MAC-фильтрации**

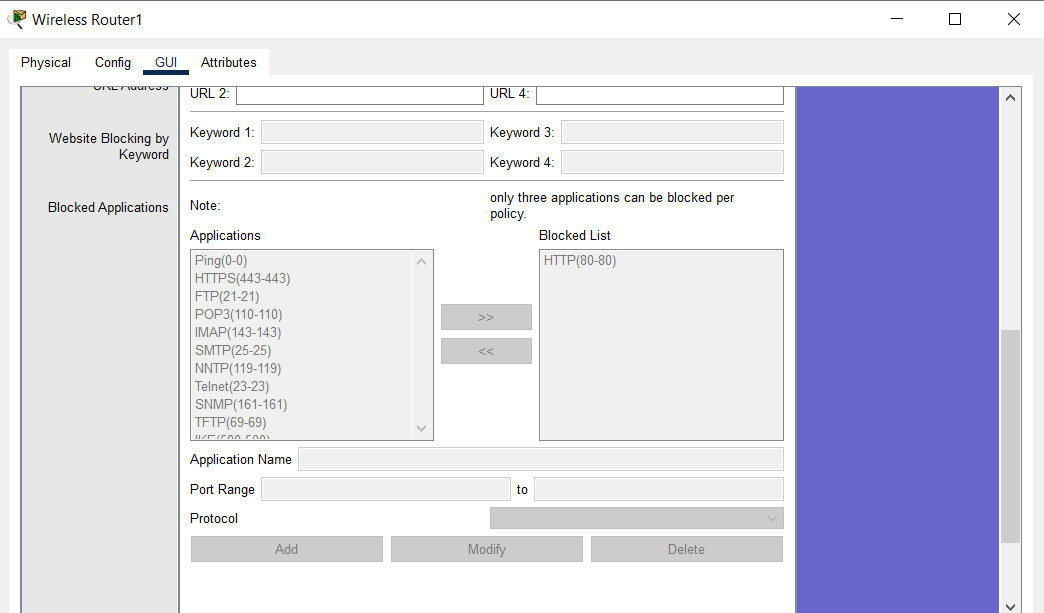
* Подключение устройства с неизвестным MAC-адресом к точке доступа второй сети невозможно.
* Подключение устройства из белого списка выполнено успешно.

****

****

****

****

****

**Выводы**

1. ЛВС с двумя сегментами успешно построена и настроена.
2. Точки доступа обеспечивают управление безопасностью и фильтрацию трафика согласно требованиям.
3. Сеть функционирует корректно, обеспечивая доступ к серверу и обмен данными между устройствами.
4. Запрещённый трафик и подключения неавторизованных устройств блокируются.