**Московский государственный технический университет**

**им. Н.Э. Баумана**

**(МГТУ им. Н.Э. Баумана)**

**Кафедра «Системы обработки информации и управления» (ИУ5)**

Лабораторная работа № 5

По дисциплине: «Сети и телекоммуникации»

# «WiFi и ограничение трафика»

Выполнил: Шакиров Т,

студент группы ИУ5-55Б

Вариант 18

г. Москва, 2024 г.

**Цель работы**

Закрепление теоретических знаний в области конструирования и исследования беспроводных локальных сетей. Изучение программы Cisco Packet Tracer 8.2, а также приобретение практических навыков проектирования и моделирования работы сети, а также оценки принятых проектных решений. Изучение способов организации сети на точках доступа Linksys.

**Задание**

Построить сеть из двух сегментов, каждый из которых состоит из 5 и 7 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:

* 192.155.18.x – для локальных компьютеров
* 10.155.18.1 – для точки доступа

Диапазон IP-адресов для второго сегмента:

* 192.155.118.x – для рабочих станций
* 10.155.118.1 – для точки доступа

Для сервера: 10.155.218.1

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 работы**

Построим сеть, состоящую из двух сегментов с соответствующим количеством ПК, а также 2 точками доступа, сервером и маршрутизатором.

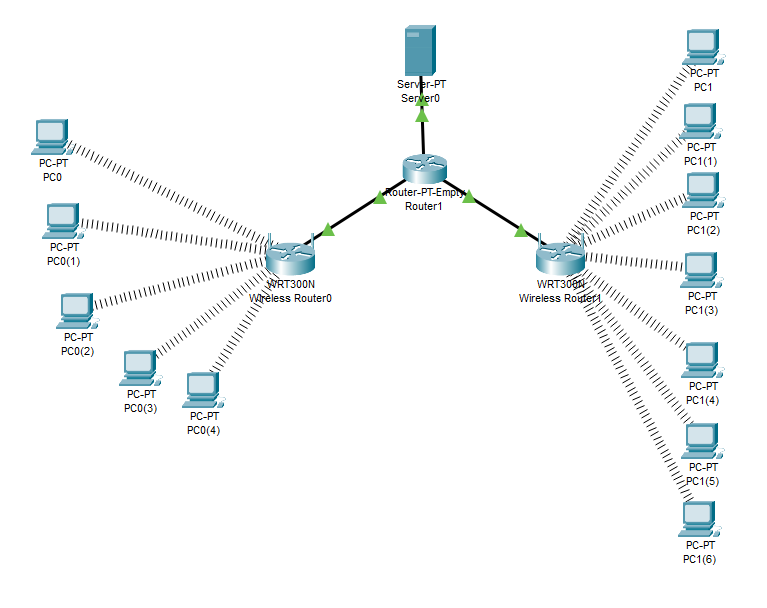


Рисунок 1 – требуемая структура сети.

Выполним настройку WiFi сети на первой точке доступа в соответствии с заданием: сеть не защищена, идентификатор сети открыт.

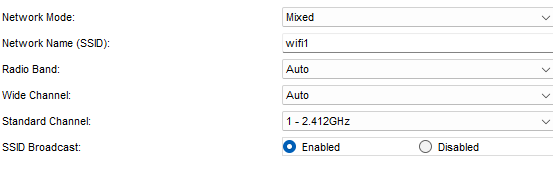


Рисунок 2 – настройки WiFi сети на первой точке доступа.

Настроим IP на интерфейсе маршрутизатора, а также сеть на точке доступа в соответствии с вариантом.

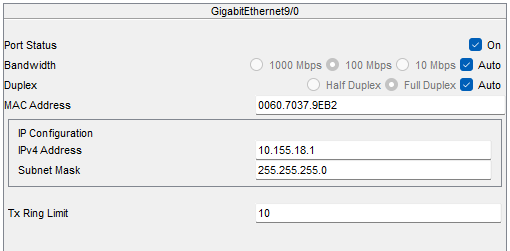


Рисунок 3 – настройки IP на интерфейсе маршрутизатора.

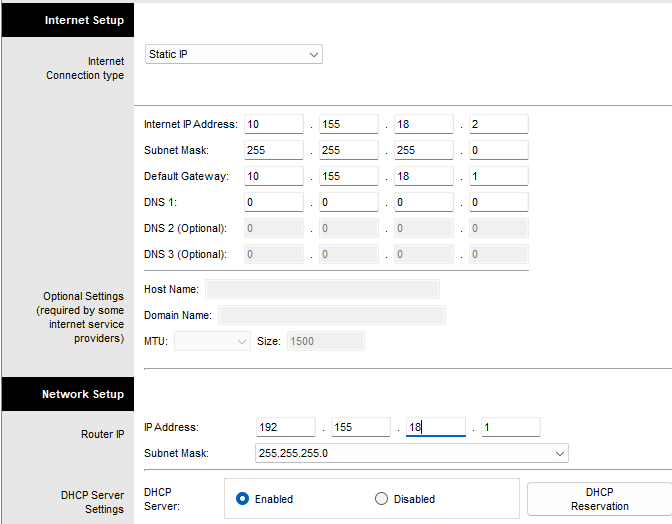


Рисунок 4 – настройки сетей в интерфейсе точки доступа.

Настроим ограничения трафика на точке доступа.

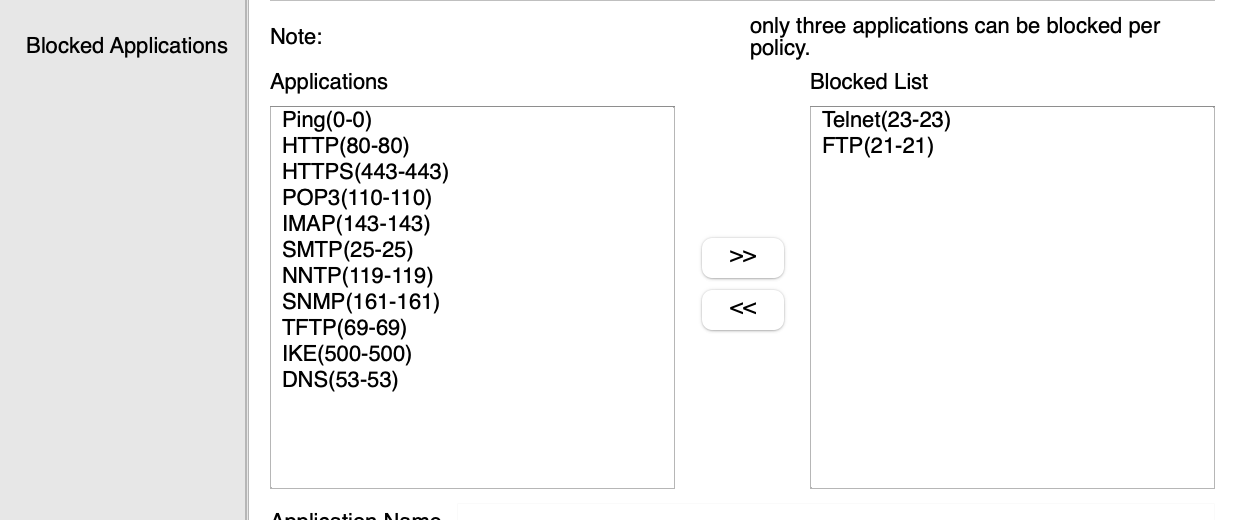


Рисунок 5 – ограничения доступных приложений для клиентов точки доступа.

Добавим требуемое количество клиентов и подключим их к точке доступа.

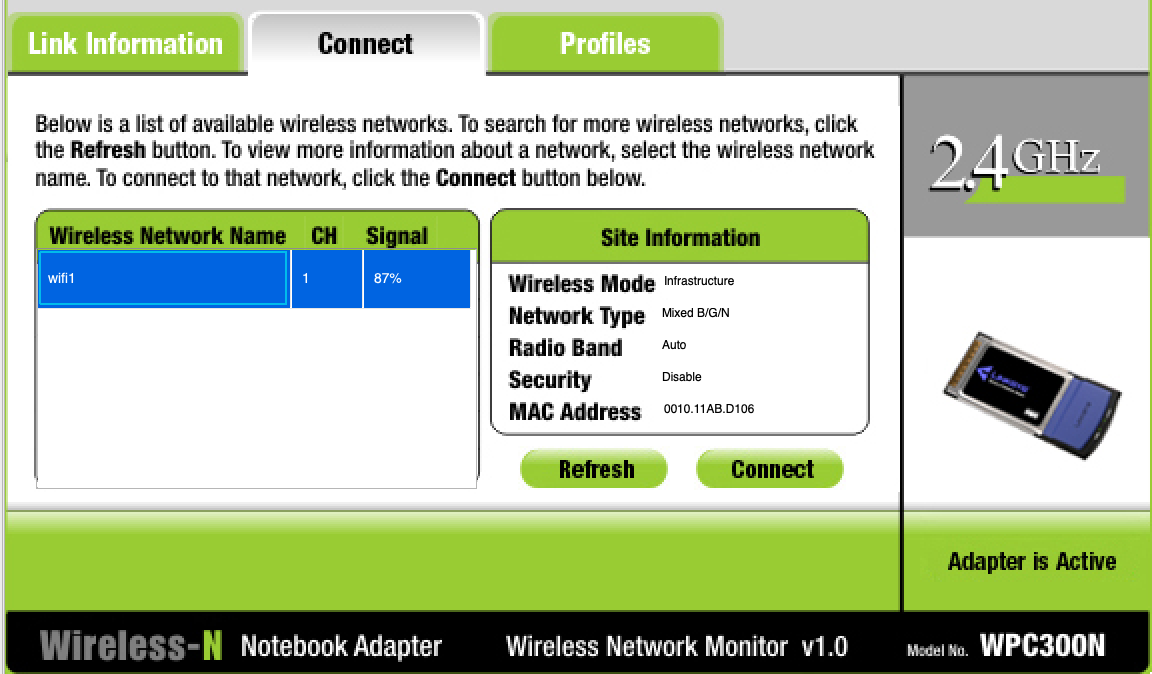


Рисунок 6 – настройки WiFi адаптера ПК.

Проверим, что ICMP трафик доходит до маршрутизатора, а FTP – нет.

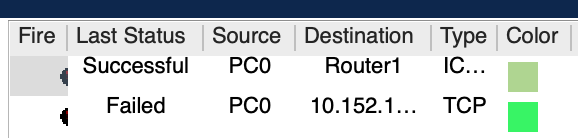


Рисунок 7 – результат отправки пакетов.

Выполним настройку WiFi сети на второй точке доступа в соответствии с заданием: защищена по технологии WPA2-PSK на основе шифрования AES, идентификатор – скрыт. IP интерфейса и сеть точки доступа настраиваются аналогично.

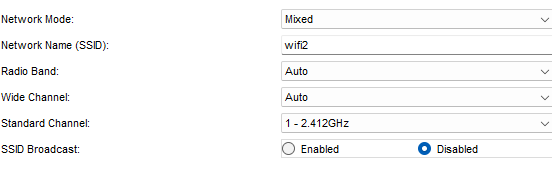


Рисунок 8 – настройки WiFi сети второй точки доступа.

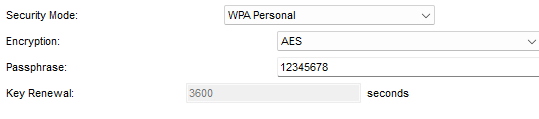


Рисунок 9 – настройки безопасности WiFi сети второй точки доступа.

Аналогично запретим передачу HTTP трафика.



Рисунок 10 – ограничения доступных приложений для клиентов точки доступа.

Добавим 7 компьютеров и ограничим им доступ к WiFi сети по MAC-адресам.

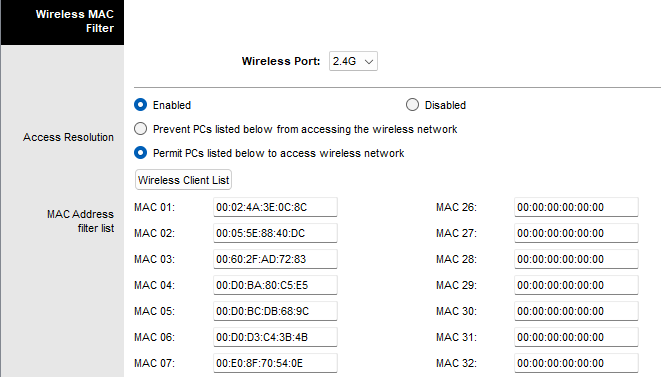


Рисунок 11 – настройки фильтрации MAC адресов.

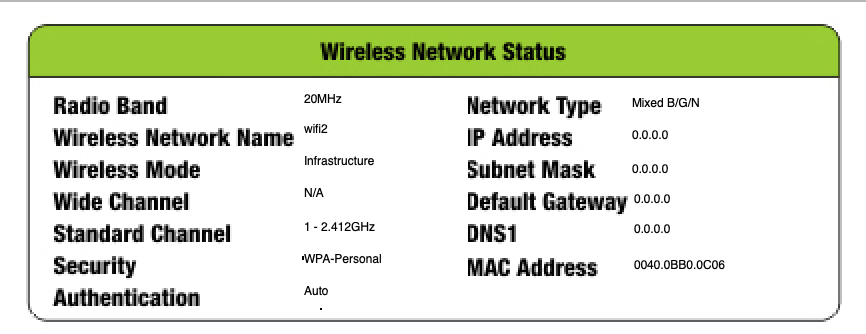


Рисунок 12 – настройки WiFi в компьютере с разрешенным MAC адресом.

Добавим компьютер, который не находится в списке разрешенных и убедимся, что он не подключится к WiFi.



Рисунок 13 – настройки WiFi в компьютере с неразрешенным MAC адресом.

Подключим сервер к маршрутизатору и зададим ему IP.



Рисунок 14 – настройки IP для сервера.

Настроим RIP в маршрутизаторе для обеспечения доступа к серверу и убедимся, что пакеты передаются и к серверу, и между устройствами в одной подсети.

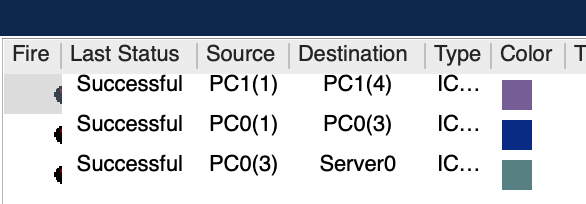


Рисунок 15 – результаты передачи пакетов.

Перейдем к выполнению дополнительного задания: добавим второй сервер и подключим его к маршрутизатору через коммутатор, назначив отдельный VLAN.

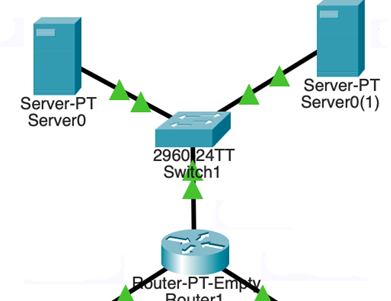


Рисунок 16 – измененная топология сети.

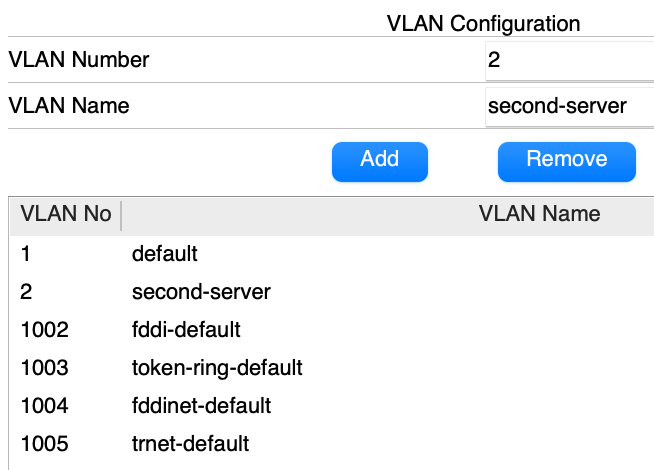


Рисунок 18 – настройка VLAN в коммутаторе.

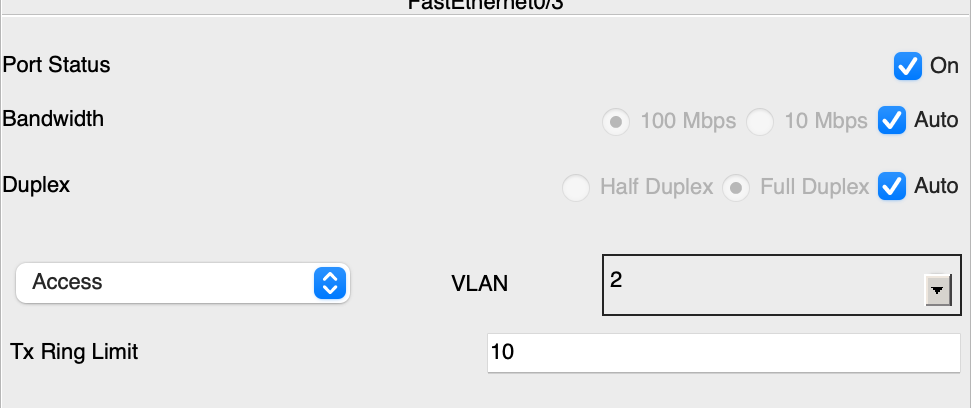


Рисунок 17 – настройка отдельного VLAN для второго сервера.

Добавим DNS запись на втором сервере, указывающую на первый.

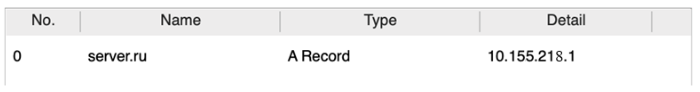


Рисунок 18 – DNS запись на втором сервере.

Настроим виртуальный интерфейс на порте маршрутизатора, подключенного к коммутатору для подключения к разным vlan.

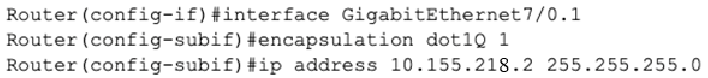


Рисунок 19 – настройка виртуального интерфейса на маршрутизаторе.

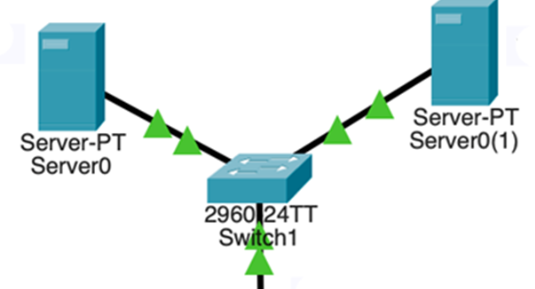


Рисунок 20 – полученные IP адреса серверов.

Настроим DNS сервер на точках доступа и убедимся, что мы можем получить доступ к серверу по доменному имени.

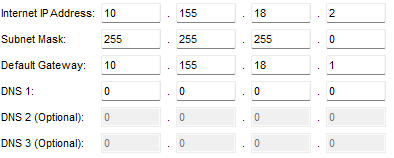


Рисунок 21 – настройки DNS на точке доступа.



Рисунок 22 – браузер с открытым ресурсом

**Вывод**

В этой лабораторной работе я закрепил теоретические знания в работе с WiFi и ограничениями доступа в компьютерных сетях.