**Московский государственный технический**

**университет им. Н.Э. Баумана**

Факультет «Информатика и системы управления»

Кафедра ИУ5 «Системы обработки информации и управления»

Курс «Сетевые технологии в АСОИУ»

Отчет по лабораторной работе №3 «Беспроводные сети»

|  |  |  |
| --- | --- | --- |
| Выполнил: |  | Проверил: |
| студент группы ИУ5-63Б |  | преподаватель каф. ИУ5 |
| Терентьева Софья  дата, подпись \_\_\_\_\_\_\_\_\_\_\_\_ |  | Антонов Артём Ильич  дата, подпись \_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |  |

Москва, 2024 г.

Цель работы:

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

Условие работы:

Построить сеть из двух сегментов, первый состоит из 3 рабочих станций и RADIUS сервера, вторая состоит из 3 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, серверов и локальных компьютеров.

Первая подсеть 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.

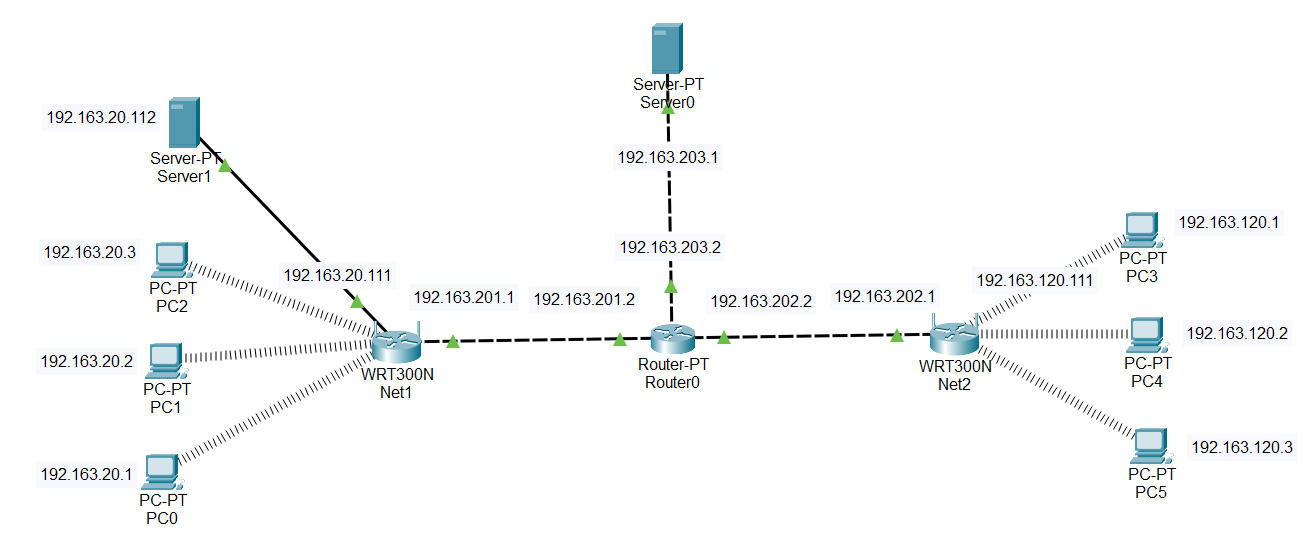
Вторая сеть защищена по технологии WPA2-PSK на основе шифрования AES. Идентификатор сети скрыт. На точке доступа включена фильтрация HTTP трафика и включен белый список MAC адресов подключаемых станций.

Необходимо добиться возможности пересылки ICMP-пакетов между устройствами внутри подсетей и сервером. Продемонстрировать невозможность прохождения запрещенного трафика и невозможность подключения станций, не внесенных в белый список.

Дополнительное задание: в любую из беспроводных сетей добавить DNS сервер, прописать в нем DNS запись для Server0 и настроить доступность Server0 по указанному имени с сохранением ограничений, которые есть в основной ЛР.

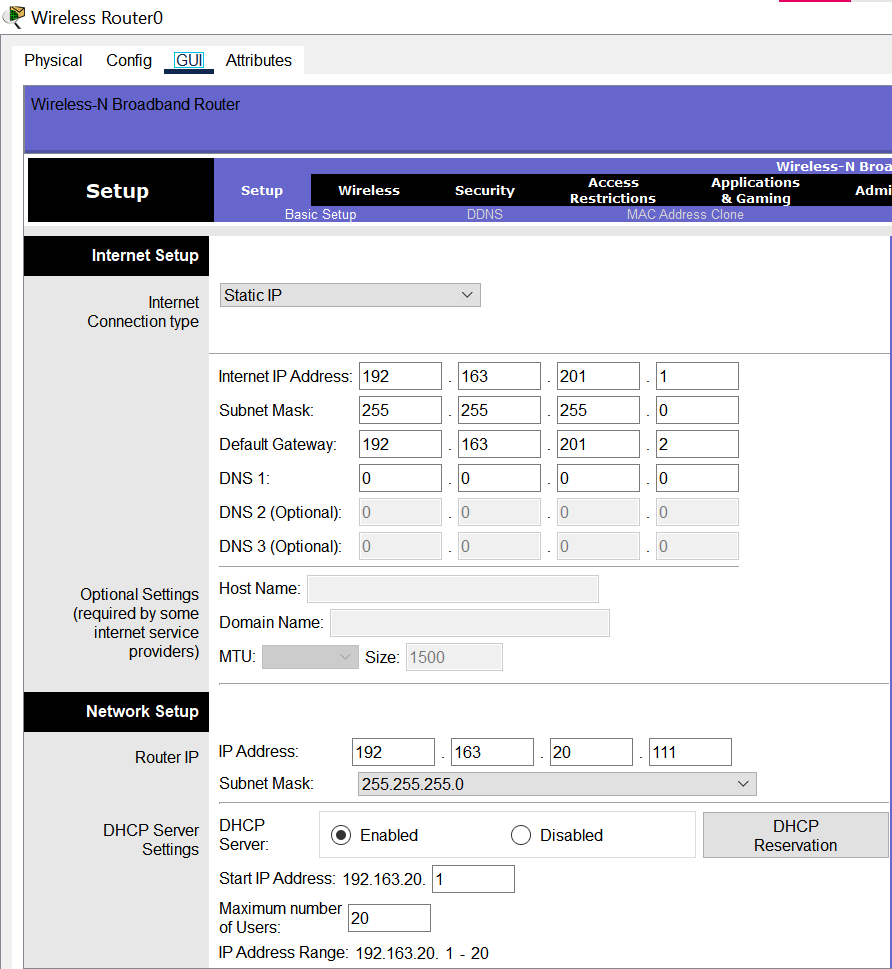
Ход работы:

1. Построим локальную сеть согласно заданию:

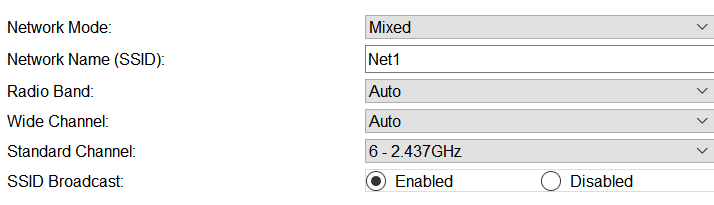


Зададим устройствам IP – адреса по номеру варианта. Для этого создадим пять подсетей: 192.163.20.0/24, 192.163.120.0/24 – с устройствами и 192.163.201.0/24, 192.163.202.0/24, 192.163.203.0/24 – для взаимодействия роутеров.

Пример настройки IP – адресов на беспроводном роутере:

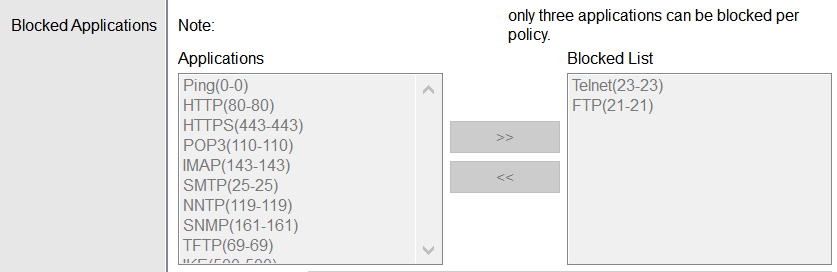
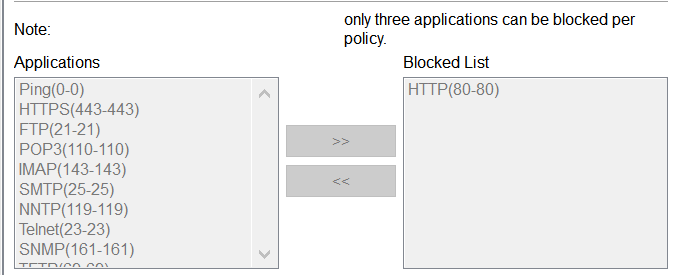


1. Изменим названия Wi-Fi сетей на роутерах и настроим фильтрацию трафика в подсетях согласно заданию:

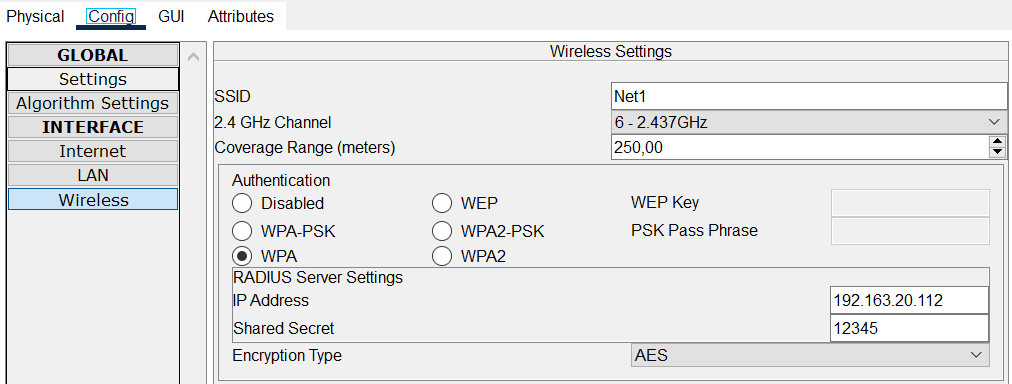


На втором роутере, соответственно, назовем Wi-Fi сеть Net2.

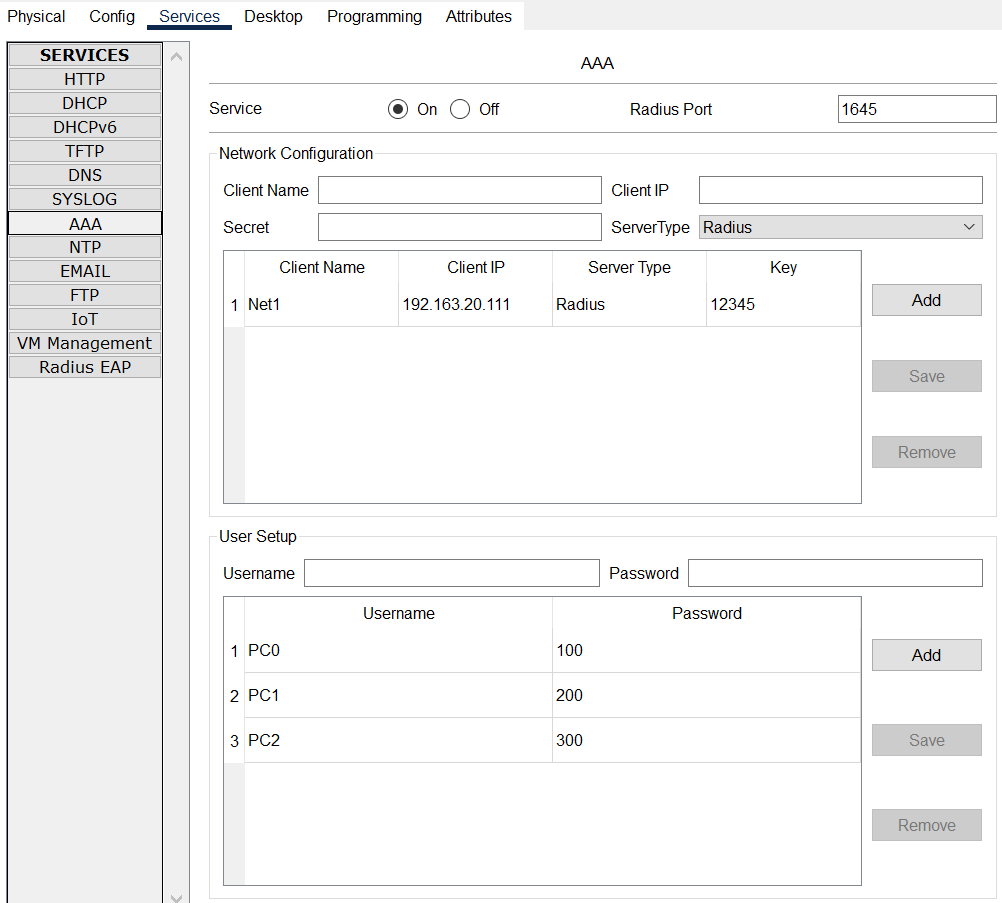
Настроим на беспроводных роутерах Access Restrictions:

Первый роутер: Второй роутер:

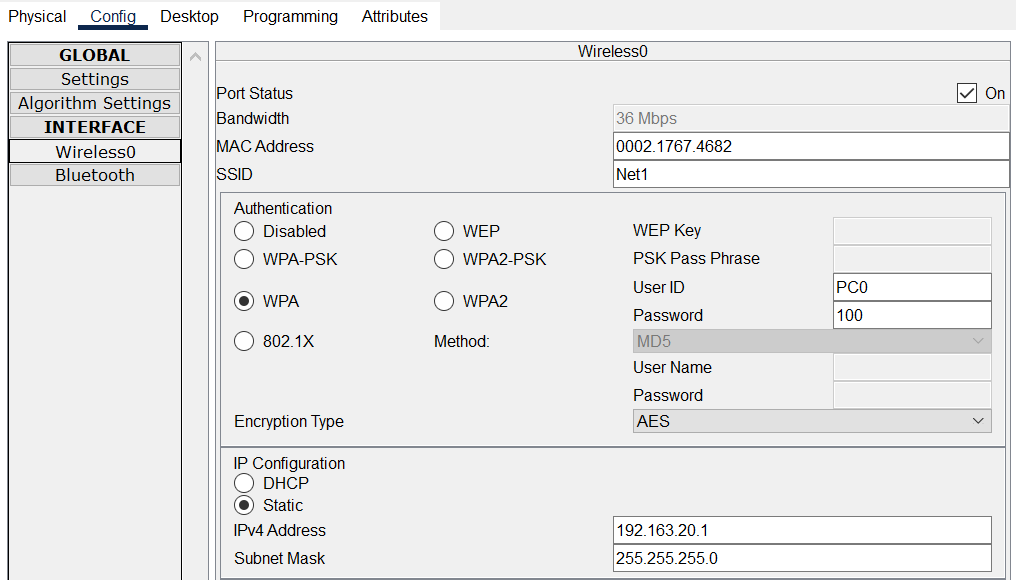
1. Настроим защиту в первой подсети. Для этого сначала настроим протокол защиты на роутере:



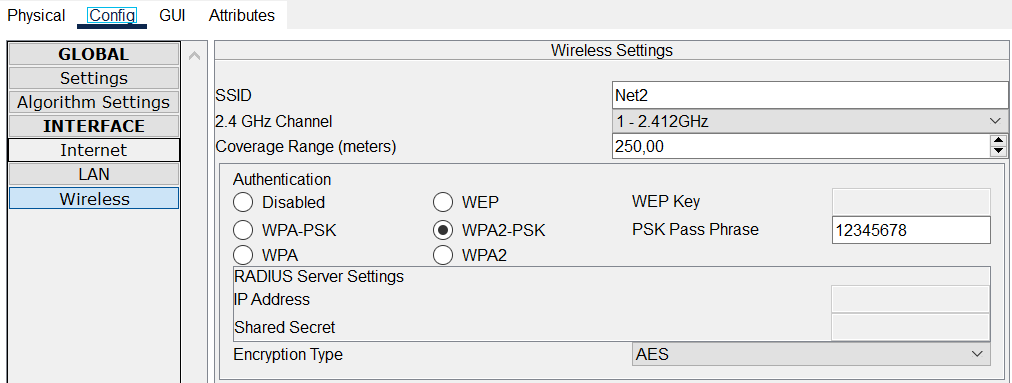
Затем настроим пользователей и их уникальные пароли на RADIUS-сервере:

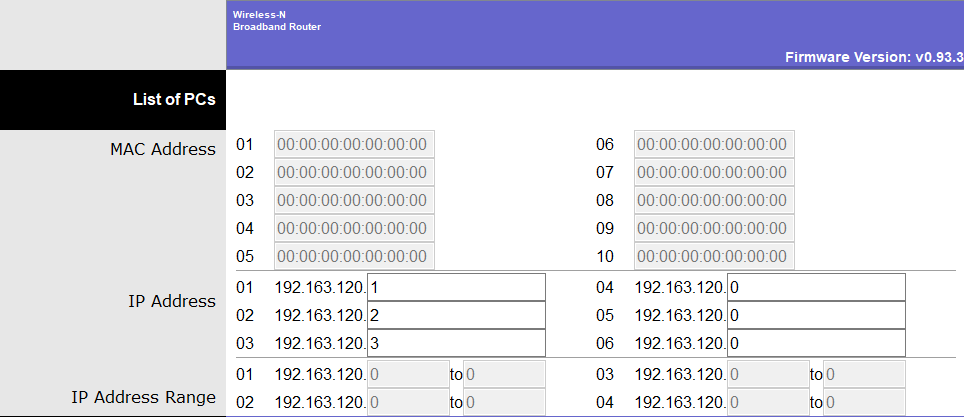


И настроим подключение для каждого устройства в подсети таким образом:

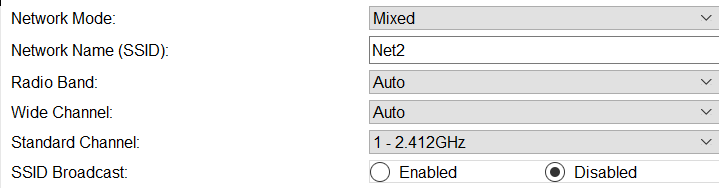


1. Настроим защиту во второй подсети. Для этого сначала настроим протокол защиты на роутере и создадим белый список устройств:

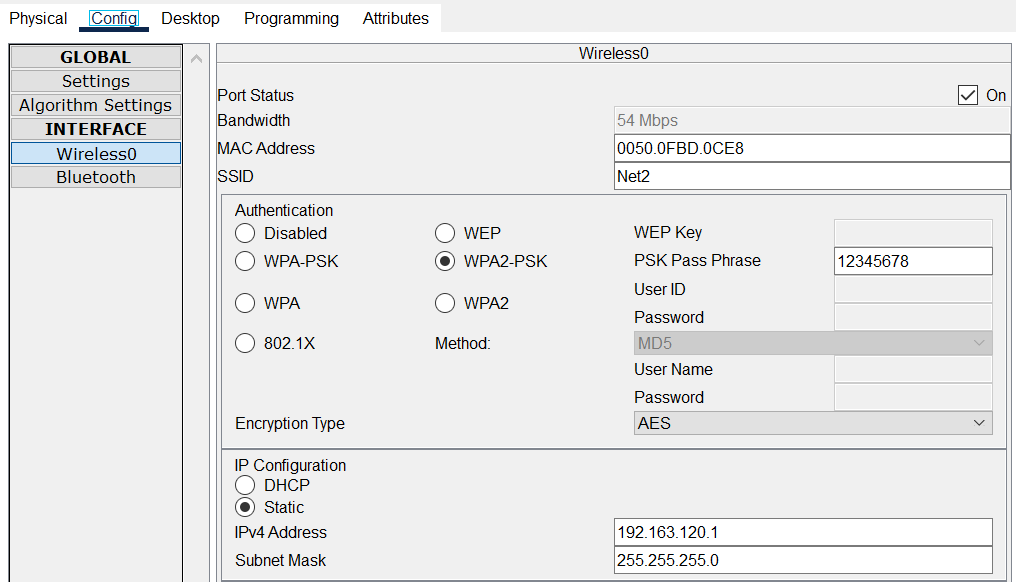




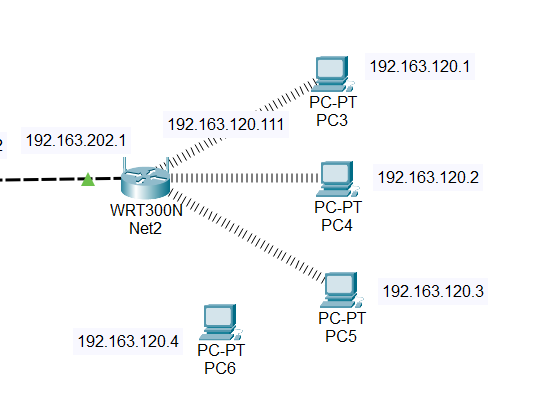
Скроем идентификатор сети (нижняя строчка):



И подключим соответствующие устройства:

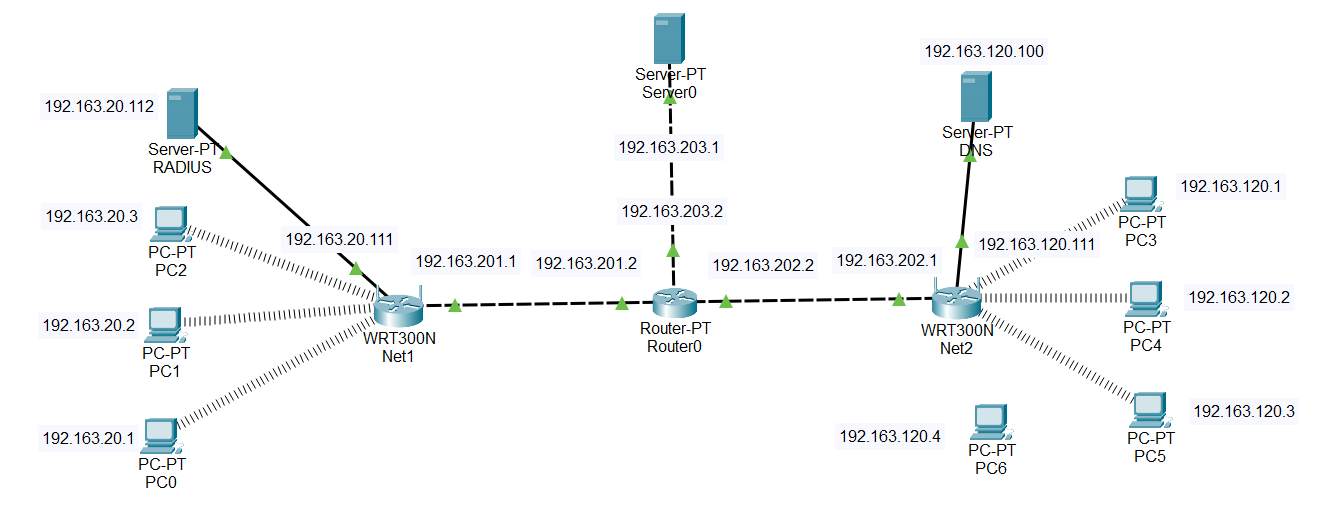


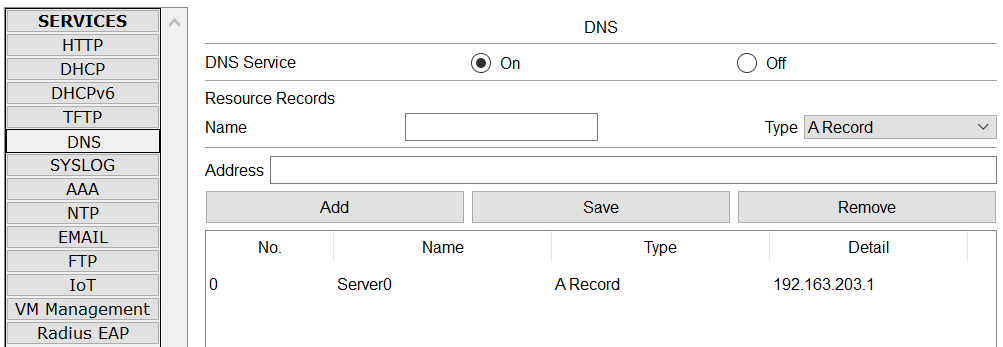
1. Проверим пересылку ICMP-пакетов и блокировку запрещенного трафика. Создадим еще один компьютер во второй подсети и попробуем подключить:



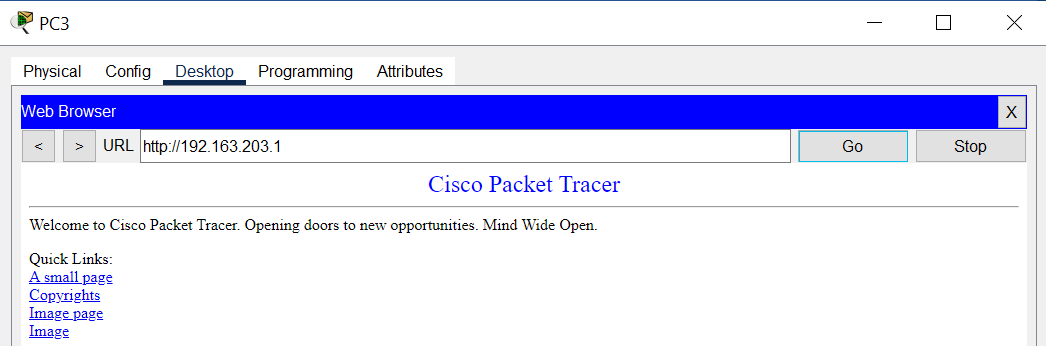
Подключение не происходит даже при вводе пароля, поскольку это устройство не находится в белом листе роутера. Трафик проходит соответственно заданию.

1. Подключим и настроим DNS-сервер:



На добавленном в локальную сеть сервере пропишем DNS запись для Server0:

С одного из компьютеров в подсети проверим достижимость:



Доступность Server0 из подсети успешно настроена.

Результаты выполнения работы:

В процессе выполнения лабораторной работы я освежила знания и навыки работы с беспроводными сетями и научилась различными способами настраивать защиту таких сетей.