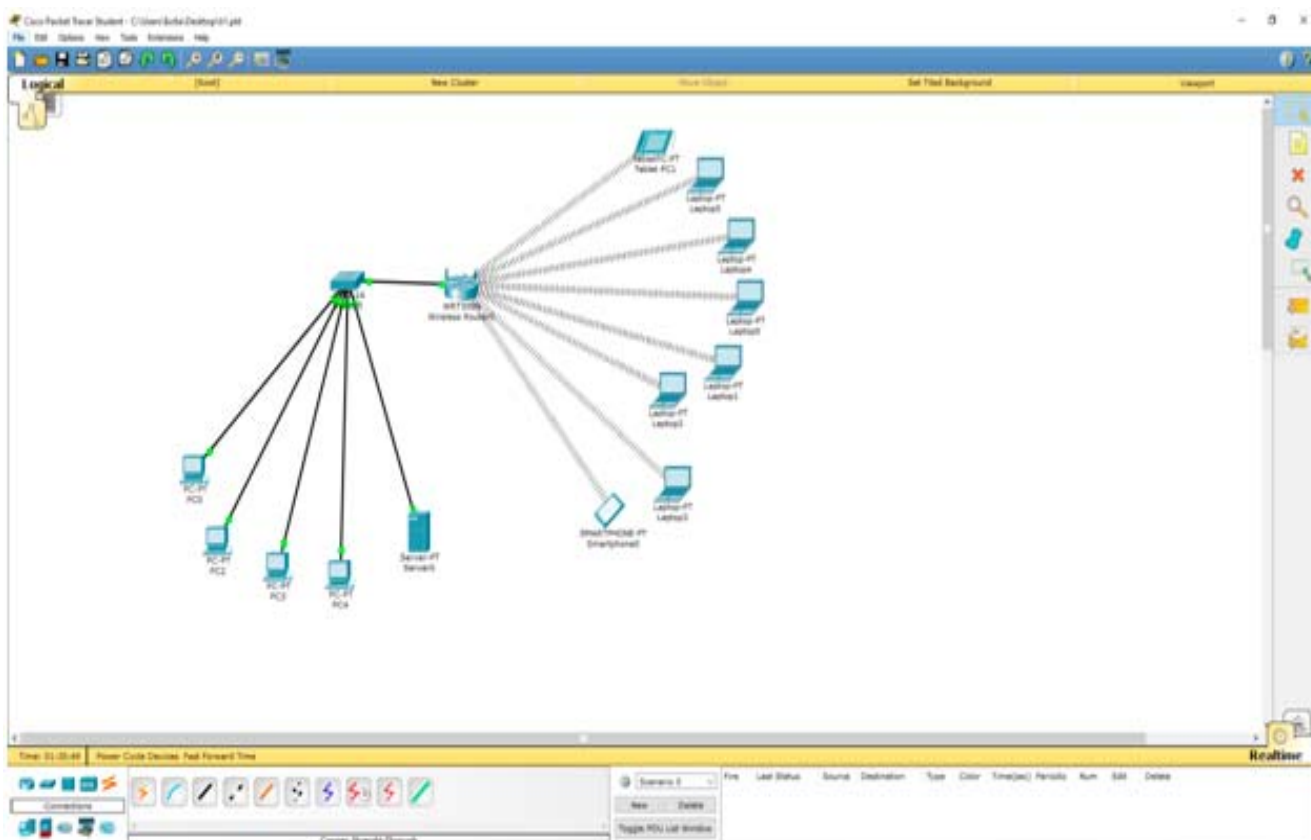


4.2 Лабораторная работа №1. Инфраструктурный режим.

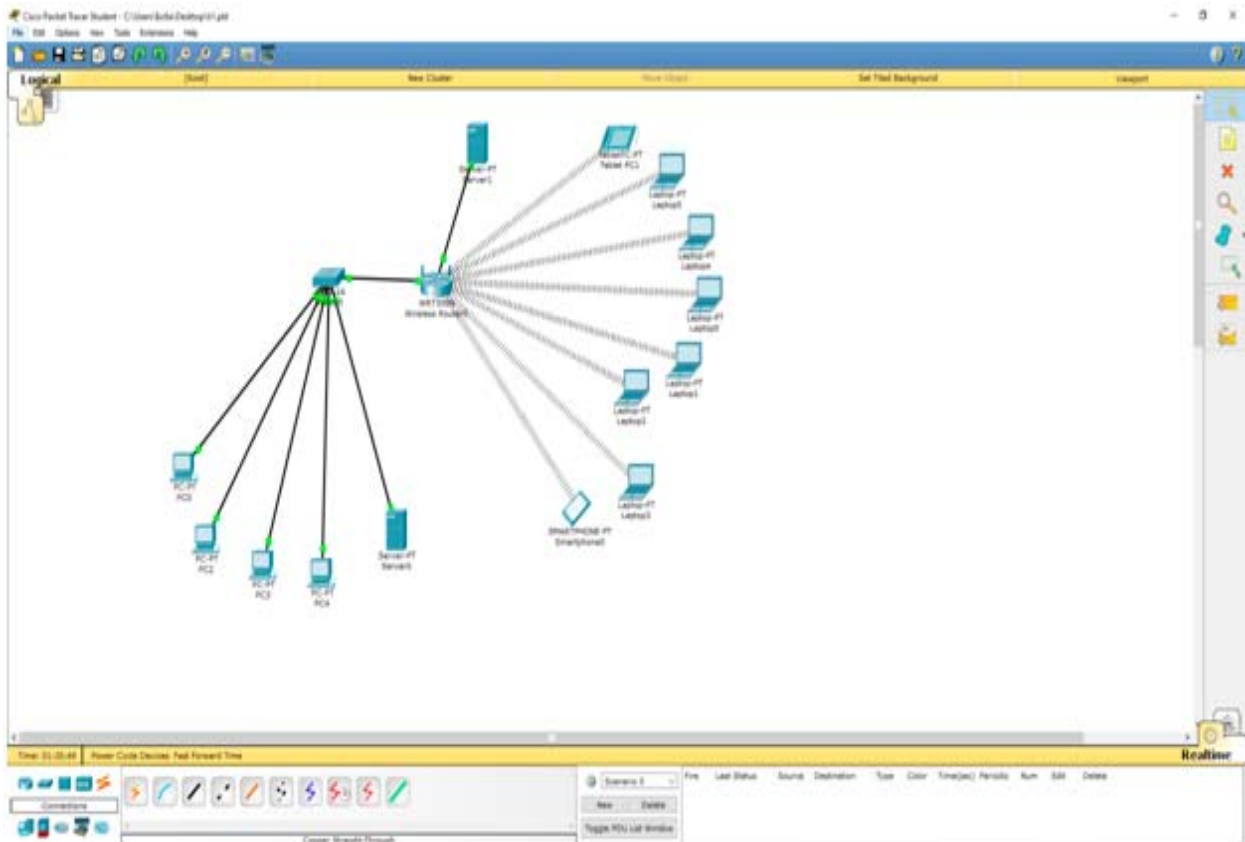
Построить сеть, состоящую из двух сегментов. Первый состоит из А рабочих станций и сервера, соединенных в сеть Fast Ethernet на основе коммутатора. IP адреса этого сегмента задаются статически и находятся в диапазоне $192.17x.100+F.y$, где F выбирается согласно варианту, x номер учебной группы, а y — произвольное число. Второй сегмент — сеть из В ноутбуков и двух любых беспроводных устройств на основе точки доступа Linksys. IP адреса этого сегмента находятся в диапазоне $192.17x.200+F.y$ и задаются динамически. Беспроводная сеть защищена по технологии WPA2-PSK на основе шифрования TKIP. Проверить доступность рабочих станций первого сегмента и сервера со стороны беспроводной сети с помощью отправки простых ICMP пакетов.



Дополнительное задание для ЛР1.

Подключить к локальной сети маршрутизатора сервер. Для нечетных вариантов настроить на нем службу WWW и прописать в параметрах веб страницы своё ФИО и группу. Для четных вариантов настроить на сервере FTP, разместить в

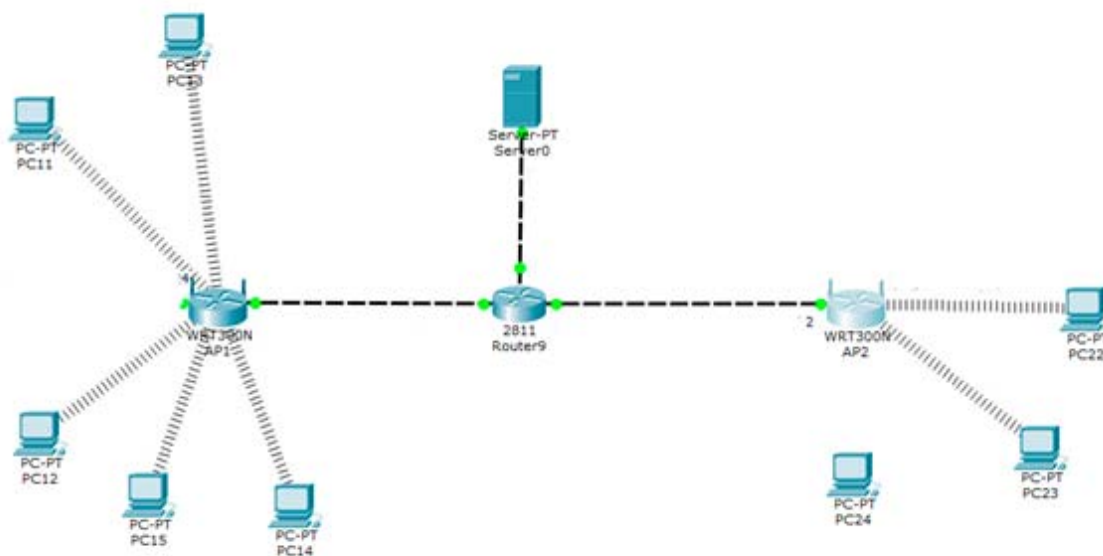
нем текстовый файл содержащий ФИО и группу. Настроить доступность указанных ресурсов из внешней сети.



4.3 Лабораторная работа №2. Защита беспроводных сетей.

Построить сеть из двух сегментов, каждый из которых состоит из D и 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 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. Правила для настройки IP адресов такие же как в ЛР№1.



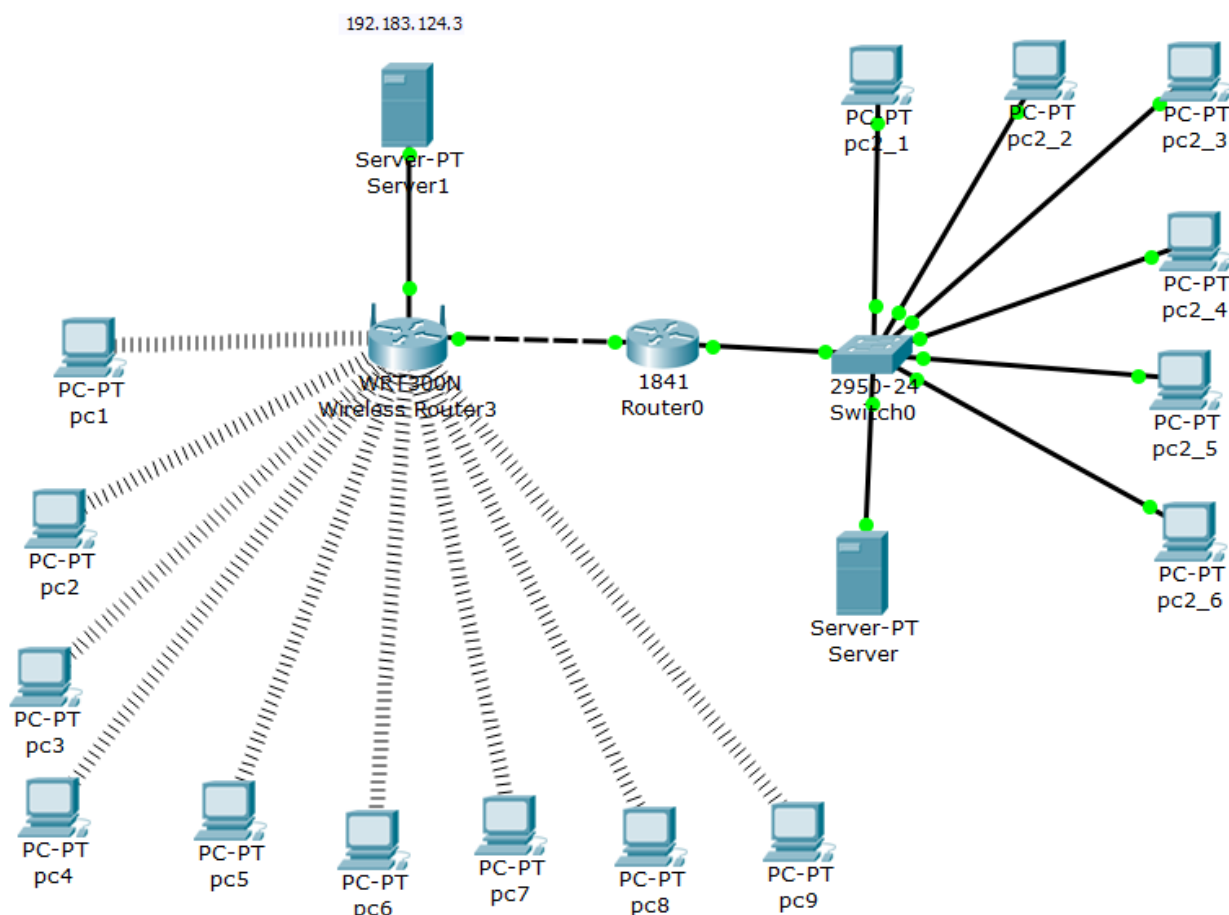
Дополнительное задание ЛР2.

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.

4.4 Лабораторная работа №3. Защита WPA. Настройка RADIUS сервера.

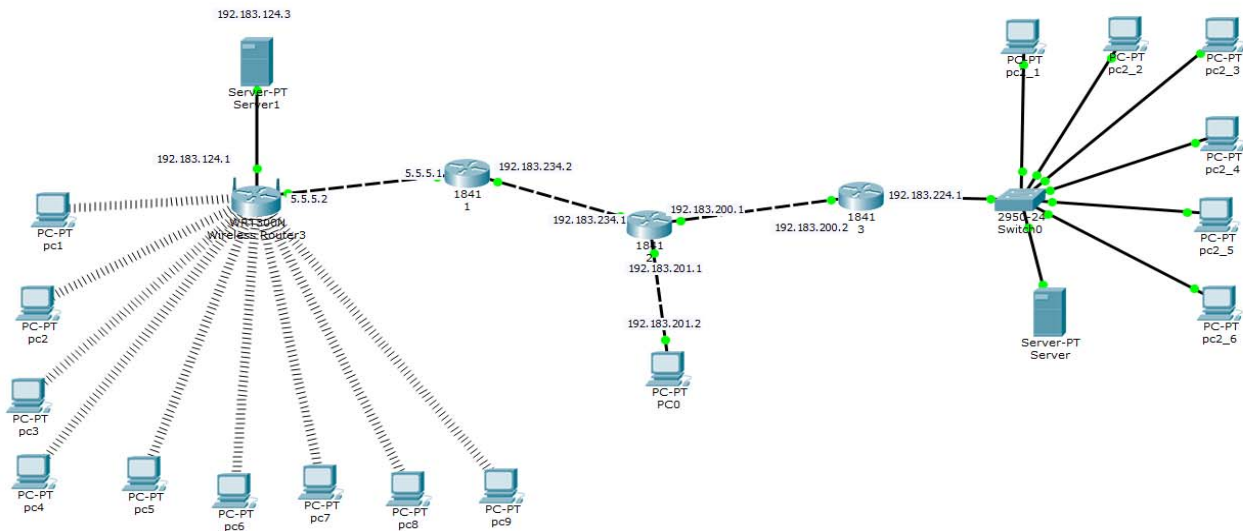
Построить сеть на основе точки доступа Linksys. Сеть содержит 8 рабочих станций и сервер, подключенный с помощью витой пары. Сеть защищена по технологии WPA. Сервер является RADIUS сервером. Выдать каждой рабочей станции свой уникальный логин и пароль для подключения к точке доступа.

К внешнему интерфейсу точки доступа подключен маршрутизатор, к которому подключен коммутатор, к которому подключены В компьютеров и файл-сервер. Необходимо добиться возможности пересылки данных по протоколу ICMP между устройствами внутри сети и файл-сервером. Правила для настройки IP адресов такие же как в ЛР№1.



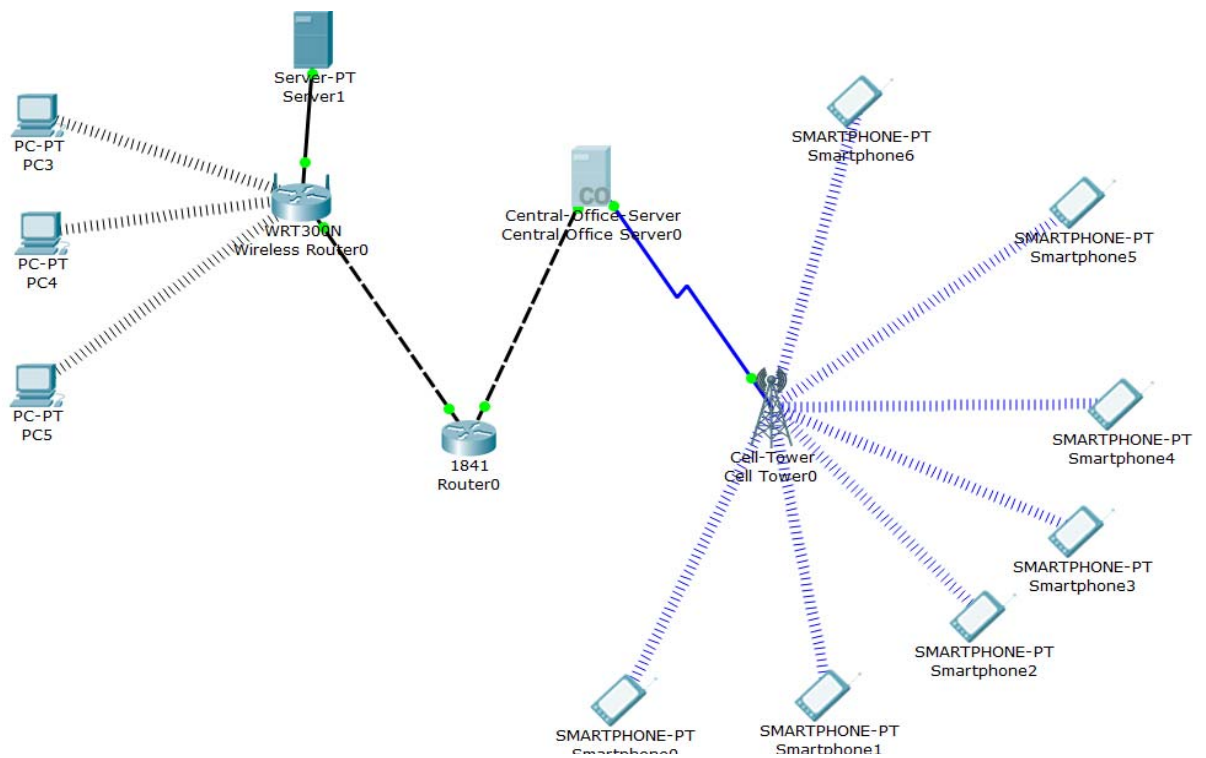
Дополнительное задание:

Между точкой доступа и коммутатором подключить еще два роутера, к роутеру 2 подключить сервер. Настроить на роутере 2 блокировку трафика из беспроводной сети. Настроить VPN туннель от роутера 1 к роутеру 3 чтобы обойти блокировку трафика.



4.5 Лабораторная работа №4. Port Forwarding.

Создайте WiFi сеть на основе точки доступа WRT300N, в которой находится А узлов и веб-сервер, содержащий сайт. На веб-сервере настройте DNS. Сеть защищена с помощью WPA2-PSK. Точка доступа подключена к маршрутизатору. Маршрутизатор подключен к Central Office серверу, а тот, в свою очередь - к базовой станции 3G/4G. В мобильной сети находится Е устройств. Необходимо добиться просмотра веб-страницы со встроенных в устройства браузеров по IP адресу и по доменному имени. Правила для настройки IP адресов такие же как в ЛР№1.



Дополнительное задание:

К роутеру 0 подключить коммутатор, к которому в свою очередь подключено 4 рабочих станции. Рабочие станции должны быть в 2-х разных подсетях и работать через VLAN. Только один VLAN должен иметь доступ к внешним ресурсам.

