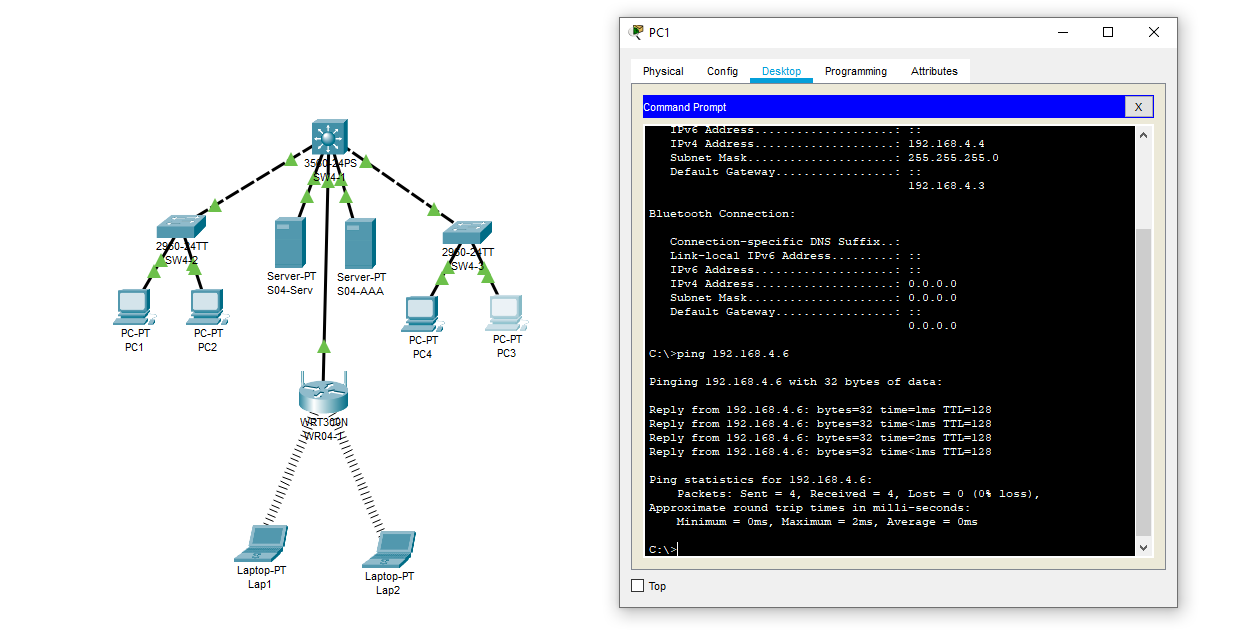
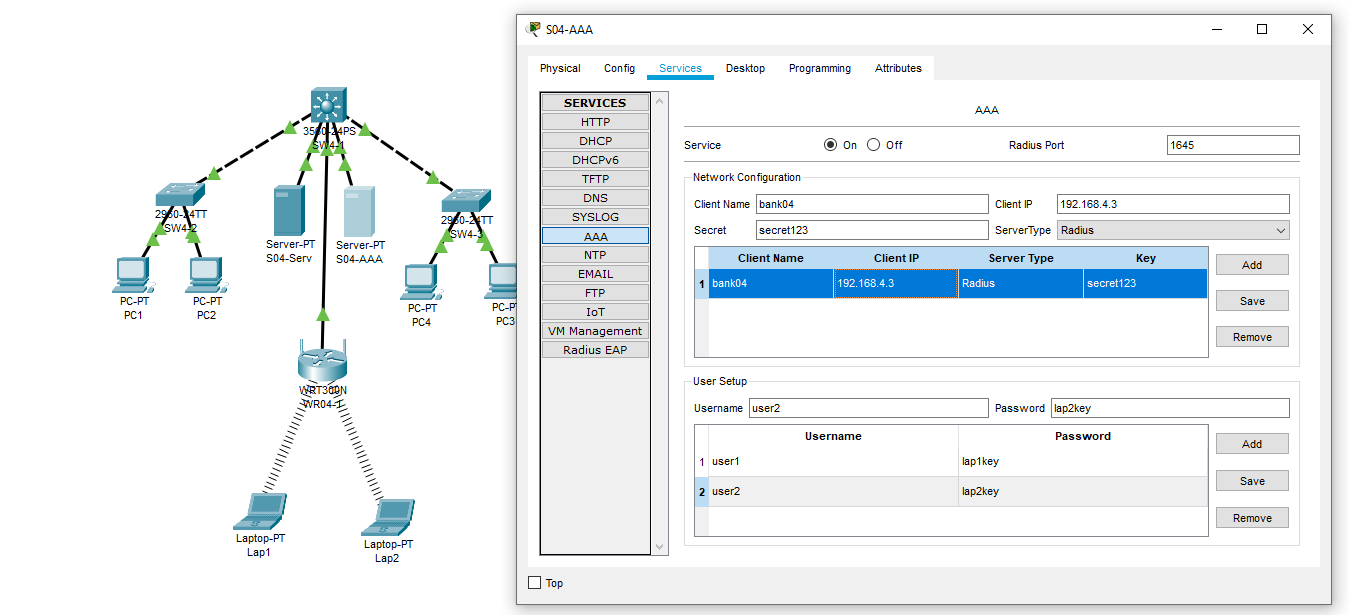
Дровосеков Д.А. КМБ-16

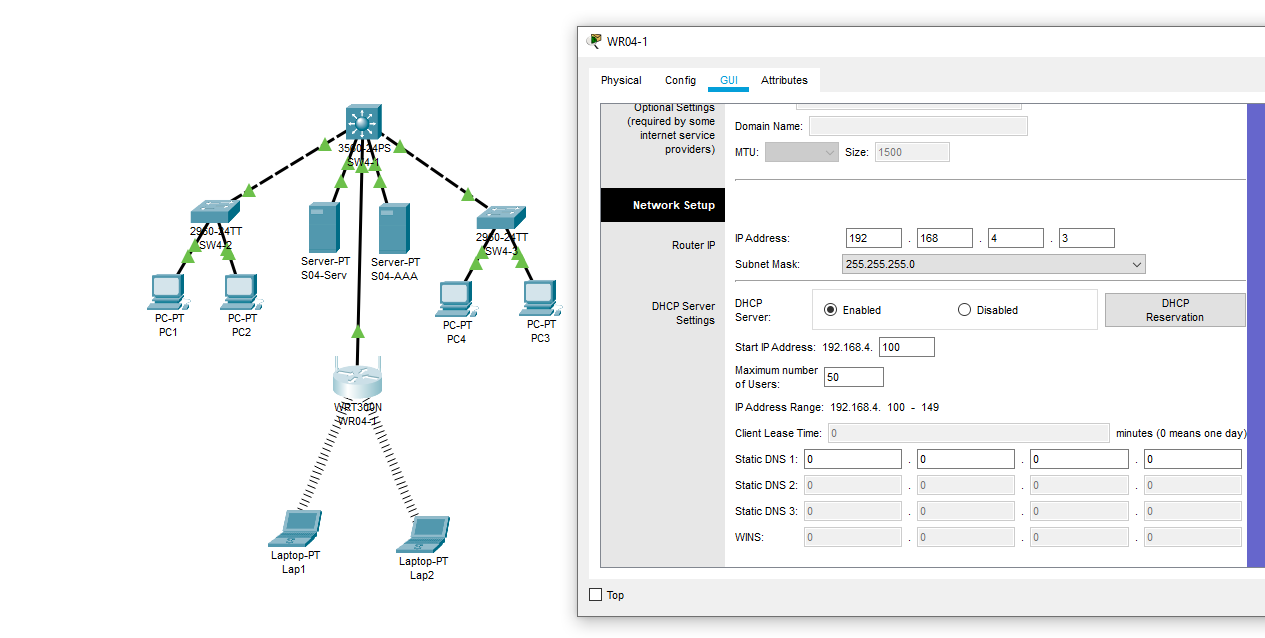
Проверим работу беспроводных подключений ping PC3 с PC1



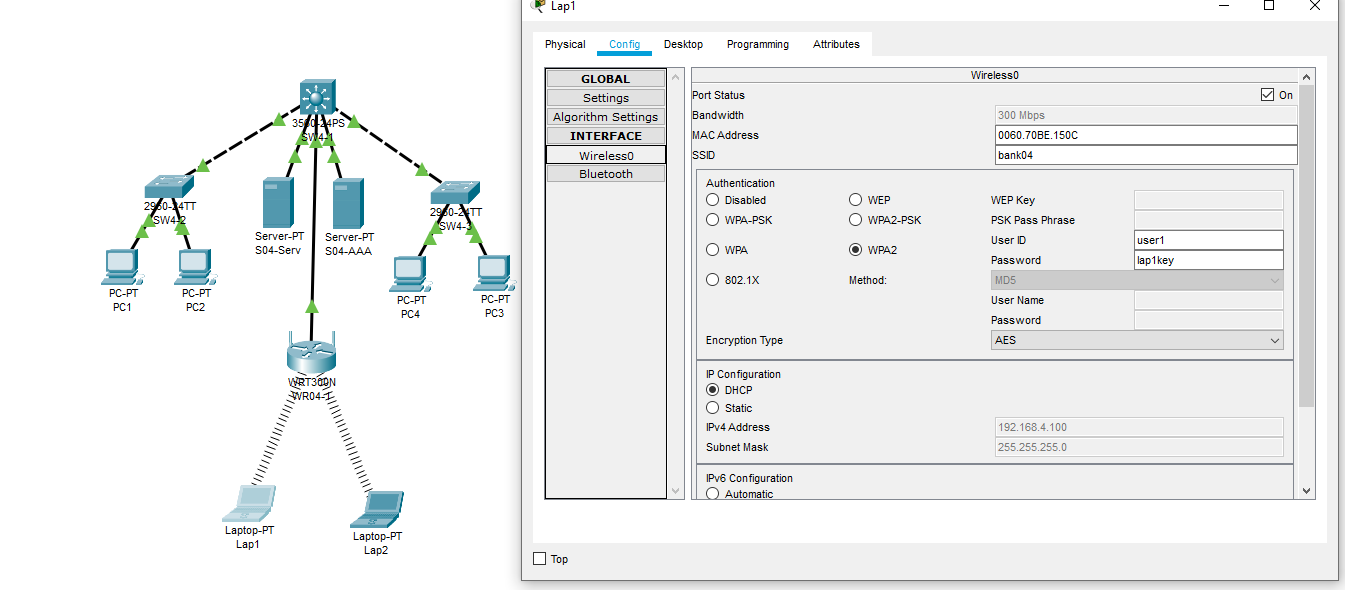
Настроим Radius-сервер



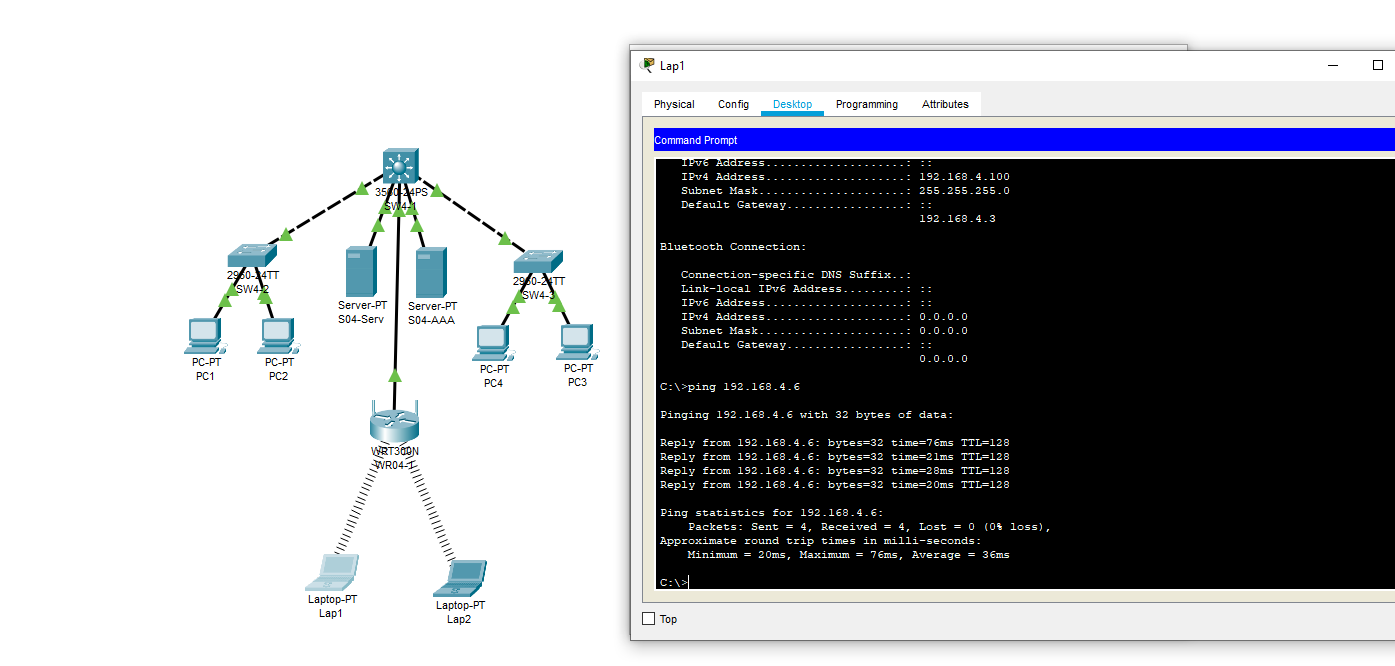
Настроим Wi-Fi маршрутизатор



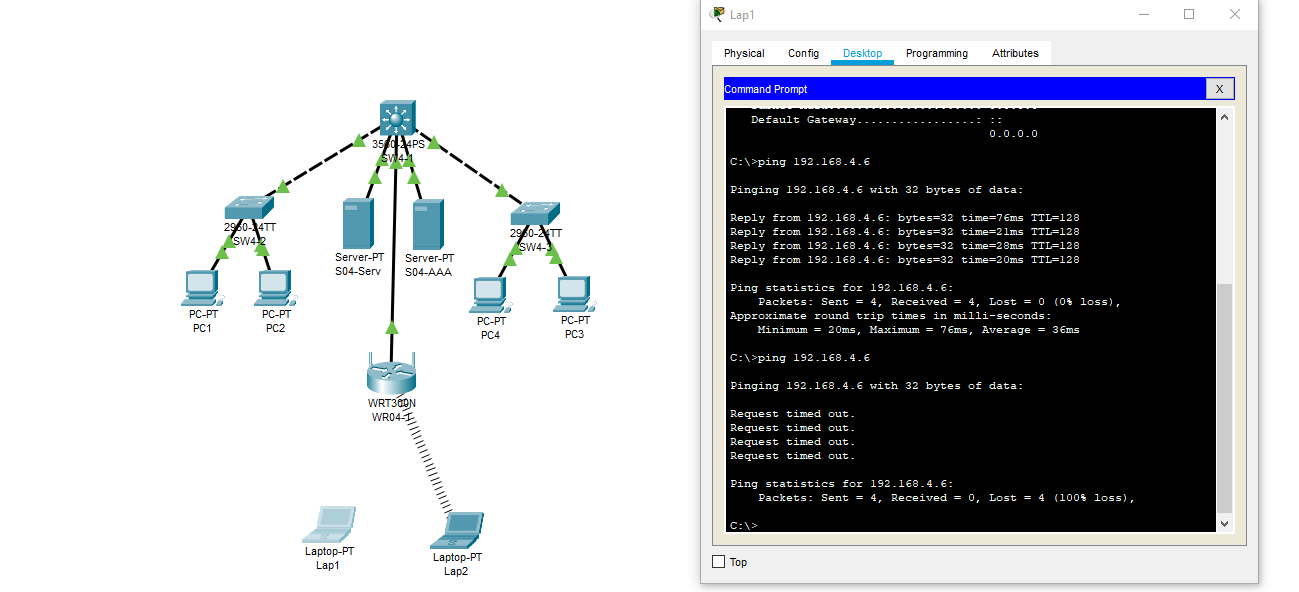
Настроим Wi-Fi на ноутбуках



Ping PC3 с Lap1



Если при настройке указать неверный пароль соединить не удается



1. Организовать дополнительный беспроводный сегмент ЛВС, предназначенный для гостевого доступа недоверенных пользователей в сеть Интернет. Обеспечить невозможность доступа из недоверенного сегмента в ЛВС филиала.

Можно добавить в архитектуру корпоративной сети wi-fi роутер, который будет подключен к маршрутизатору, находящемуся на стыке корпоративной сети и сети Интернет, ограничение доступа из беспроводной сети в корпоративный сегмент будет осуществляться межсетевым экраном.

2. Изучить рекомендации и известные подходы к построению беспроводных ЛВС.

При построении системы обеспечения безопасности важно определить модель угроз, т.е. решить, чему собственно защита будет противостоять. По сути, в беспроводных сетях угрозы две: несанкционированное подключение и прослушивание, но их список можно расширить, выделить следующие основные угрозы, связанные с беспроводными устройствами:

* неконтролируемое использование и нарушение периметра;
* несанкционированное подключение к устройствам и сетям;
* перехват и модификация трафика;
* нарушение доступности;
* позиционирование устройства.

Основными механизмами обеспечения безопасности беспроводной ЛВС являются:

* базовые методы защиты и протоколы аутентификации IEEE 802.11i;
* управление доступом в соответствии со стандартом IEEE 802.1x;
* сегментирование сетей с помощью технологии VLAN;
* управление доступом к сети на основе атрибутов пользователей и средств доступа;
* межсетевое экранирование и VPN;
* минимизация привилегий пользователей;
* физическая безопасность

3. Предложить техническое решение (разработать схему) по организации доступа из беспроводного сегмента к ЛВС корпоративной сети с использованием технологий VPN.

При использовании технологии OpenVPN возможно организовать общий доступ к сети (с ограничениями на использование broadcast’a) для устройств извне (при необходимости) локальной сети и для устройств в локальной сети без прямого доступа к интернету.