3 РАЗРАБОТКА И ОБОСНОВАНИЕ СТРУКТУРНОЙ СХЕМЫ ПРОЕКТИРУЕМОЙ СЕТИ

Для выполнения требований технического задания необходимо разработать структурную схему ведомственной сети. На рисунке 3.1 представлена модель сети, реализованная c использованием Cisco Packet Tracer.

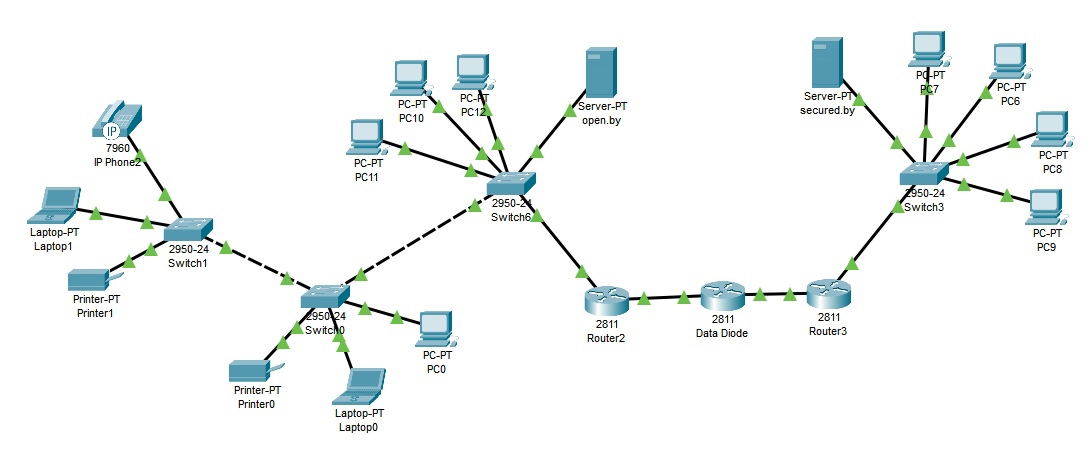


Рисунок 3.1 – Модель реализованная в Cisco Packet Tracer

В представленной модели однонаправленной ведомственной сети важную роль играет диод данных (однонаправленный шлюз), который позволяет осуществить фильтрацию трафика. В данном случае он реализован программно, посредством конфигурации маршрутизатора. Для корректной реализации однонаправленного шлюза на базе маршрутизатора в Cisco Packet Tracker использовался универсальный и мощный механизм фильтрации: список контроля доступом (Access Control List).

Согласно техническому заданию, в сети происходит односторонняя передача данных из публичной подсети в закрытую подсеть. Для передачи данных между подсетями в представленной модели ведомственной сети, используется FastEthernet, со скоростью работы до 100 Мбит\с, что соответствует техническому заданию.

Между публичной и закрытой сетью расположен программный однонаправленный шлюз, пропускающий данные только в направлении закрытой сети, предотвращая возможные утечки данных. В подсетях расположены два сервера, которые предназначены для публикации данных из публичной подсети в закрытую.

Публичная подсеть, изображена на рисунке 3.2.

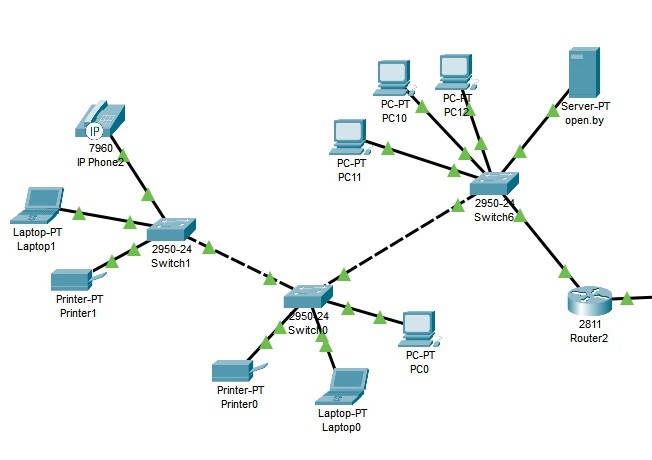


Рисунок 3.2 – Публичная подсеть

В открытой сети находится ftp-сервер open.by c ipv4-адресом 192.168.100.10/28, позволяющий хранить, обрабатывать и передавать информацию. Устройства, находящиеся в одной сети с сервером, могут беспрепятственно публиковать данные в специальный каталог, размещенный на сервере.

Защищенная сеть, изображена на рисунке 3.3.

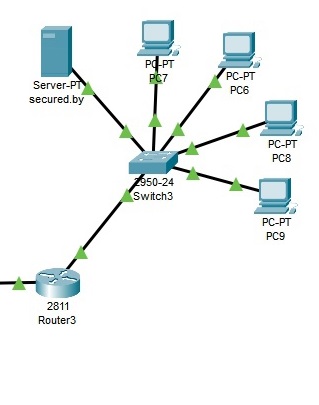


Рисунок 3.3 – Защищенная подсеть

В защищенной подсети расположен ftp-сервер secured.by c ipv4-адресом 192.168.50.10/28, который позволяет хранить информацию и передавать ее только в пределах своей сети.

Для демонстрации принципа работы сети, рассмотрим ситуацию, когда пользователю PC0, расположенного в публичной сети, требуется передать данные на PC9, расположенный в закрытой сети.

Для этого, на первом шаге, пользователь PC0, подключается к серверу open.by и открывает каталог для отправки данных в защищенную сеть. Далее происходит загрузка данных на публичный сервер, пользователь PC0 по завершению загрузки, может отключиться от сервера. Передача данных в публичной сети изображена на рисунке 3.4

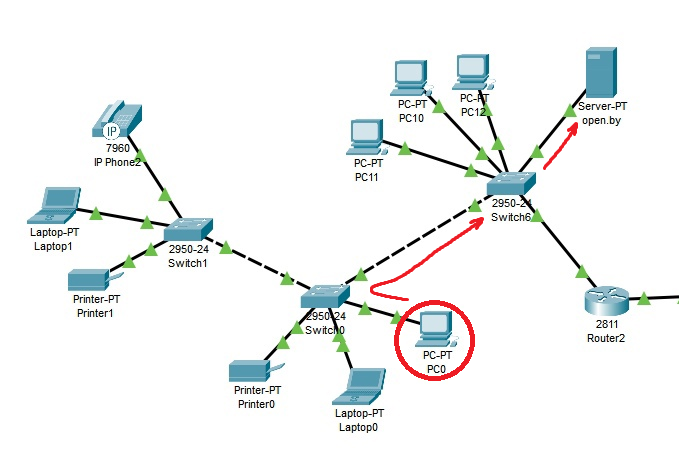


Рисунок 3.4 – Передача данных в публичной подсети

После загрузки информации на сервер open.by, начинается процесс однонаправленной передачи данных посредством пакетов UDP через диод данных на защищенный сервер secured.by. Движение трафика изображено на рисунке 3.5. С сервера open.by, трафик поступает на Router2, тот в свою очередь перенаправляет трафик через диод данных на Router3. После чего, данные поступают на сервер secured.by, находящийся в защищенной сети.

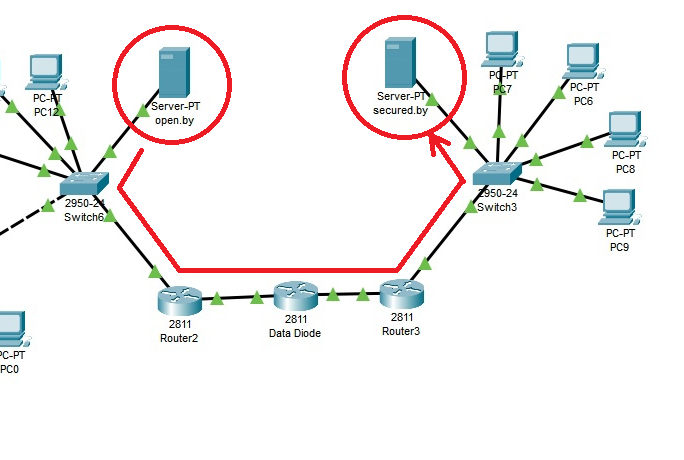


Рисунок 3.5 – Передача данных в публичной подсети

После передачи данных на сервер secured.by, они становятся доступны для пользователей внутренней сети. Пользователь PC9 подключается к серверу и может скачать данные с защищенного сервера на свой ПК в случае необходимости. Схема передачи данных изображена на рисунке 3.6.

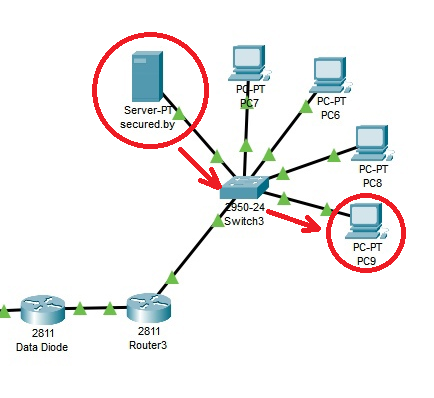


Рисунок 3.6 – Передача данных в закрытой подсети