ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
СТЕРЛИТАМАКСКИЙ МНОГОПРОФИЛЬНЫЙ ПРОФЕССИОНАЛЬНЫЙ КОЛЛЕДЖ
(ГАПОУ СМПК)

КУРСОВАЯ РАБОТА

«МОДЕЛИРОВАНИЕ РЕАЛИЗАЦИИ ТЕХНОЛОГИИ VPN ДЛЯ ПОЛЬЗОВАТЕЛЕЙ ЛОКАЛЬНОЙ СЕТИ»

Выполнил:
студент III курса группы ССА-39
специальности 09.02.06 Системное и
сетевое администрирование
Фурман Борис Леонидович.

Руководитель:
Агибалова Кристина Евгеньевна.

Стерлитамак, 2020

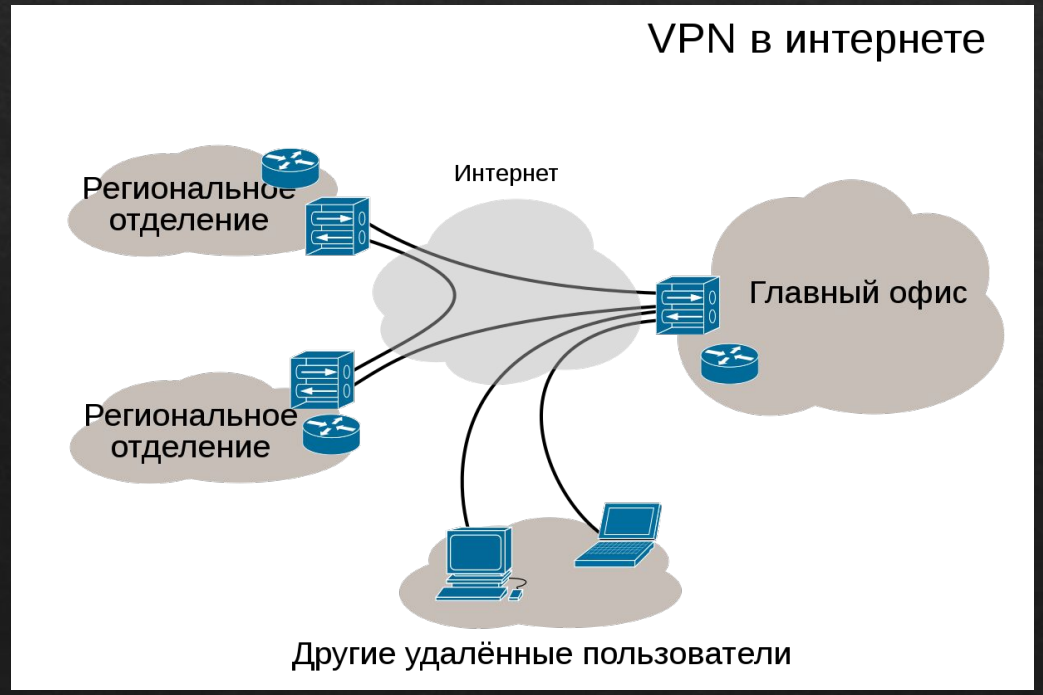
Цель проекта: смоделировать реализацию технологии VPN для пользователей локальной сети.

Задачи проекта:

- 1. Рассмотреть учебно-техническую литературу по теме курсовой работы.
- 2. Раскрыть понятия, назначение и функции технологии VPN.
- 3. Описать этап реализации технологии VPN для пользователей локальной сети.
- 4. Смоделировать объекты сетевой инфраструктуры локальной сети.
- 5. Описать этапы реализации технологии VPN для смоделированной локальной сети.

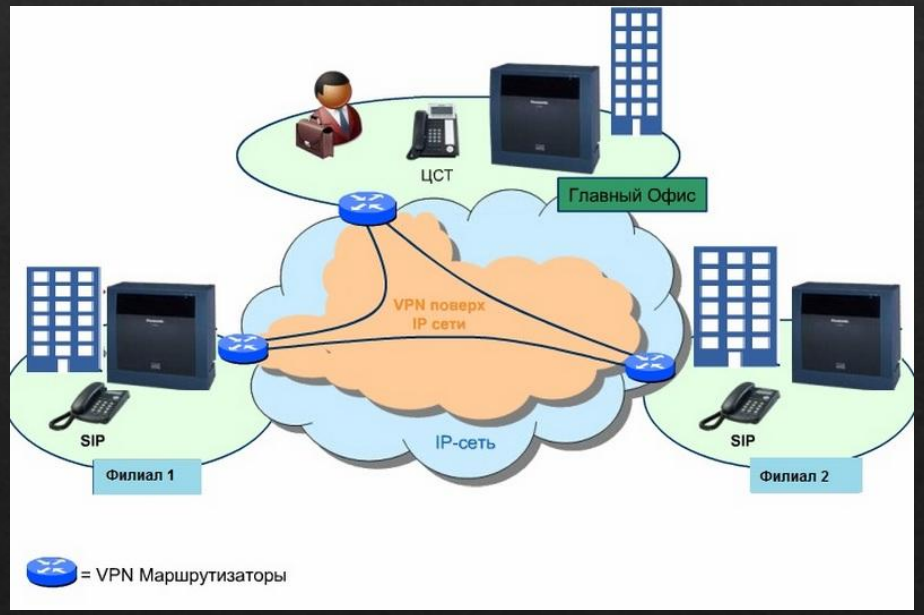
Современное развитие информационных технологий и, в частности, сети Интернет, приводит к необходимости защиты информации, передаваемой в рамках распределенной корпоративной сети, использующей сети открытого доступа. Интернет является незащищенной сетью, поэтому приходиться изобретать способы защиты конфиденциальных данных, передаваемых по незащищенной сети.

VPN (англ. Virtual Private Network «виртуальная частная сеть») — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например Интернет).



В основе концепции построения виртуальных сетей VPN лежит достаточно простая идея: если в глобальной сети имеются два узла, которым нужно обменяться информацией, то между этими двумя узлами необходимо построить виртуальный защищенный туннель для обеспечения конфиденциальности и целостности информации, передаваемой через открытые сети; доступ к этому виртуальному туннелю должен быть чрезвычайно затруднен всем возможным активным и пассивным внешним наблюдателям.

Преимущества, получаемые компанией от создания таких виртуальных туннелей, заключаются прежде всего в значительной экономии финансовых средств, поскольку в этом случае компания может отказаться от построения или аренды дорогих выделенных каналов связи для создания собственных Интернет сетей и использовать для этого дешевые Интернет-каналы, надежность и скорость передачи которых в большинстве своем уже не уступает выделенным линиям. Очевидная экономическая эффективность от внедрения VPN-технологий стимулирует предприятия к активному их внедрению.



Основные компоненты VPN

- VPN-шлюз – сетевое устройство, подключенное к нескольким сетям, выполняет функции шифрования, идентификации, аутентификации, авторизации и туннелирования. Может быть решен как программно, так и аппаратно.
- VPN-клиент (хост) решается программно. Выполняет функции шифрования и аутентификации. Сеть может быть построена без использования VPN-клиентов.
- Туннель – логическая связь между клиентом и сервером. В процессе реализации туннеля используются методы защиты информации.
- Граничный сервер – это сервер, являющийся внешним для корпоративной сети. В качестве такого сервера может выступать, например, брендмауэр или система NAT.
- Обеспечение безопасности информации VPN – ряд мероприятий по защите трафика корпоративной сети при прохождении по туннелю от внешних и внутренних угроз.

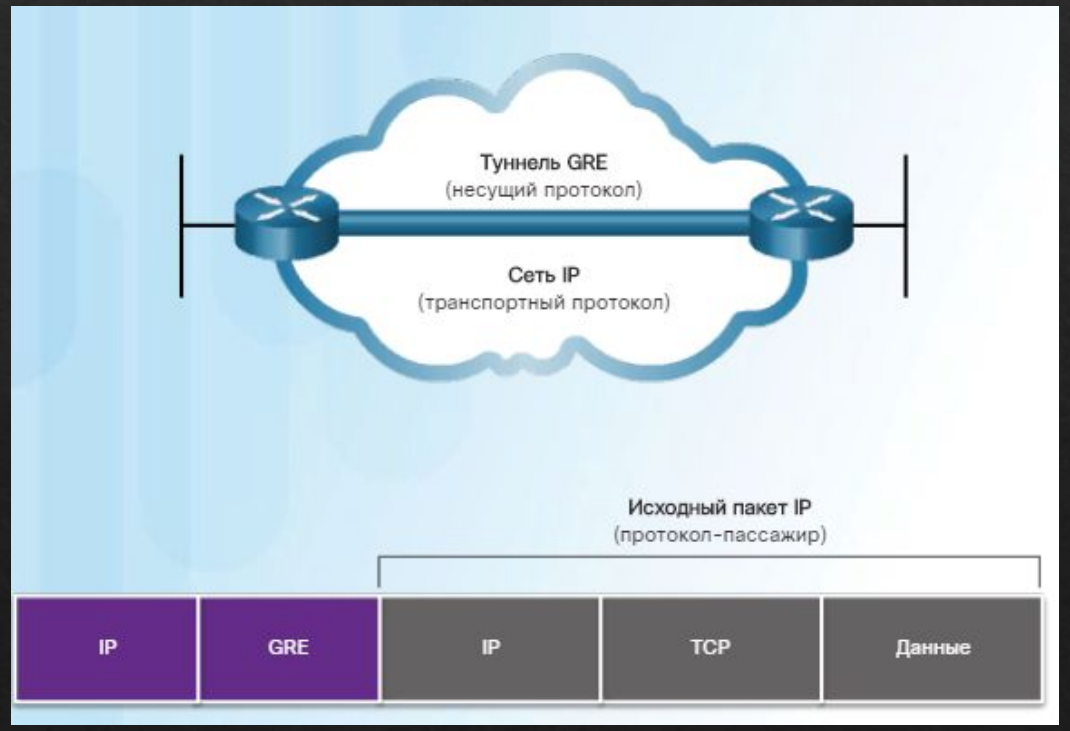
Технология программного GRE туннелирования в VPN сети

Универсальная инкапсуляция при маршрутизации (Generic Routing Encapsulation, GRE) – один из примеров базового, незащищенного протокола создания туннелей для site-to-site VPN. GRE – это протокол туннелирования, разработанный компанией Cisco, позволяющий инкапсулировать пакеты протоколов различного типа внутри IP-туннелей. Благодаря этому создается виртуальный канал «точка-точка» до маршрутизаторов Cisco в удаленных точках поверх IP-сети.

Сети VPN типа «узел-узел» – создается, когда устройства на обеих сторонах подключения VPN заранее знают настройки сети VPN (см. рисунок). Сеть VPN остается статической, и внутренние узлы не знают о существовании VPN. В межузловой сети VPN оконечные компьютеры отправляют и получают обычный трафик TCP/IP через шлюз VPN. Шлюз VPN отвечает за инкапсуляцию и шифрование исходящего трафика для всего трафика, поступающего с конкретного объекта. Затем шлюз VPN передает этот трафик через туннель VPN по Интернету в равноправный соседний шлюз VPN на стороне приема. При получении данных соседний шлюз VPN удаляет заголовки, расшифровывает содержимое и передает пакет в узел назначения по своей частной сети.

GRE предназначен для управления процессом передачи многопротокольного и группового IP-трафика между двумя и более площадками, между которыми связь может обеспечиваться только по IP. Он может инкапсулировать пакеты протоколов различного типа в IP-туннеле.

Интерфейс туннеля поддерживает заголовки для всех указанных ниже протоколов

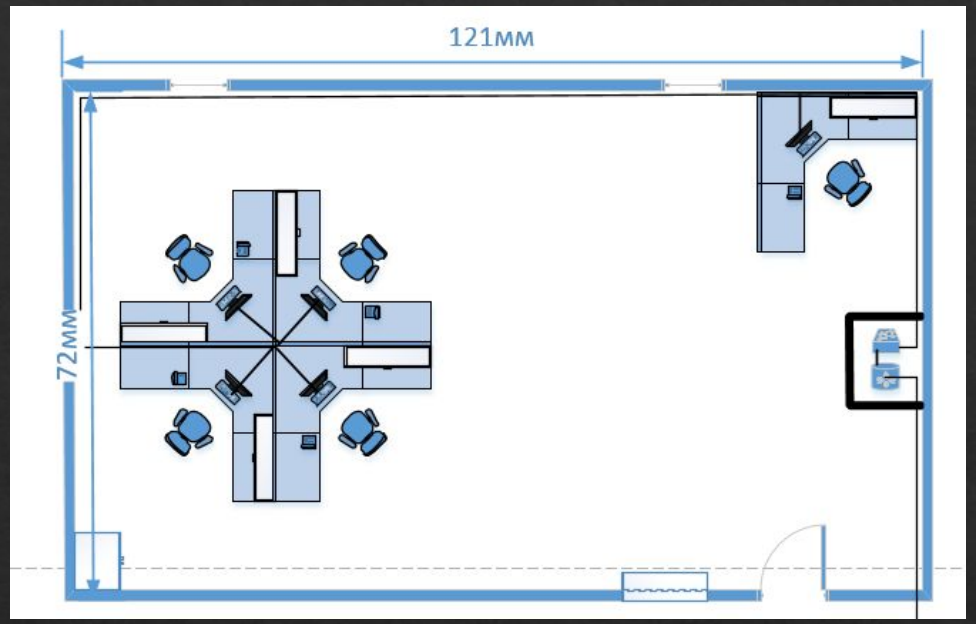


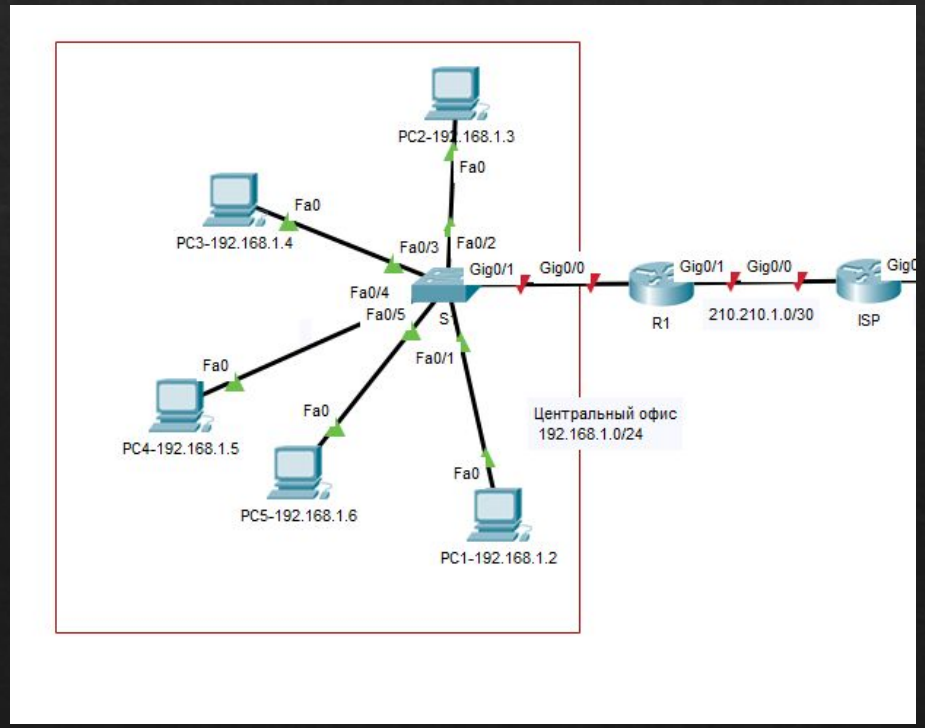
Центральный офис

Локальная сеть главного офиса состоит из:

- 5 компьютеров пользователей;
- 1 коммутатор: Cisco 2960;
- 1 роутер Cisco 1941.

Локальная сеть Главного офиса подключена к Интернету с использованием Ethernet кабеля, посредством роутера Cisco 1941



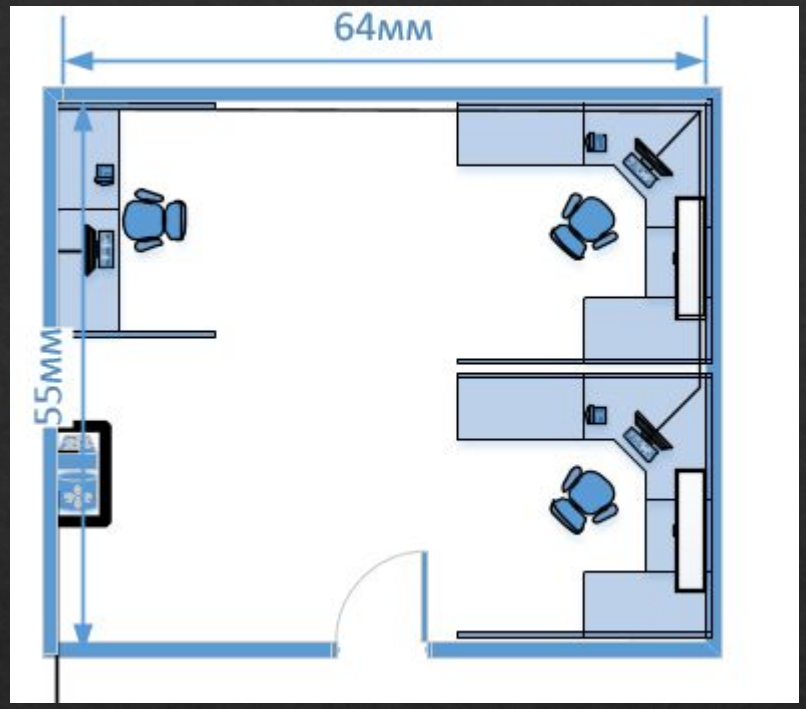


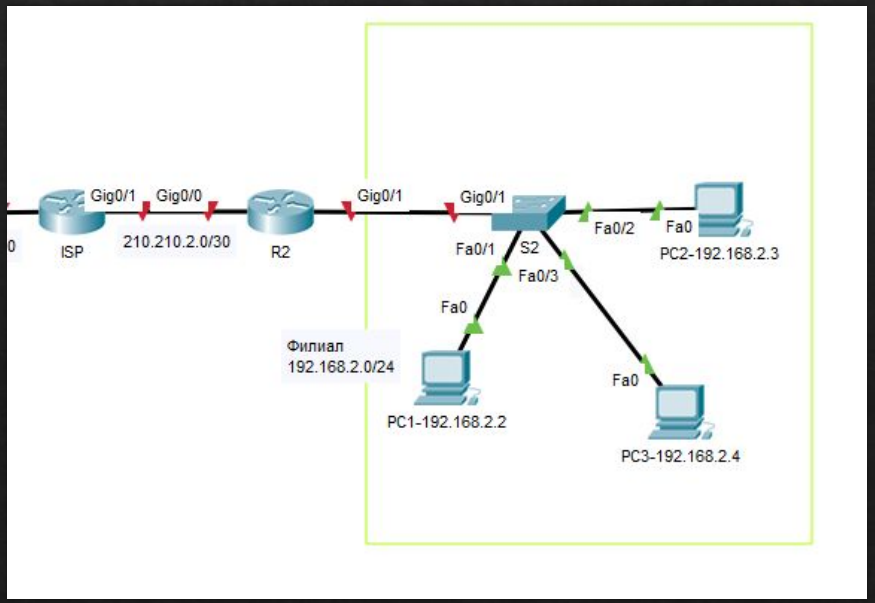
Филиал

Локальная сеть филиала:

- 3 компьютера пользователей;
- 1 коммутатор: Cisco 2960;
- 1 роутер Cisco 1941.

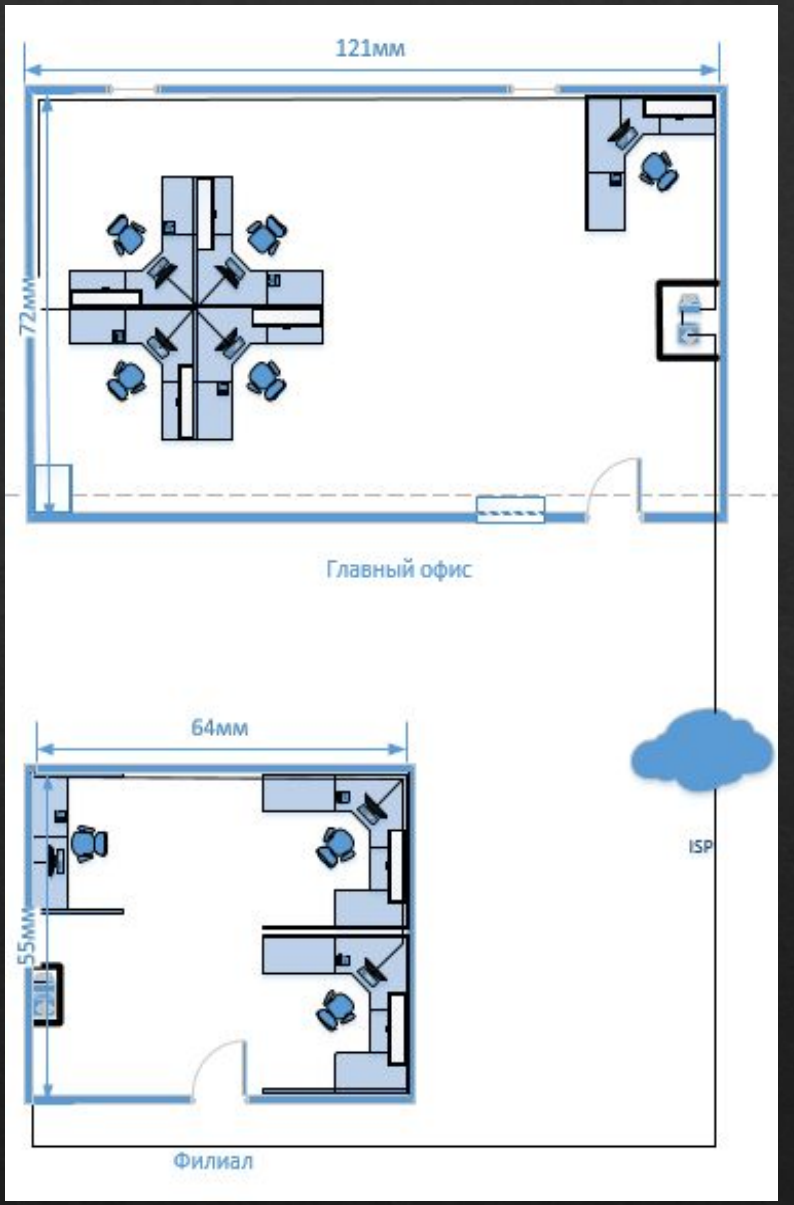
Локальная сеть Филиала подключена к Интернету с использованием Ethernet кабеля, посредством роутера Cisco 1941.

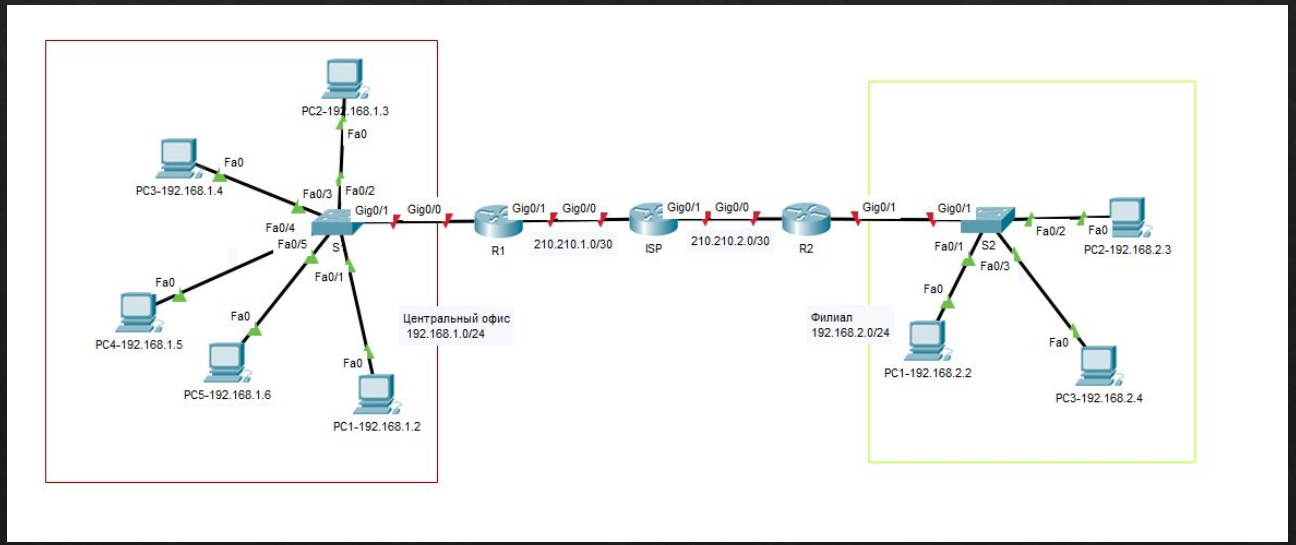




Cisco IOS (от англ. Internetwork Operating System – Межсетевая Операционная Система) – программное обеспечение, используемое в маршрутизаторах и сетевых коммутаторах Cisco. Cisco IOS является многозадачной операционной системой, выполняющей функции сетевой организации, маршрутизации, коммутации и передачи данных.

IP адреса оконечные устройства, получают динамически, от провайдерского DHCP сервера. Локальная сеть предприятия разделена на две части, на главный офис и на филиал взаимодействующие посредством туннеля GRE.





Для реализации выполнения практического задания, были сделаны следующие шаги:

- Смоделирована и составлена физическая и логическая топология сети.
- Оба офиса были объединены в одну локальную сеть по средствам VPN, а именно туннель GRE. Она производилась на маршрутизаторах Cisco 1941, которые находятся в главном офисе, и филиале соответственно. Настройка производилась стандартными средствами операционной системы Cisco IOS 15.2. Для того чтобы настроить коммутаторы Cisco 2960, понадобилась базовая настройка, в виде установки, и зашифровки паролей.
- По итогу была проведена проверка всех узлов связи, с помощью команд show ip route, traceroute, ping, show ip interface brief. Путём этих проверок удалось проверить, и убедится в работоспособности туннеля GRE.

С помощью раннее найденной учебно-технической литературы, были рассмотрены понятия, описаны основные этапы моделирования VPN в локальной сети. В частности, было описано:

- Структура VPN- состоит из внутренней и внешней сети.
- Классификация VPN- бывают защищенный и доверительные среды.
- По способу реализации- в виде аппаратного и программного решения.
- По назначению- использование защищённого канала для сегментов корпоративной сети, и подключение удаленного сотрудника к локальной сети.
- По типу протокола- основные протоколы для реализации VPN TCP/IP, IPX и AppleTalk.
- По уровню сетевого протокола- ISO/OSI.

В соответствии с вышеизложенным, цель курсового проекта достигнута путем решения поставленных задач, смоделирована технология VPN для пользователей локальной сети.