

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)**

Факультет Информатика и вычислительная техника

(наименование факультета)

Кафедра Кибербезопасность информационных систем

(наименование кафедры)

**ОТЧЕТ**

по лабораторным работам по предмету: Компьютерные сети

Выполнил:

ст. гр. ВКБ31 Котелевец К.А.

Ростов-на-Дону

2024

**ЛАБОРАТОРНАЯ РАБОТА №1**

**Создание сети из двух ПК в программе Cisco Parket Tracer**

Задание 1. Создание сети из двух ПК в программе Cisco Parket Tracer.

Для начала построим простейшую сеть из двух ПК, представленную на рисунке 1.1. Соединим их кроссовым кабелем.

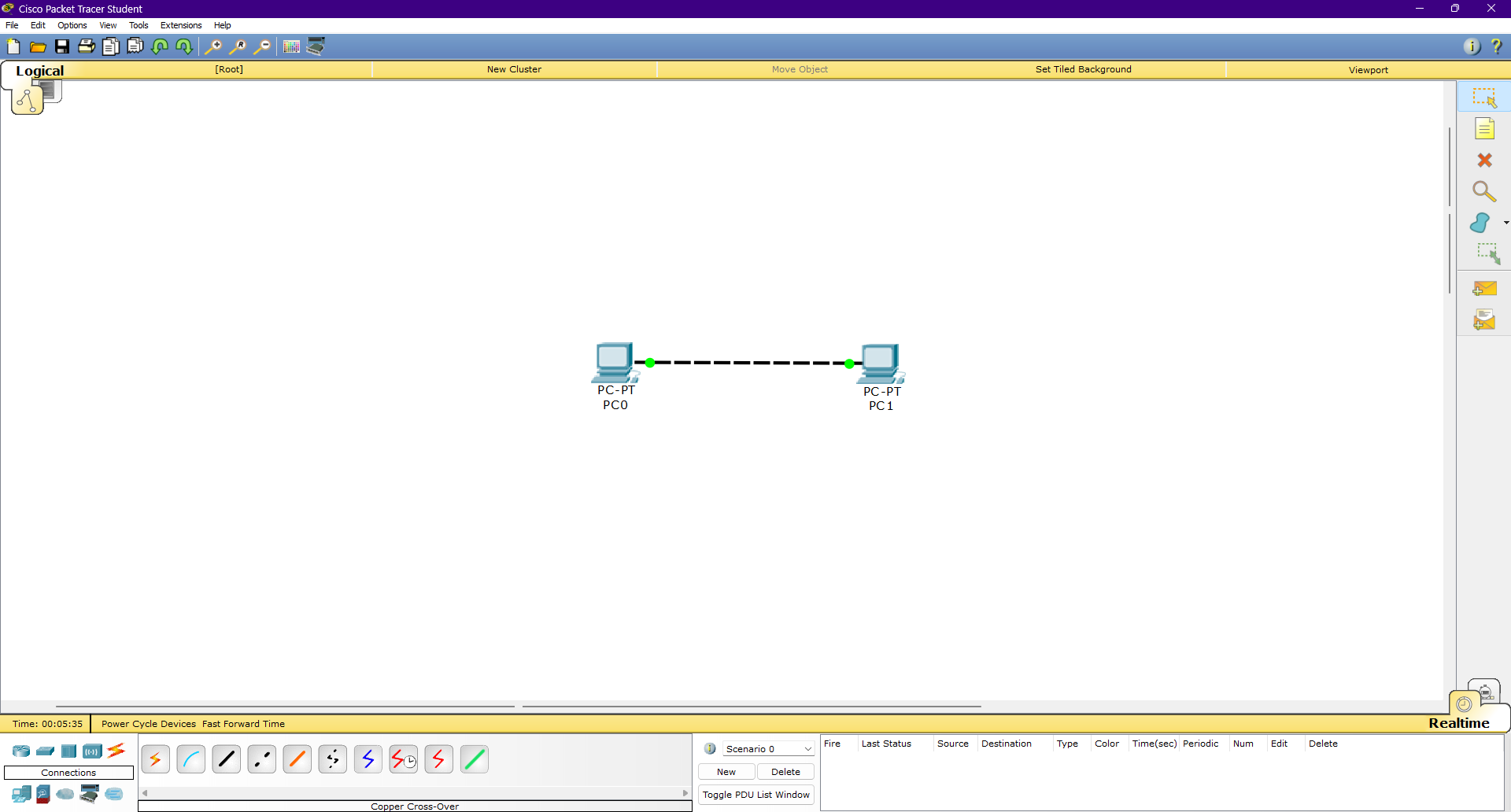


Рисунок 1.1 – Простейшая сеть из двух ПК

Теперь настроим первый ПК. На рисунке 1.2 представлена вся конфигурация первого ПК. Аналогичным образом и настроим второй ПК. Его настройка отображена на рисунке 1.3

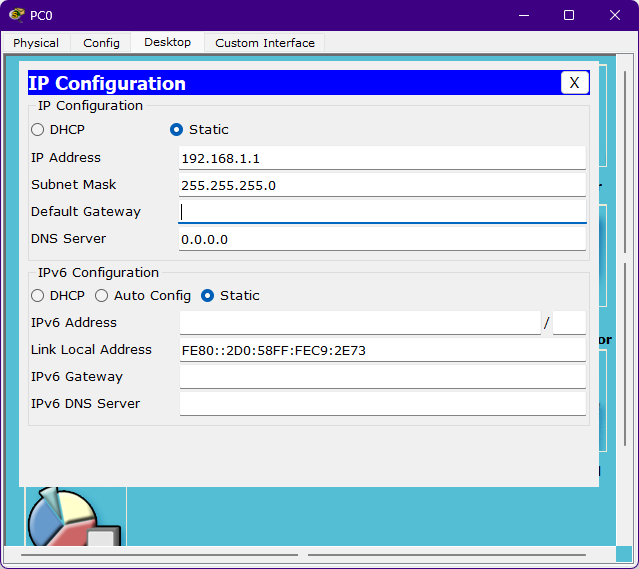


Рисунок 1.2 – Настройка первого ПК

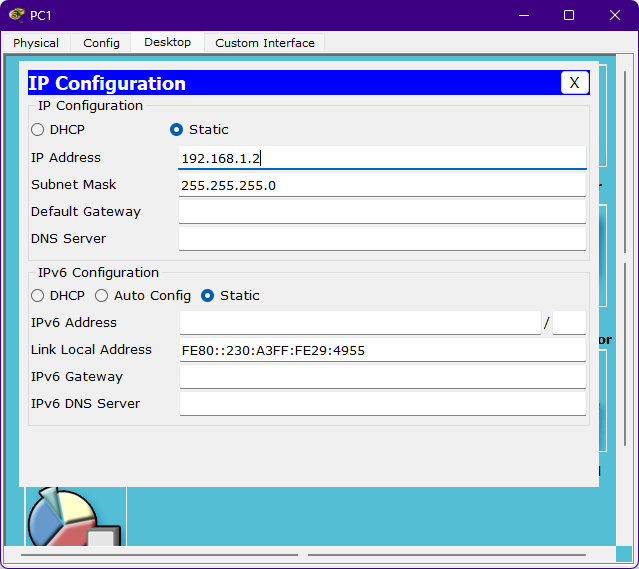


Рисунок 1.3 – Настройка второго ПК

Теперь проверим наличие связи ПК. Для этого заходим в командную строку нашего ПК и пропингуем второй ПК. Все это отображено на рисунке 1.4.

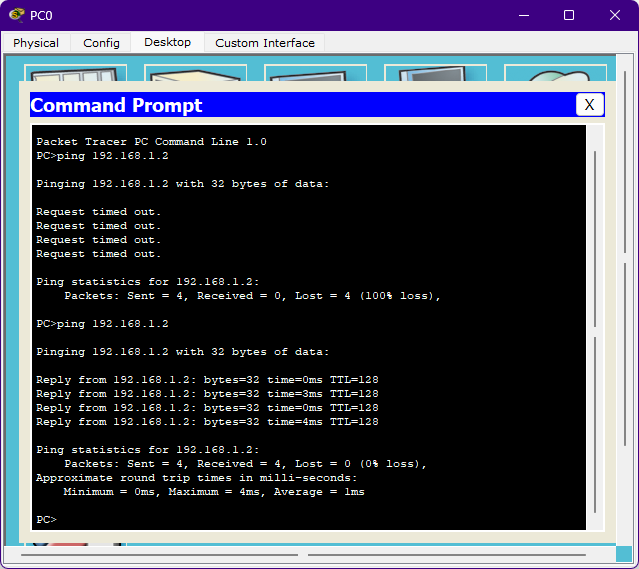


Рисунок 1.4 – Успешный пинг второго ПК

Задание 2. Организация Режима симуляции работы сети.

Сформируем схему сети, представленную на рисунке 1.5 и зададим каждому ПК ip 192.168.0.X и маску 255.255.255.0.

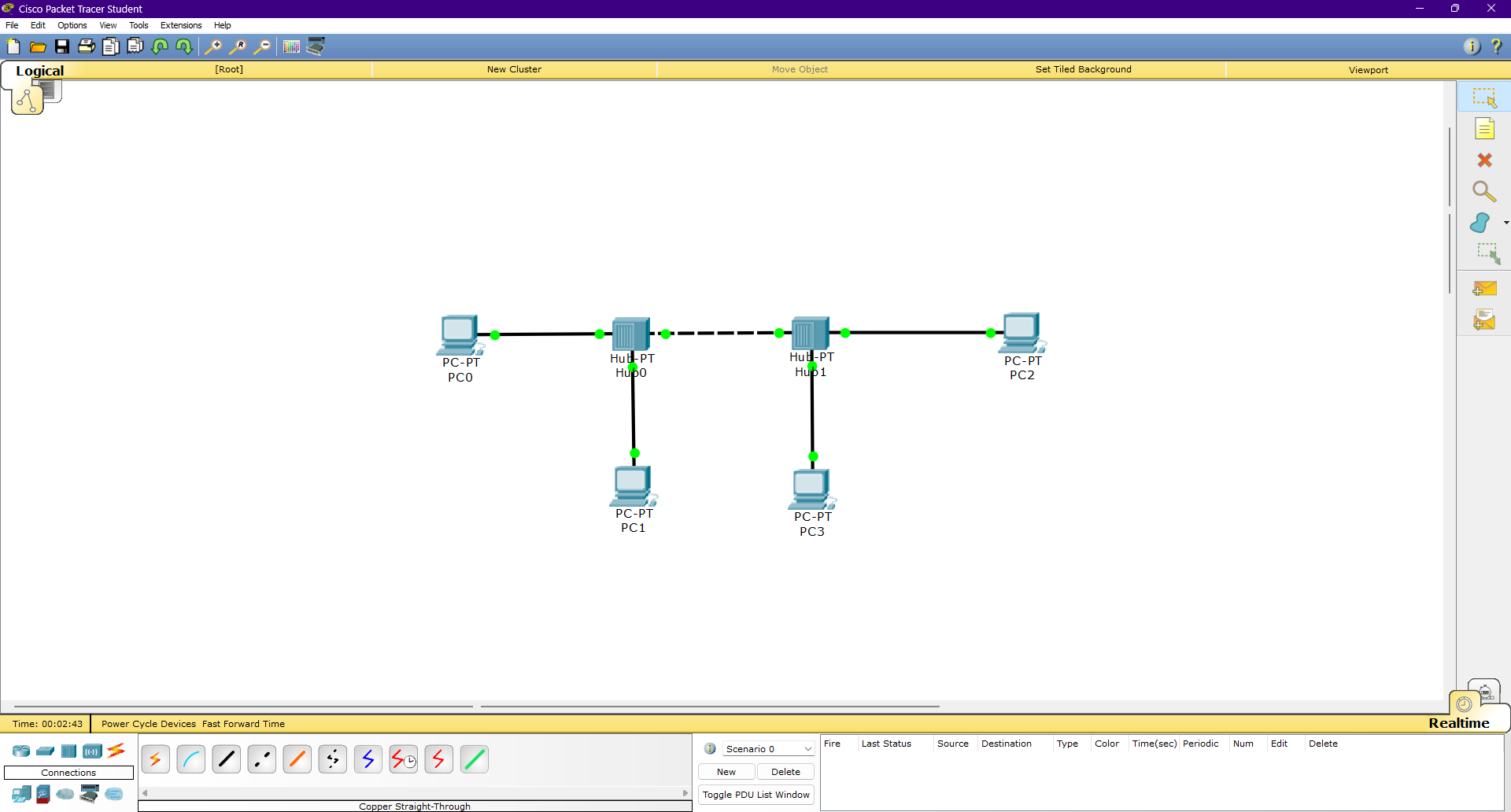


Рисунок 1.5 – Схема сети из 4 ПК и 2 Хабов

Запустим симуляцию и в фильтрах оставим только сетевой протокол ICMP. Он в основном используется для передачи сообщений об ошибках и других исключительных ситуациях, возникших при передаче данных.

С одного из хостов попробуем пропинговать другой узел. Для этого выбираем далеко расположенные друг от друга узлы для того, чтобы наглядней увидеть, как будут проходить пакеты по сети в режиме симуляции. На рисунке 1.6 с PC1 пингуем PC2.

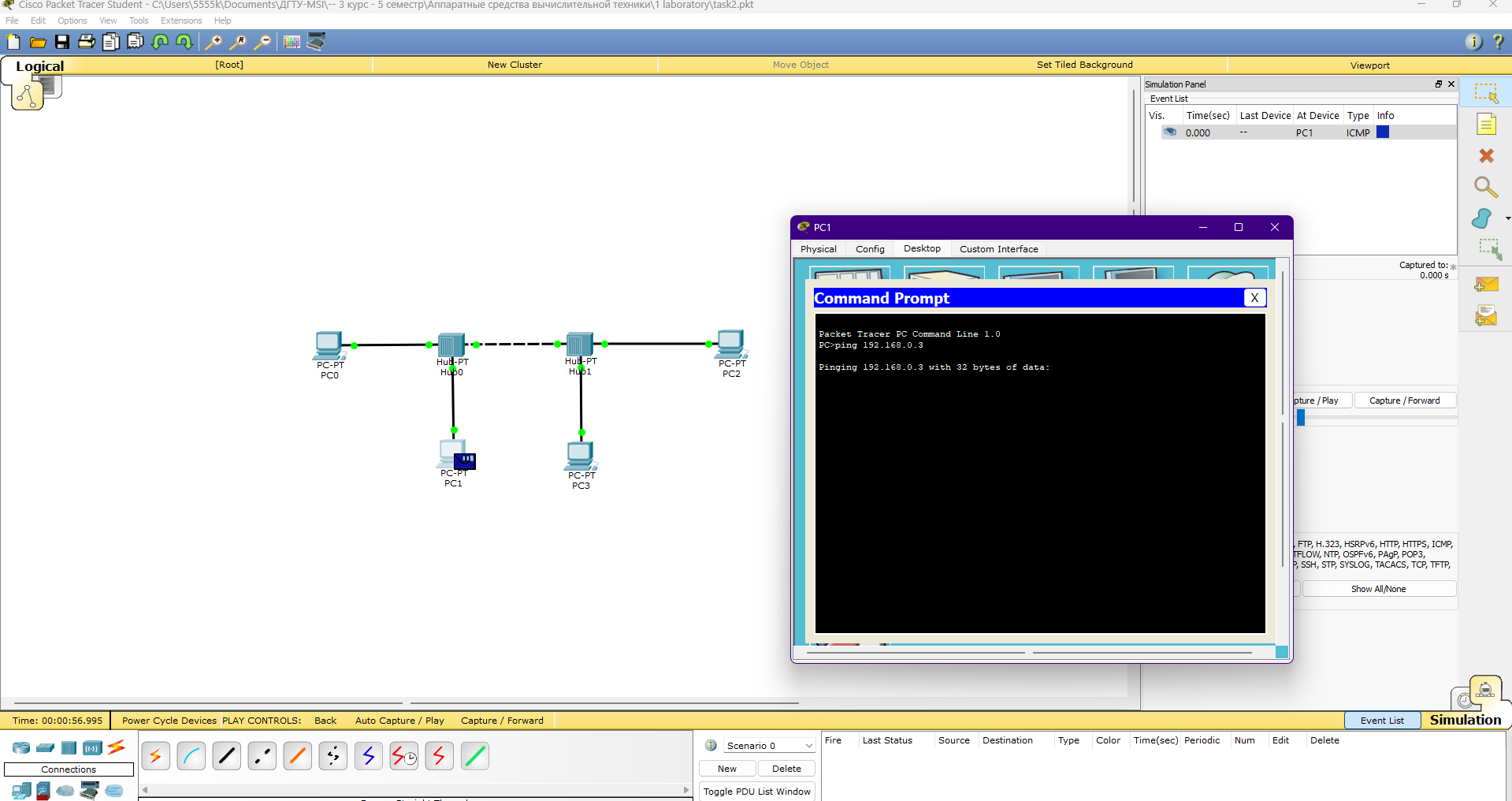


Рисунок 1.6 – ПК1 пингует ПК2 (начало процесса)

На PC1 образовался пакет, который ждёт начала движения его по сети. Запустить продвижение пакет в сеть пошагово можно, нажав на кнопку Вперёд в окне симуляции. Если нажать на кнопку Воспроизведение, то мы увидим весь цикл прохождения пакета по сети. Мы можем видеть успешный результат пинга на рисунке 1.7.

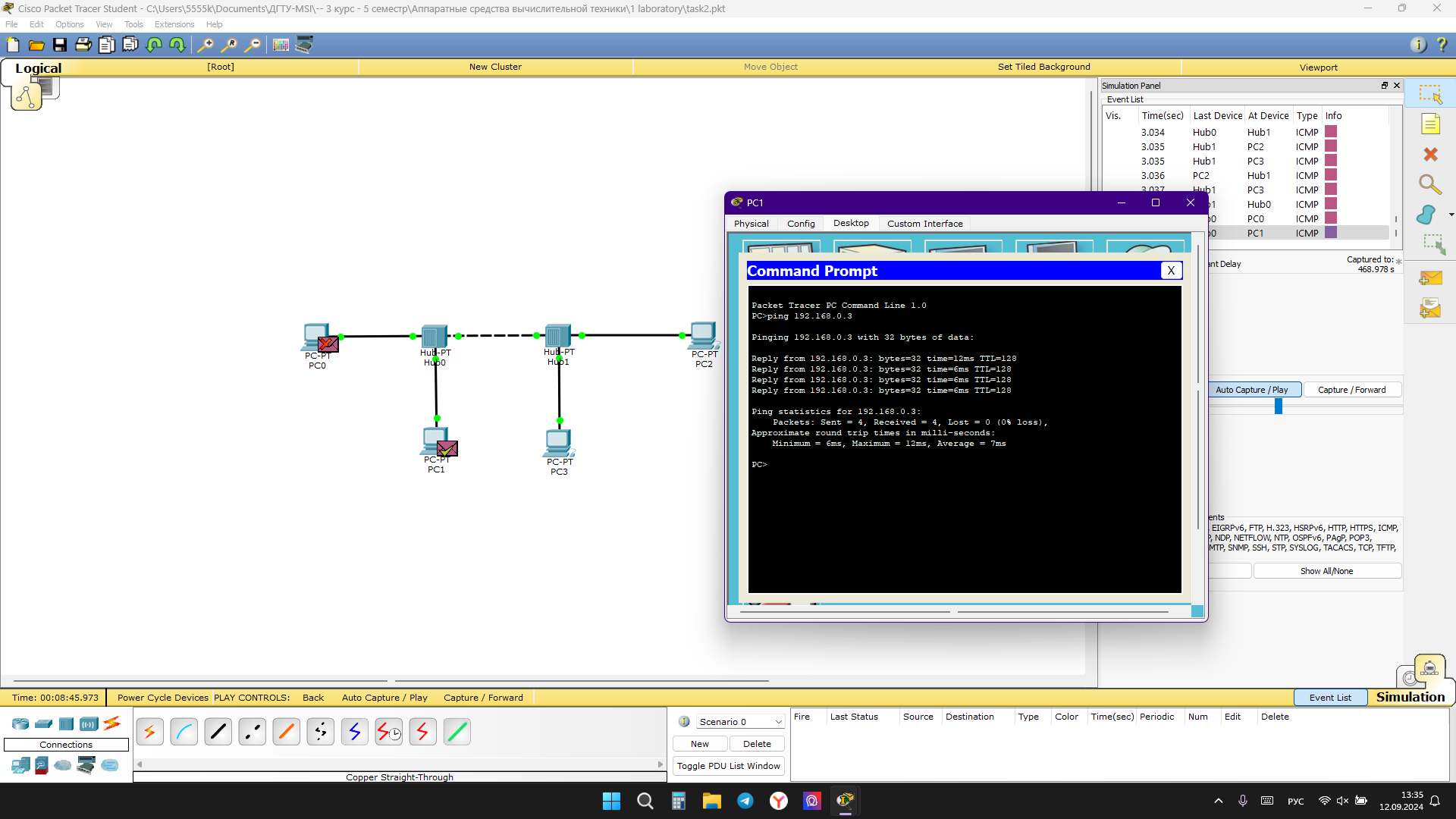


Рисунок 1.7 – Успешный пинг

Щелчок мышью на конверте покажет нам дополнительную информацию о движении пакета по сети. При этом на первой вкладке мы увидим модель OSI на рисунке 1.8. На вкладке OSI Model (Модель OSI) представлена информация об уровнях OSI, на которых работает данное сетевое устройство.

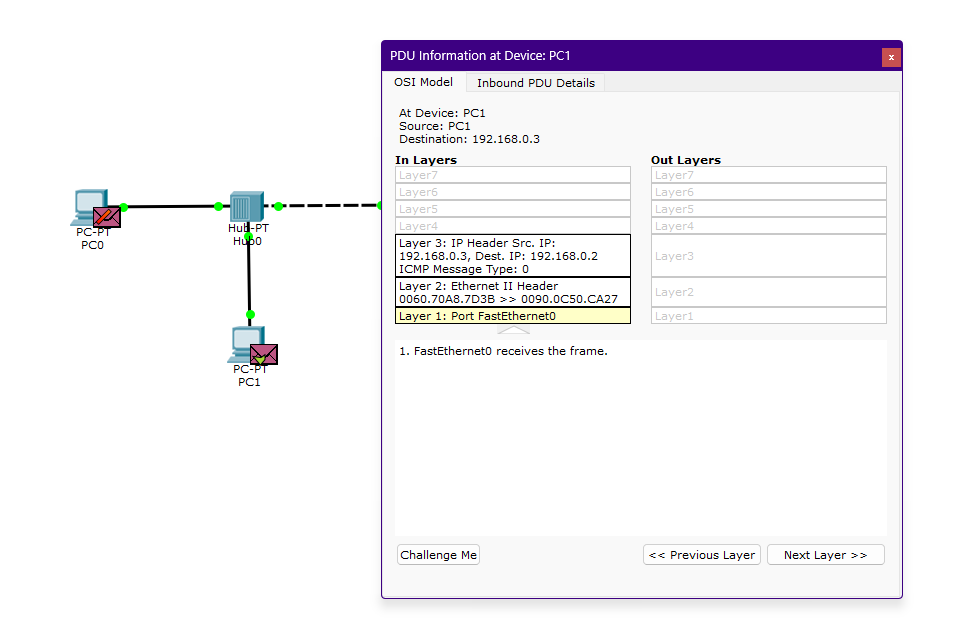


Рисунок 1.8 - Мониторинг движения пакета на модели OSI

**ЛАБОРАТОРНАЯ РАБОТА №2**

**Моделирование сети Traffic Generator**

Задание 1.1. Моделирование сети с топологией звезда на базе концентратора.

Построим сеть с топологией Звезда на базе концентратор, представленную на рисунке 2.1

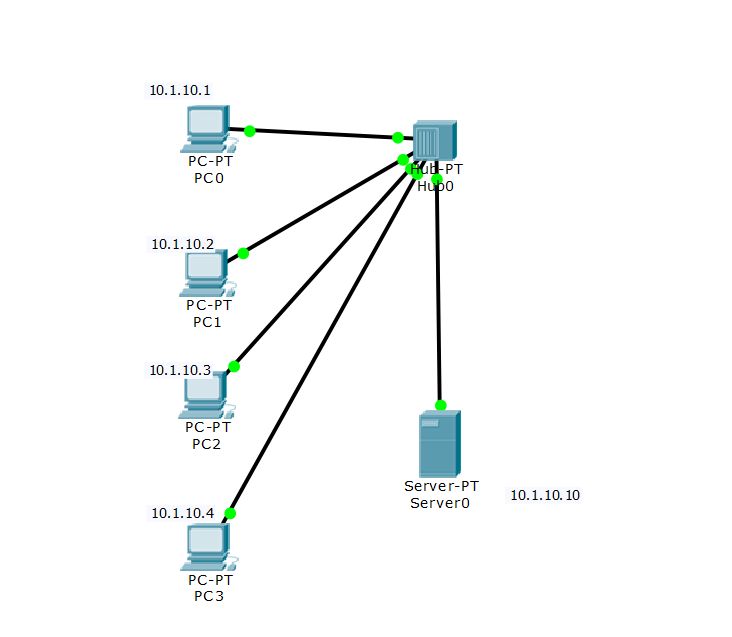


Рисунок 2.1 - Моделирование сети с топологией звезда на базе концентратора

Для проверки работоспособности сети отправим с компьютера на другой ПК тестовый сигнал ping и переключимся в режим Simulation (Симуляция). В окне Event list (Список событий), с помощью кнопки Edit filters (Изменить фильтры), сначала очистите фильтры от всех типов сигнала, а затем установим тип контроля сигнала: только ICMP.

Задание 1.2. Полезные приемы работы в CPT.

Предположим, что вам нужно спроектировать и настроить следующую сеть (рисунок 2.2). Рассмотрим, как можно ускорить и упростить этот процесс. Для создания копий ПК можно зажать ctrl и перекопировать все ПК. Итог показан на рисунке 2.3

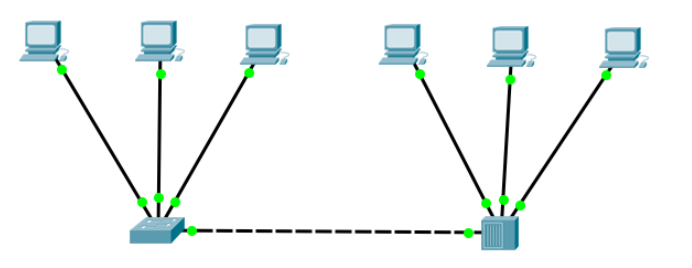


Рисунок 2.2 – Что нужно получить

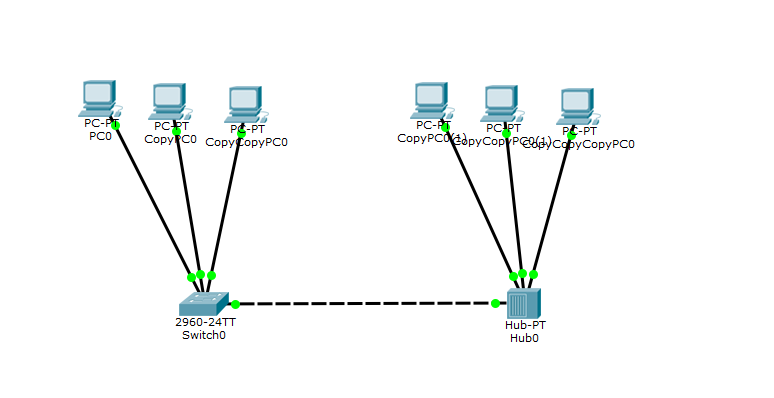


Рисунок 2.3 – Итог

Задание 2. Моделирование сети с топологией звезда на базе коммутатора.

Теперь рассмотрим аналогичную сеть (на базе Звезда) на базе коммутатора. Готовое решение представлено на рисунке 2.4.

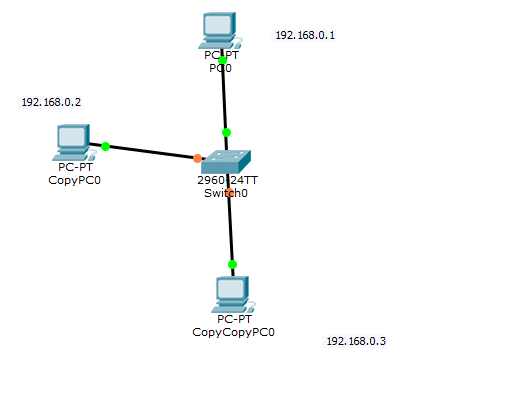


Рисунок 2.4 - Звезда на базе коммутатора модели 2960

Задание 1.3 Произведите проектирование локальной сети из хаба, коммутатора и 4х ПК.

Произведем данную схему, итоговое решение показано на рисунке 2.5



Рисунок 2.5 – Проектируемая сеть

Перед выполнением симуляции необходимо задать фильтрацию пакетов. Для этого нужно нажать на кнопку "Изменить фильтры", откроется окно, в котором нужно оставить только протоколы "ICMP" и "ARP". Кнопка "Авто захват/Воспроизведение" подразумевает моделирование всего ping-процесса в едином процессе, тогда как "Захват/Вперед" позволяет отображать его пошагово.

Задание 2. Исследование качества передачи трафика по сети

При исследовании пропускной способности ЛВС (качества передачи трафика по сети) желательно увеличить размер пакета и отправлять запросы с коротким интервалом времени, не ожидая ответа от удаленного узла для того, чтобы создать серьезную нагрузку на сеть. Однако, утилита ping не позволяет отправлять эхо-запрос без получения эхо-ответа на предыдущий запрос и до истечения времени ожидания. Поэтому для организации существенного трафика воспользуемся программой Traffic Generator. Для работы создадим и настроим следующую сеть (рисунок 2.6)

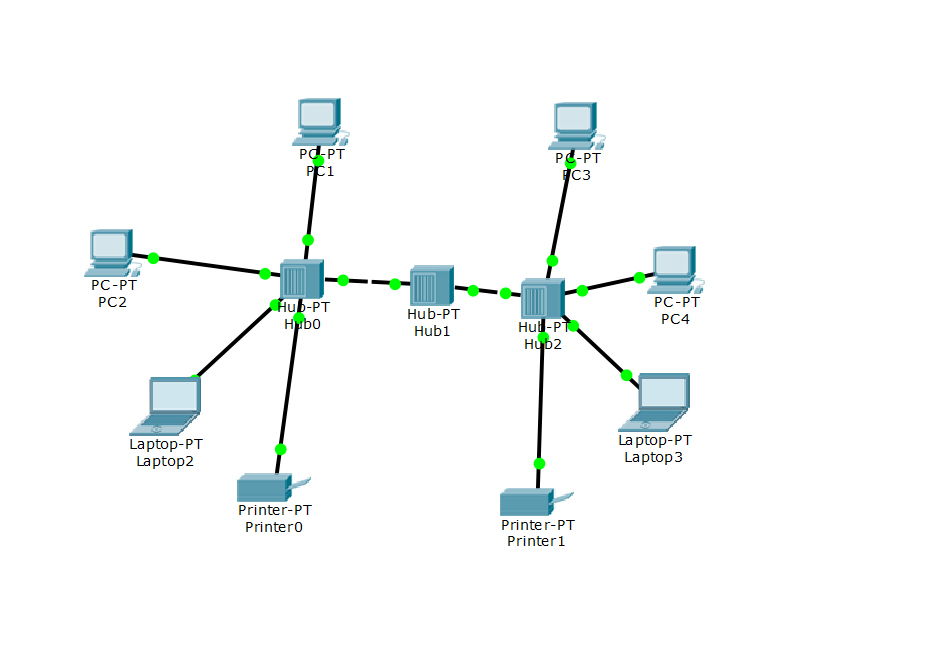


Рисунок 2.6 - Топология сети для нашей работы

В окне управления PC1 во вкладке Desktop выберите приложение Traffic Generator и задайте настройки, как на рис. 2.7 для передачи трафика от PC1 на PC3.

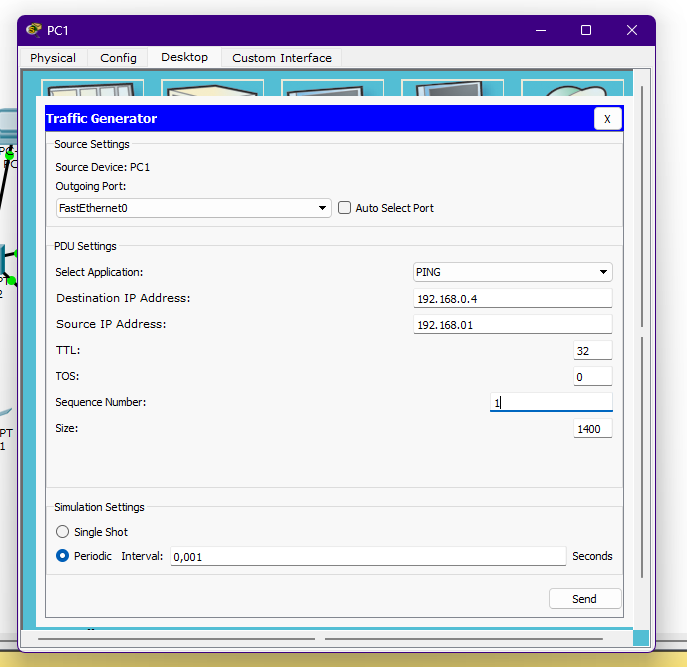
******

Рисунок 2.7 – Настройка генератора трафика

Для оценки качества работы сети передадим поток пакетов между РС1 и РС3 при помощи команды ping –n 200 192.168.0.4 и будем оценивать качество работы сети по числу потерянных пакетов. Параметр "–n" позволяет задать количество передаваемых эхо-запросов (у нас их 200) – рис. 2.8.

Одновременно с пингом, нагрузите сеть, включив генератор трафика на компьютере РС2 (узел назначения – РС3, размер поля данных–2500 байт, период повторения передачи - 0,1 сек. – рис. 2.9. На рисунке 2.10 видно, что было потеряно 3 пакета.

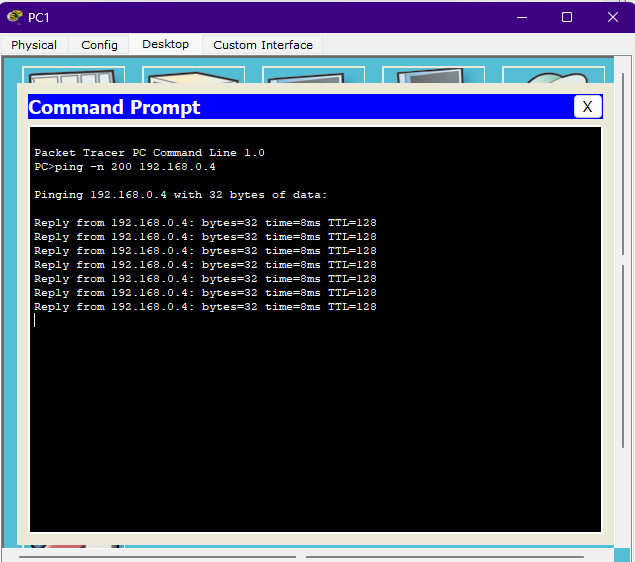


Рисунок 2.8 - отправляем 200 пакетов на PC3

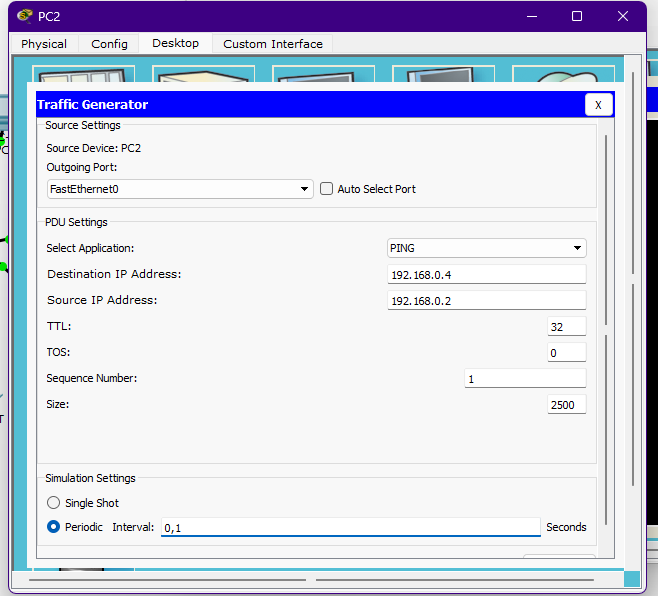


Рисунок 2.9 - Увеличиваем нагрузку на сеть

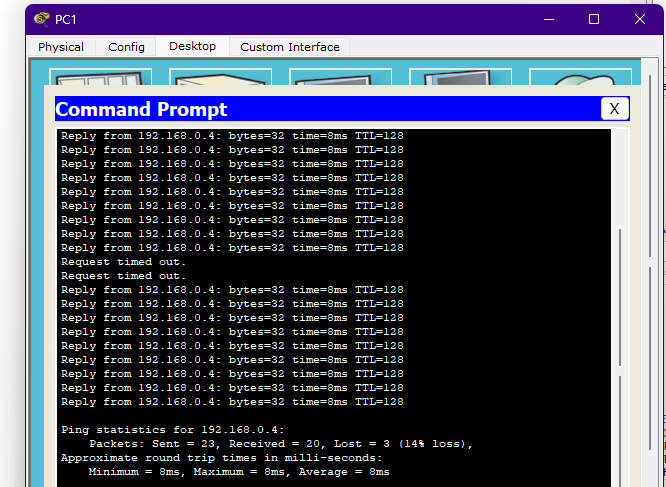


Рисунок 2.10 – Потеряно 3 пакета, отправлено 23, получено 20

Проверим тот факт, что установка коммутаторов вместо хабов устраняет возможность возникновения коллизий между пакетами пользователей сети. Замените центральный концентратор на коммутатор (рис. 2.11). Немного подождите и убедитесь, что сеть находится в рабочем состоянии - все маркеры портов не красные, а зеленые. Сделаем тоже самое, что и в прошлом опыте и получим, что потерялся уже один пакет (рисунок 2.12)



Рисунок 2.11 - Топология сети при замене центрального концентратора на коммутатор

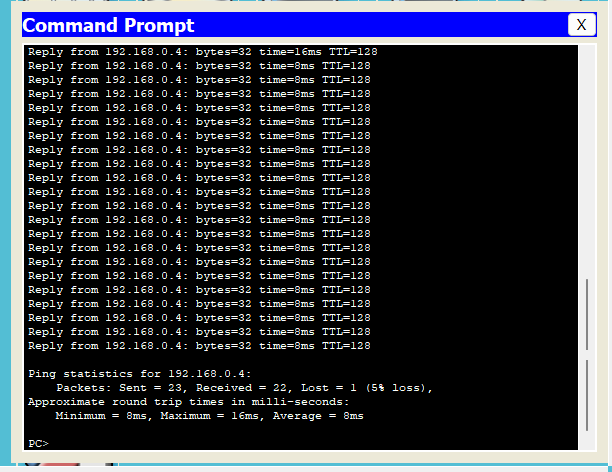


Рисунок 2.12 - Потерян 1 пакет

**ЛАБОРАТОРНАЯ РАБОТА №3**

**Знакомство с командами Cisco IOS**

Задание 1. Знакомство с командами Cisco IOS

Сделаем сеть для выполнения команд ОС Cisco IOS. Она представлена на рисунке 3.1

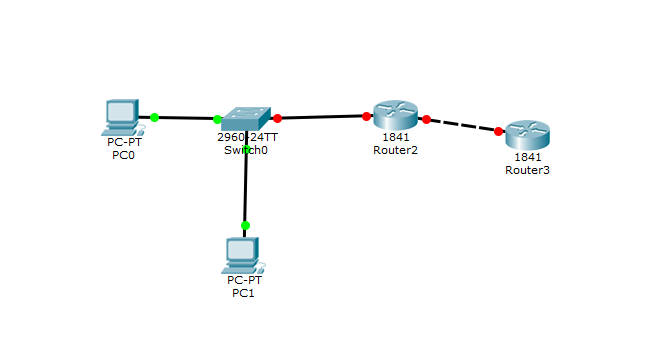


Рисунок 3.1 - Сеть для выполнения команд ОС CiscoIOS

Установим пароль на вход в привилегированный режим. Весь процесс отображен на рисунке 3.2.

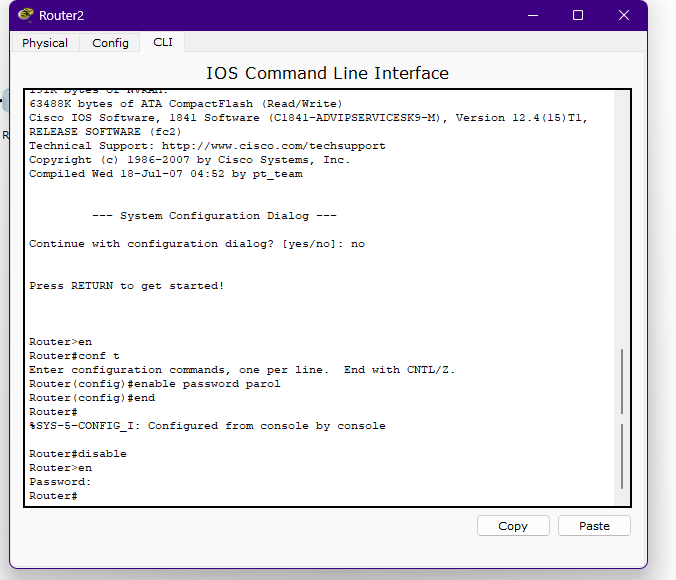


Рисунок 3.2 - Установка пароля на вход в привилегированный режим

Задание 2. Разработаем другую схему и сделаем всё то же самое. (рисунок 3.3)

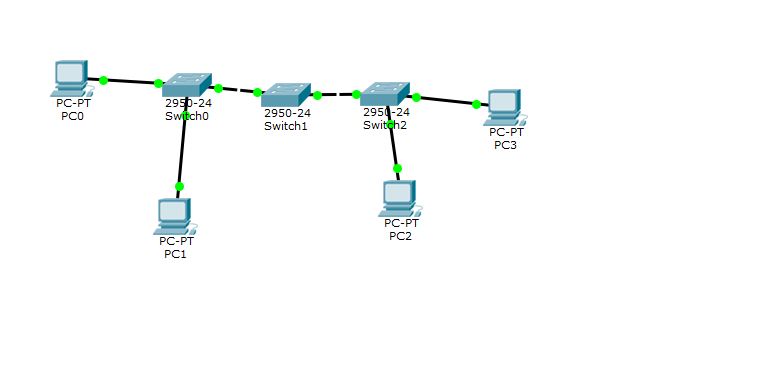


Рисунок 3.3 – Другая схема

**ЛАБОРАТОРНАЯ РАБОТА №4**

**Настройка WEB сервера**

Задание 1. Настраиваем WEB сервер

Для начала сделаем схему сети, она представлена на рисунке 4.1

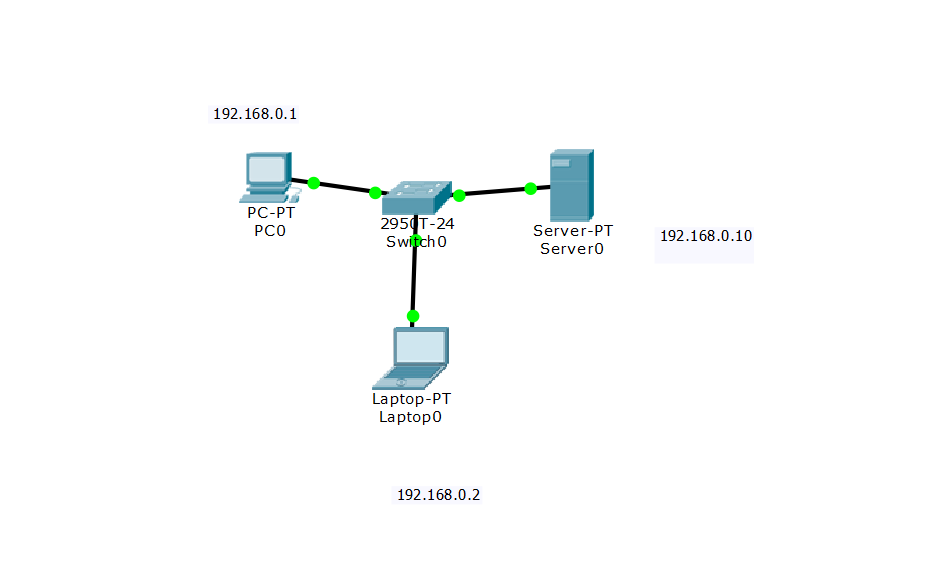


Рисунок 4.1 – Схема сети

Теперь создадим WEB-документ на сервере. Для создания HTTP-сервера открываем на сервере вкладку HTTP и редактируем первую страницу сайта с названием index.html. Включаем службу HTTP переключателем On (рисунок 4.2).

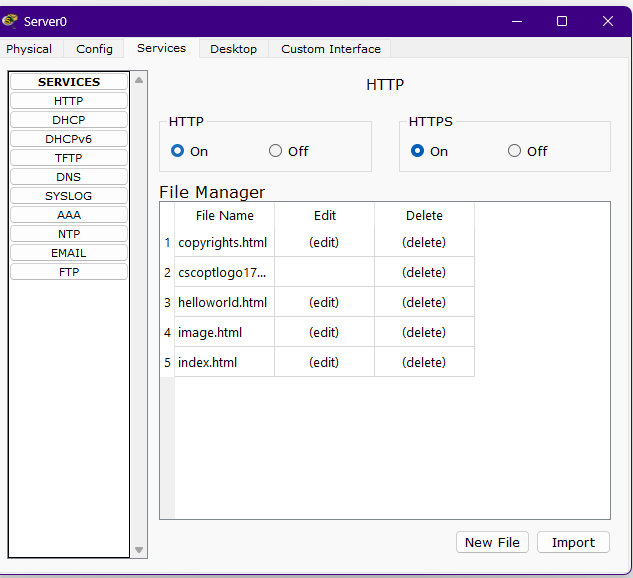


Рисунок 4.2 – Включение службы HTTP

В index.html введем другой текст (рисунок 4.3) и получим новую страничку (рисунок 4.4)

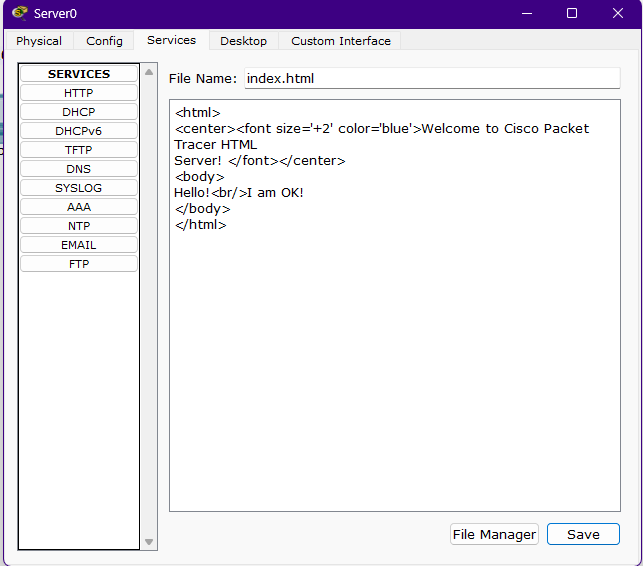


Рисунок 4.3 – Текст HTTP-файла

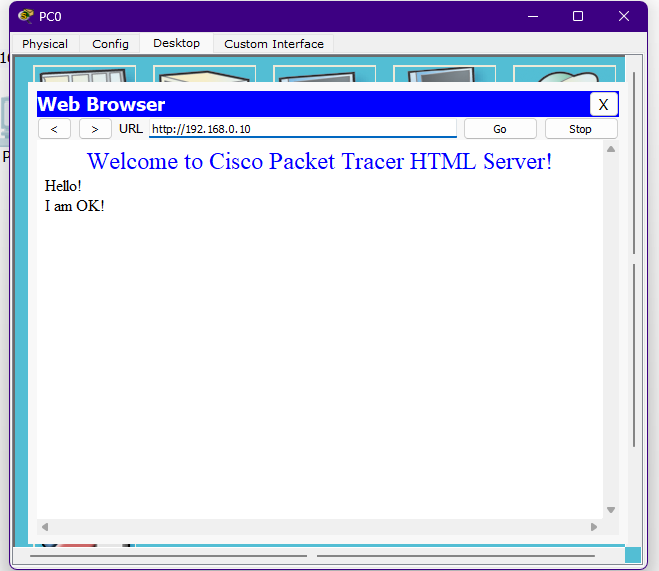


Рисунок 4.4 – Полученный результат

Задание 2. Настройка сетевых сервисов DNS, DHCP и Web

Создадим новую схему, представленную на рисунке 4.5.

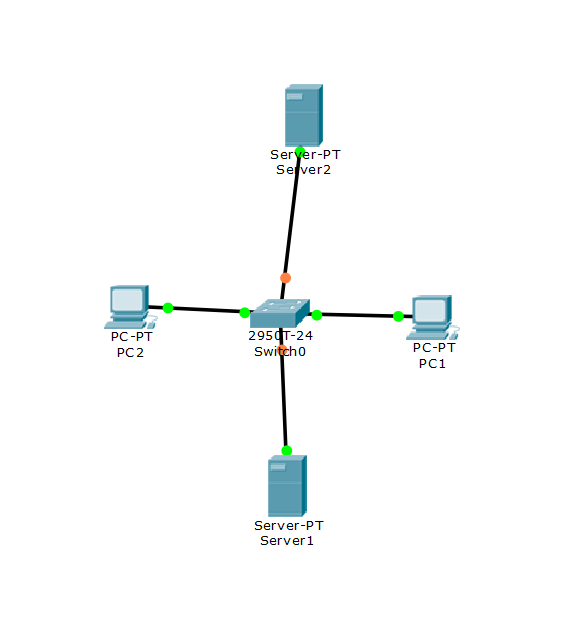


Рисунок 4.5 – Схема сети

Наша задача состоит в том, чтобы настроить Server1 как DNS и Web-сервер, а Server2 как DHCP сервер. Работа DNS-сервера заключается в преобразовании доменных имен серверов в IP адреса. DHCP сервер позволяет организовывать пулы для автоматического конфигурирования сетевых интерфейсов, то есть, обеспечивает автоматическое распределение IP-адресов между компьютерами в сети. Иначе говоря, в нашем случае компьютеры получают IP-адреса благодаря сервису DHCP Server2 и открывают, например, сайт на Server1.

Войдем в конфигурацию PC1 и PC2 и установите настройку IP через DHCP сервер рис. 4.6

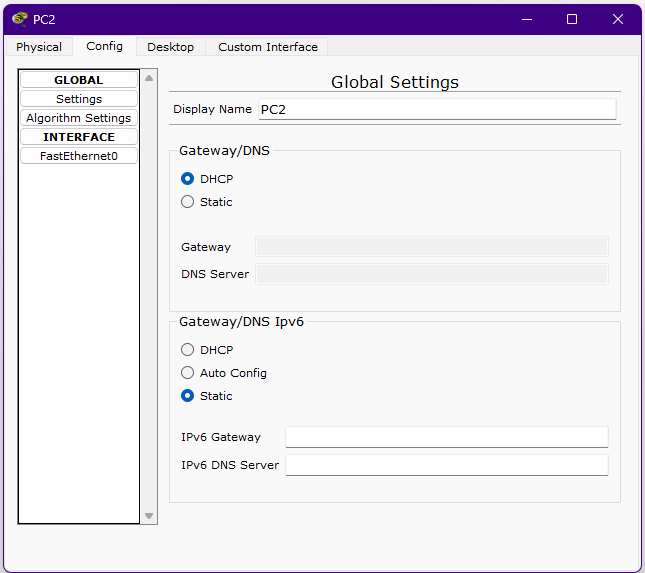


Рисунок 4.6 – Настройка IP на PC2

Зададим в конфигурации серверов настройки IP: Server1 – 10.0.0.1 (рис. 4.7), Server2 – 10.0.0.2 (рис. 4.8). Маска подсети установится автоматически как 255.0.0.0.

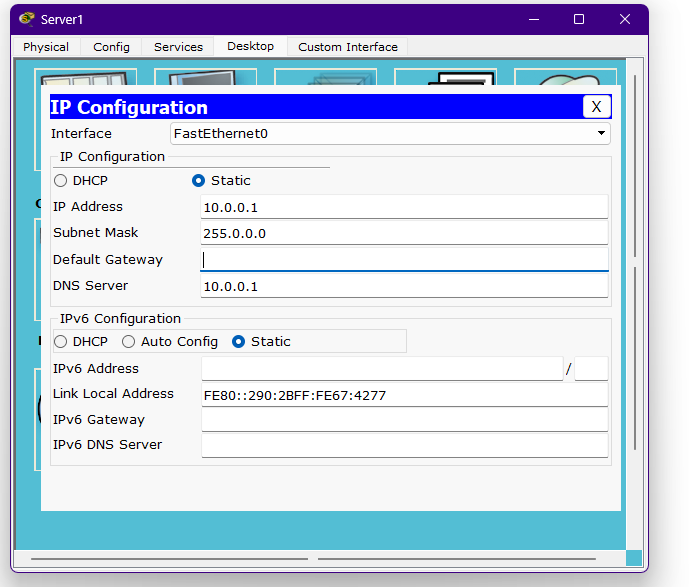


Рисунок 4.7

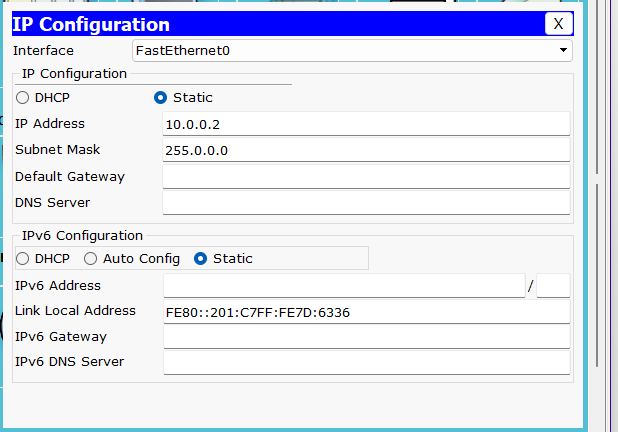


Рисунок 4.8

Теперь в конфигурации Server1 войдем на вкладку DNS и зададим две ресурсные записи (Resource Records) в прямой зоне DNS. (Рисунок 4.9)

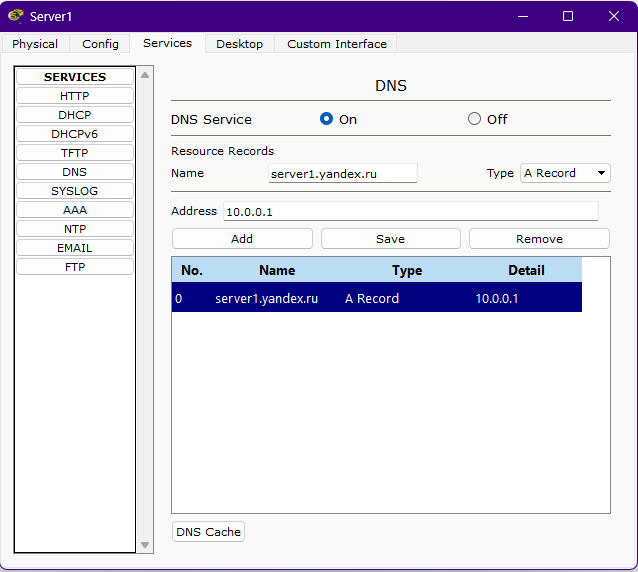


Рисунок 4.9 - Ввод ресурсной записи типа A Record

Далее в ресурсной записи типа CNAME свяжите название сайта с сервером и нажмите на кнопку Add (добавить) – рис. 4.10.

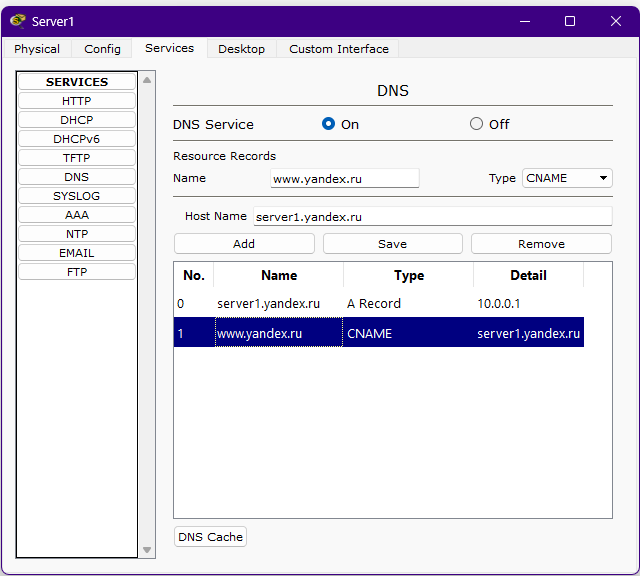


Рисунок 4.10 - Ввод ресурсной записи типа CNAME

Теперь настроим службу HTTP. В конфигурации Server1 войдите на вкладку HTTP и создайте стартовую страницу сайта (рис. 4.12).

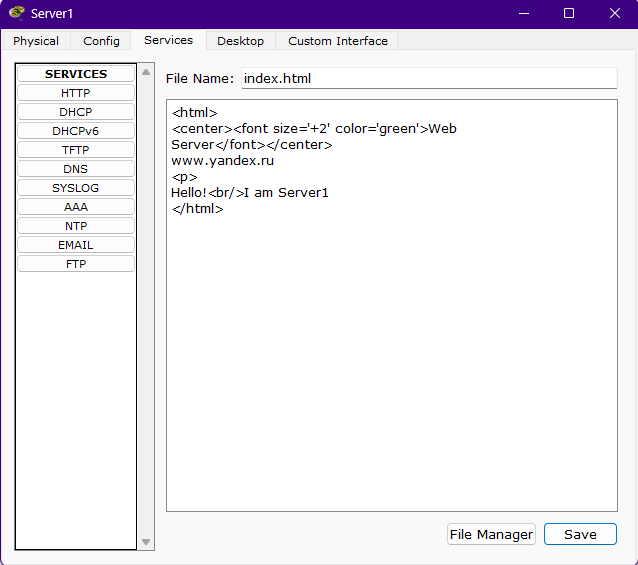


Рисунок 4.12 – Стартовая страница сайта

Включаем командную строку на Server1 и проверяем работу службы DNS. Для проверки правильности работы прямой зоны DNS сервера введите команду SERVER>nslookup . Если все правильно настроено, то вы получите отклик на запрос с указанием доменного имени DNS сервера в сети и его IP адреса (рис. 4.13).

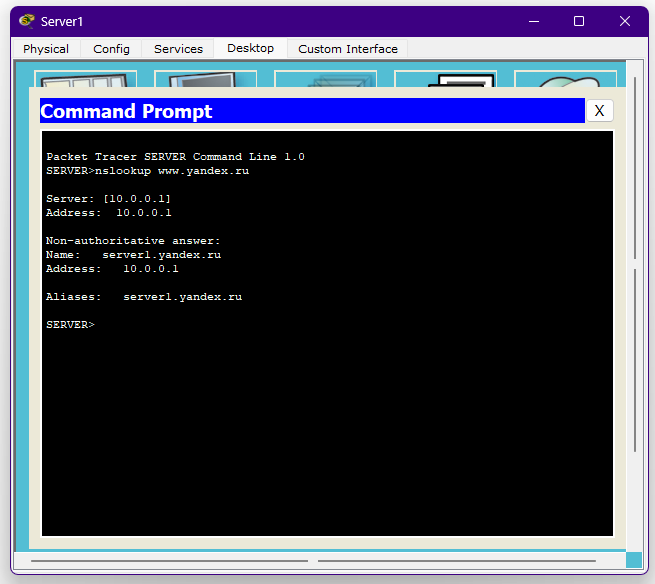


Рисунок 4.13 - Служба DNSв прямой зоне DNSна Server1 настроена правильно

Теперь войде в конфигурацию Server2 и на вкладке DHCP настроим службу DHCP. Для этого набере новые значения пула, установим переключатель On и нажмем на кнопку Save (Сохранить) - рис. 4.14.

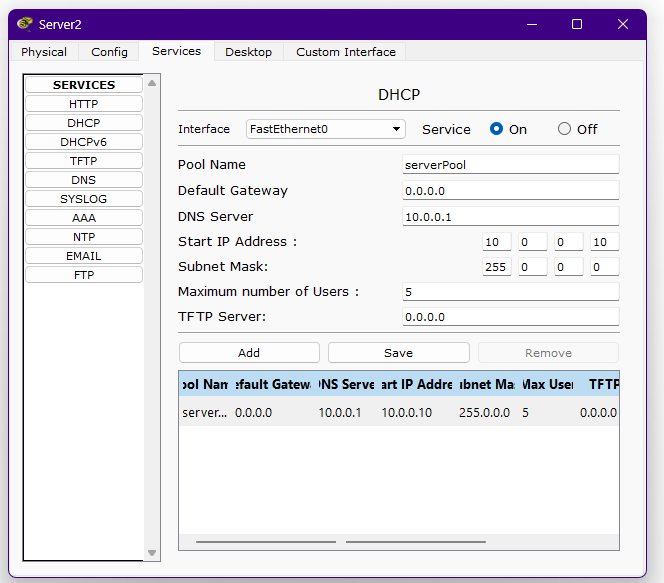


Рисунок 4.14 - Настройка DHCP сервера

Войдем в конфигурации хоста PC1 и PC2 и в командной строке сконфигурируйте протокол TCP/IP. Для этого командой PC> ipconfig /release сбросим (очистим) старые параметры IP адреса (рис. 4.15).

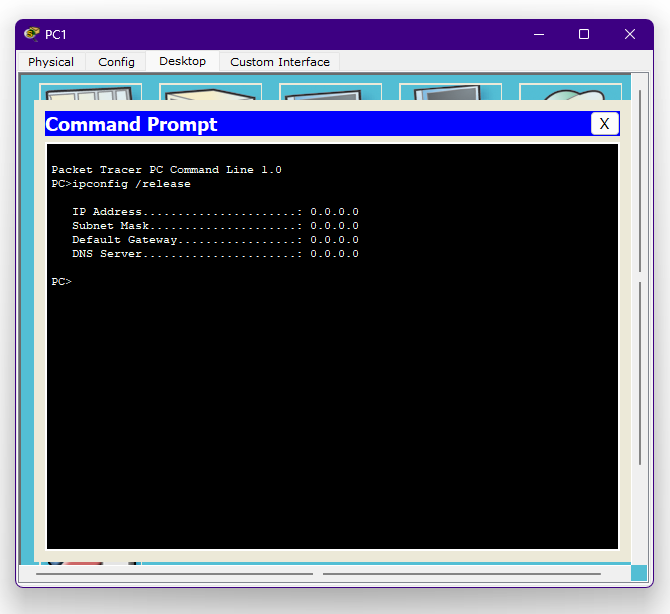


Рисунок 4.15 - Удаление конфигурации IP-адресов для всех адаптеров

Теперь командой PC> ipconfig /renew получим новые параметры от DHCP сервера (рис. 4.16).

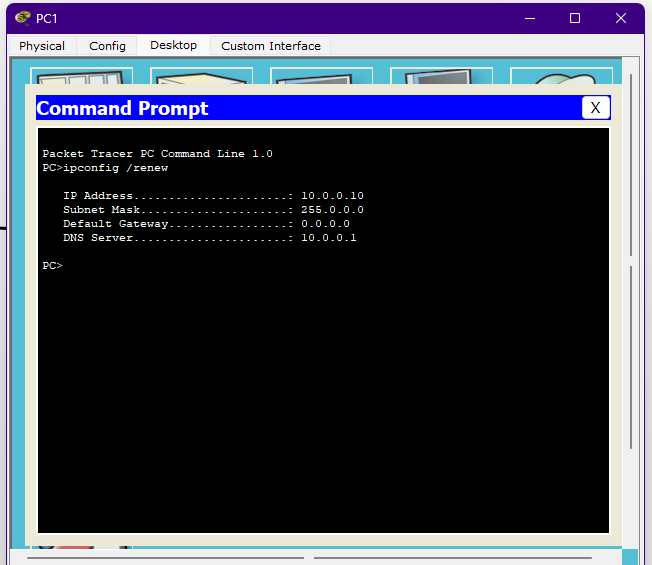


Рисунок 4.16 - Конфигурация протокол TCP/IP клиента от DHCP сервера

Осталось проверить работу WEB сервера Server1 и открыть сайт в браузере на PC1 или PC2 (рис. 4.18).

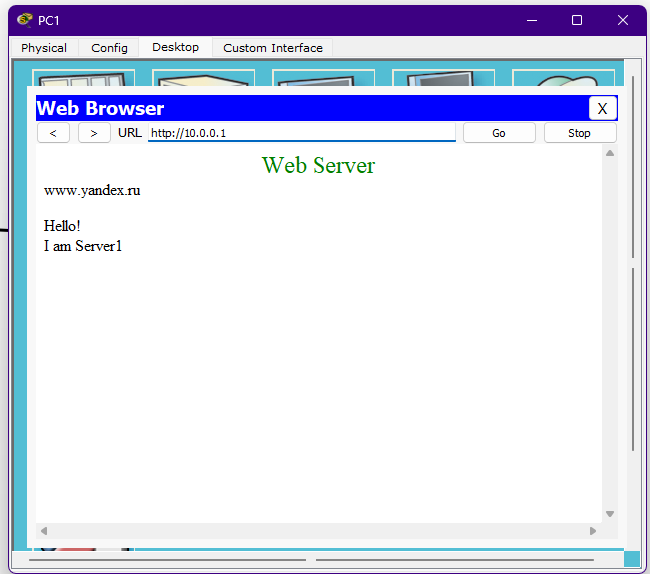


Рисунок 4.18 - Проверка работы службы HTTP на Server1

Задание 2. Конфигурирование DHCP сервера на маршрутизаторе

Создадим новую схему, приведенную на рисунке 4.19

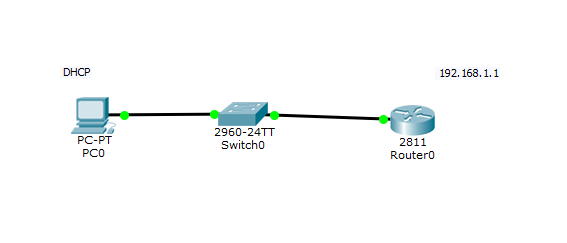


Рисунок 4.19 – Схема сети

Произведем настройку R0:

Router (config)#ip dhcp pool TST создаем пул IP адресов для DHCP сервера с именем TST

Router (dhcp-config)#network 192.168.1.0 255.255.255.0 указываем из какой сети мы будем раздавать IP адреса (первый параметр - адрес данной сети, а второй параметр ее маска)

Router (dhcp-config)#default-router 192.168.1.1 указываем адрес основного шлюза, который будет рассылать в сообщениях DHCP

Router (dhcp-config)#dns-server 5.5.5.5 указываем адрес DNS сервера, который так же будет рассылаться хостам в сообщениях DHCP

Router (dhcp-config)#exit

Router (config)#ip dhcp excluded-address 192.168.1.1 этот хост исключен из пула, то есть, ни один из хостов сети не получит от DHCP сервера этот адрес.

Полный листинг этих команд приведен на рис. 4.20. На рисунке 4.21 представлен факт того, что всё работает

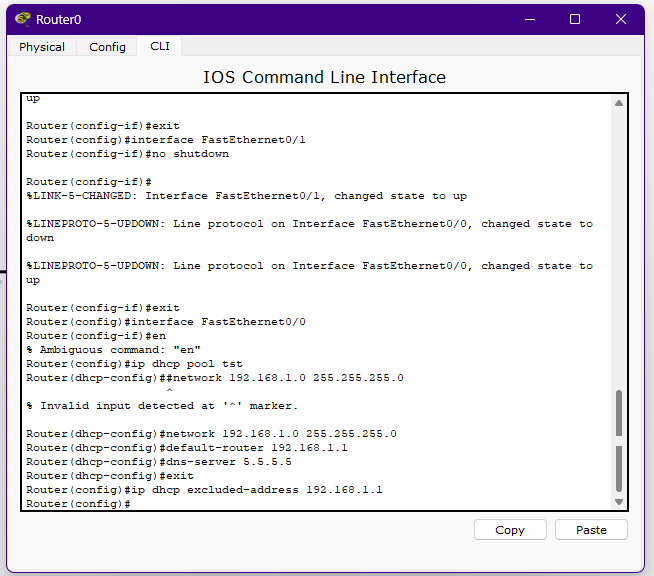


Рисунок 4.20 - Команды для конфигурирования R0

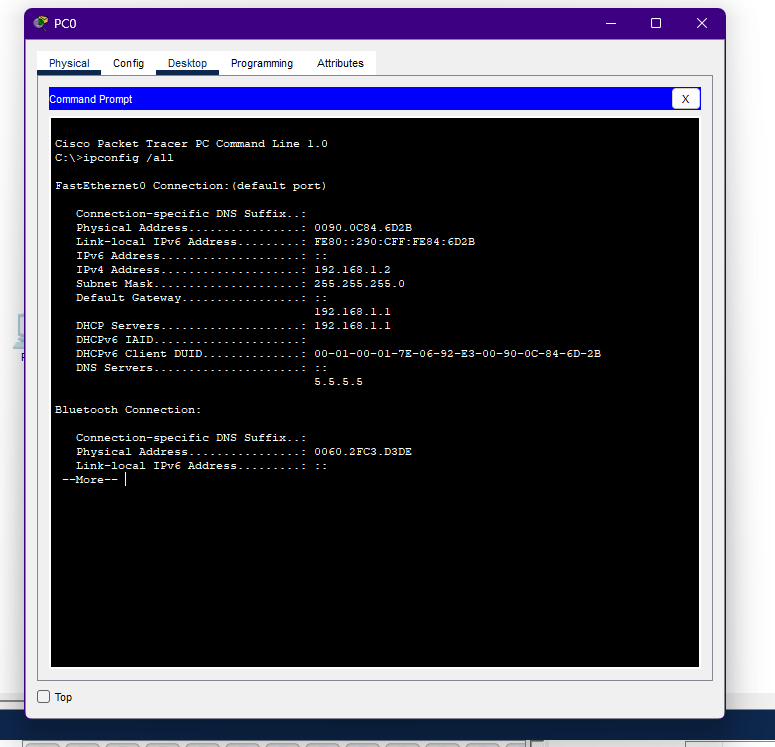


Рисунок 4.21 – Всё успешно

Задание 3. Построим схему. (Рисунок 4.22). Затем конфигурируем интерфейс Fa0/0 для R0 (рисунок 4.23).

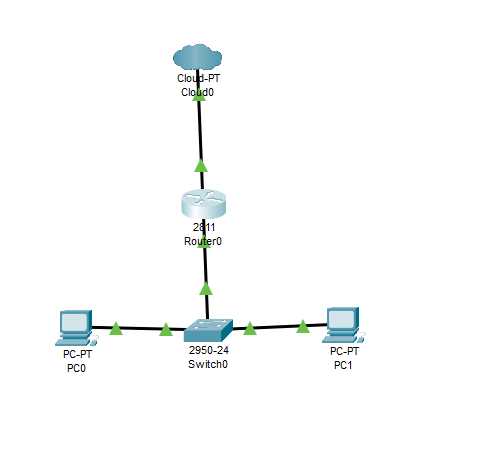


Рисунок 4.22 – Схема сети

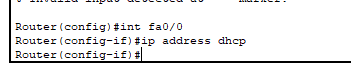


Рисунок 4.23 – Конфигурация интерфейса

После заходим в любой пк и пишем в терминале ipconfig /all и наблюдаем, что ничего больше не работает (Рисунок 4.24)

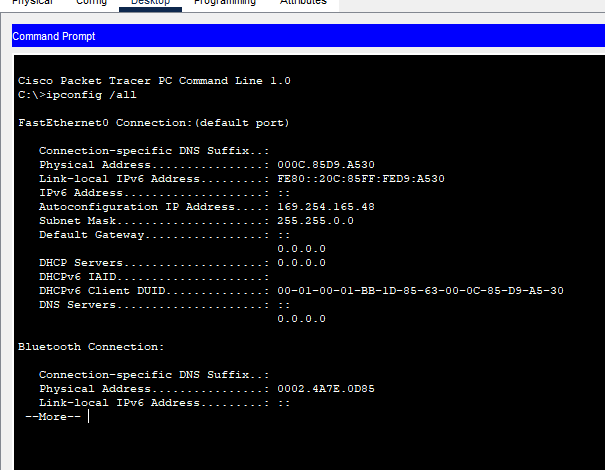


Рисунок 4.24 – Ничего не работает

После настройки интерфейса роутера на получение настроек по DHCP, DHCP клиент на PC0 перестал получать IP-адрес – IP из диапазона 169.254.x.x/16 назначается автоматически самим ПК при проблемах с получением адреса по DHCP. Интерфейс роутера IP-адрес так же не получит т.к. в данной подсети нет DHCP серверов.

Задание 4. DHCP сервис на маршрутизаторе 2811.

Будем конфигурировать маршрутизатор 2811, а именно, настраивать на нем DHCP сервер, который будет выдавать по DHCP адреса из сети 192.168.1.1 (рис. 4.25). PC0 и PC1 буду получать настройки динамически, а для сервера желательно иметь постоянный адрес, т.е., когда он задан статически.

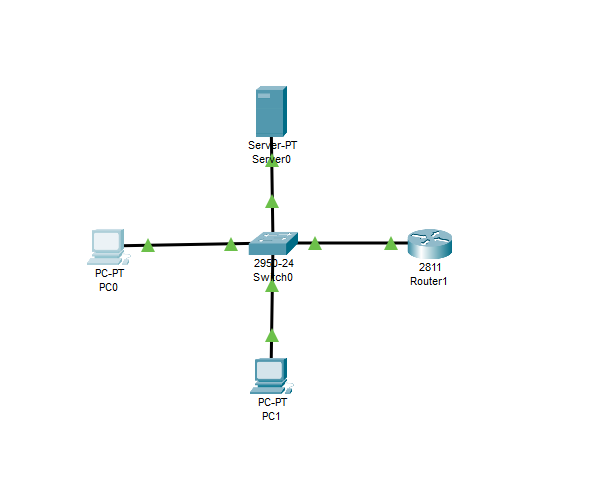


Рисунок 4.25 – Схема сети

Далее настроим конфигурацию (рисунок 4.26) и проверим всё на пк (рисунок 4.27)

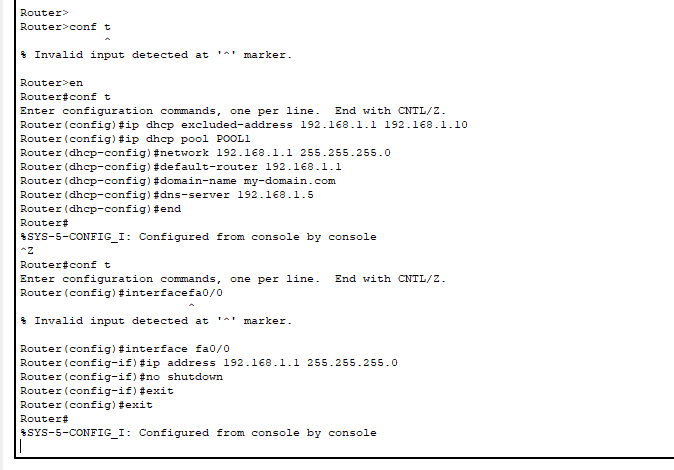


Рисунок 4.27 - Конфигурация

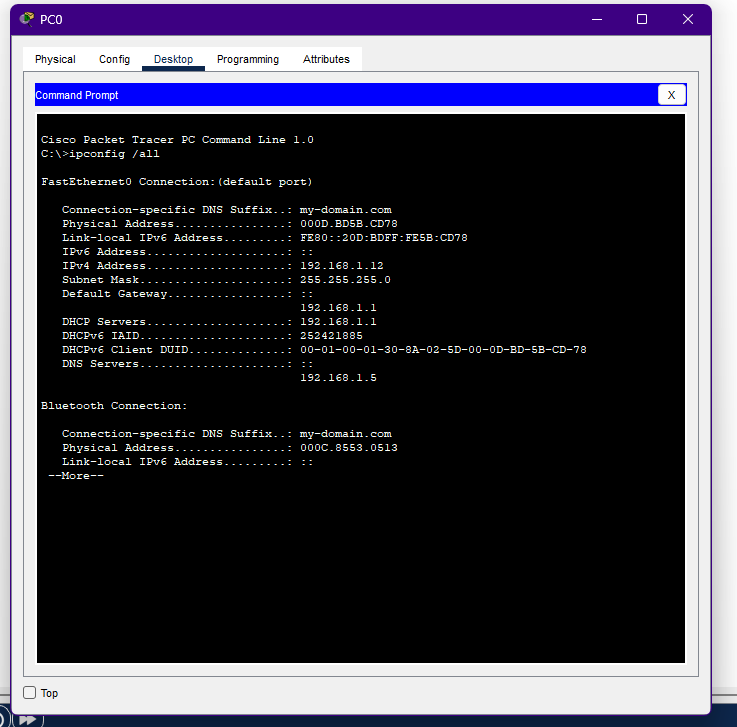


Рисунок 4.28 – Всё успешно

**ЛАБОРАТОРНАЯ РАБОТА №5**

**Статическая маршрутизация**

Задание 1. Настраиваем связь двух сетей через маршрутизатор

Построим следующую сеть, представленную на рисунке 5.1

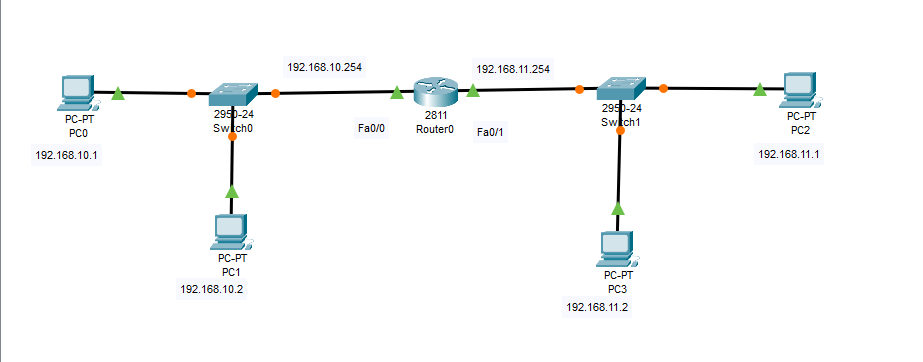


Рисунок 5.1 – Постановка задачи

Сделаем следующее:

1. Задали статические IP, подмаски и шлюзы во всех ПК
2. Задали IP роутеру на оба подключения (рисунок 5.2) - Аналогично настраиваем роутер как шлюз 192.168.11.254 для второй сети на интерфейсе Fa0/1

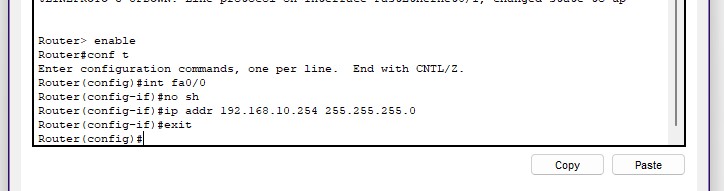


Рисунок 5.2 – Настройка роутера

1. Проверяем таблицу маршрутизации командой show ip route (рисунок 5.3)

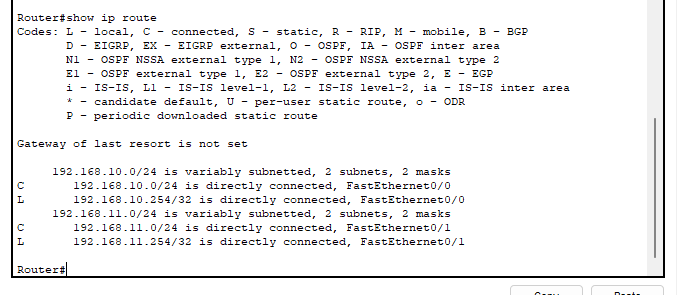


Рисунок 5.3 – Проверяем таблицу маршрутизации

1. Проверяем связь роутера и ПК (рисунок 5.4) + аналогично с 192.168.11.0

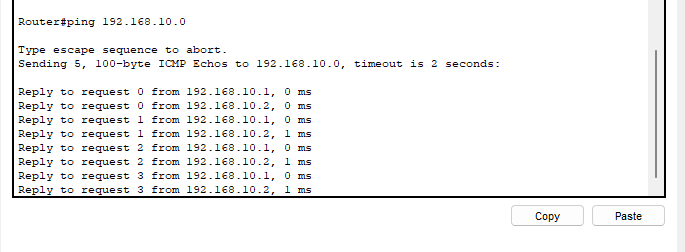


Рисунок 5.4 – Проверяем связь роутера со всеми ПК

1. Проверяем связь роутера с подсетями (рисунок 5.5) + аналогично 192.168.10.0

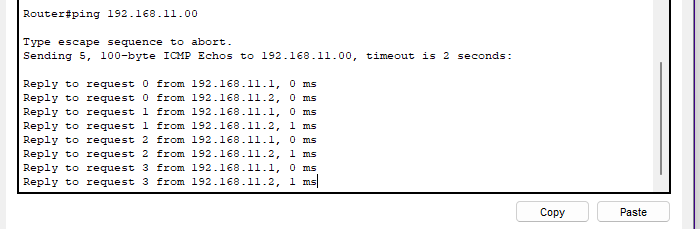


Рисунок 5.5 – Проверяем связь роутера с подсетями

1. Проверяем связь между PC0 и PC2 (рисунок 5.6)

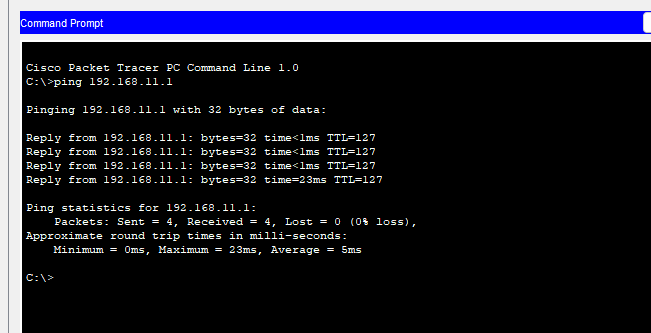


Рисунок 5.6 – Проверяем связь между PC0 и PC2

Задание 2. Настройка трех сетей с WEB сервером. Понятие маршрута по умолчанию

Для начала построим следующую схему, представленную на рисунке 5.7.

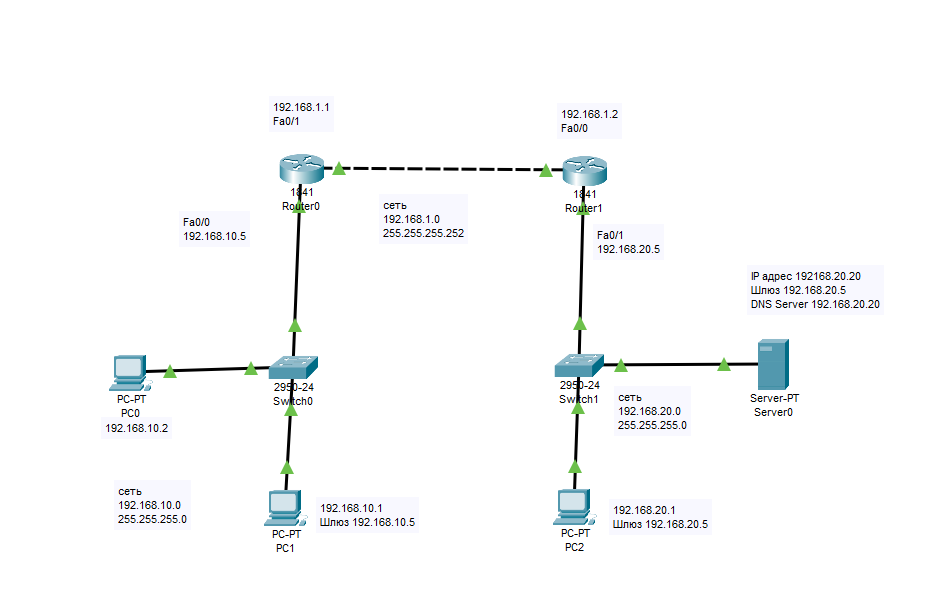


Рисунок 5.7 – Постановка задачи

Настроим порт 0/1 для маршрутизатора R0 (рисунок 5.8)

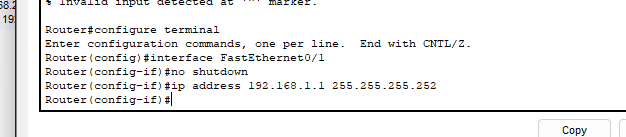


Рисунок 5.8 – Настраиваем порт 0/1 для маршрутизатора R0

Теперь настроим порт Fa0/0 маршрутизатора R0 на работу с сетью 192.168.10.0 (рисунок 5.9)

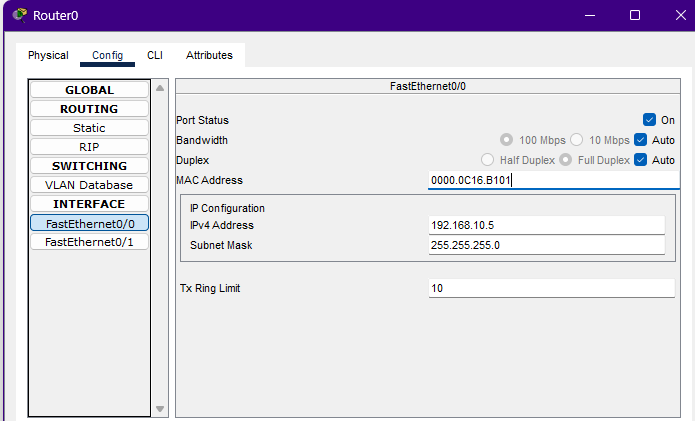


Рисунок 5.9 – Настройка порта 0/0 R0 на работу с сетью 192.168.10.0

Аналогично для порта Fa0/1 маршрутизатора R1 настроим на работу с сетью 192.168.20.0 (рисунок 5.10)

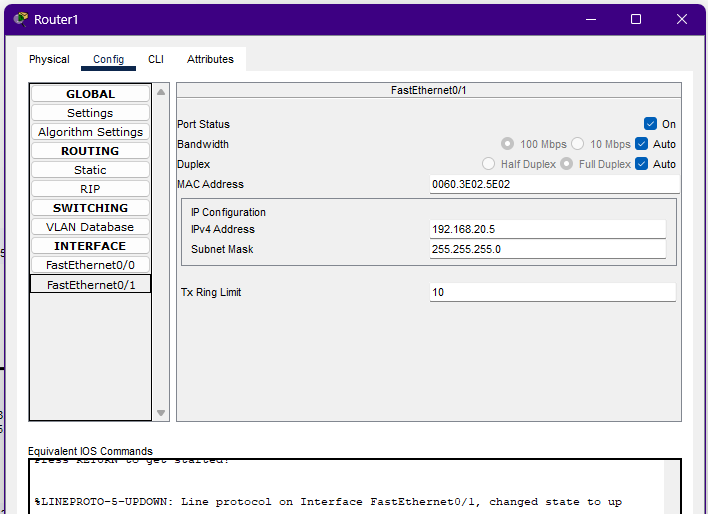


Рисунок 5.10 - Порт Fa0/1 маршрутизатораR2 настроим на работу с сетью 192.168.20.0

Теперь настроим PC1 и PC2 (рисунок 5.11)

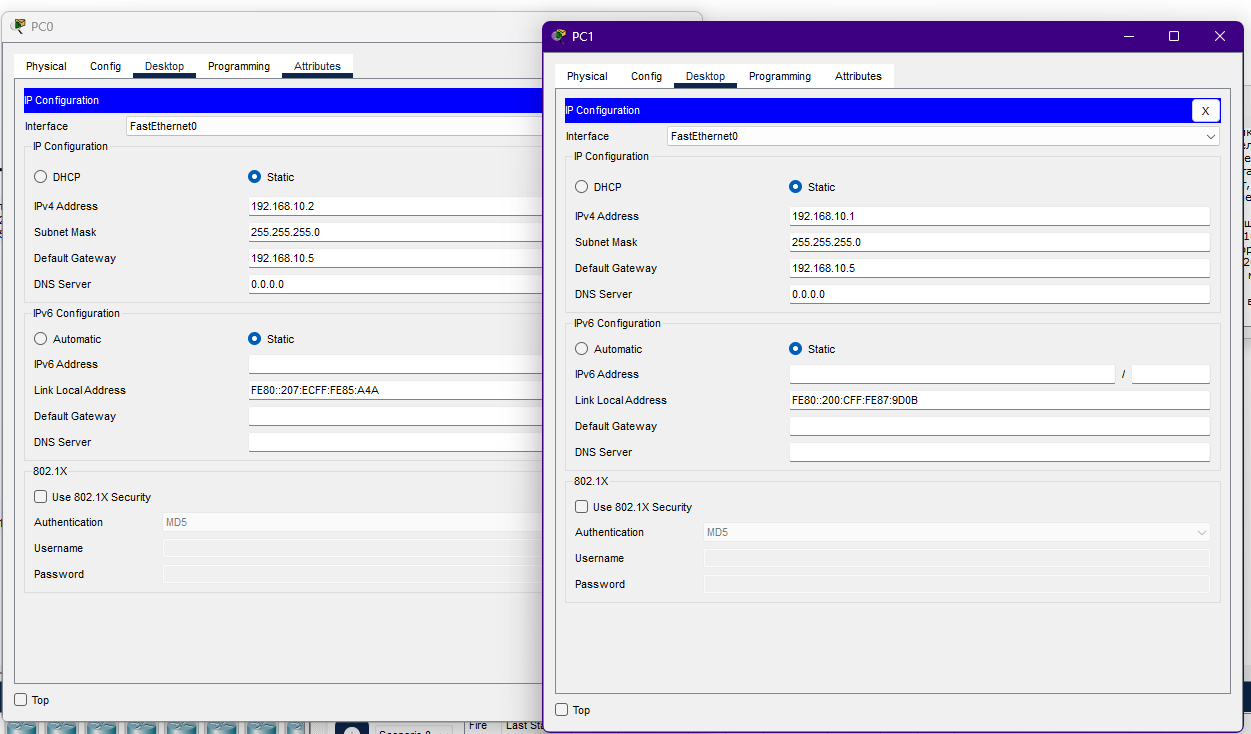


Рисунок 5.11 – Настройка PC1 и PC2

Теперь настроим PC2 и сервер в сети 192.168.20.0 (рисунок 5.12)

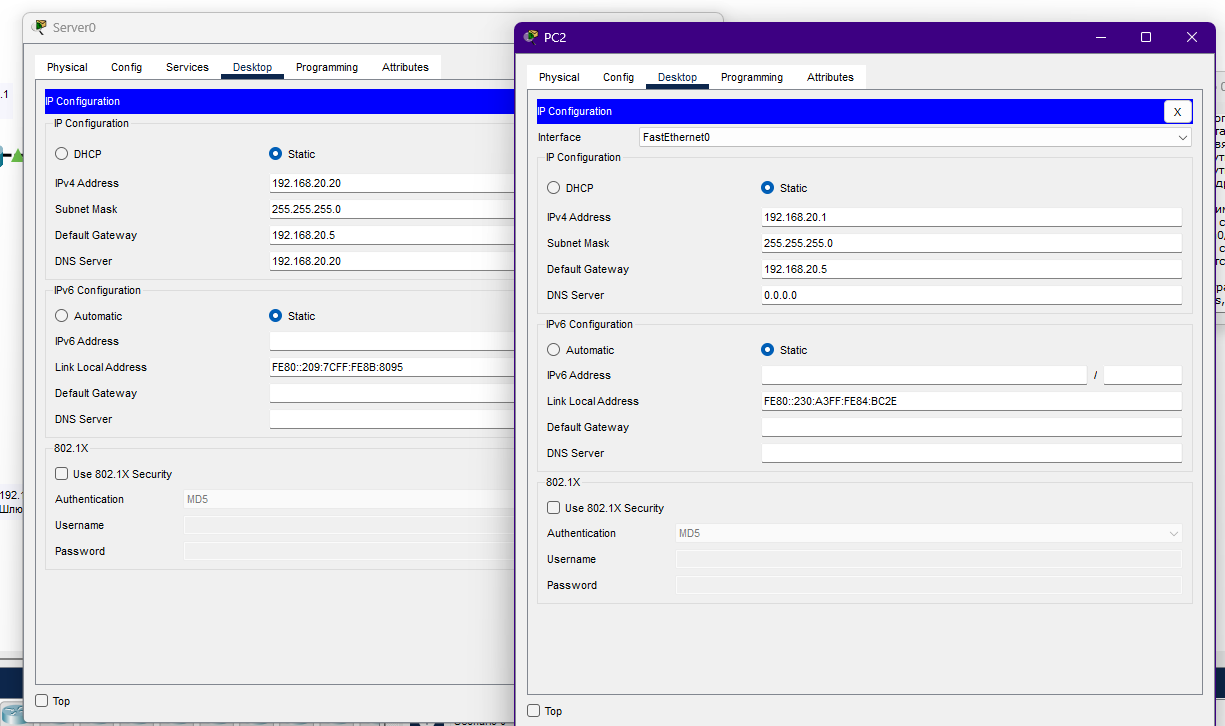


Рисунок 5.12 – Настройка сервера и PC2

Теперь настроим маршрутизацию на маршрутизаторах R0 и R1 (рисунок 5.13)

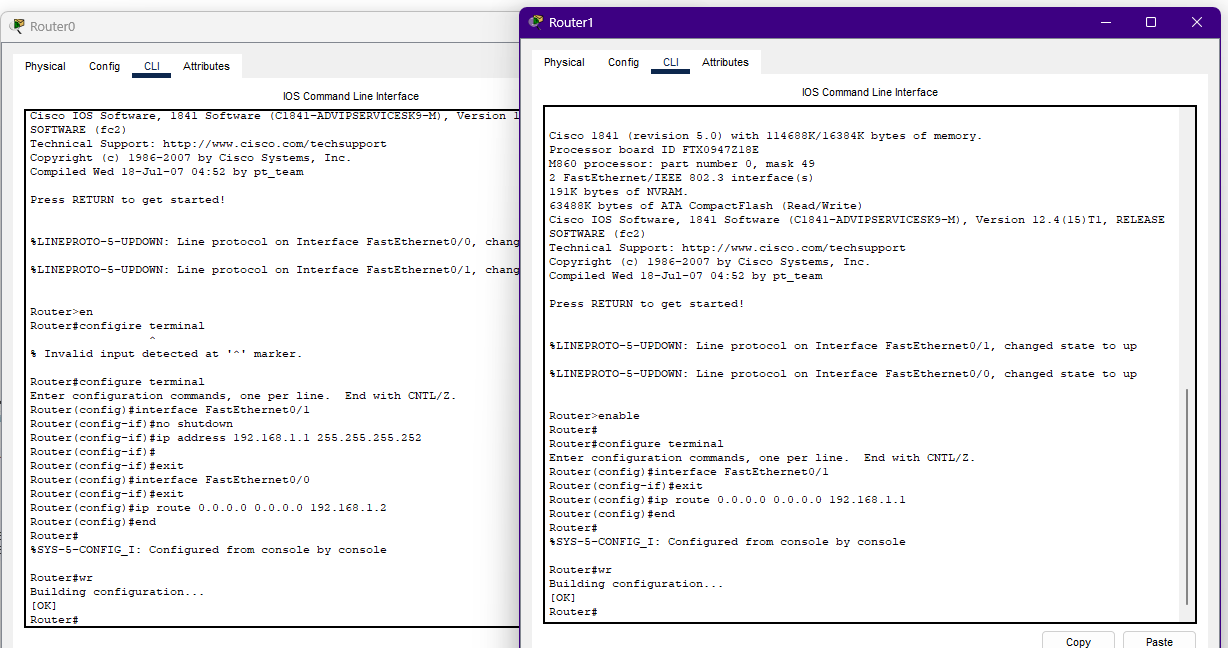


Рисунок 5.13 – Настройка маршрутизации на маршрутизаторах

Проверяем теперь работу сети (рисунок 5.14)

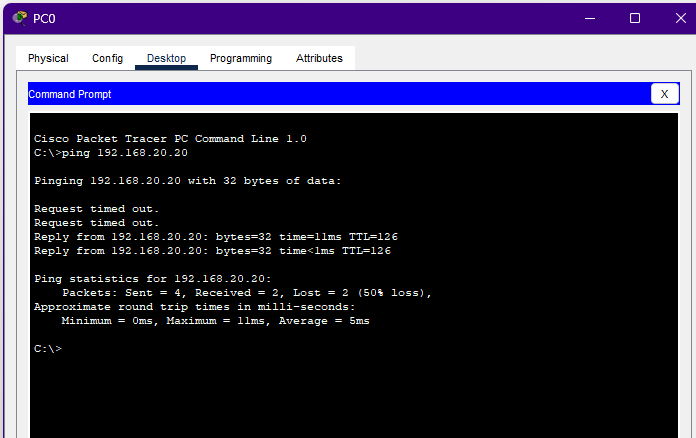


Рисунок 5.14 – Связь есть, но она не идеальная

Просмотрим маршрут пакетов по сети (рисунок 5.15)

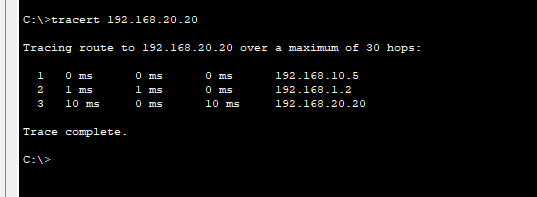


Рисунок 5.15 – Маршрут пакетов

Задание 3. Сеть на двух маршрутизаторах

Создадим следующую схему (рисунок 5.16)

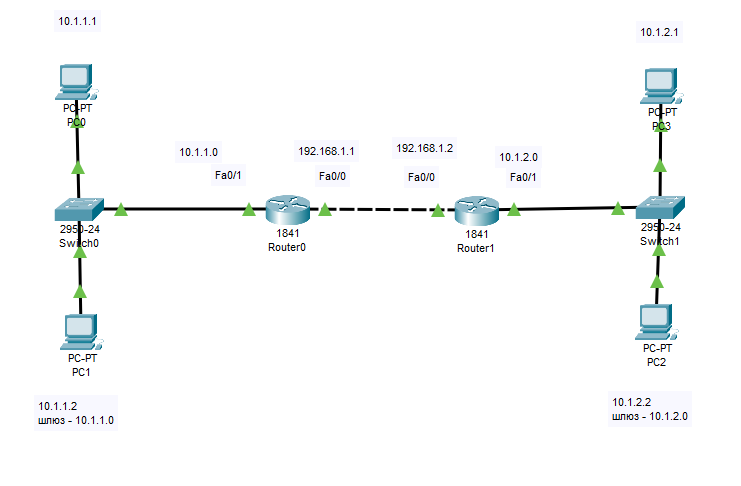


Рисунок 5.16 – Схема сети

На рисунке 5.17 показана таблица маршрутизации на 1 маршрутизаторе

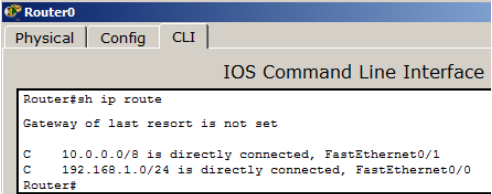


Рисунок 5.17 – Таблица маршрутизации на 1-ом маршрутизаторе

Мы видим, что в данный момент в нашей таблице есть только сети, подключенные напрямую. R0 не знает сеть 10.1.2.0, а R1 не знает сеть 10.1.1.0. Поэтому, чтобы настроить маршрутизацию, следует добавим эти маршруты в таблицы маршрутизаторов:

R0 (config)#ip route 10.1.2.0 255.255.255.0 192.168.1.2

R1 (config)#ip route 10.1.1.0 255.255.255.0 192.168.1.1

Теперь мы видим (рисунок 5.18), что маршрутизация настроена

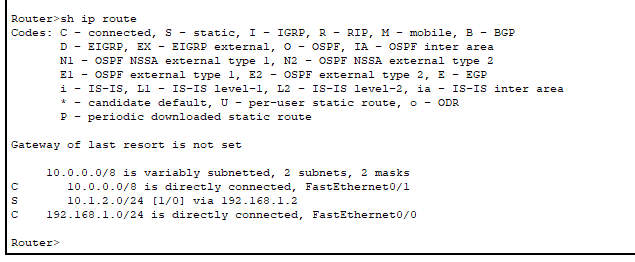


Рисунок 5.18 – Маршрутизация настроена

Задание 4. Статическая маршрутизация для пяти сетей и роутеров с тремя портами

Построим следующую схему сети (рисунок 5.19)

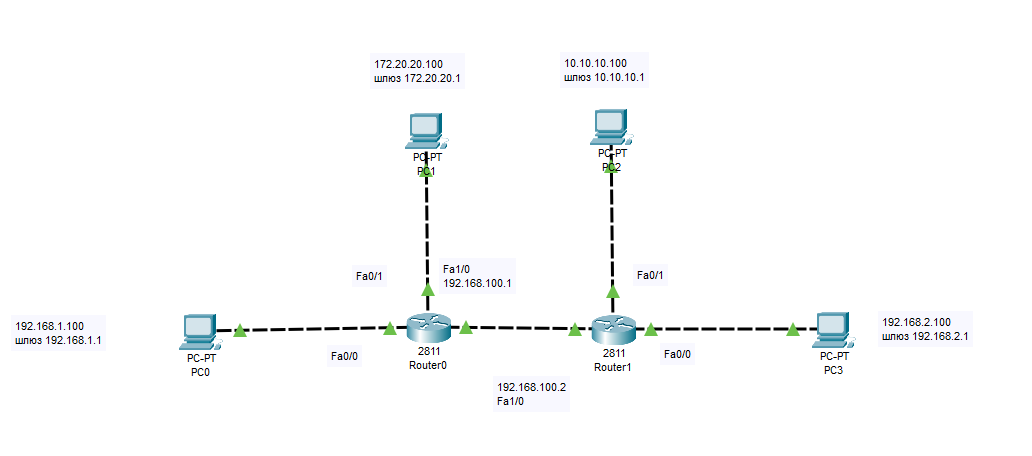


Рисунок 5.19 – Схема сети

Добавим к маршрутизатору интерфейсную плату (рисунок 5.20)

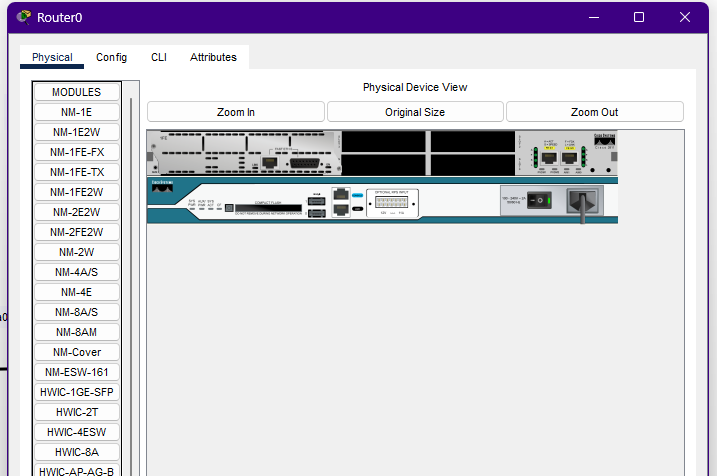


Рисунок 5.20 – Вставляем интерфейсную плату в маршрутизатор

Нам требуется произвести необходимые настройки для того, чтобы все ПК могли общаться друг с другом, то есть, необходимо обеспечить доступность компьютеров из разных сетей между собой.

Для начала настроим маршрут по умолчанию на R0 (рисунок 5.21)

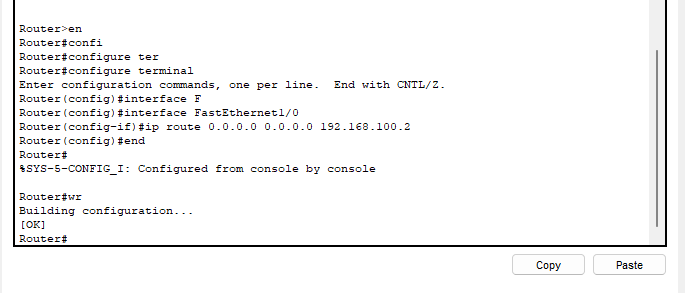


Рисунок 5.21 – Настройка маршрута по умолчанию на R0

Тоже самое сделаем для R1

Отправим с компьютера PC0 с IP адресом 192.168.1.100 пакет на интерфейс Fa1/0 с IP адресом 192.168.100.2 маршрутизатора R1 и посмотрим, что изменилось (рисунок 5.22)

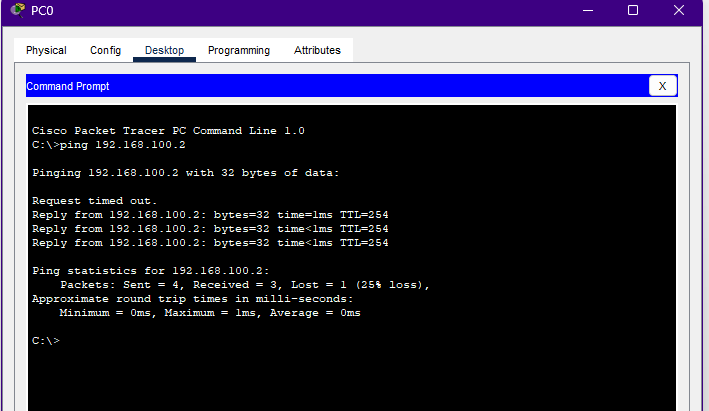


Рисунок 5.22 – Всё успешно

**ЛАБОРАТОРНАЯ РАБОТА №6**

**Динамическая маршрутизация на протоколах RIP и EIGRP**

**Задание 1.** Настройка протокола RIP версии 2 для сети из шести устройств

Для начала построим схему (рисунок 6.1) и настроим на ней маршрутизацию (рисунок 6.2)

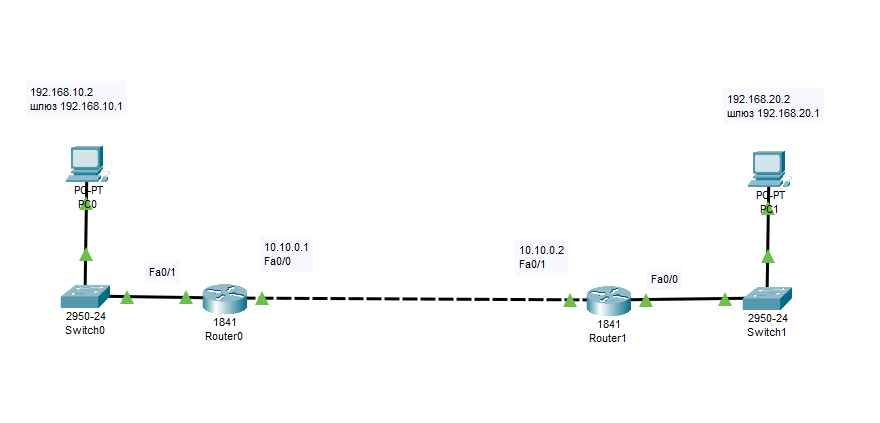


Рисунок 6.1 – Схема сети

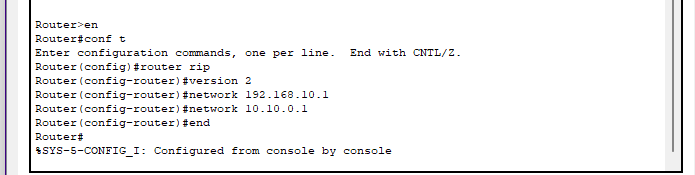


Рисунок 6.2 – Настройка протокола RIPv2 на маршрутизаторе R0

Сделаем аналогичные действия на роутере R1 (рисунок 6.3)

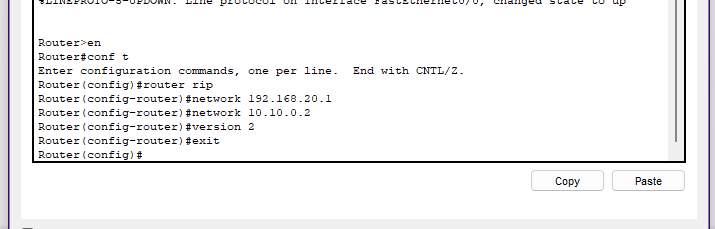


Рисунок 6.3 – настройка протокола на втором маршрутизаторе

Теперь проверим настройки коммутаторов и протоколов RIPv2 (рисунок 6.4)

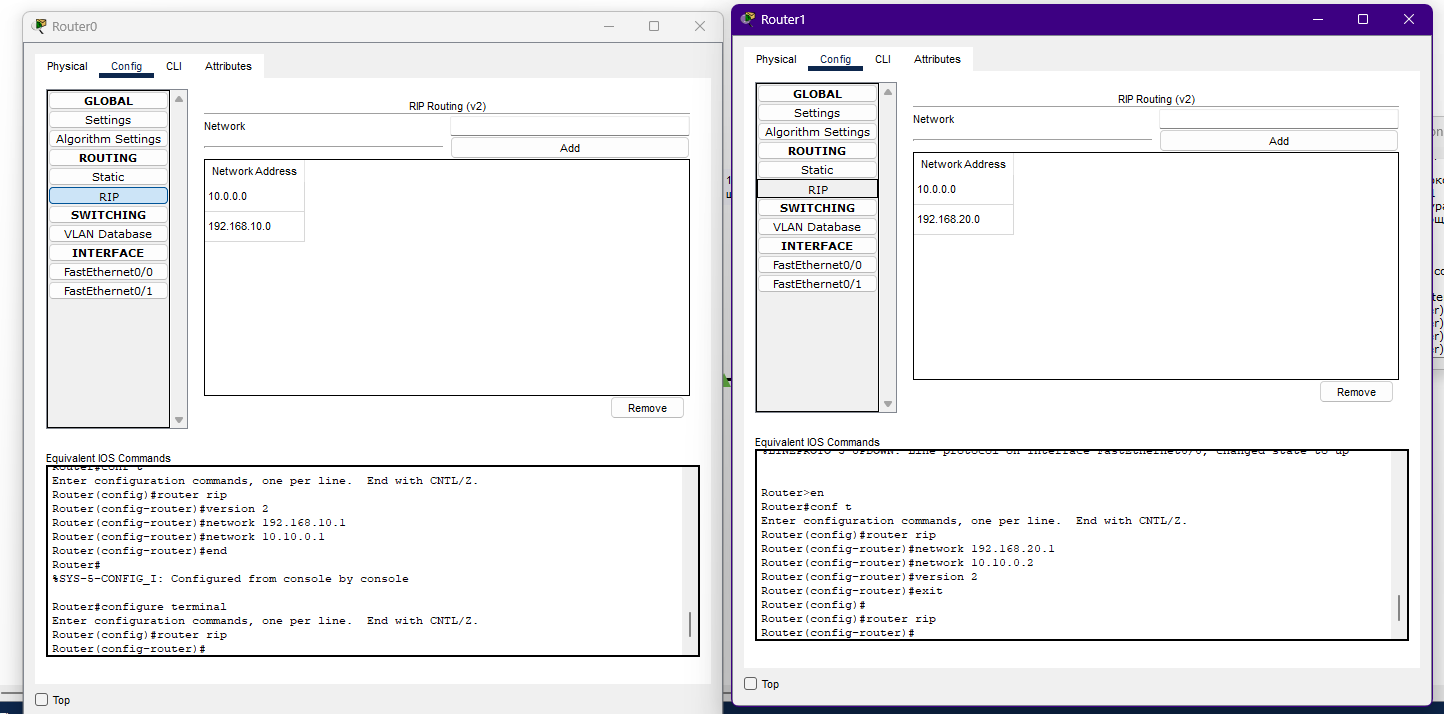


Рисунок 6.4 – Настройка маршрутизаторов

Проверим связь между PC1 и PC2 (рисунок 6.5)

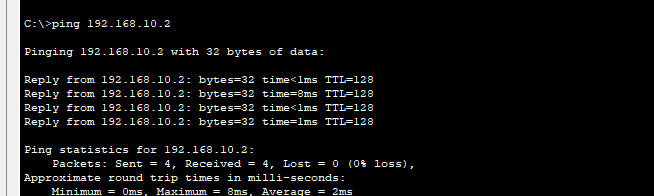


Рисунок 6.5 – Проверяем связь между ПК

Задание 2. Конфигурирование протокола RIP версии 2 для сети из четырех устройств

Построим схему, представленную на рисунке 6.6

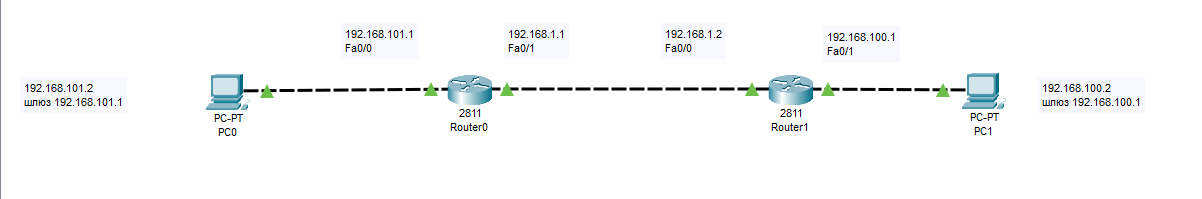


Рисунок 6.6 – Схема сети

Конфигурируем R0 (рисунок 6.7)

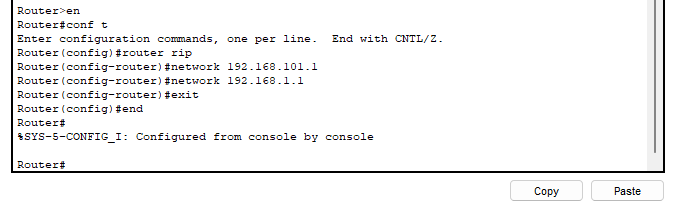


Рисунок 6.7 – Настройка RIP на R0

Аналогично делаем на R1 и проверяем связь между ПК (рисунок 6.8)

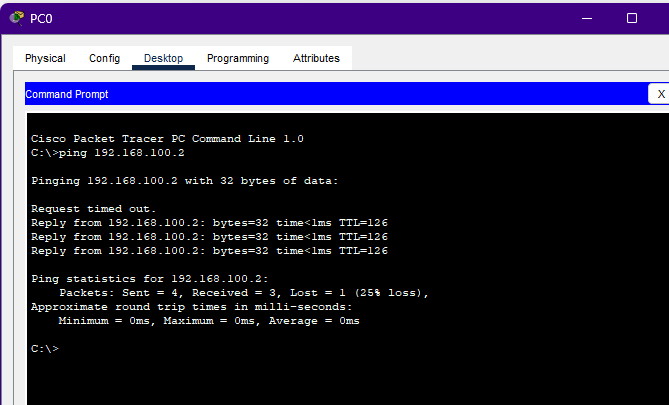


Рисунок 6.8 – Результат пинга

Задание 3. Конфигурирование протокола EIGRP

На рисунке 6.9 представлена схема сети для конфигурации данного протокола

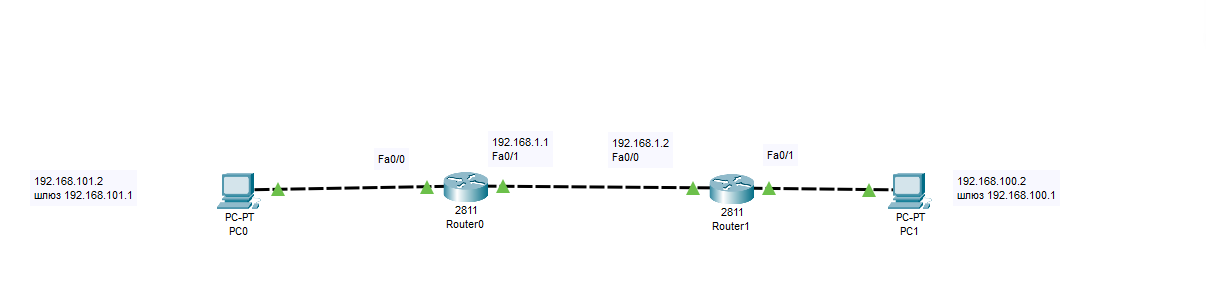


Рисунок 6.9 – Схема сети

Конфигурируем R0 и R1 (рисунок 6.10) и проверяем работу сети (рисунок 6.11)

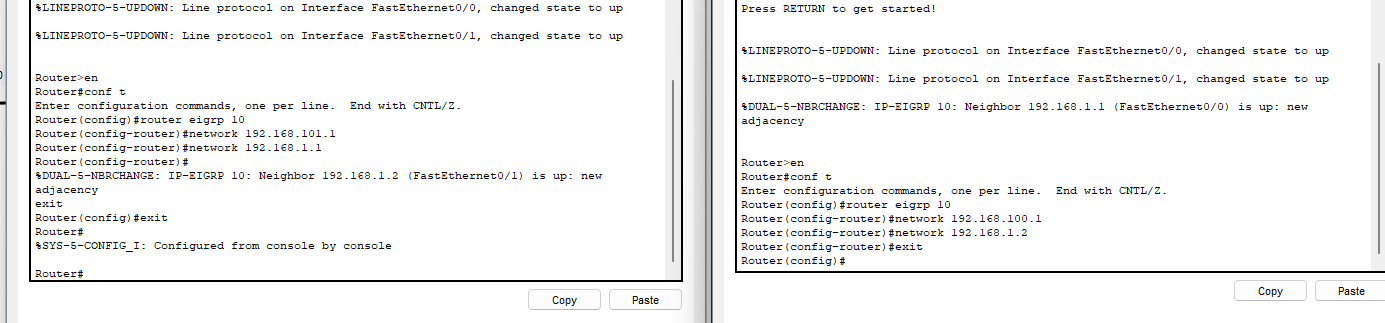


Рисунок 6.10 – Конфигурируем роутеры

Проверяем работу сети (рисунок 6.11)

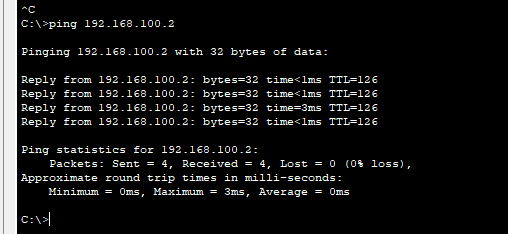


Рисунок 6.11 – Проверка сети

Задание 4. Пример конфигурирования протокола OSPF для 4-х устройств

Построим схему (рисунок 6.12)

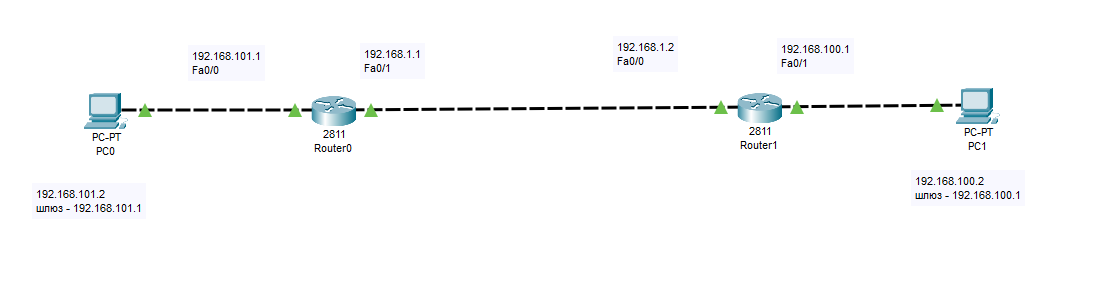


Рисунок 6.12 – Схема сети

Настроим роутеры (рисунок 6.13)



Рисунок 6.13 – Настройка роутеров

Проверяем результат (рисунок 6.14)

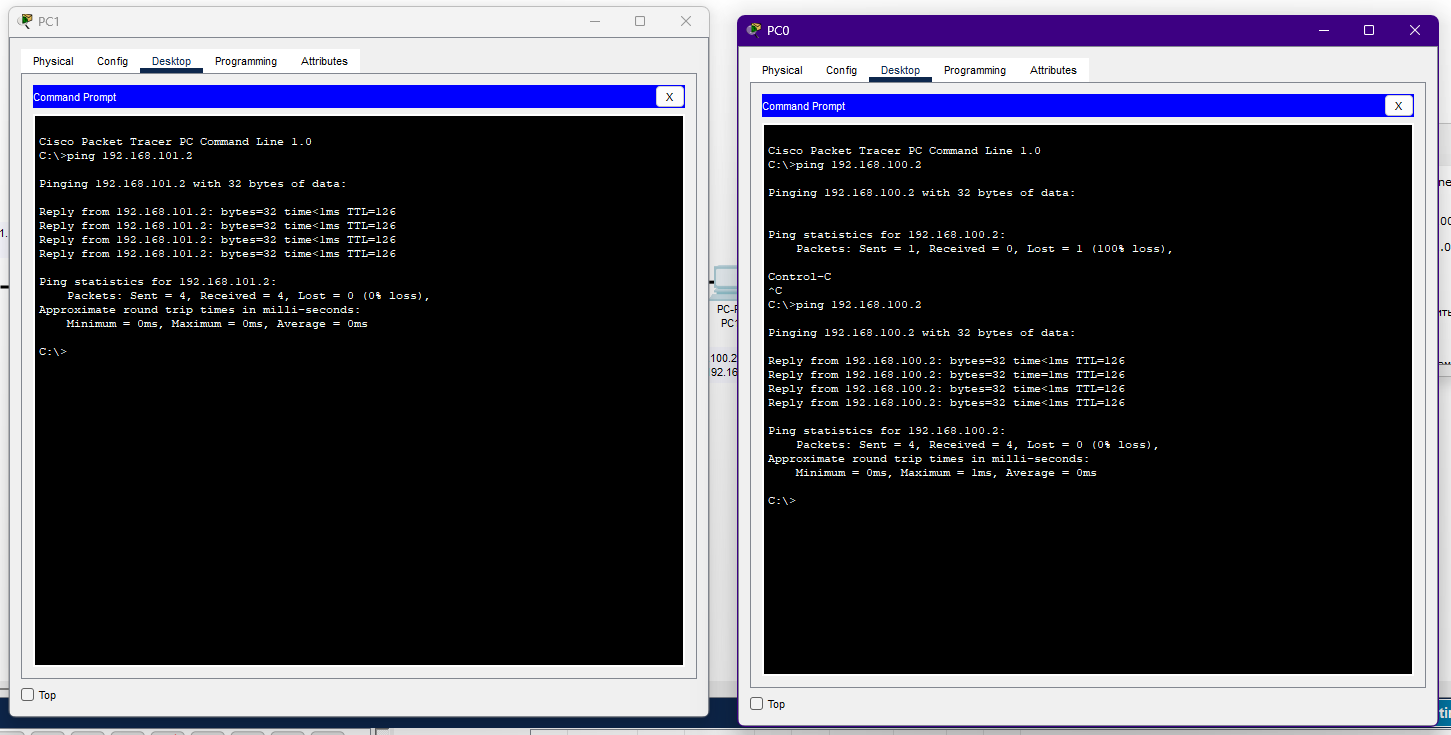


Рисунок 6.14 – Проверка результатов

Задание 5. Настройка маршрутизации по протоколу OSPF для 6 устройств

Построим схему (рисунок 6.15)

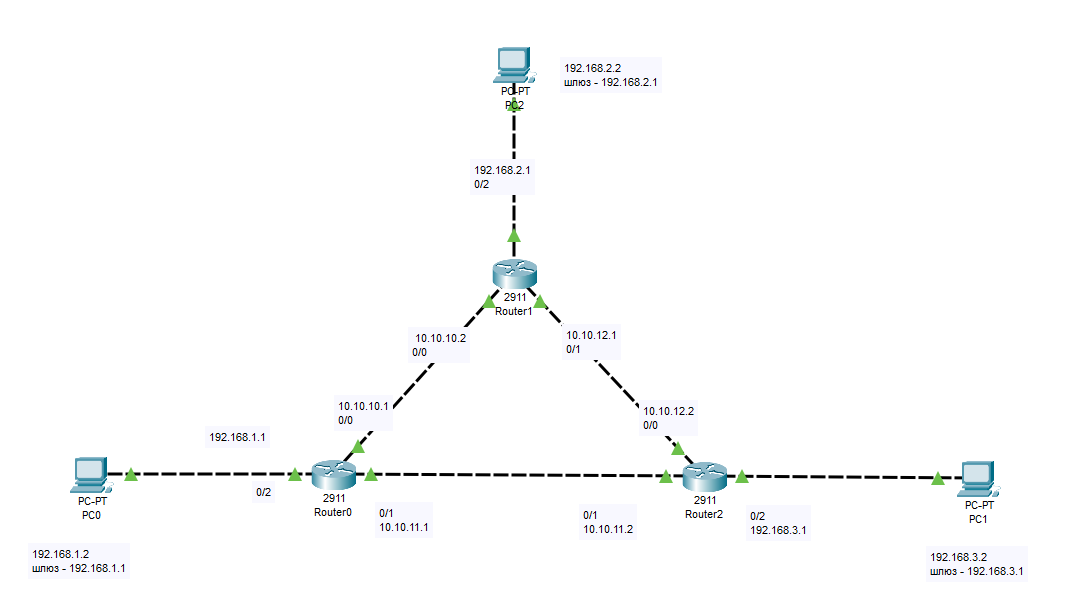


Рисунок 6.15 – Схема сети

Настроим loopback интерфейс - алгоритм, который направляет полученный сигнал (или данные) обратно отправителю – на R0 (рисунок 6.16)

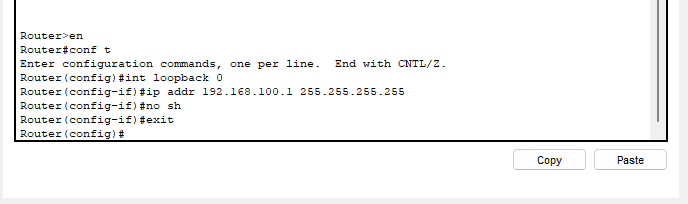


Рисунок 6.16 – Настройка loopback R0

Теперь на нем настроим OSPF (рисунок 6.17)

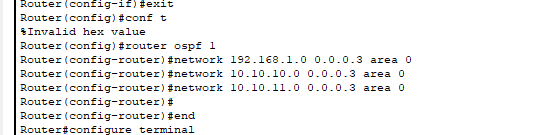


Рисунок 6.17 – OSPF на R0

Проверяем результат настройки (рисунок 6.18)

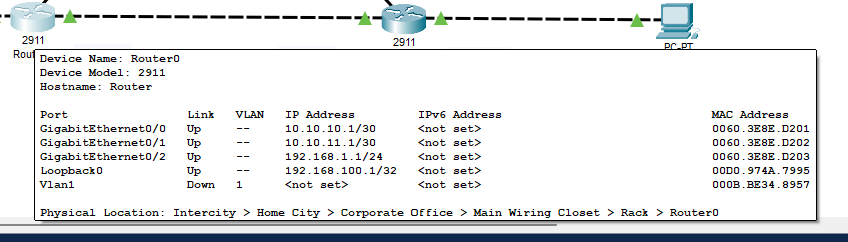


Рисунок 6.18 – Настроено всё

Аналогично настраиваем остальные роутеры

После проверим, что роутер R2 видит остальные роутеры (рисунок 6.19)

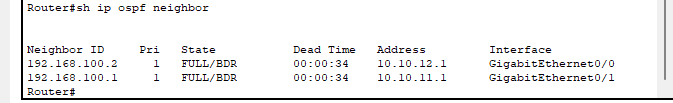


Рисунок 6.19 – Проверка роутера R2

Теперь посмотри таблицу маршрутизации на нем же (рисунок 6.20)

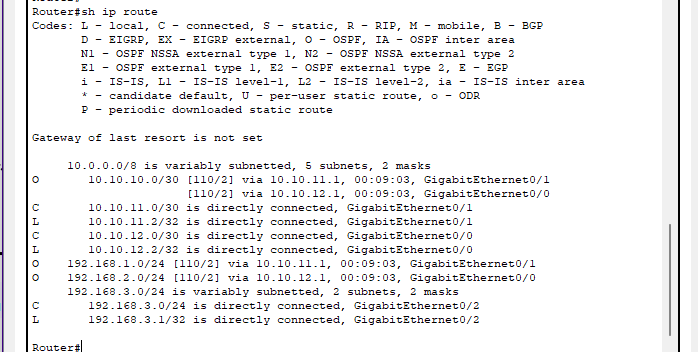


Рисунок 6.20 – Таблица маршрутизации

Проверим доступность разных сетей (рисунок 6.21)

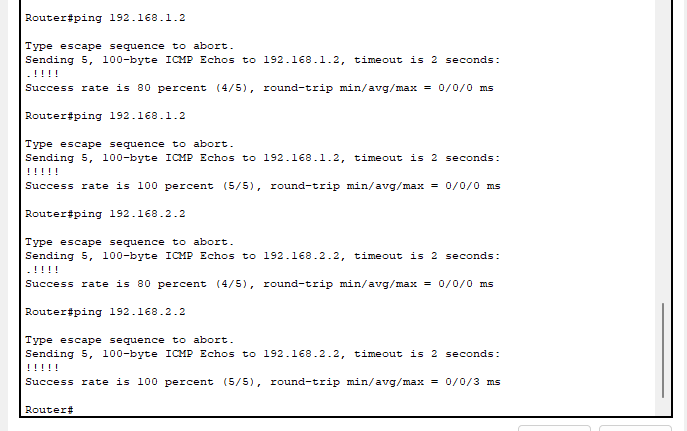


Рисунок 6.21 – Проверка доступности разных сетей.

**ЛАБОРАТОРНАЯ РАБОТА №7**

**Списки доступа ACL. Настройка статического и динамического NAT**

**Задание 1.** Создание стандартного списка доступа

Составим схему сети (рисунок 7.1)

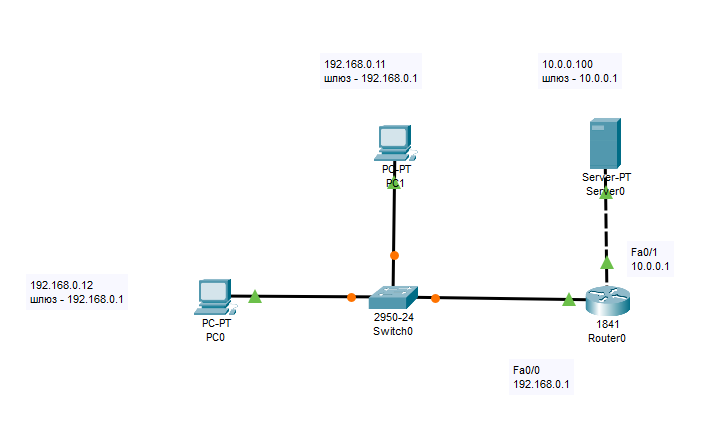


Рисунок 7.1 – Схема сети

Требуется разрешить доступ на сервер PC0 с адресом 172.178.0.12, а PC1 c адресом 172.178.0.11 – запретить

Для начала настроим роутер R0 (рисунок 7.2)

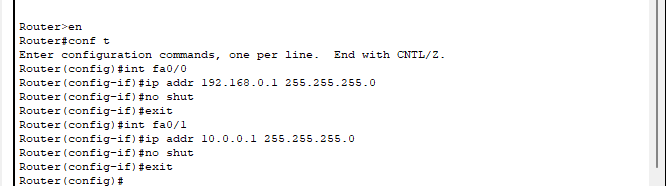


Рисунок 7.2 – Настройка роутера

Также настроим сервер (рисунок 7.3)



Рисунок 7.3 – Настройка сервера

Теперь проверим связь ПК из разных сетей (рисунок 7.4)

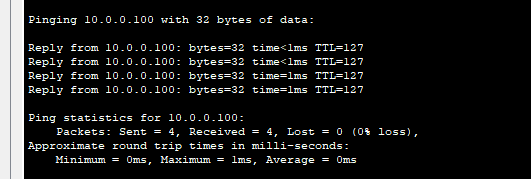


Рисунок 7.4 – ПК из разных сетей могут общаться

Правило запрета и разрешения доступа будем составлять с использованием стандартных списков доступа (ACL). Пока не задан список доступа на интерфейсе всё разрешено (permit). Но, стоит создать список, сразу действует механизм "Всё, что не разрешено, то запрещено". Поэтому нет необходимости что-то запрещать (deny) – указываем что разрешено, а "остальным – запретить" подразумевается автоматически. По условиям задачи нам нужно на R0 пропустить пакеты с узла 172.178.0.12 на сервер. Сделаем это следующим образом (рисунок 7.5)

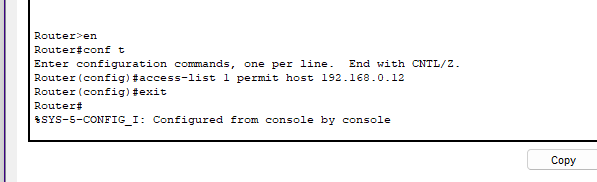


Рисунок 7.5 – Создаем на роутере разрешающий ACL

Применяется данное правило на интерфейс в зависимости от направления (PC0 расположен со стороны порта Fa0/0) Эта настройка означает, что список доступа (правило с номером 1) будет действовать на интерфейсе fa0/0 на входящем (in) от PC0 направлении. Применим правило (рисунок 7.6)

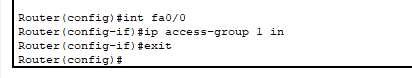


Рисунок 7.6 – Применяем правилу к порту fa0/0

Проверим связь ПК с сервером, а также узел 192.168.0.12 (рисунок 7.7)



Рисунок 7.7 – Проверка сети

**Задание 2.** Расширенные списки доступа ACL

Соберем схему (рисунок 7.8).

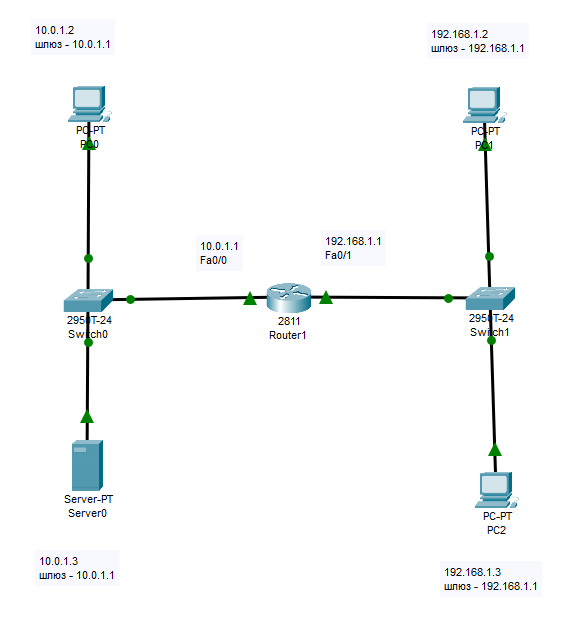


Рисунок 7.8 – Схема сети

Нам необходимо разрешить доступ к FTP серверу 10.0.1.3 для узла 172.178.1.2 и запретить для узла 172.178.1.3. (рисунок 7.9)

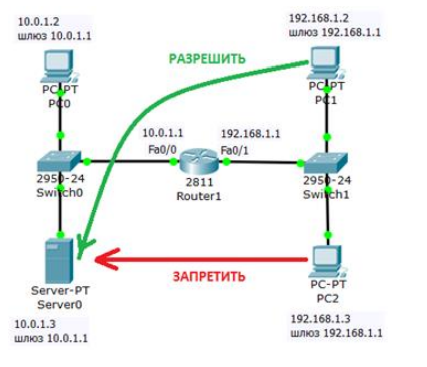


Рисунок 7.9 – Задание из методички

Изначально на сервере 10.0.1.3 FTP сервис поднят по умолчанию со значениями имя пользователя Cisco, пароль Cisco. Убедимся, что узел S0 доступен и FTP работает, для этого заходим на PC0 и связываемся с сервером (рисунок 7.10). Выполняем какие-либо команды, например, DIR – чтение директории.

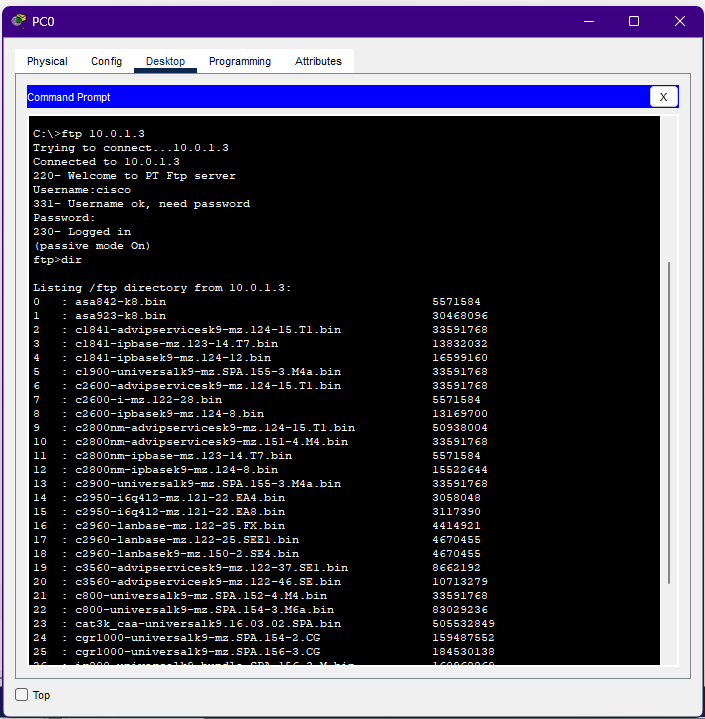


Рисунок 7.10 – FTPсервер доступен

Теперь создадим список правил с номером, 101 в котором укажем 2 разрешающих и по 2 запрещающих правила для портов сервера 21 и 20 (Эти порты служат для FTP - передачи команд и данных) (Рисунок 7.11)

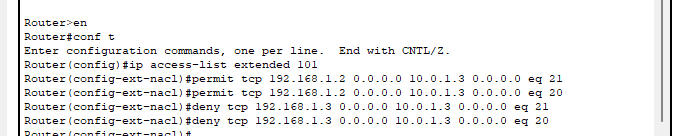


Рисунок 7.11 – Составляем расширенные списки доступа

А теперь применяем наш список с номером 101 на вход (in) Fa0/1 потому, что трафик входит на этот порт роутера со стороны сети 172.178.1.0 (рисунок 7.12)

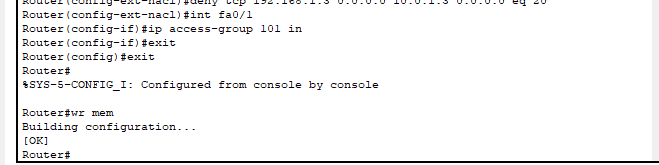


Рисунок 7.12 – Применяем правило с номером 101 к порту 0/1 роутера

Проверяем связь сервера с PC2 (рисунок 7.13)

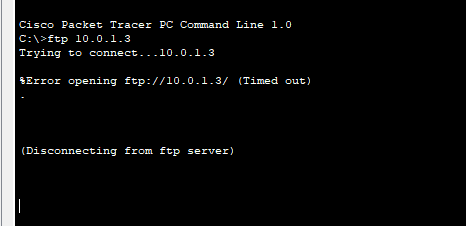


Рисунок 7.13 – для PC2 сервер не доступен

Проверим тоже самое, но для PC1

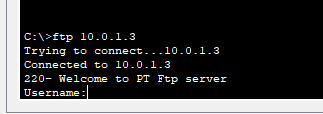


Рисунок 7.13 – Для PC1 всё доступно

**Задание 3.** Статическая трансляция адресов NAT

Составим схему (рисунок 7.14)



Рисунок 7.14 – Схема сети

На роутере добавляем access-list и разрешаем всё (рисунок 7.15)

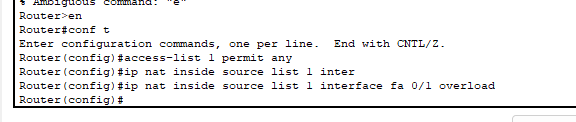


Рисунок 7.15 – Составляем лист допуска

Далее настроим трансляцию на интерфейсах (рисунок 7.16)

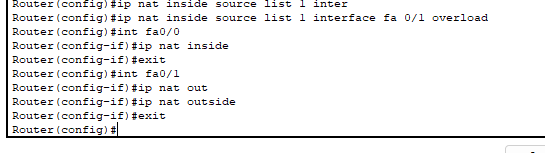


Рисунок 7.16 – Назначаем внутренний и внешние порты

Выходим из режима глобального конфигурирования и записываем настройки роутера в микросхему памяти (wr mem)

Проверяем работу сети (рисунок 7.17)

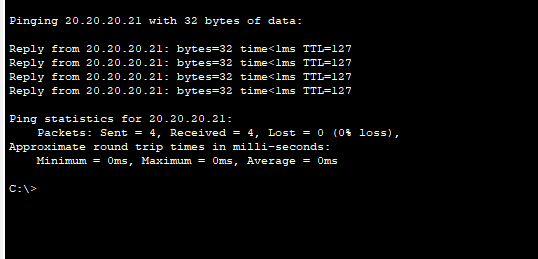


Рисунок 7.17 – Пингуем

Для просмотра состояния таблицы NAT, одновременно с пингом используйте команду Router#sh ip nat translations (я запустил пинг с машины 10.10.10.1, т.е., с PC1 на адрес 20.20.20.21, т.е., на S0) (рисунок 7.18)

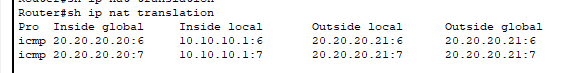


Рисунок 7.18 – Во время пинга просматриваем состояние таблицы NAT

**Задание 4.** Настройка статического NAT

Составим схему сети (рисунок 7.19)

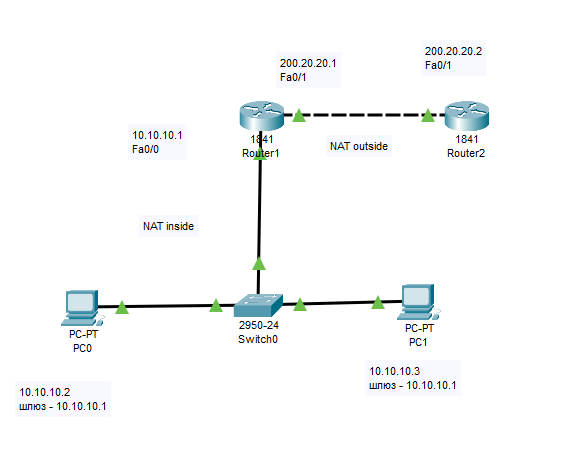
****

Рисунок 7.19 – Схема сети

Настроим R1 (рисунок 7.20)

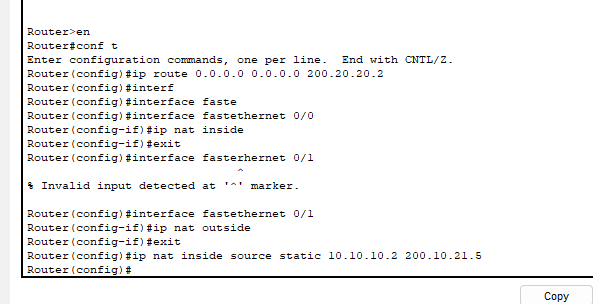


Рисунок 7.20 – Настраиваем роутер

Теперь проверим связь PC0 и R2 (рисунок 7.21)

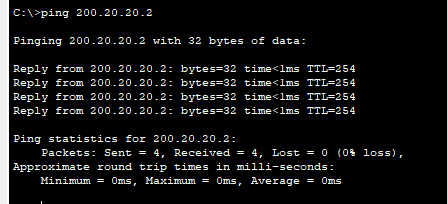


Рисунок 7.21 – PC0 видит R2

Проверим, что роутер R1 видит соседние сети (рисунок 7.22)

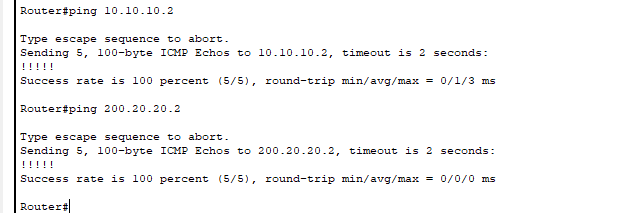


Рисунок 7.22 – Роутер видит соседние сети

Проверим механизм работы статического NAT: команда show ip nat translations выводит активные преобразования, а команда show ip nat statistics выводит статистику по NAT преобразованиям (рисунок 7.23)

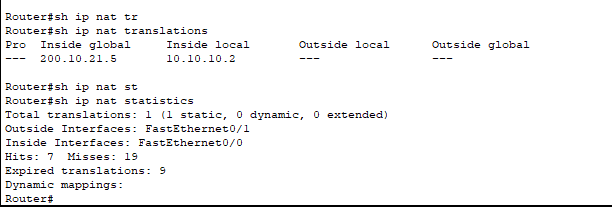


Рисунок 7.23 – Проверяем механизм работы статического NAT

Из иллюстрации видим, что глобальному ip-адресу 200.10.21.5 соответствует локальный ip-адрес 10.10.10.2, а также, какой интерфейс является внешним, а какой -внутренним.

**Задание 5.** Настройка динамического NAT на маршрутизаторе R1 по шагам.

Построим схему (рисунок 7.24)

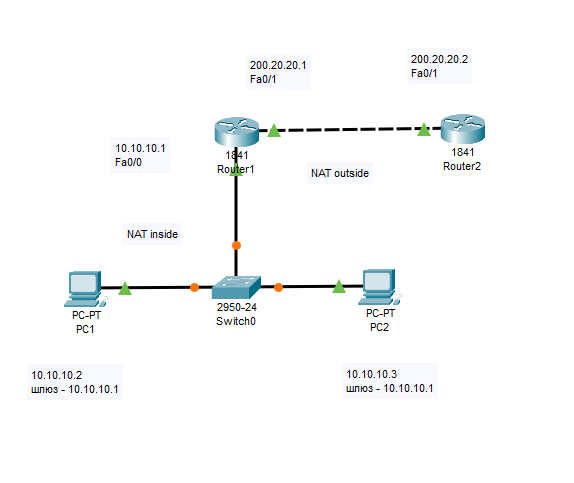


Рисунок 7.24 – Схема сети

Настроим список доступа, пулы адресов, трансляции, внутренний и внешние интерфейсы на роутере R1 (рисунок 7.25)

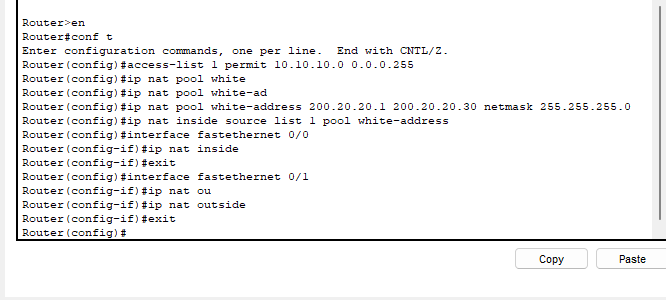


Рисунок 7.25 – Настройка роутера

Проверим связь PC1 и R2 (рисунок 7.26)

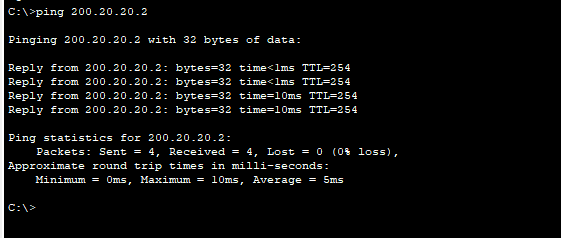


Рисунок 7.26 – PC1 видит R2

Проверим, что R1 видит соседние сети (рисунок 7.27)

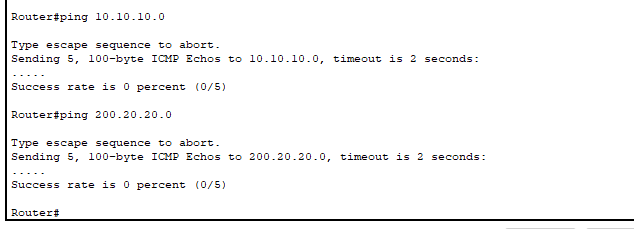


Рисунок 7.27

Проверим механизм работы динамического NAT: для этого выполним одновременно (параллельно) команды ping и show ip nat translations (рисунок 7.28)

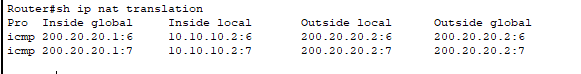


Рисунок 7.28 – Адреса – глобальный, внутренний, внешний

Командой show ip nat statistics выведем статистику по NAT преобразованиям (рисунок 7.29)

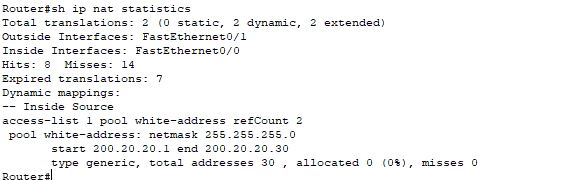


Рисунок 7.29 – Статистика работы динамического NAT

**Задание 6.** Динамический NAT Overload: настройка PAT (маскарадинг)

Построим схему (рисунок 7.30)

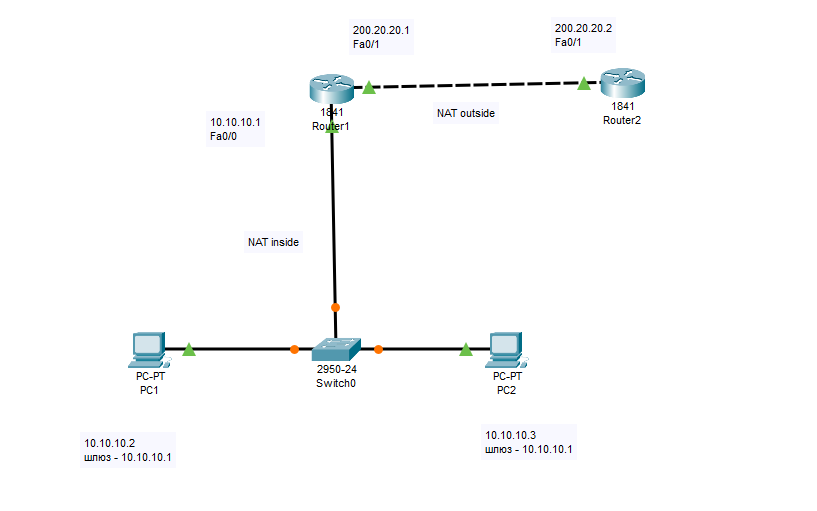


Рисунок 7.30 – Схема сети

Настроим всё в роутере R1 (рисунок 7.31)

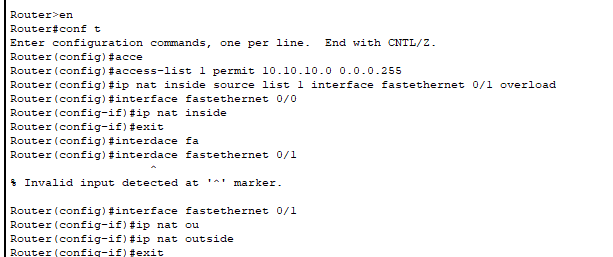


Рисунок 7.31 – Настройка роутера

Проверим связь между пк и роутером 2 (рисунок 7.32)

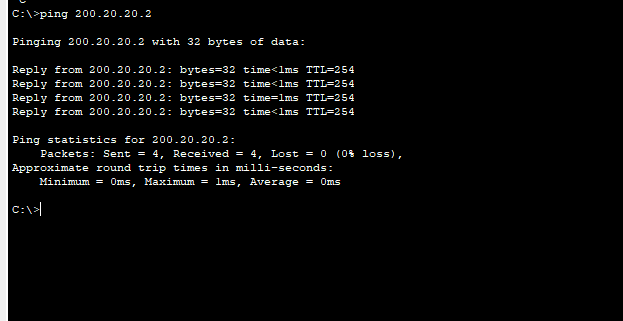


Рисунок 7.32 – Всё пингуется

Проверим, что роутер 1 видит соседние сети (рисунок 7.33)

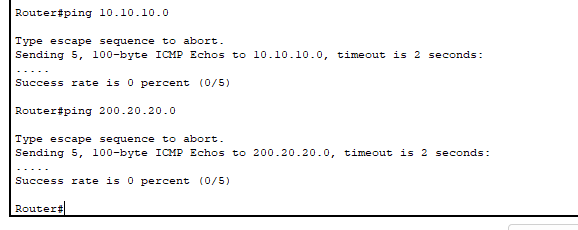


Рисунок 7.33

Проверим механизм работы динамического NAT: для этого выполним одновременно (параллельно) команды ping и show ip nat translations (рисунок 7.34)

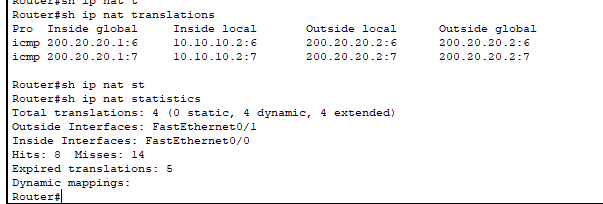


Рисунок 7.34

**ЛАБОРАТОРНАЯ РАБОТА №8**

**Беспроводная сеть WEP**

**Задание 1.** Беспроводная сеть с точкой доступа

Построим схему (рисунок 8.1)

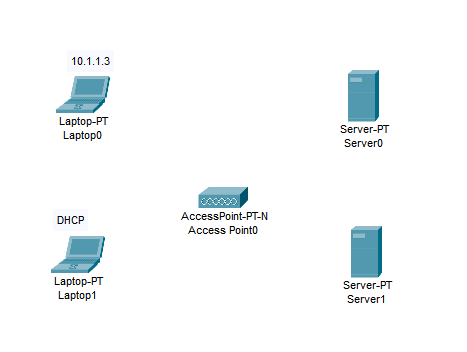


Рисунок 8.1 – Схема сети

Проверим настройку точки доступа и убедимся, что там всё по умолчанию (рисунок 8.2)

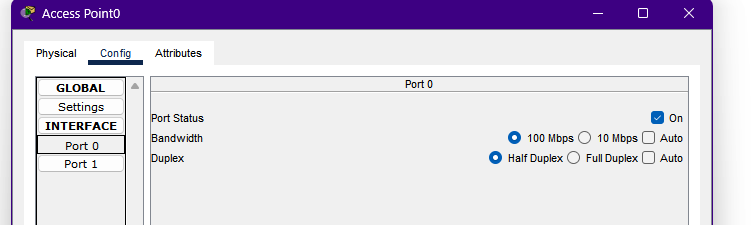


Рисунок 8.2 – Всё по умолчанию

Зададим статическую настройку первого ноутбука (рисунок 8.3)

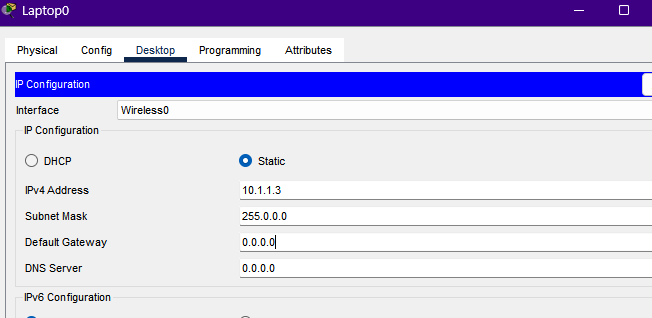


Рисунок 8.3 – Конфигурация ноутбука

Далее настраиваем сервера по умолчанию, т.е. оставляем как было

По желанию можно добавить еще устройства.

На рисунке 8.4 видно, что всё настроено

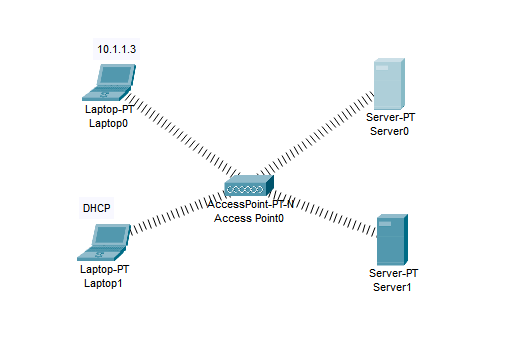


Рисунок 8.4 – Всё настроено

**Задание 2.** Беспроводная сеть между офисами

Составим схему (рисунок 8.5)

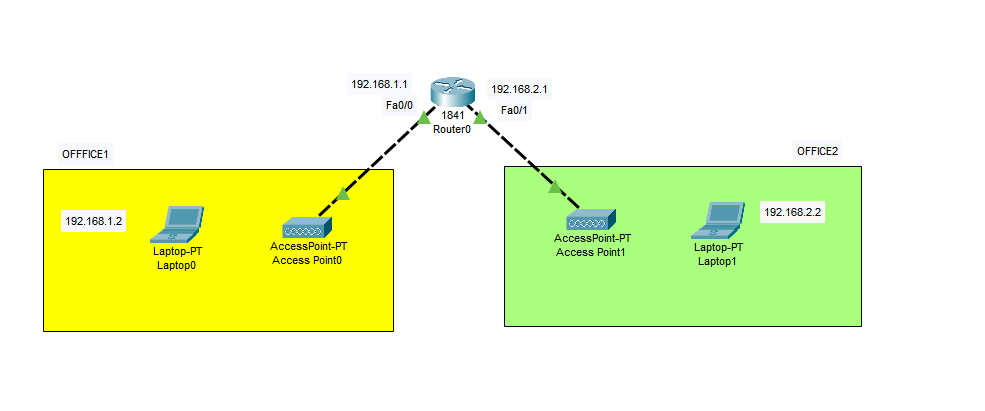


Рисунок 8.5 – Схема сети

Снабжаем все ноутбуки необходимым модулем для Wireless и настраиваем (рисунок 8.6)

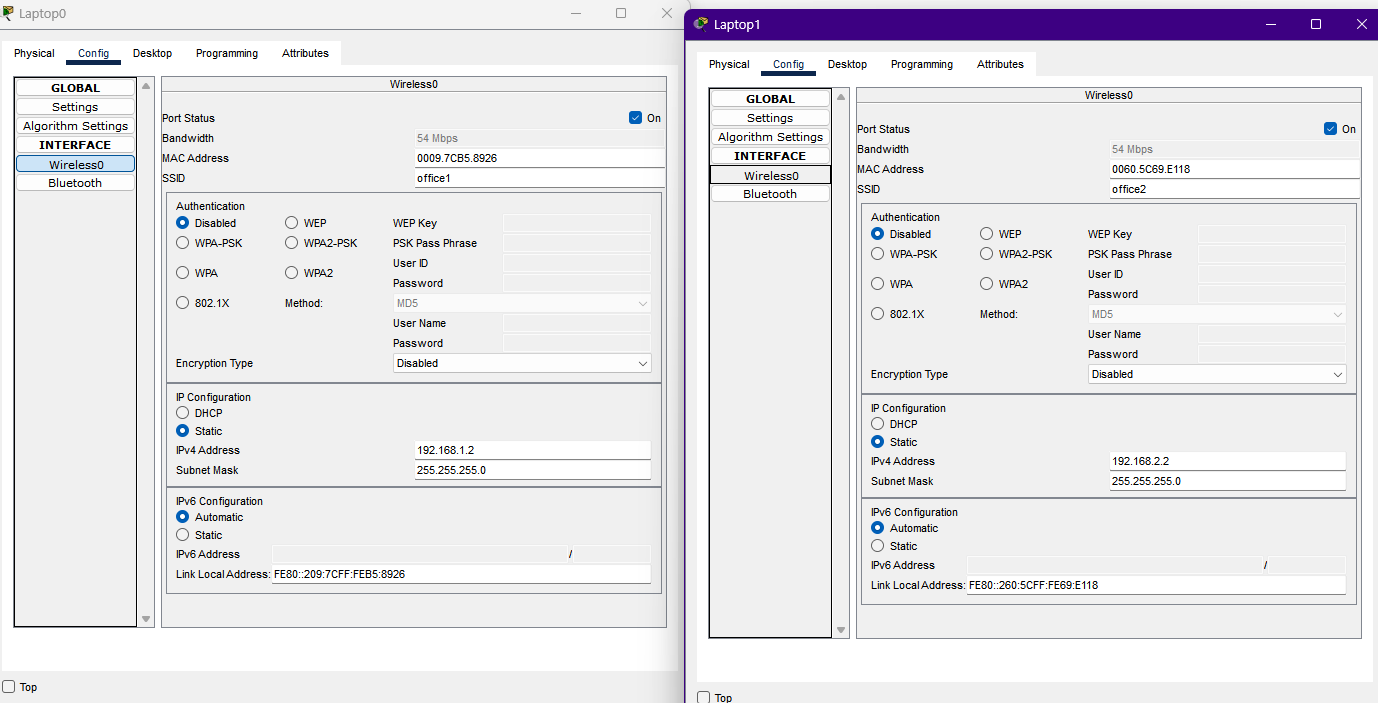


Рисунок 8.6 – Настраиваем Wireless

Также настроим и IP (рисунок 8.7)

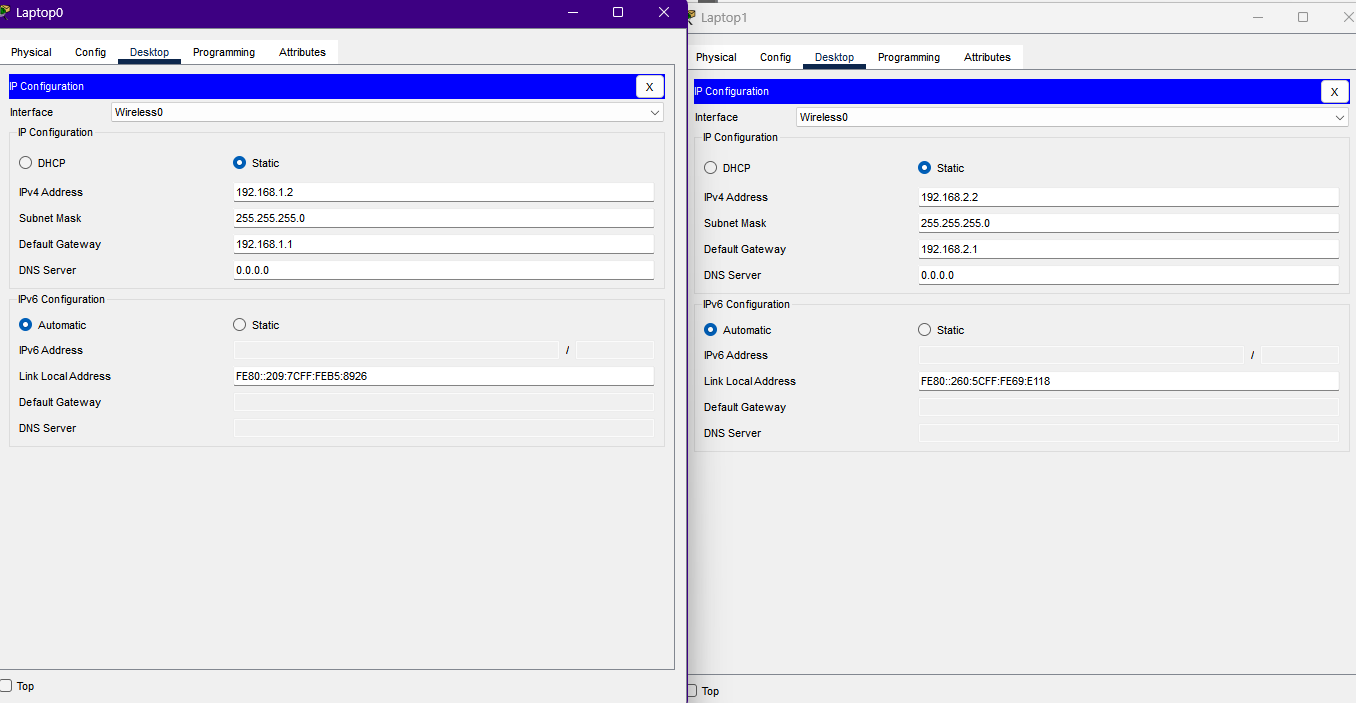


Рисунок 8.7 – Настраиваем ноутбуки

Зададим SSID на точках доступа (рисунок 8.8)

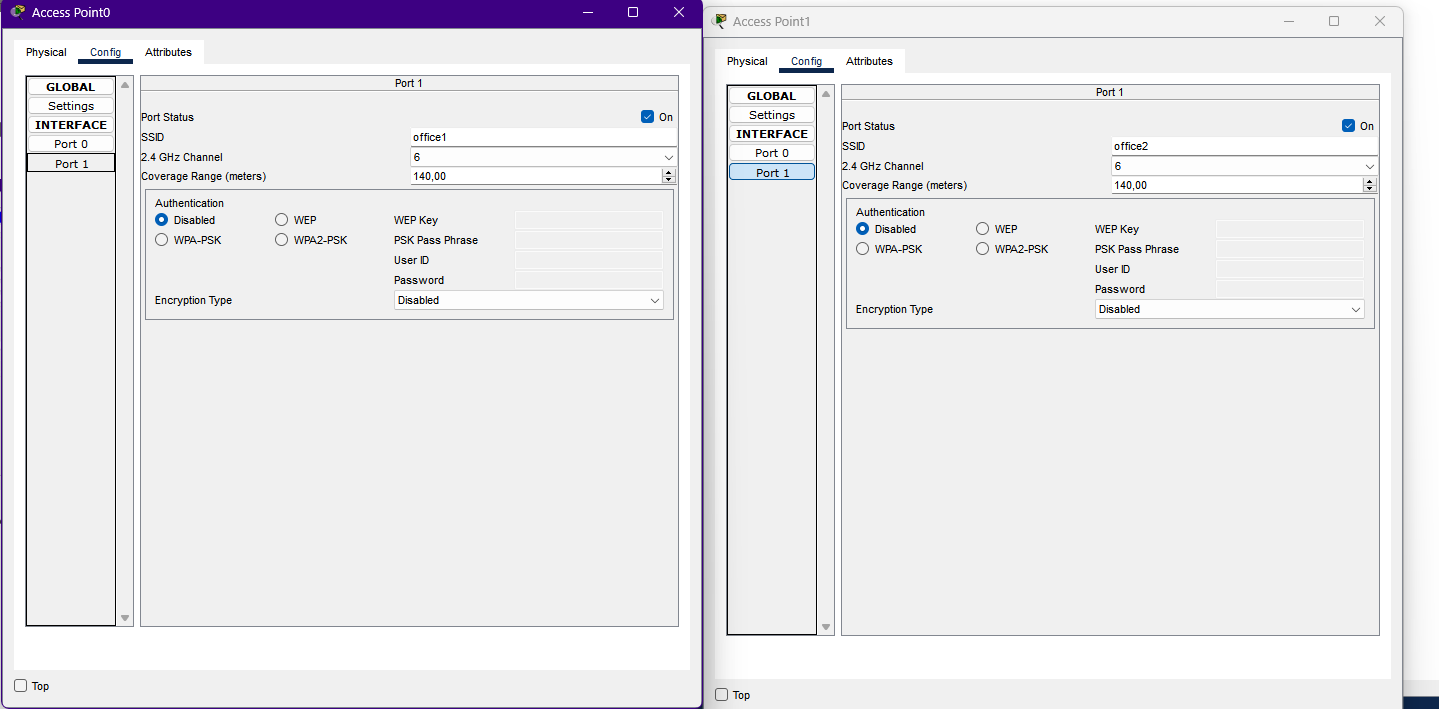


Рисунок 8.8 – Настраиваем точки доступа

Проверяем связь ПК (рисунок 8.9)



Рисунок 8.9 – Всё настроено

**Задание 3.** Настройка коммутируемого WI-FI соединения

Построим следующую схему (рисунок 8.10)

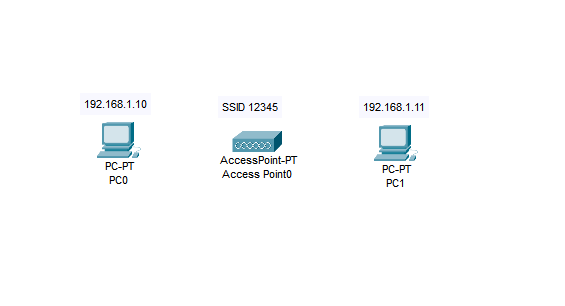


Рисунок 8.10 – Схема сети

Сначала зададим имя сети (SSID) на точке доступа (рисунок 8.11)

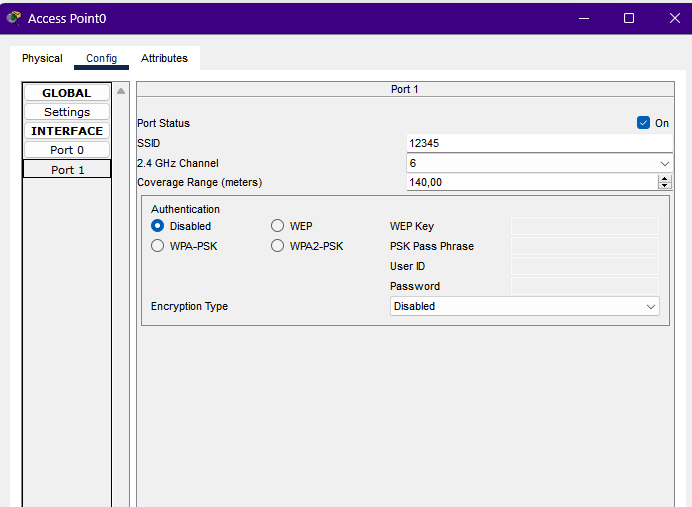


Рисунок 8.11 – Настройка точки доступа

В оба ПК вставляем беспроводной адаптер WPM-300N и устанавливаем связь точки доступа и PC0, для этого нажимаем на кнопку PC Wireless и настраиваем (рисунок .8.12)

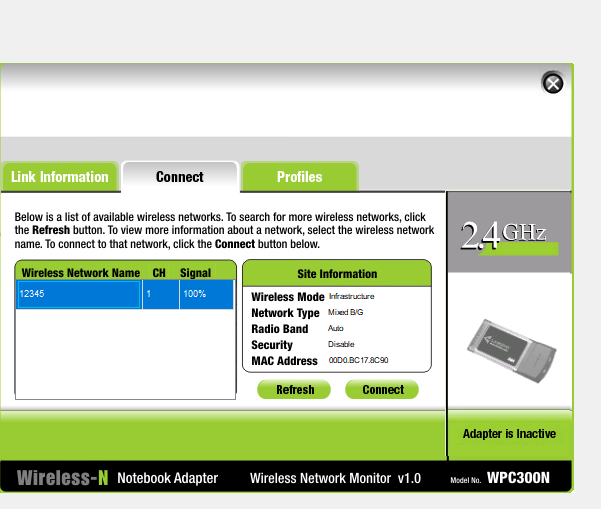


Рисунок 8.12 – Настройка подключения к точке доступа

На рисунке 8.13 видно, что всё подключено

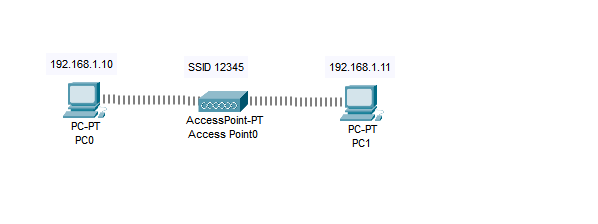


Рисунок 8.13 – Всё подключено

Меняем динамический адрес на статический (рисунок 8.14)

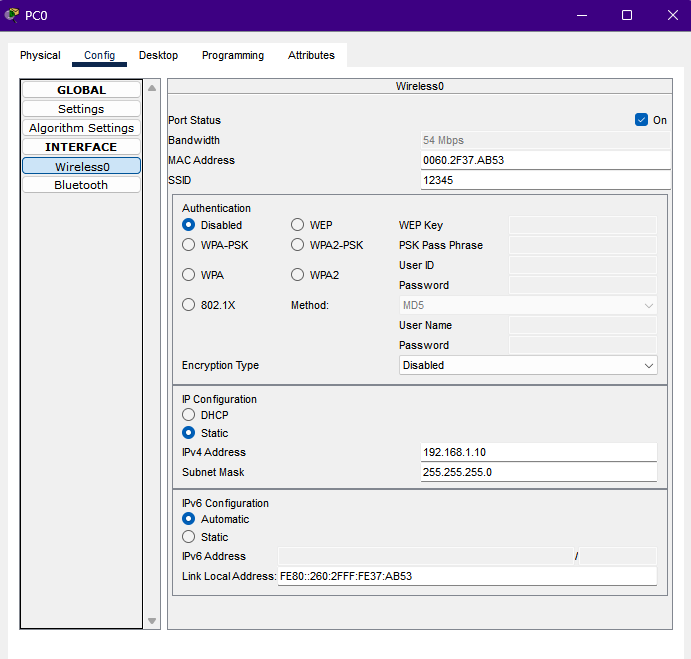


Рисунок 8.14

Проверяем связь между ПК (рисунок 8.15)

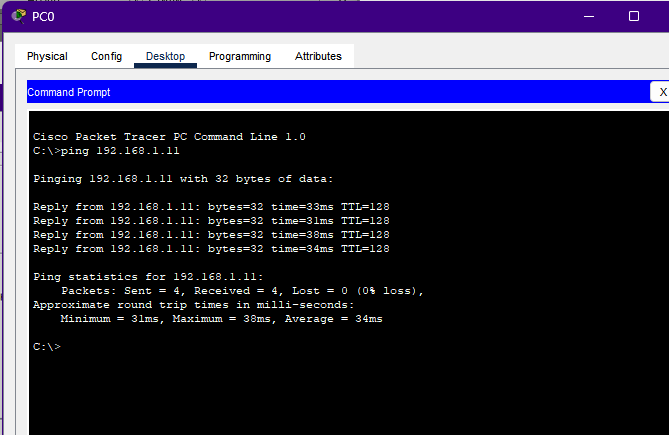


Рисунок 8.15 – Пинг

**Задание 4.** Беспроводная связь в Packet Tracer с беспроводным роутером

Построим следующую схему (рисунок 8.16)

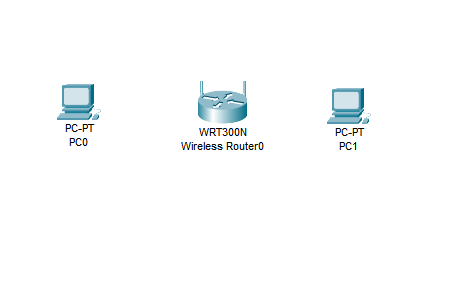
****

Рисунок 8.16 – Схема сети

Снабдим ПК беспроводными модулями и у нас будет наблюдаться появление вай фай сети

Зайдем на роутер и посмотрим на его IP address. Как видим, включен DHCP service и роутер получает IP адрес автоматически (рисунок 8.17)

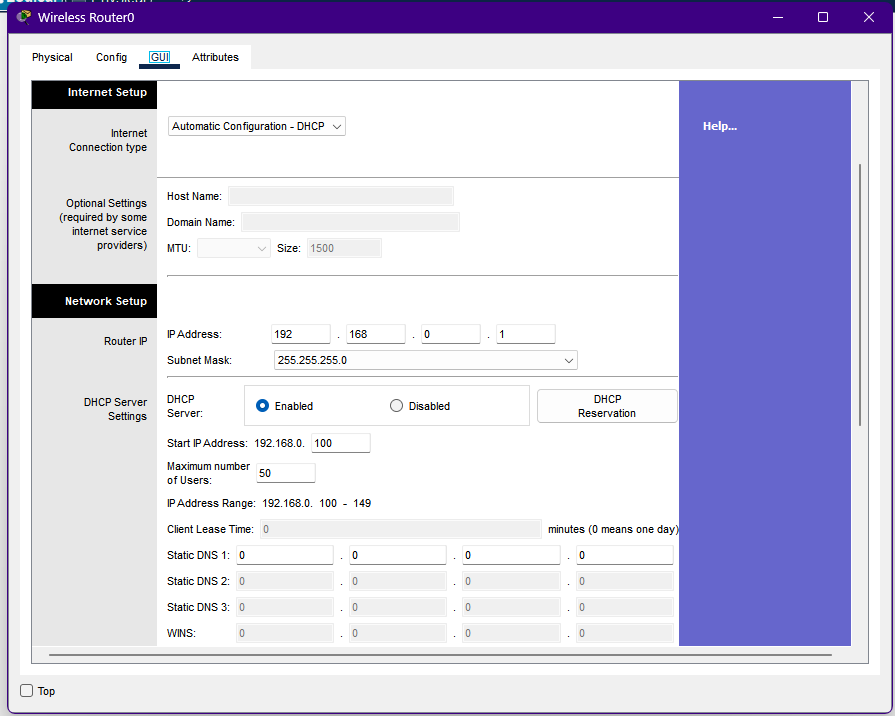


Рисунок 8.17

Теперь на вкладке Config настроим аутентификацию роутера (рисунок 8.18)

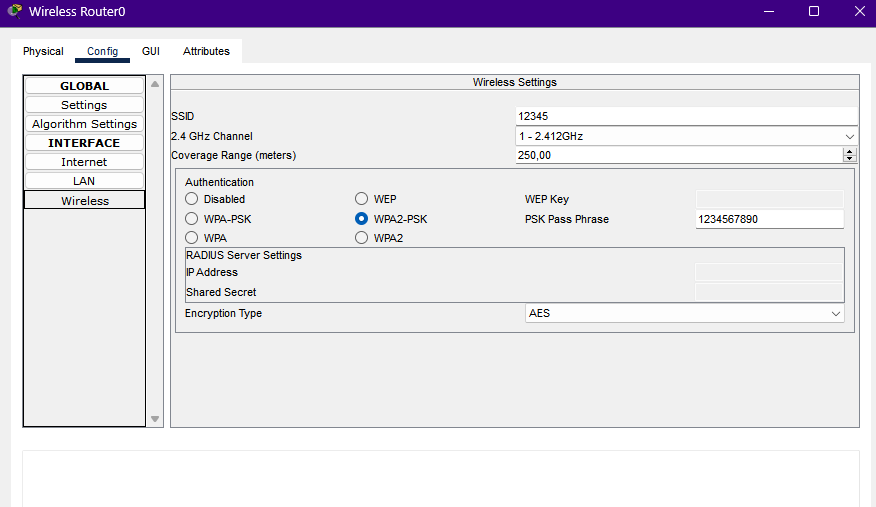


Рисунок 8.18 – Конфигурация роутера

Теперь в ПК 0 установим связь с точкой доступа (рисунок 8.19)



Рисунок 8.19 – GUI Wireless

Выберем и введем ключ аутентификации (1234567890)

Аналогично делаем со вторым ПК

Теперь узнаем IP первого ПК (рисунок 8.20) и пропингуем его со второго (рисунок 8.21)

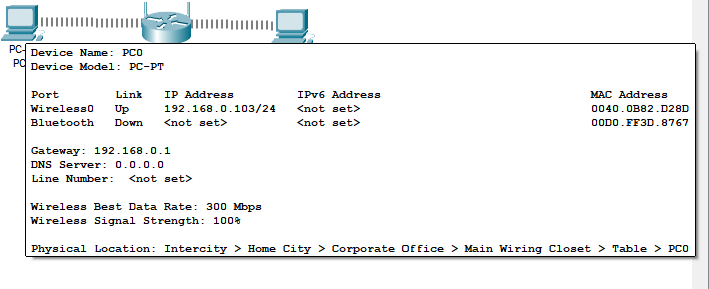


Рисунок 8.20 – Узнаем IP ПК



Рисунок 8.21 – Пингуем ПК