

Лабораторная работа №5

«Исследование топологии и способов построения локальных компьютерных сетей»

1 ЦЕЛЬ РАБОТЫ

Целью работы является углубление теоретических знаний по архитектуре локальных компьютерных сетей (ЛКС), исследование способов построения локальных сетей и конфигурации коммуникационного оборудования. А также приобретение практических навыков конфигурации и исследования функционирования ЛКС.

2 ПОСТАНОВКА ЗАДАЧИ

1. Изучить теоретический материал, касающийся принципам построения локальных компьютерных сетей (выполняется в процессе домашней подготовки).
2. Ознакомиться с особенностями построения системы Packet Tracer и способами построения локальных компьютерных сетей на основе концентратора и коммутатора.
3. Изучить способы конфигурации активного оборудования локальных компьютерных сетей.
4. Построить простейшую локальную сеть на основе концентратора (рисунок 1,а) и исследовать ее функционирование в режиме симуляции и в реальном режиме. IP-адреса рабочих станций при конфигурации выбираются произвольно. **Важно:** адрес сети всех рабочих станций должен быть одинаков!
5. Построить простейшую локальную сеть на основе коммутатора (рисунок 1,б) и исследовать ее функционирование в режиме симуляции и в реальном режиме. IP-адреса рабочих станций при конфигурации выбираются произвольно.

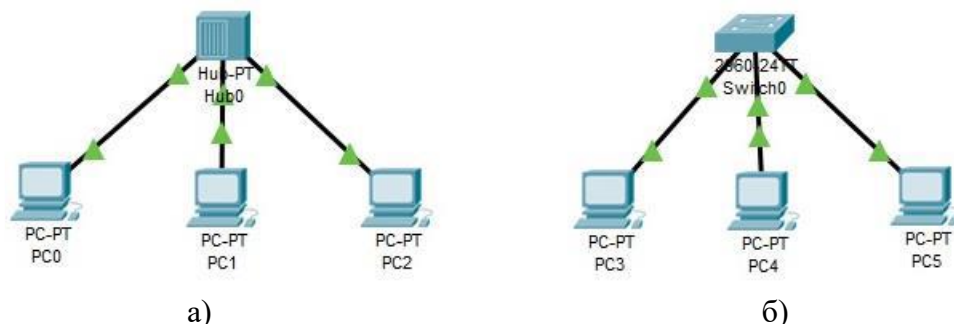


Рисунок 1 – Схемы простейших локальных компьютерных сетей на основе концентратора (а) и на основе коммутатора (б)

6. Построить в программе Cisco Packet Tracer модель локальной компьютерной сети (рисунок 2) на одном коммутаторе и одной беспроводной точке доступа с оконечными устройствами пользователей, количество которых перечислены в таблице 1. Компьютеры должны быть оснащены интерфейсами FastEthernet, ноутбуки – беспроводными интерфейсами, а сервера – интерфейсами GigabitEthernet. Сетевой интерфейс сервера необходимо заменить на модуль *PC-HOST-NM-1CGE*, модуль с проводным интерфейсом на ноутбуке – на модуль с беспроводным интерфейсом *Linksys-WPC300N*.

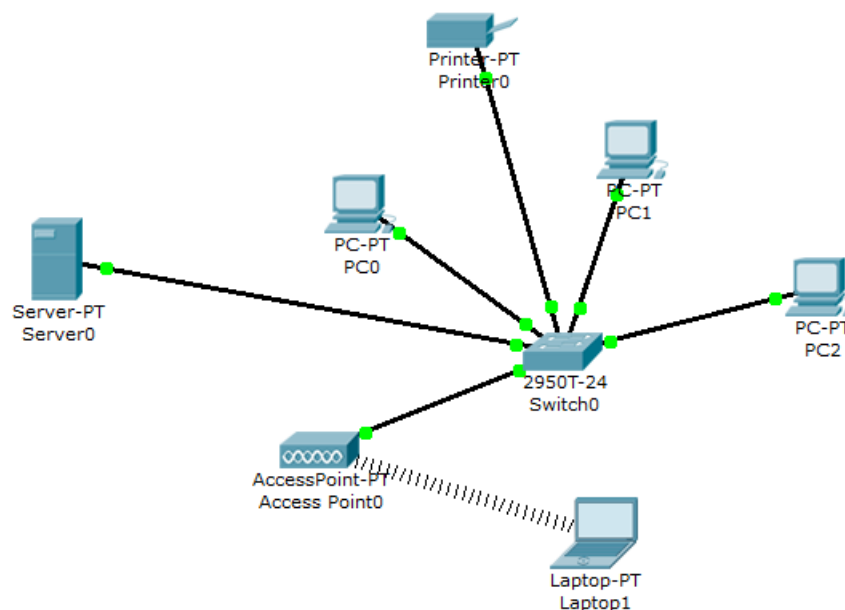


Рисунок 2 – Завершенная топология локальной компьютерной сети

7. Установить на коммутаторе пароль на вход в консоль и в привилегированный режим (для нечетных вариантов пароль хранится в открытом виде, для четных вариантов – в зашифрованном).
8. Задать сетевые имена для компьютеров с PC1 по PCM, для серверов – с Server1 по Server2, для сетевых принтеров с Printer1 по Printer2, для ноутбуков с Laptop1 по Laptop L.
9. Задать IP-адреса пользовательским устройством, выбрав их из диапазона адресов IP-сети 192.168.v.0-192.168.v.255, имеющей маску подсети 255.255.255.0. В начале диапазона IP-адресов разместите сервера, затем принтеры, ПК и ноутбуки. Приведите в отчет таблицу с сетевыми именами и IP-адресами, заданными устройствам, а также названиями сетевых интерфейсов коммутатора, к которым эти устройства подключены.
10. *Реализовать возможность динамического назначения IP-адресов для хостов.
11. Выполнить проверку связи между одним из ноутбуков и любым ПК, любым сервером, любым принтером. Привести в отчете скриншоты с результатами проверки.
12. Изменить IP-адреса первой половины Ваших ПК на адреса из диапазона адресов IP-сети 192.168.(v+1).0-192.168.(v+1).255, имеющей маску подсети 255.255.255.0. Проверьте связь на сетевом уровне между PC1 и PCM (М – максимальный ПК). Проверить связь между PC1 и PC2. Приведите результаты исследования в отчет.
13. Проверить связь с сервером, открыв на нем Web-страницу с помощью Web-браузера, которым оснащен ПК. Но прежде на сервере в HTML-странице HTTP-сервера введите следующую информацию: Ваше Ф.И.О., номер группы и вариант.
14. *Реализовать возможность удаленного подключения к коммутатору по протоколу telnet. При доступе к коммутатору через telnet должен запрашиваться логин (Ваше имя) и пароль (Ваша фамилия).

Таблица 1 – Вариант задания

Вариант	ПК	Сервера	Принтеры	Ноутбуки
10	22	2	1	2

ХОД РАБОТЫ

Построим простейшую локальную сеть на основе Hub (рис. 3). На рисунке 4 изображены присвоенные IP-адреса.

Сперва произведем соединение по IP-адресу в режиме реального времени (рис. 5), а потом в режиме симуляции (рис. 6).

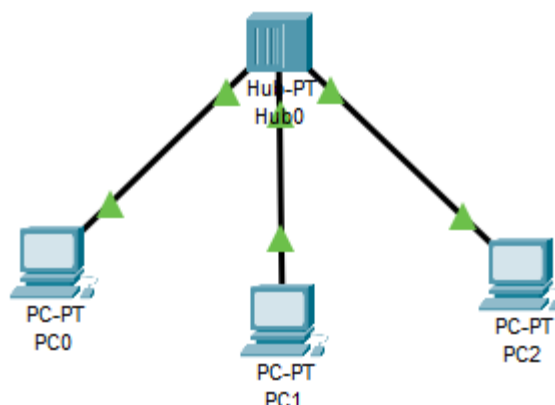


Рисунок 3 – Составленная сеть с Hub

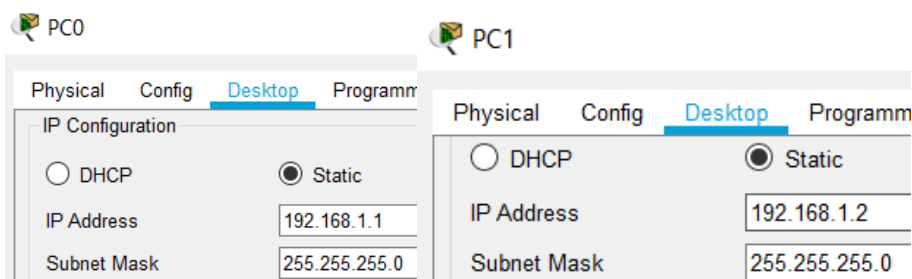


Рисунок 4 – IP-адреса

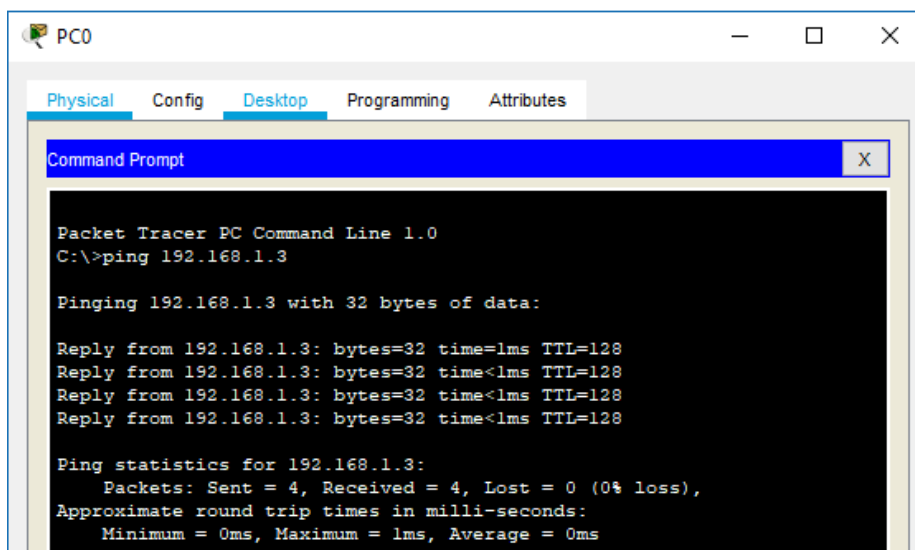


Рисунок 5 – Пингование в режиме реального времени

Как видно с консоли, соединение прошло успешно и ни один пакет не был потерян.

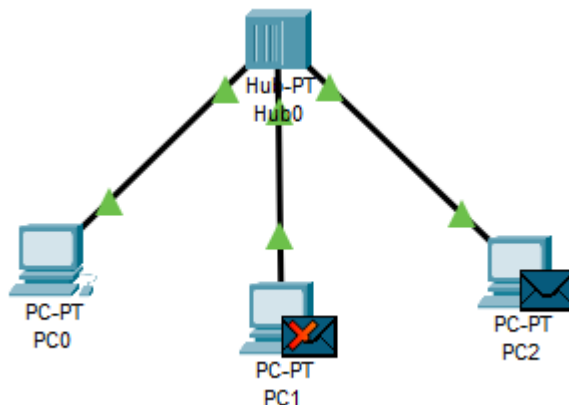


Рисунок 6 – Пингование в режиме симуляции

Как видно из симуляции, Hub отправляет посылку по всем адресам, а принимает и обрабатывает ее только нужный нам адрес.

Построим простейшую локальную сеть на основе Switch (рис. 7). Сперва произведем соединение по IP-адресу в режиме реального времени (рис. 8), а потом в режиме симуляции (рис. 9).

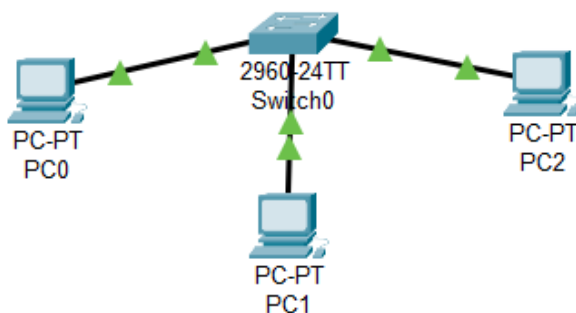


Рисунок 7 – Составленная сеть со Switch

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Рисунок 8 – Пингование в режиме реального времени

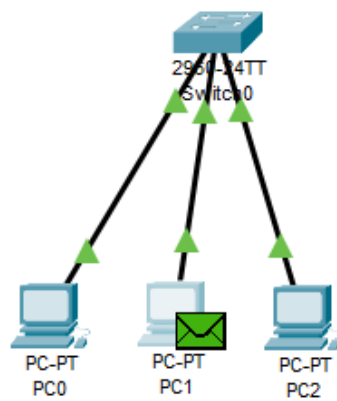


Рисунок 9 – Пингование в режиме симуляции

При первом пинговании switch ведет себя так же как и hub, но каждый раз при доставлении посылки IP-адрес запоминается в таблицу адресов и в дальнейшем, если еще раз использовать этот IP-адрес, то switch уже будет знать куда отправлять данные (рис. 9).

Далее построим в программе модель локальной компьютерной сети (рис. 10) на одном коммутаторе и одной беспроводной точке доступа с оконечными устройствами пользователей, количество которых перечислены в таблице 1.

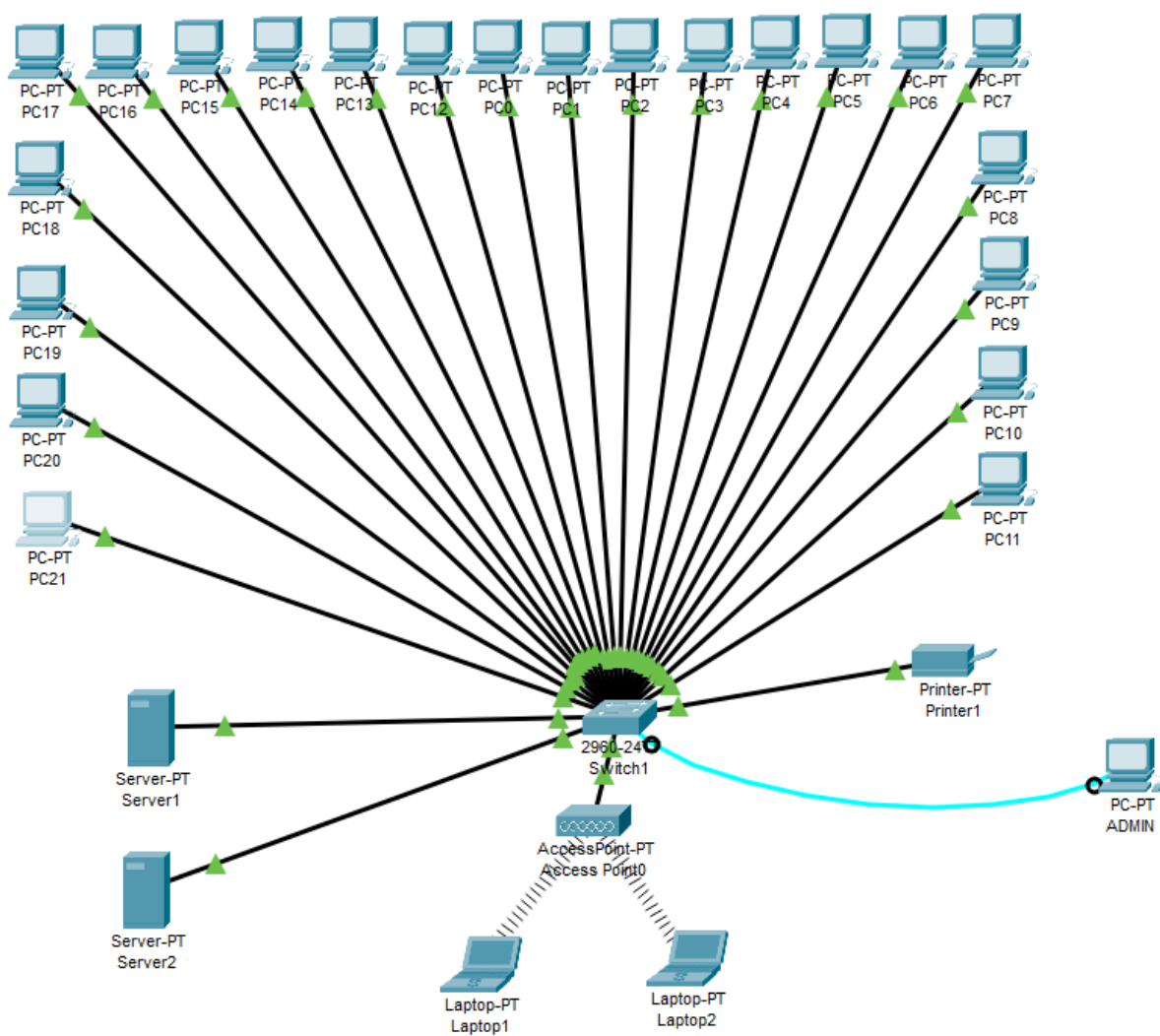


Рисунок 10 – Завершенная топология локальной компьютерной сети по варианту

Установим на коммутаторе пароль на вход в консоль. Для этого соединим вход компьютера PC0 RS 232 консольным кабелем со входом Switch *Console*. Зайдем в настройки коммутатора и перейдем на вкладку *CLI*. Установка пароля показана на рисунке 11.

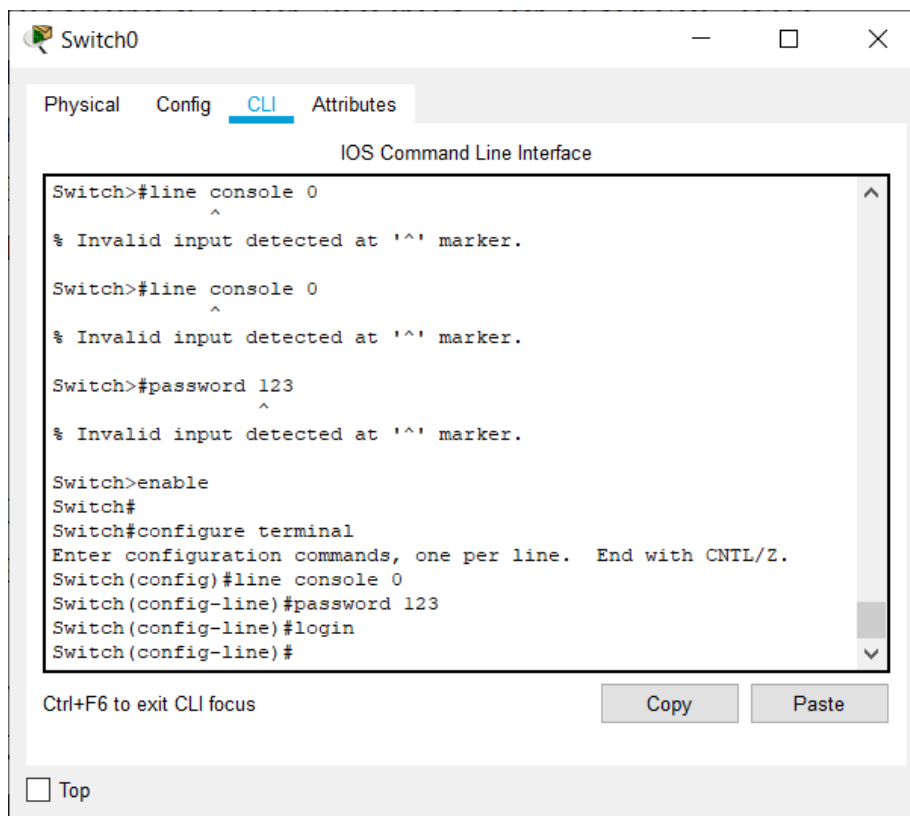


Рисунок 11 – Установка пароля на Switch

Далее реализуем возможность динамического назначения IP-адресов для хостов. Для этого выполним следующие шаги:

- 1) У всех оконечных устройств на вкладке *Config* изменим подключение со статического на DHCP как показано на рисунке 12.

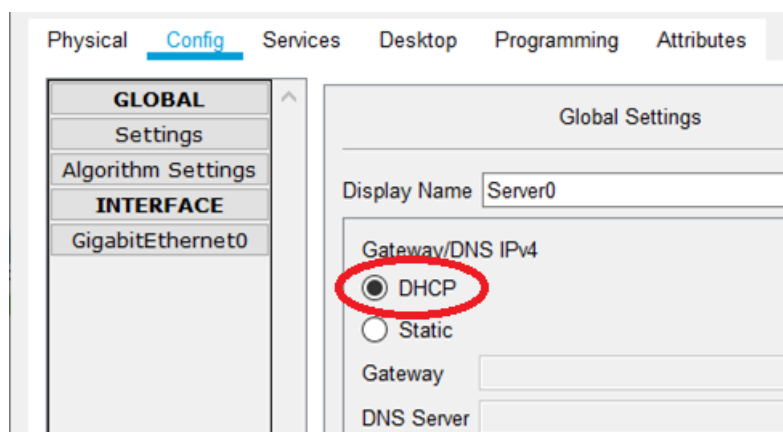


Рисунок 12 – Выбор DHCP подключения

- 2) Далее развернем DHCP-сервер на устройстве *Server1*. У сервера оставим статический IP-адрес 192.168.10.1 в IP-configuration.
- 3) Перейдем на вкладку *Services* и установим такие параметры как показано на рисунке 13. И нажмем кнопку *Save*.

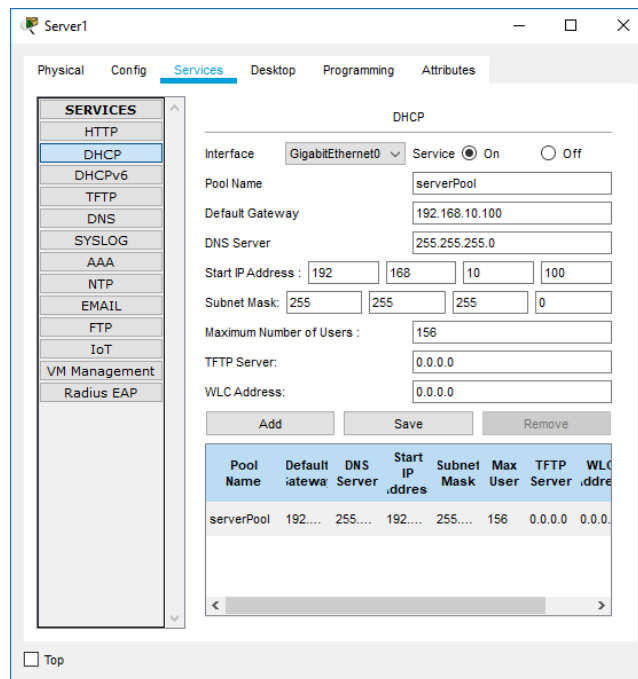


Рисунок 13 – Настройка DHCP-сервера

- 4) После этого спустя некоторое время на всех устройствах будут динамически настроены свои IP-адреса.

В результате все адреса устройств были изменены.

Проверим соединение PC2 с PC8, Laptop1 и PC2 с Printer0. Результат приведен на рисунках 14-16.

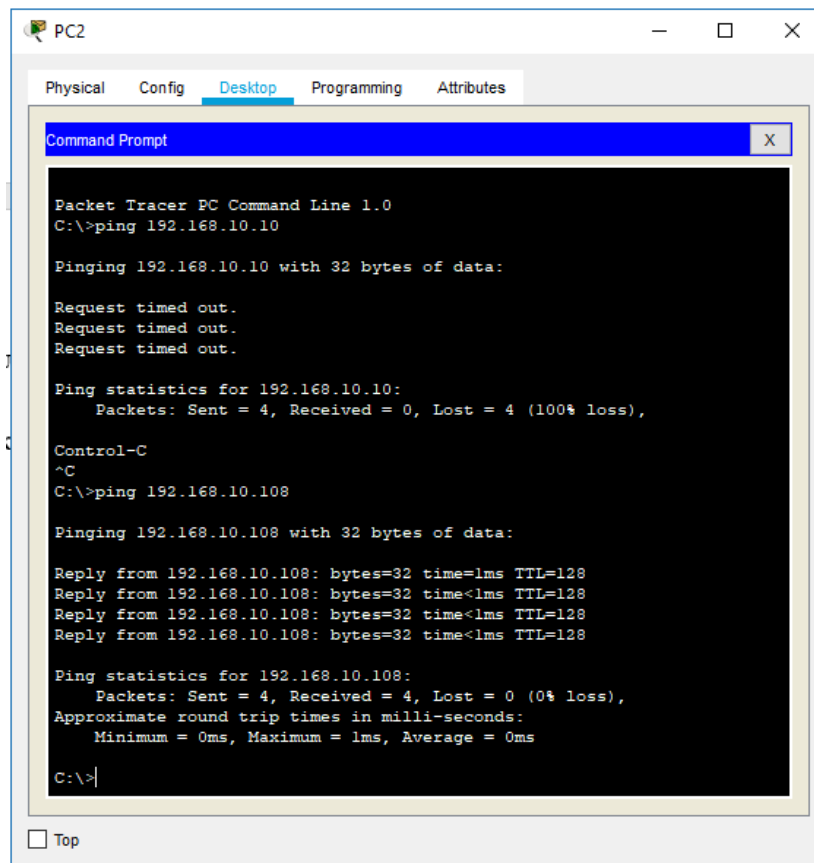


Рисунок 14 – Проверка соединения компьютера с компьютером

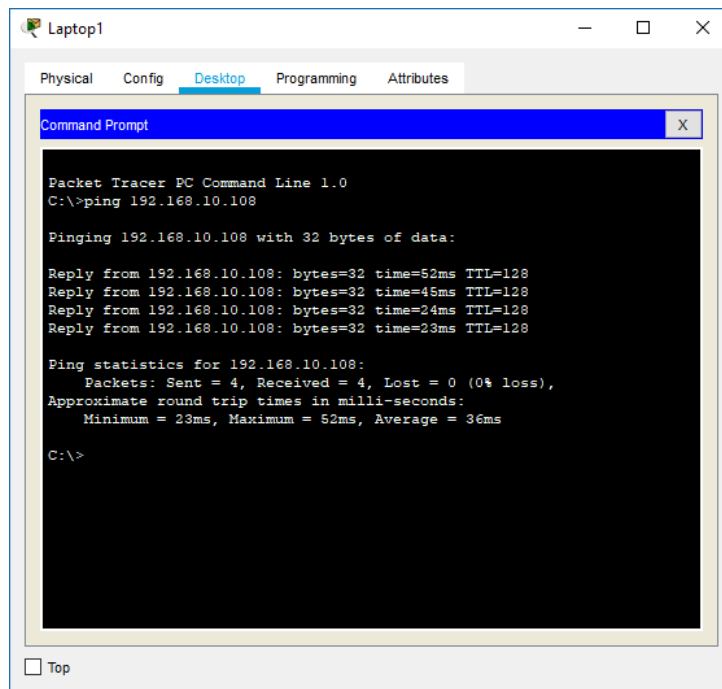


Рисунок 15 – Проверка соединения компьютера с ноутбуком

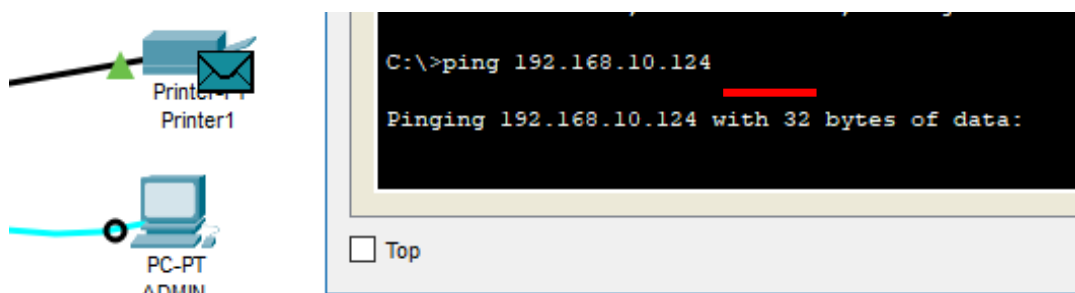


Рисунок 16 – Проверка соединения компьютера с принтером

Теперь изменим на компьютерах PC4 и PC5 на статические 192.168.**2.x**, т.е. изменим их подсеть (рис. 17). Проверим соединение между ними (рис.18) и соединение между PC1 и PC4 (у PC4 адрес не менялся) (рис. 19).

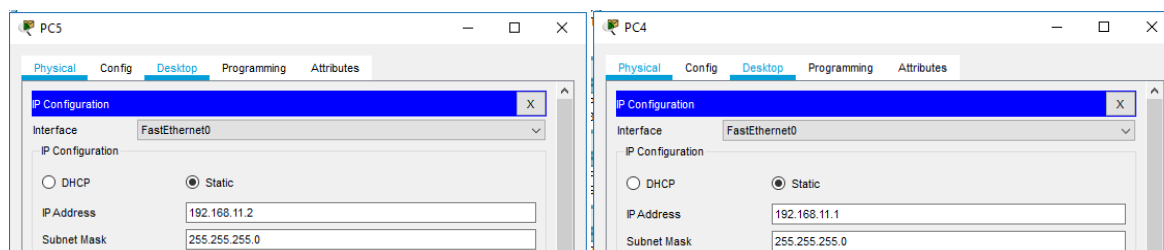


Рисунок 17 – Изменение подсети

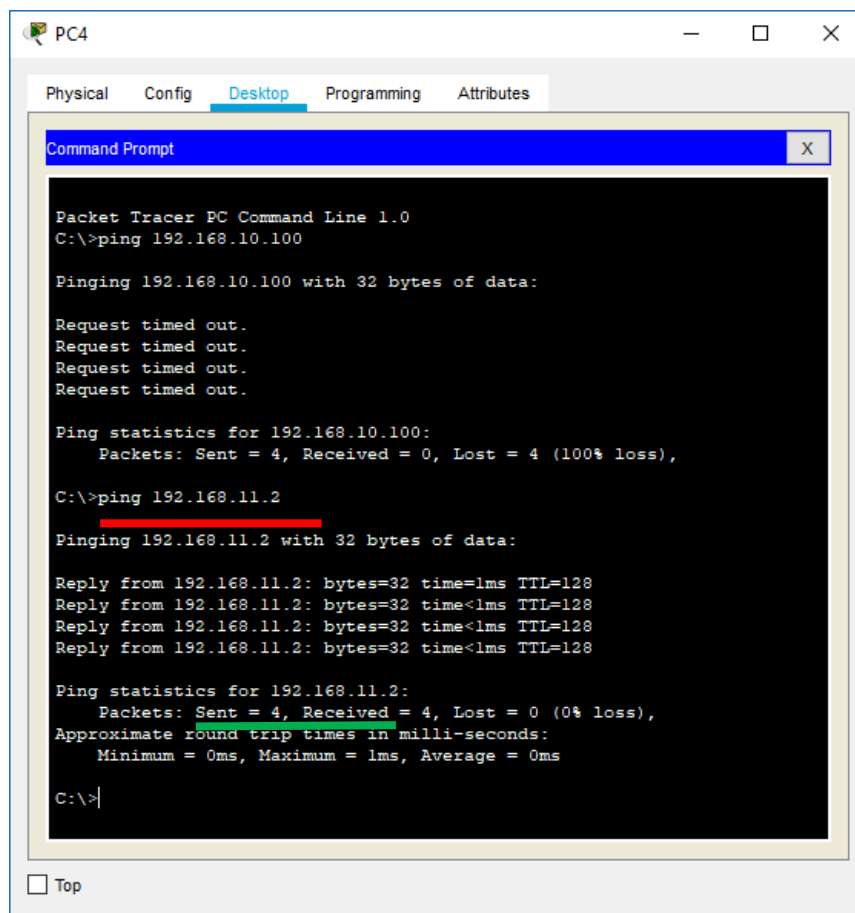


Рисунок 18 – Соединение PC4 с PC5

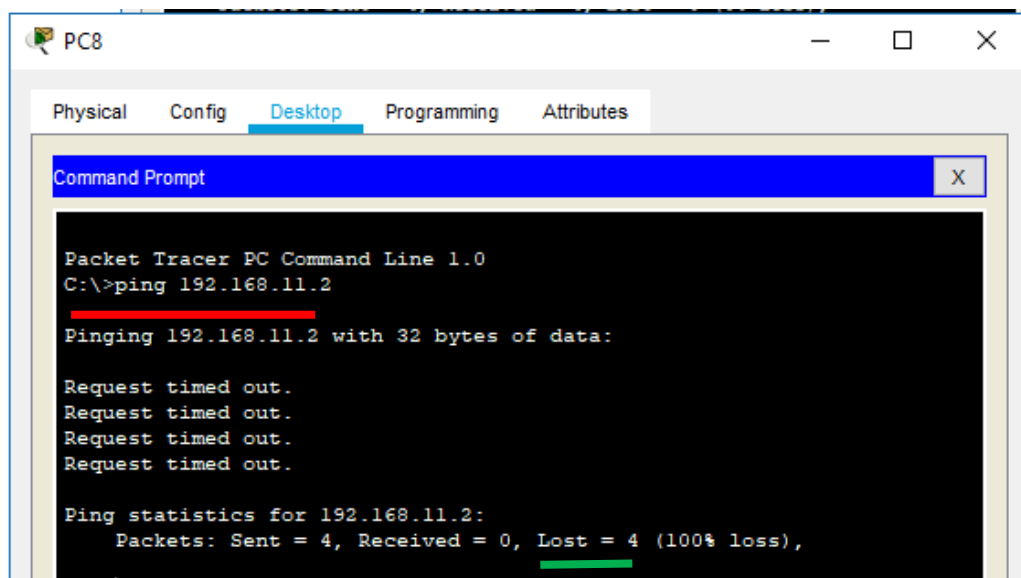


Рисунок 19 – Соединение PC8 с PC4

По рисункам 18 и 19 можно сделать выводы, что компьютеры имеют соединение между собой только в своей подсети.

Теперь проверим работоспособность сервера. Для этого зайдём в его настройки и во вкладки *Config* установим тумблер *on* напротив HTTP сервера (рис. 20).

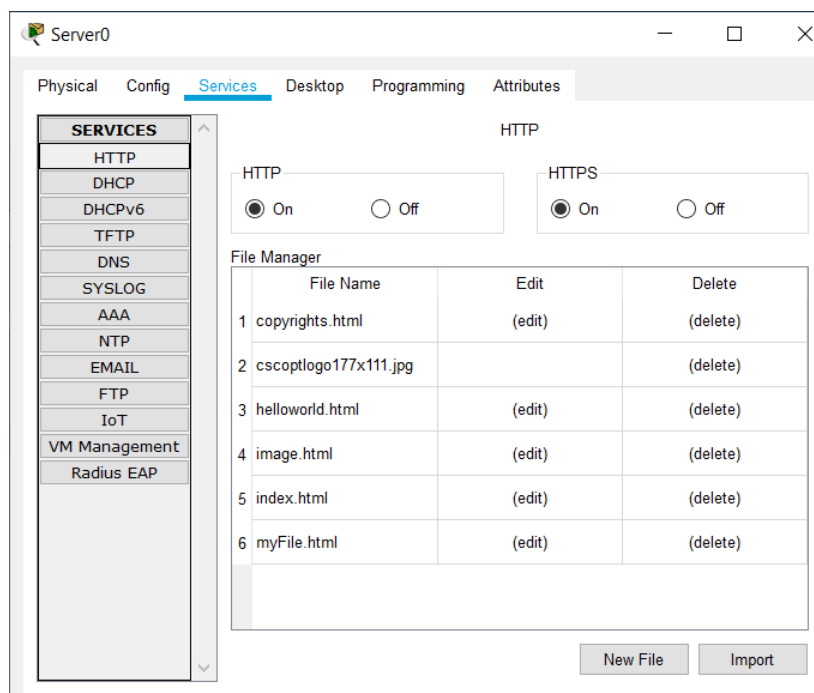


Рисунок 20 – Включение HTTP-сервера

Нажмем на кнопку *New File*, создадим новую страницу (рис. 21) и сохраним ее.

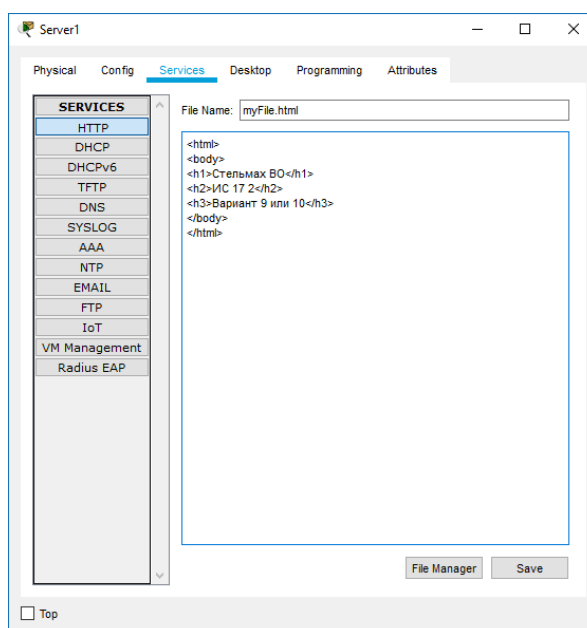


Рисунок 21 – Создание новой web-страницы

Теперь проверим сервер. Зайдем в настройки компьютера PC4, откроем web-браузер и в адресной строке введем IP-адрес Server1 и путь к созданной странице. Созданная страница была открыта в браузере без проблем (рис. 22).

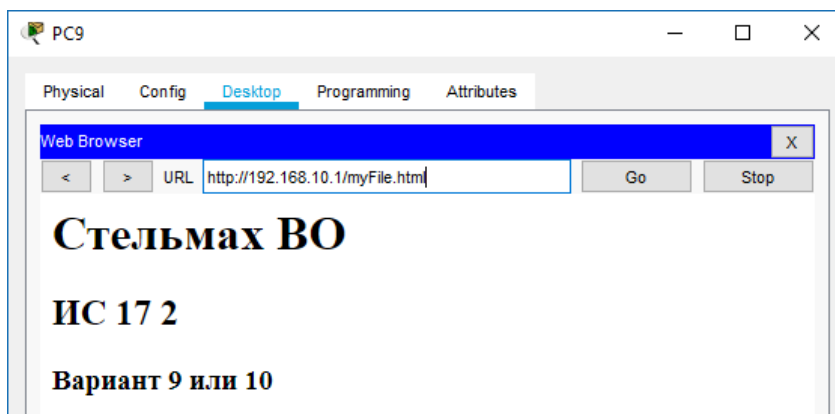


Рисунок 22 – Web-страница с сервера

Далее реализуем возможность удаленного подключения к коммутатору по протоколу telnet. Для этого зайдем в CLI коммутатора и введем следующие команды:

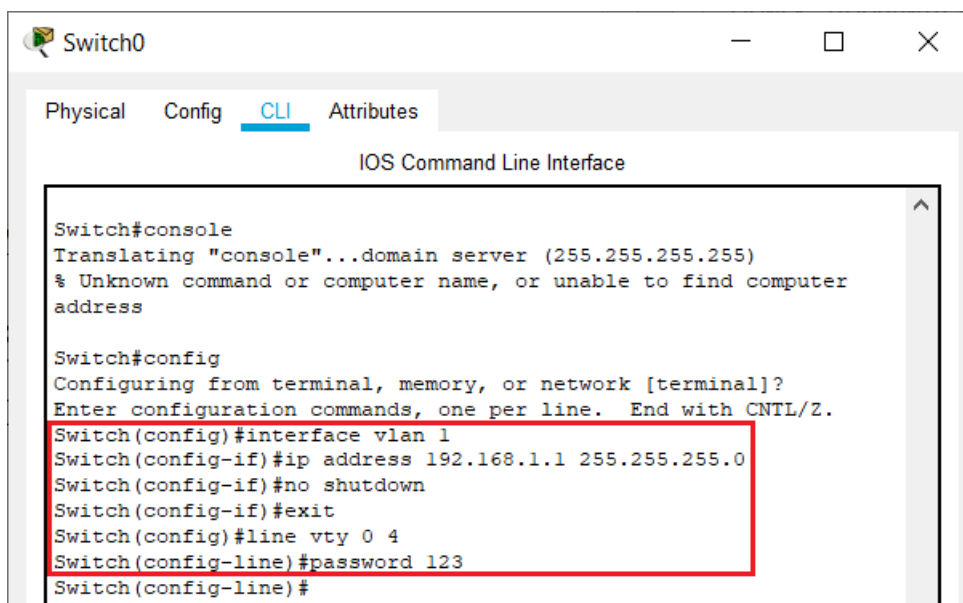


Рисунок 23 – Конфигурация коммутатора

Первыми четырьмя строчками задается IP-адрес виртуальному интерфейсу VLAN 1 коммутатора.

Команда `line vty 0 4` позволяет сконфигурировать линии виртуальных терминалов. Командой `password 123` задается пароль 123 для доступа. 0 4 – это 5 пользовательских виртуальных терминалов = telnet сессий.

Теперь перейдем к консоли компьютера (рис. 24). Компьютер запрашивает нас пароль. Вводим его (123). Создадим пользователя и зададим теперь логин на коммутатор с помощью созданного пользователя.

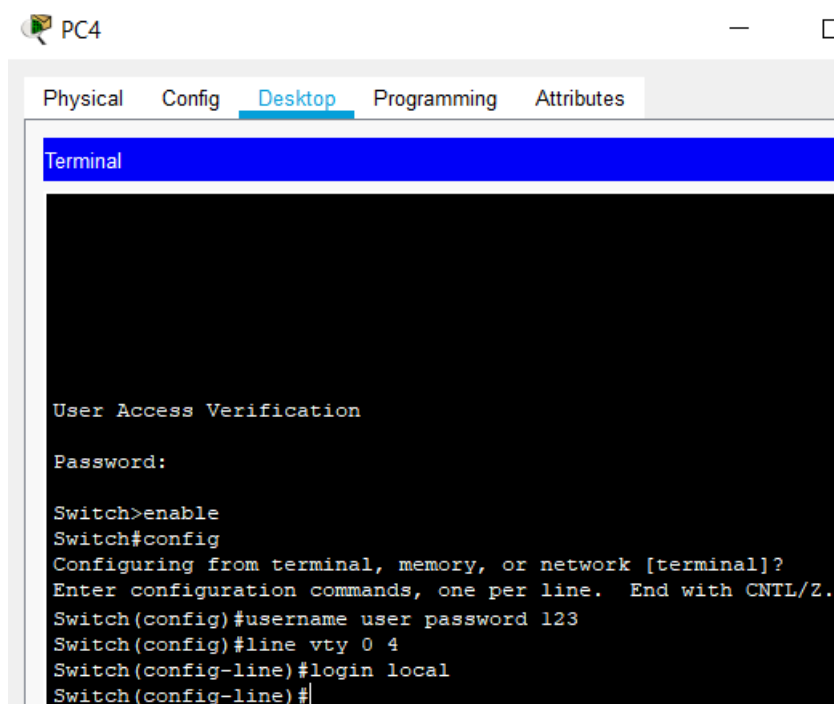


Рисунок 24 – Конфигурация контроллера на компьютере

Настройка закончена, теперь можно перейти в Telnet/SSH Client, ввести адрес, к которому хотим подключиться (192.168.1.1 - шлюз), и компьютер попросит нас ввести логин и пароль, которые мы создали ранее (рис. 25).

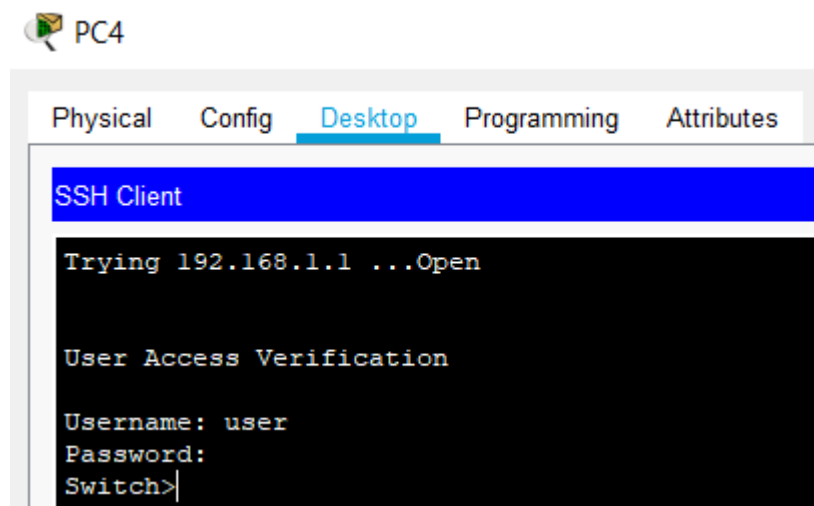


Рисунок 25 – Подключение по telnet

ВЫВОДЫ

В ходе выполнения лабораторной работы были углублены теоретические знания по архитектуре локальных компьютерных сетей (ЛКС), исследованы способы построения локальных сетей и конфигурации коммуникационного оборудования. А также приобретены практические навыки конфигурации и исследования функционирования ЛКС.