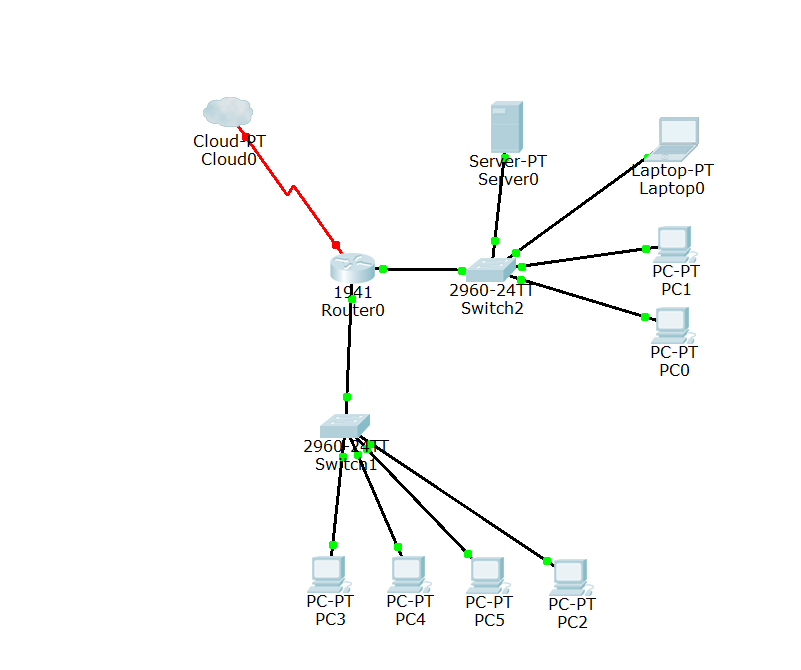
### Лабораторная работа № 010300-204

# Организация межсетевого соединения

В предыдущей работе вами была сконфигурирована и настроена локальная сеть. Все узлы этой сети были размещены в единственной IP сети с адресом 192.168.1.0. В данной работе вам необходимо модифицировать эту сеть, разделив её на две логические сети, и организовать доступ в глобальную сеть.

Для этого в состав оборудования необходимо включить маршрутизатор, а адресное пространство организовать по-прежнему в пределах сети 192.168.1.0:



Расположение и количество рабочих мест сотрудников, сервера, коммутаторов и рабочего места администратора сохранить в соответствии с вводными данными работы № 010300-203. Конфигурацию дополнить маршрутизатором Cisco-1941. Физическую топологию сети организовать в соответствии с рисунком.

Подключение к глобальной сети будет описано далее.

Логическую структуру сети организовать в виде двух подсетей с маской /25. В качестве шлюза по умолчанию в каждой подсети будет выступать соответствующий интерфейс маршрутизатора. В первую сеть включить рабочие станции 4-го этажа и соответствующие сетевые устройства. Во вторую сеть включить все остальные оконечные устройства, расположенные на 28-м этаже, и соответствующие сетевые устройства.

Шлюзу по умолчанию присвоить младший адрес из диапазона подсети. В качестве адресов коммутаторов использовать старшие адреса подсетей. Рабочим станциям, серверу и компьютеру администратора назначать адреса начиная с 10-го в каждой из подсетей.

После назначении IP адреса интерфейсу коммутатора командой вида ***Router(config-if)#ip address .....................................*** необходимо перевести интерфейс в активное состояние командой ***Router(config-if)#no shut***

Просмотреть текущее состояние таблицы маршрутизации можно командой ***Router#show ip route***

Для доступа к внешним сетям, маршрутизатор должен уметь отправлять пакеты, адресованные в любую сеть кроме 192.168.1.0, через интерфейс подключения к внешней сети. На рисунке внешние сети изображены в виде облака. Подключение к удаленным внешним сетям реализуется через сервисы провайдеров. Подключение к провайдеру обычно осуществляется через последовательный интерфейс. С развитием и удешевлением оптоволоконных технологий, такие подключения могут выполняться и через Ethernet - интерфейсы.

В данной работе необходимо эмулировать подключение к внешним сетям через виртуальный интерфейс типа Loopback. IOS Cisco позволяет создавать такие интерфейсы и присваивать им IP адреса. Если маршрутизатор в таблице маршрутизации имеет маршрут, выходным интерфейсом для которого значится интерфейс типа Loopback, то пакет будет на него направлен и маршрутизатор будет считать, что пакет обработан корректно, хотя, конечно, никуда физически этот пакет переправлен не будет. Для виртуального интерфейса используйте младший адрес сети 10.0.0.0.

В представленной на рисунке конфигурации маршрутизатор имеет два активных физических интерфейса, каждый из которых подключен к одной из двух логических сетей. Такие сети маршрутизатор воспринимает как непосредственно подключенные и в таком статусе отражает информацию о них в таблице маршрутизации. При приходе пакета, адресованного в одну из этих сетей, будет просмотрена таблица маршрутизации, и на основании имеющихся там записей пакет будет перенаправлен в нужную сеть.

Если же пакет будет иметь адрес назначения вне сети 192.168.1.0, у маршрутизатора должно быть дополнительное явное указание, как с ним поступить. Для этого в таблицу маршрутизации необходимо добавить ***статический маршрут***, по которому он будет отправлять все такие пакеты.

Это можно сделать командой вида ***ip route 0.0.0.0 0.0.0.0 interface***, где 0.0.0.0 0.0.0.0 - IP адрес и маска для "маршрута по умолчанию", а interface - имя интерфейса, через который надо отправить этот пакет.

**Задания**

1. Составить и заполнить адресную таблицу в виде:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **устройство** | **интерфейс** | **IP адрес** | **маска сети** | **шлюз по умолчанию** |
| Маршрутизатор | G0/0 |  |  |  |
| G0/1 |  |  |  |
| Loopback1 |  |  |  |
| Коммутатор\_1 | Vlan 1 |  |  |  |
| РС\_этаж4\_1 | Сетевая карта (NIC) |  |  |  |
| ....................... | Сетевая карта (NIC) |  |  |  |
| ....................... | Сетевая карта (NIC) |  |  |  |
| ....................... | Сетевая карта (NIC) |  |  |  |
| Коммутатор\_2 | Vlan 1 |  |  |  |
| РС\_администратора | Сетевая карта (NIC) |  |  |  |
| Сервер | Сетевая карта (NIC) |  |  |  |
| РС\_этаж28\_1 | Сетевая карта (NIC) |  |  |  |
| ....................... | Сетевая карта (NIC) |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

2. Запустите Packet Tracer и воспроизведите физическую конфигурацию. Воспользуйтесь для этого результатами предыдущей работы.

3. С помощью компьютера администратора и консольного подключения выполните базовое конфигурирование маршрутизатора:

- задайте уникальное имя

- задайте пароль на консольное подключение

- задайте пароль на доступ к привилегированному пользовательскому режиму

- установите уведомление MOTD, сообщающее о недопустимости несанкционированного доступа к маршрутизатору

- установите пароли доступа на линии виртуальных терминалов и проверьте их действие

- назначьте IP адреса Ethernet интерфейсам и включите их

- сохраните конфигурацию

- отключите консольный кабель

4. С помощью компьютера администратора и консольного подключения при необходимости внесите изменения в конфигурации коммутаторов.

5. Внесите необходимые изменения в настройки IP на рабочих станциях, сервере и компьютере администратора.

6. Проверьте доступность с компьютера администратора всех рабочих станций собственной подсети и сервера.

7. Проверьте доступность с компьютера администратора коммутатора, расположенного в его собственной подсети.

8. Проверьте доступность с компьютера администратора порта маршрутизатора, расположенного в его собственной подсети.

9. Проверьте доступность с компьютера администратора порта маршрутизатора, расположенного в соседней подсети.

10. Проверьте доступность с компьютера администратора коммутатора, расположенного в соседней подсети.

11. Проверьте доступность с компьютера администратора рабочих станций, расположенного в соседней подсети.

12. При наличии проблем выявите их причины и устраните.

13. Проверьте доступность с компьютера администратора устройства с IP адресом 100.100.100.100.

14. Используя протокол Telnet, выполните удалённое подключение к маршрутизатору

15. Просмотрите содержание таблицы маршрутизации

16. Настройте виртуальный интерфейс на маршрутизаторе

17. Внесите в таблицу маршрутизации статический маршрут по умолчанию командой **ip route 0.0.0.0 0.0.0.0** с указанием виртуального интерфейса

18. Просмотрите содержание таблицы маршрутизации, прокомментируйте изменения

19. Еще раз проверьте доступность с компьютера администратора устройства с IP адресом 100.100.100.100. Прокомментируйте результат

19. Сохраните сделанные изменения в конфигурациях

20. Сохраните результаты работы в виде файла в формате Packet Tracer и представьте её преподавателю