**Лабораторная работа 5**Выполнил: Дорохов Михаил, ПММ, 3 курс, 62 группа

**Вариант 1**

Ход работы

1. Ознакомиться с требованиями в Moodle:  
   *“Построить модель сети, конфигурация которой изображена на рисунке (вариант соответствует номеру по списку в подгруппе). Предусмотреть хотя бы один участок сети, имеющий альтернативные маршруты. Дополнить сеть сетью организации(фирмы), в которой предусмотреть маршрутизатор, 5 рабочих станций, настроить службы DNS, Email, HTTP. Провести настройку всей сети, проверить работоспособность и объяснить прохождения пакетов при работе. Организовать демилитаризованную зону с использованием списков доступа”.*
2. Открыть (скачать при необходимости) программу Cisco Packet Tracer и создать новый файл
3. В соответствии с исходной схемой, расположить следующие устройства:
   1. 4 сетевых коммутатора (Switch), использовались “2960-24”
   2. 16 ПК (PC)
   3. 4 Ноутбука (Laptop)
   4. 4 Маршрутизаторов (Router), использовались “2911”
   5. 1 Точку доступа (Access Point)
4. Также, необходимо дополнить схему сетью организации. Для этого необходимо расположить:
   1. 1 Маршрутизатор
   2. 2 Сетевых коммутатора
   3. 5 ПК
   4. 3 Сервера
5. Далее необходимо соединить все устройства в соотвествии со схемой. Для соединения используем инструмент для автоматического соединения проводов из вкладки Connections. Для ноутбуков добавим модули беспроводного соединения, чтобы они могли подключиться к точке доступа.
6. В сети организации: соединим с одним коммутатором 3 сервера, а с другим 5 ПК, соединив коммутаторы с маршрутизатором, который соединим с маршрутизатором Router0.
7. Организуем альтернативный маршрут, соединив Router2, Router1 и Router0 по оптоволокну, предварительно добавив модуль с соответствующим портом. Для альтернативно маршрута зададим IP-адреса 20.0.0.0 и 30.0.0.0.
8. Далее необходимо задать всем остальным устройствам IP-адреса и маски подсетей (маски задаются автоматически):
   1. Для этого в каждом из устройств во вкладке Config перейдём в боковую вкладку, отвечающую за настройку модуля интернета   
      (находится INTERFACE, название представляет собой по сути тип соединения; например в ПК, соединённым обычным образом, эта вкладка может называться “FastEthernet0” и т.п.)
   2. В случае с сетью маршрутизаторов будем использовать примерно следующие IP-адреса: 10.0.0.1, 10.0.0.2, 10.0.0.3 и т.д.;
   3. В случае с остальными устройствами, укажем в каждом из них адреса стандартного шлюза (это адрес маршрутизатора в этой подсети), а в настройке интерфейса будем отдельно указывать для каждого устройтва уникальный IP-адрес, например для одного ПК зададим 192.168.1.2, для второго – 192.168.1.3 и т.д.
9. Далее настроим маршрутизацию используя протокол RIP. Необходимо в каждом маршрутизаторе прописать все адреса тех сетей, с которыми он напрямую соединён. Например, для роутера номер 1 мы укажем: 10.0.0.0, 20.0.0.0, 30.0.0.0, 192.168.2.0; для роутера номер 2 мы укажем: 10.0.0.0, 30.0.0.0, 192.168.3.0 и т.д.
10. Далее настроим сервера. Разделим ответственность между серверами: один будет отвечать за HTTP, другой за EMAIL, третий за DNS. Для почтового сервиса зададим адрес “comp.org” и создадим несколько учётных записей. Для DNS сервера добавим адреса EMAIL и HTTP серверов, для последнего зададим имя “website.org”.
11. Далее настроим DMZ (демилитаризованную зону) при помощи списков доступа. Настраивать эти списки будем в Router4 (сеть организации), который соединяет коммутатор серверов с коммутатором рабочих станций. Откроем CLI маршрутизатора и пропишем следующие команды:  
     **enable  
    conf t  
    access-list 101 permit udp 192.168.15.0 0.0.0.255 192.168.5.0 0.0.0.255 eq domain**

**access-list 101 permit udp 192.168.5.0 0.0.0.255 192.168.15.0 0.0.0.255 eq domain**

**access-list 101 permit tcp 192.168.15.0 0.0.0.255 192.168.5.0 0.0.0.255 eq pop3  
access-list 101 permit icmp 192.168.15.0 0.0.0.255 any echo-reply**

**access-list 101 deny icmp 192.168.15.0 0.0.0.255 any**

**access-list 101 permit ip any any  
interface GigabitEthernet0/2   
ip access-group 101 in   
exit  
  
access-list 102 deny ip any 192.168.5.0 0.0.0.255**

**access-list 102 permit ip any any  
interface GigabitEthernet0/1  
ip access-group 102 in**

**exit**

**access-list 103 deny icmp any 192.168.5.0 0.0.0.255**

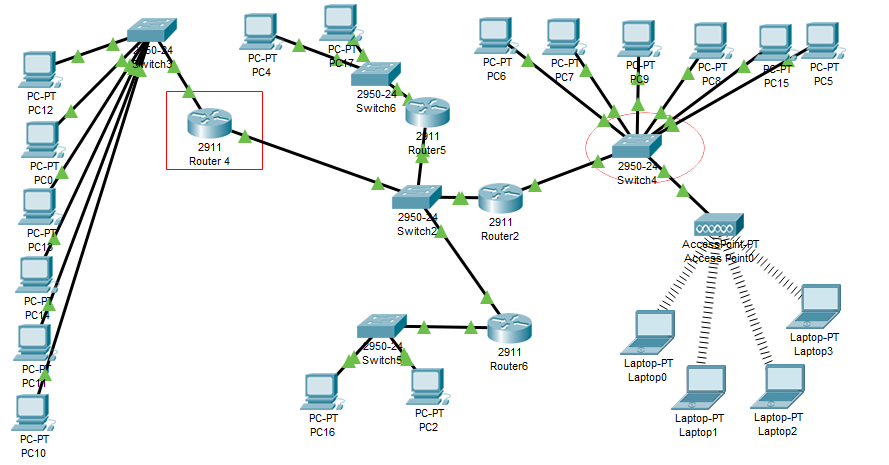
**access-list 103 permit ip any any**

**interface GigabitEthernet0/3**

**ip access-group 103 in  
  
do write**  
  
Где: **access-list 101** – это список доступа, разрешающий: DNS-запросы из DMZ в LAN и обратно, POP3-запросы из DMZ в LAN, блокирует возможность DMZ пинговать любые другие сети;  
**access-list 102** – блокирует весь трафик из внешней сети в LAN, но разрешает остальной трафик (из WAN в DMZ);  
**access-list 103** – блокирует возможность пинговать внешнюю сеть из LAN, но разрешает остальной трафик (например, DNS-запросы в DMZ и т.п.)

1. Финальным шагом протестируем работоспособность сети. При успешном подключение устройств по проводу и правильной настройки маршрутизаторов, оба конца помечаются зелёными треугольниками. Для тестирования работоспособности, отправим несколько пакетов с одних разных устройств, на другие. Для этого:
   1. Выбрать инструмент для отправки пакетов (нажать клавишу “P”)
   2. Выбрать отправителя и получателя
   3. Если пакет успешно доставлен, то в панели справа снизу должна отобразиться строчка с “Last Status” равным “Successful”.
2. В продолжении тестирования, попробуем проверить работоспособность DMZ. Если всё настроено корректно, то мы можем пользоваться DNS-сервером из WAN и LAN, отправлять письма, но при этом DMZ сама не может никого пинговать, а WAN не может пинговать LAN.

*Исходная схема:*



*Итоговая схема:*

