**Практическая работа № 14. Списки доступа.**

Создайте схему сети, как показано на рис.10.1.

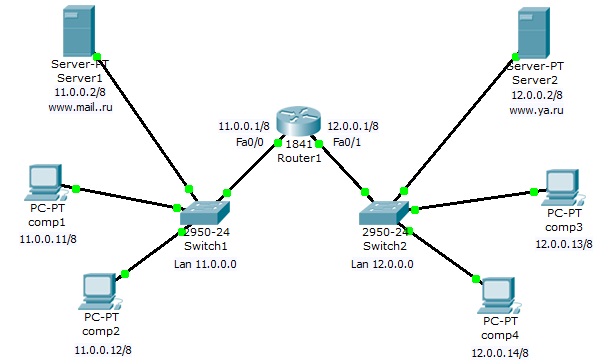


Рис.10.1. Схема корпоративной сети.

Задача:

1 - Компьютеры comp1 и comp2 должны открывать все сайты, но им запрещено входить на компьютеры comp3 и comp4.

2 - Компьютеры comp3 и comp4 доступны друг для друга и должны открывать только сайт своей сети, сеть 11.0.0.0 для них недоступна.

Создадим стандартный список доступа, где укажем правила блокировки на хосты comp3 и comp4 и применим этот список на выход интерфейса Fa0/0.

Включите привилегированный режим и войдите в конфигурацию роутера:

Router1>**en**

Router1#**conf t**

Создадим стандартный список доступа и введем правила доступа:

Router1(config)#**ip access-list standard 10**

Router1(config-std-nacl)#**deny host 12.0.0.13**

Router1(config-std-nacl)#**deny host 12.0.0.14**

Router1(config-std-nacl)#**permit any**

Здесь мы разрешили весь трафик, за исключением двух адресов: 12.0.0.13 и 12.0.0.14.

Просмотрим созданный список доступа в настройках роутера. Для этого надо выйти из режима конфигурации роутера и ввести команду просмотра списков на устройстве **sh access-list**:

Router1#**sh access-list**

Standard IP access list 10

deny host 12.0.0.13

deny host 12.0.0.14

permit any

Router1#

Применим созданный список на выход интерфейса Fa0/0:

Router1#

Router1#**conf t**

Router1(config)#**interface fa0/0**

Router1(config-if)#**ip access-group 10 out**

В результете того, что список доступа был применен к выходу интерфейса сети 11.0.0.0 мы получили следующую политику доступа:

1 – пакеты, входящие на роутер из сети 11.0.0.0 получают блокировку на два внешних адреса – 12.0.0.13 и 12.0.0.14;

2 – всем внешним пакетам, входящим из роутера в сеть 11.0.0.0 разрешается все, кроме двух адресов - 12.0.0.13 и 12.0.0.14 (этим адресам запрещен вход в сеть 11.0.0.0)

Просмотрим привязку списка доступа к интерфейсу Fa0/0 в конфигурации роутера:

Router1(config-if)#**exit**

Router1(config)#**exit**

Router1#

Router1#**sh running-config**

Используя данную команду, вы увидите полную конфигурацию роутера, в том числе и привязку списка доступа к конкретному интерфейсу (в данном случае на выход интрфейса):

interface FastEthernet0/0

ip address 11.0.0.1 255.0.0.0

ip access-group 10 out

duplex auto

speed auto

!

Проверьте созданную политику доступа к ресурсам сети. Должны выполняться следующие правила:

1 - компьютеры comp3 и comp4 доступны друг для друга и должны открывать только сайт своей сети, вход в сеть 11.0.0.0 им заблокирован;

2 – сервера Server2 доступен всем ресурсам сети;

3 - компьютерам comp1 и comp2 доступны все ресурсы, кроме адресов 12.0.0.13 и 12.0.0.14.