Министерство науки и Высшего образования Российской Федерации
Севастопольский государственный университет
Кафедра ИС

Отчет

По дисциплине: «Инфокоммуникационные системы и сети»

Лабораторная работа № 3

«Исследование способов назначения списков контроля доступа в локальных компьютерных сетях»

Выполнил ст. гр. ИС/б-17-2-о
Горбенко К. Н.

Проверил:
Чернега В.С.

Севастополь
2020

1 ЦЕЛЬ РАБОТЫ

Исследование методов контроля доступа к сетевым ресурсам и способов составления списков ограничения доступа, приобретение практических навыков составления стандартных и расширенных списков доступа. а также конфигурации сетевого оборудования.

2 ПОСТАНОВКА ЗАДАЧИ

1. Создать в рабочем окне Packet Tracer схему сети, изображенную на рисунке 1.

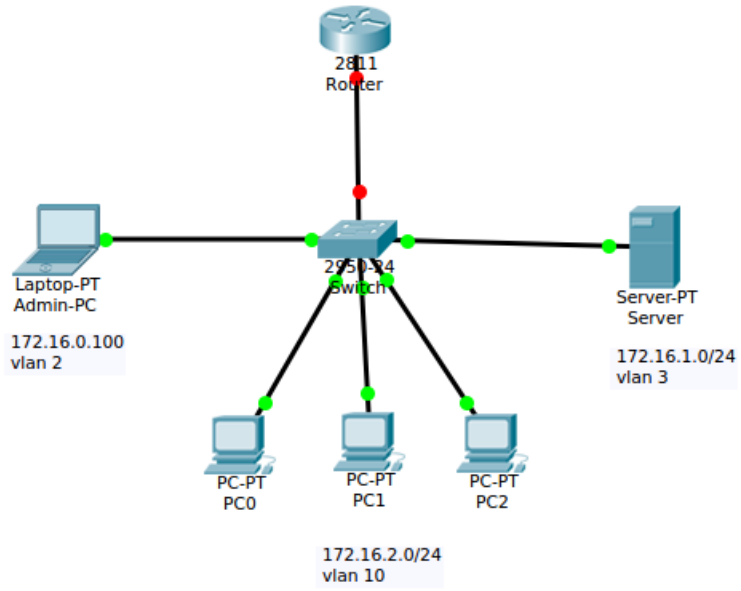

Рисунок 1 – Схема исследуемой компьютерной сети

2. Сконфигурировать коммутатор таким образом, чтобы компьютер администратора с адресом 172.16.0.100 находился в vlan 2, сервер с адресом 172.16.1.0/24 размещался в vlan 3, а рабочие станции представляли собой подсеть vlan 10 с адресом 172.16.2.0/24. Конфигурацию оборудования выполнить с командной строки.

3. Сконфигурировать оборудования т.о., чтобы доступ к серверу имел только администратор.

4. Проверить путем пингования, что требования, изложенные в пункте 2 и 3 выполнены.

5. Переконфигурировать оборудования т.о., чтобы пользователи рабочих станций PC0-PC2 имели доступ к файл-серверу и к HTTP (порт 80) и FTP (порт 21) серверам. При этом предусмотреть функционирование DNS (порт 53) сервера.

3 ХОД РАБОТЫ

1. В рабочем окне Packet Tracer была собрана схема сети, представленная на рисунке 2.

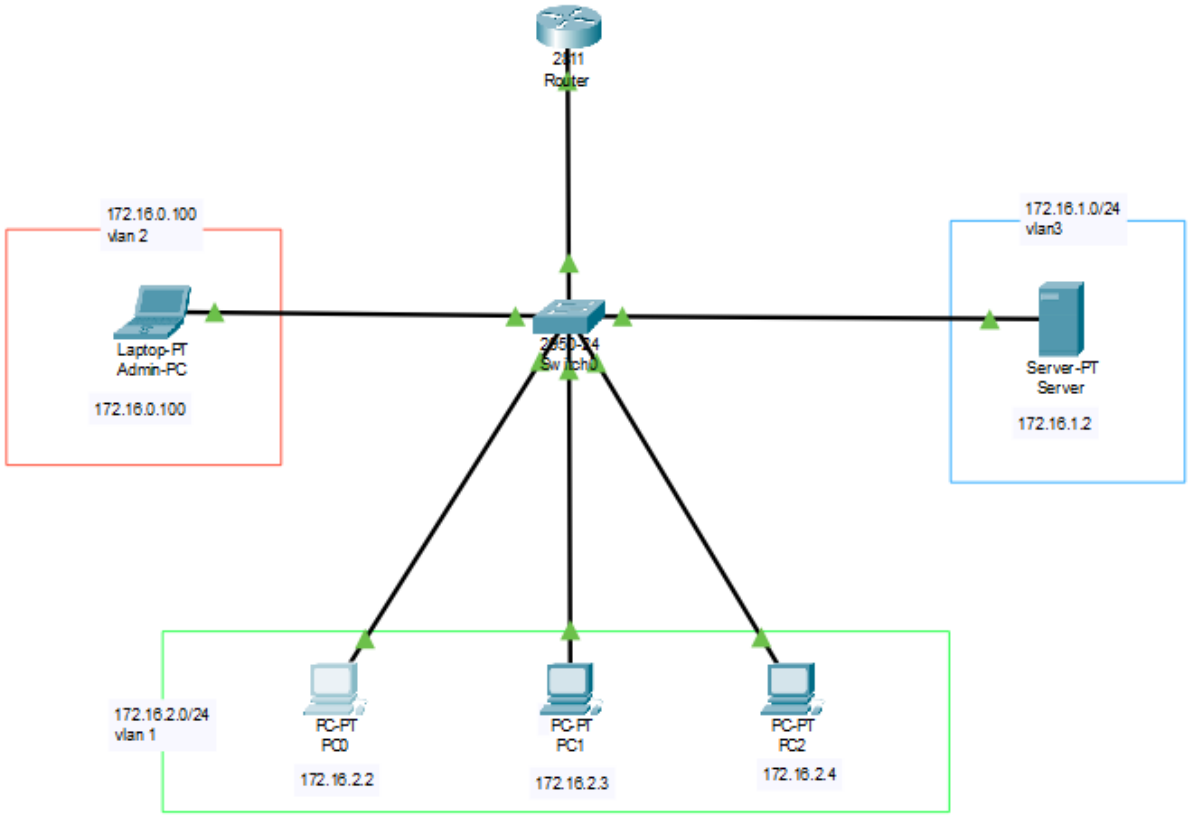

Рисунок 2 – Схема сети

Заполним таблицу сетевых адресов:

Устройство	Интерфейс	IP-адрес	Маска	Шлюз
Router 0	Gig0/0.2	172.16.0.1/24	255.255.255.0	
	Gig0/0.3	172.16.1.1/24	255.255.255.0	
	Gig0/0.10	172.16.2.1/24	255.255.255.0	
Laptop	Fa0/0	172.16.0.100	255.255.255.0	172.16.0.1
PC0	Fa0/0	172.16.2.2	255.255.255.0	172.16.2.1
PC1	Fa0/0	172.16.2.3	255.255.255.0	172.16.2.1

PC2	Fa0/0	172.16.2.4	255.255.255.0	172.16.2.1
Server	Fa0/0	172.16.1.2	255.255.255.0	172.16.1.1

2. Создание vlan’ов:

```
Switch(config)#vlan 10
Switch(config-vlan)#name one
Switch(config-vlan)#exit
Switch(config)#vlan 2
Switch(config-vlan)#name two
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name three
Switch(config-vlan)#exit
```

Описание портов коммутатора:

```
Switch(config)#interface range fastEthernet 0/1-5
Switch(config-if-range)#switchport mode access
Switch(config)#interface range fastEthernet 0/2-4
Switch(config-if-range)#switchport access vlan 10
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport access vlan 2
Switch(config)#interface fastEthernet 0/5
Switch(config-if)#switchport access vlan 3
Switch(config)#interface fastEthernet 0/6
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10,2,3
```

Настраиваем подинтерфейсы для подсетей на роутере:

```
Router#configure terminal
Router(config)#interface fa0/0
Router(config-if)#description Switch
Router(config-if)#no shutdown
Router(config)#interface fa0/0.2
```

```
Router(config-subif)#description Admin
Router(config-subif)#encapsulation dot1q 2
Router(config-subif)#ip address 172.16.0.1 255.255.255.0
Router(config)#interface fa0/0.3
Router(config-subif)#description Server
Router(config-subif)#encapsulation dot1q 3
Router(config-subif)#ip address 172.16.1.1 255.255.255.0
Router(config)#interface fa0/0.10
Router(config-subif)#description Users
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 172.16.2.1 255.255.255.0
```

3. На данный момент доступ к серверу не имеет никто. Нам же необходимо, чтобы доступ имел только админ. Для этого нам необходимо создать список доступа (пусть он будет иметь порядковый номер 10), в котором мы разрешим всем пакетам от администратора (172.16.0.100) доступ в подсеть серверов (172.16.1.0/24). После чего применим это правило на подинтерфейсе fa0/0.3 (для серверов) для всех исходящих пакетов:

```
Router(config)#ip access-list extended Server-out
Router(config-ext-nacl)#permit ip host 172.16.0.100 host 172.16.1.2
Router(config-ext-nacl)#permit tcp any host 172.16.1.2 eq 80
Router(config-ext-nacl)#permit tcp any host 172.16.1.2 eq 21
Router(config-ext-nacl)#permit tcp any host 172.16.1.2 eq 53
Router(config-ext-nacl)#exit
Router(config)#interface fa0/0.3
Router(config-if)#ip access-group Server-out out
```

4. Пропингуем сервер:

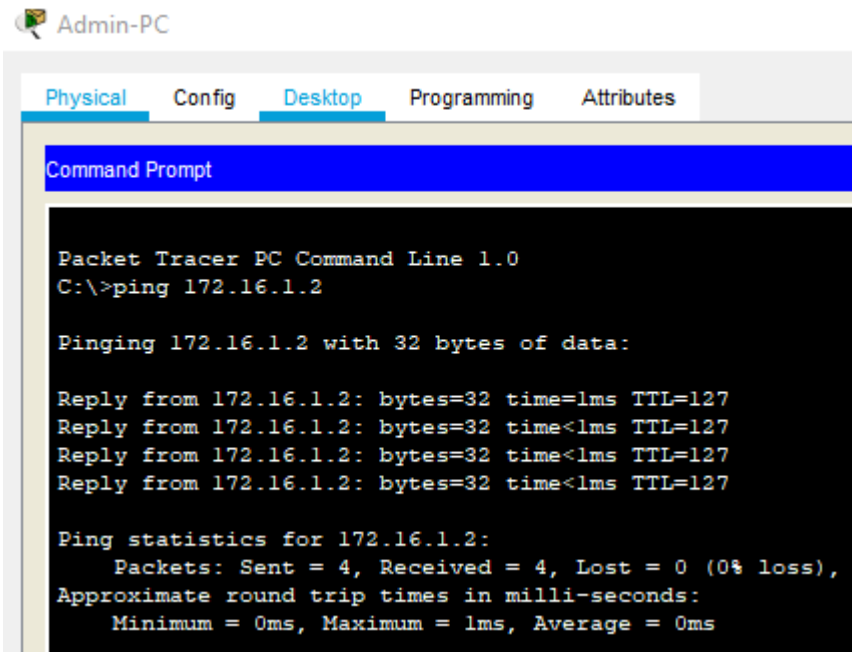

Рисунок 3 – Пингование сервера с ноутбука

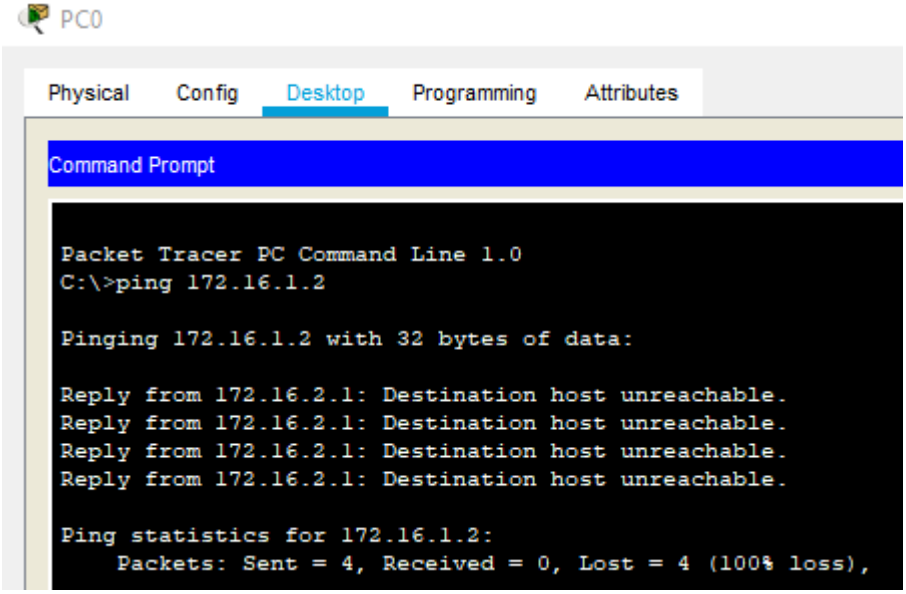

Рисунок 4 – Пингование сервера с PC0

Проверим доступ к созданному на сервере Web-сайту через браузер с PC0 (рисунок 5):

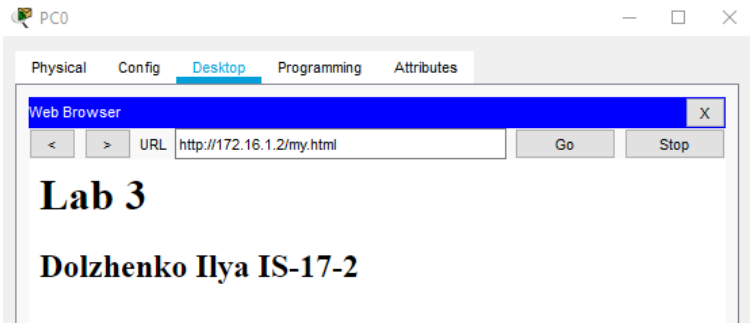

Рисунок 5 – Успешный доступ к сайту, расположенному на сервере

Подключимся к FTP-серверу с PC2:

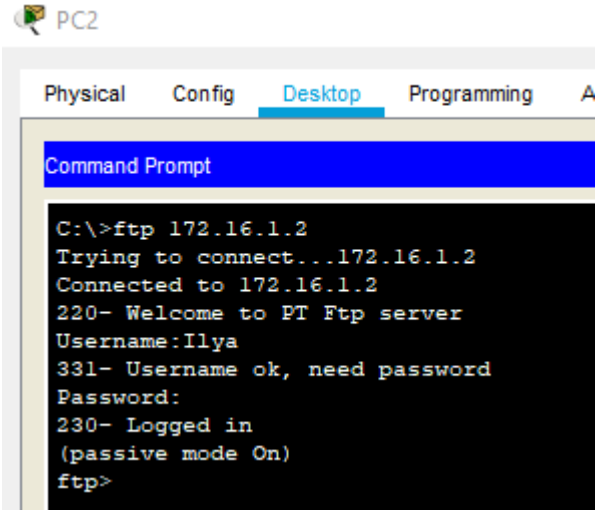

Рисунок 6 - Подключение к FTP-серверу с компьютера пользователя

ВЫВОДЫ

В ходе выполнения данной лабораторной работы были исследованы методы контроля доступа к сетевым ресурсам и способы составления списков ограничения доступа, приобретены практические навыки составления стандартных и расширенных списков доступа, а также конфигурации сетевого оборудования.