

САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ  
ПЕТРА ВЕЛИКОГО

---

Институт компьютерных наук и технологий  
Высшая школа интеллектуальных систем и суперкомпьютерных технологий

Дисциплина  
«Администрирование компьютерных сетей»

Курсовое проектирование  
«Проектирование корпоративной компьютерной сети для  
офиса завода-производителя трубопроводной арматуры»

выполнил:  
Дроздов Никита Дмитриевич  
группа: 3540901/02001  
преподаватель:  
Малышев Игорь Алексеевич

Санкт-Петербург  
2021

## Цели работы

1. Создать и настроить компьютерную сеть для офиса завода-производителя трубопроводной арматуры средствами Cisco Packet Tracer;
2. Установить необходимые сервисы;
3. Настроить выход во внешнюю сеть;
4. Разграничить области компьютерной сети;
5. Выполнить проверку работы сети.

## Требования

- Необходимо наличие нескольких подсетей: сети, обеспечивающей взаимодействие между компьютерами сотрудников, сеть для обеспечения хранения важных корпоративных данных компании;
- Сотрудники компании должны иметь постоянный доступ к сети Интернет.

## Функциональность подсетей

1. Пользовательская, то есть для сотрудников. Настроенный DHCP сервере, для автоматического получения адреса сотрудниками;
2. Подсеть с TFTP сервером для хранения файлов.

## Создание сети

Была создана компьютерная сеть (Рисунок 1)

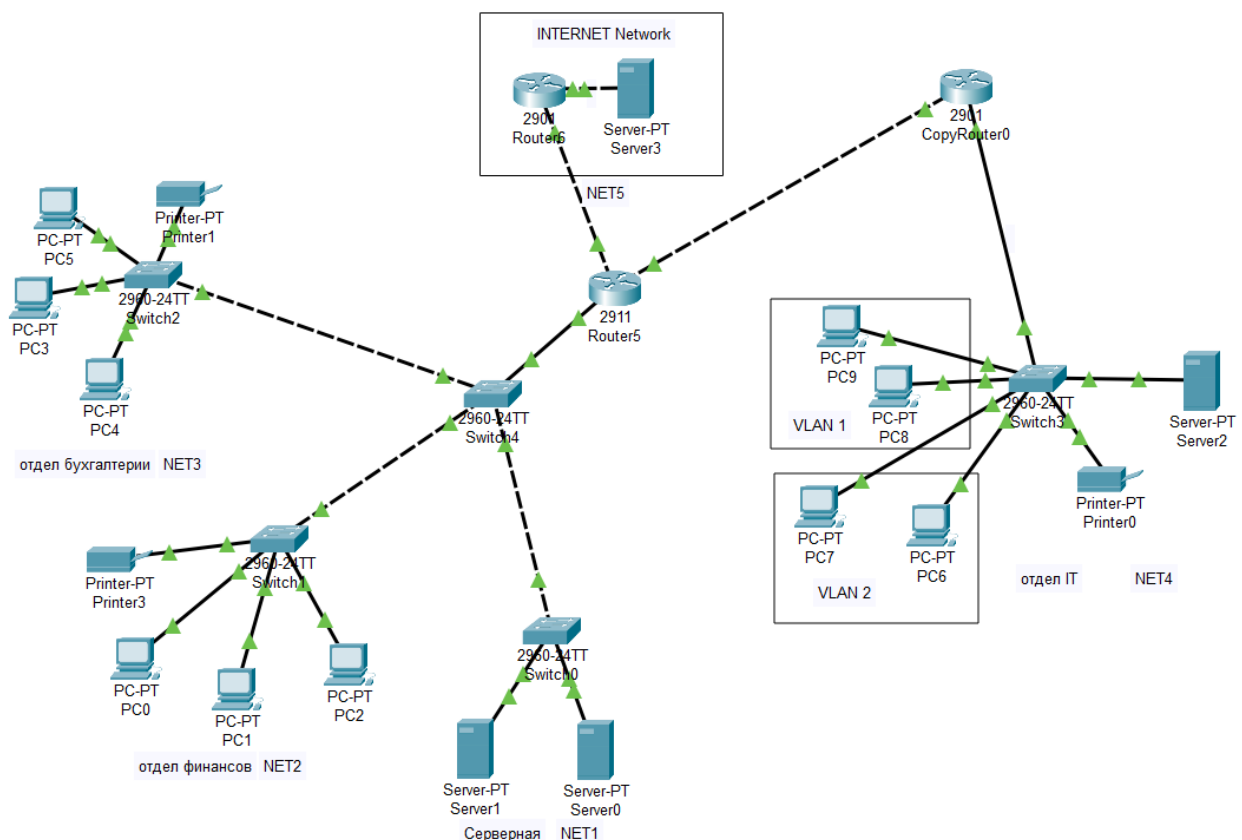


Рисунок 1 - схема сети

Сеть строилась в программе Cisco Packet Tracer. Для построения были использованы следующие элементы:

- PC-PT – компьютер;
- Server-PT – сервер;
- Printer-PT – принтер.

Сетевые устройства:

- Router-2911 – роутер;
- 2960 – коммутатор на 24 порта.

Подсети:

- Net1 – Серверная к которой есть доступ из Net2 и Net3;
- Net2 – отдел финансов;
- Net3 – отдел бухгалтерии;
- Net4 – отдел IT, который имеет две виртуальной локальной сети;
- Net5 – эмуляция сети интернет.

### **Ход работы**

Связь между устройствами была произведена с использованием инструмента Automatically choose connection type, который автоматически подключает интерфейсы устройств (Рисунок 1).

### **Настройка сети**

В подсеть Net1 входят коммутатор и два сервера:

- Ip первого сервера – 192.168.10.2;
- Ip второго сервера – 192.168.10.3.

На одном из двух серверов устанавливаем DHCP, чтобы компьютеры в подсети Net2 и Net3 получали динамический Ip-адрес. Адрес у серверов должен быть статическим.

На коммутаторе создаем VLAN4, так как сервера определяются в отдельный VLAN. Далее настраиваем два Access-порта и один Trunk-порт на следующий коммутатор, на котором во все стороны настроены Trunk-порты. Через него подсоединяемся к маршрутизатору. На маршрутизаторе поднимаем Sub-Interface, задаем ему IP-адрес 192.168.4.1 и прописываем команду «encapsulation dot1Q 4», где «4» означает номер VLAN.

DHCP сервер настроен следующим образом:

DHCP

Interface FastEthernet0 Service ☒ On ☐ Off

Pool Name DHCP-VLAN2

Default Gateway 192.168.2.1

DNS Server 8.8.8.8

Start IP Address : 192 168 2 0

Subnet Mask: 255 255 255 0

Maximum Number of Users : 256

TFTP Server: 0.0.0.0

WLC Address: 0.0.0.0

Add Save Remove

| Pool Name  | Default Gateway | DNS Server | Start IP Address | Subnet Mask   | Max User | TFTP Server | WLC Address |
|------------|-----------------|------------|------------------|---------------|----------|-------------|-------------|
| DHCP-VLAN5 | 192.168.5.1     | 8.8.8.8    | 192.168.5.0      | 255.255.255.0 | 256      | 0.0.0.0     | 0.0.0.0     |
| DHCP-VLAN3 | 192.168.3.1     | 8.8.8.8    | 192.168.3.0      | 255.255.255.0 | 256      | 0.0.0.0     | 0.0.0.0     |
| DHCP-VLAN2 | 192.168.2.1     | 8.8.8.8    | 192.168.2.0      | 255.255.255.0 | 256      | 0.0.0.0     | 0.0.0.0     |
| serverPool | 0.0.0.0         | 0.0.0.0    | 192.168.4.0      | 255.255.255.0 | 256      | 0.0.0.0     | 0.0.0.0     |

Рисунок 2 - настройка DHCP сервера

В коммутаторе подсети NET1 создается VLAN2, и на интерфейсах: Access-порт и Trunk-порт. Далее подключаемся к маршрутизатору через еще один коммутатор, в котором в обе стороны настроены Trunk-порты. На маршрутизаторе поднимаем Sub-Interface и задаем ему IP-адрес 192.168.2.1. Аналогично, как и в настройке NET1, прописываем команду «encapsulation dot1Q 4». Настраиваем IP helper-address, прописывая в него IP-сервера DHCP. На конечных устройствах указываем динамический IP.

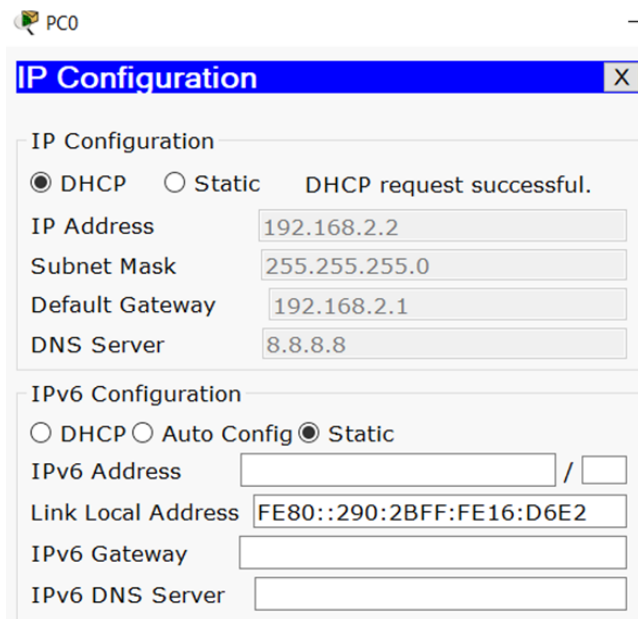


Рисунок 3 - настройка IP PC0

Таким же образом настраивается подсеть Net3. В промежуточный коммутатор на одном из интерфейсов прописываем Trunk-порт для VLAN 2-4.

```

:
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/1.1
encapsulation dot1Q 1 native
ip address 192.168.1.1 255.255.255.0
ip helper-address 192.168.4.3
shutdown
!
interface GigabitEthernet0/1.2
encapsulation dot1Q 2
ip address 192.168.2.1 255.255.255.0
ip helper-address 192.168.4.3
!
interface GigabitEthernet0/1.3
encapsulation dot1Q 3
ip address 192.168.3.1 255.255.255.0
ip helper-address 192.168.4.3
!
interface GigabitEthernet0/1.4
encapsulation dot1Q 4
ip address 192.168.4.1 255.255.255.0
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!

```

Рисунок 4 - настройка маршрутизатора

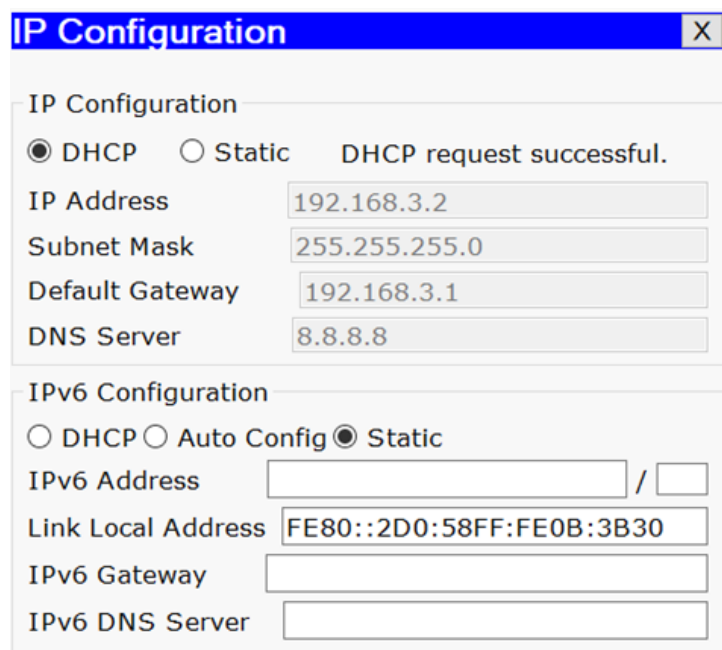


Рисунок 5 - IP-конфигурация одного из ПК в Net3

Подсеть Net4 была поделена на два VLAN. Два компьютера и принтер на одном VLAN, и другие два компьютера на другом VLAN. Также в подсети NET4 имеется отдельный сервер с TFTP и DHCP. Настраиваем всё также, как и в предыдущих пунктах.

В итоге у нас имеется: VLAN2, VLAN3, VLAN4.

VLAN2 и VLAN3 получают IP-адрес автоматически. Адрес сервера статичен – 192.168.44.2.

```
interface FastEthernet0/1
  switchport access vlan 2
  switchport mode access
!
interface FastEthernet0/2
  switchport access vlan 2
  switchport mode access
!
interface FastEthernet0/3
  switchport access vlan 2
  switchport mode access
!
interface FastEthernet0/4
  switchport access vlan 3
  switchport mode access
!
interface FastEthernet0/5
  switchport access vlan 3
  switchport mode access
!
interface FastEthernet0/6
  switchport access vlan 4
  switchport mode access
!
interface FastEthernet0/7
  switchport trunk allowed vlan 2-4
  switchport mode trunk
!
```

Рисунок 6 - конфигурация коммутатора в подсети Net4

```

interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/1.2
encapsulation dot1Q 2
ip address 192.168.22.1 255.255.255.0
ip helper-address 192.168.33.2
ip helper-address 192.168.44.1
ip helper-address 192.168.44.2
!
interface GigabitEthernet0/1.3
encapsulation dot1Q 3
ip address 192.168.33.1 255.255.255.0
ip helper-address 192.168.44.1
ip helper-address 192.168.44.2
!
interface GigabitEthernet0/1.4
encapsulation dot1Q 4
ip address 192.168.44.1 255.255.255.0
!

```

Рисунок 7 - конфигурация маршрутизатора

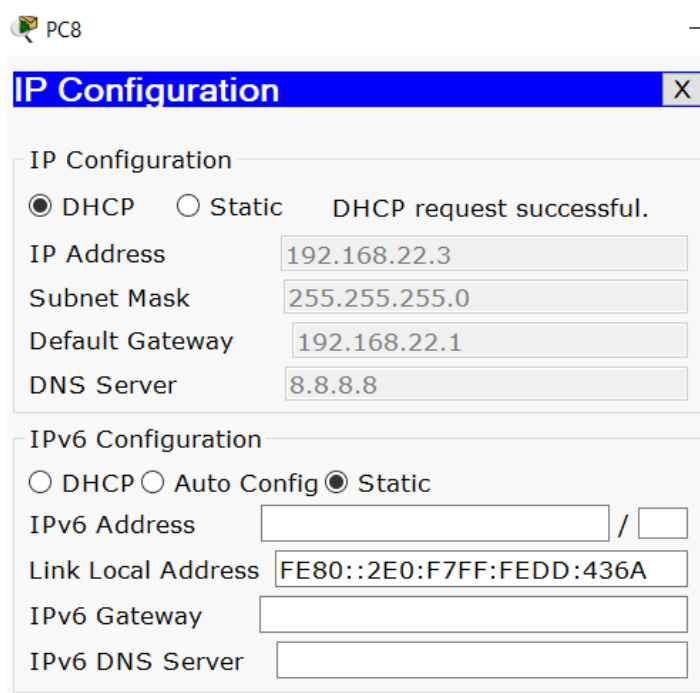


Рисунок 8 - IP-конфигурация одного из ПК в подсети Net4

### Настройка NAT

На внешней сети у нас имеется два элемента: маршрутизатор и сервер. У обоих элементов публичные («белые») IP-адреса. В маршрутизаторе на оба интерфейса прописываются «белые» IP. Один интерфейс смотрит на сеть самой организации, а другой - на доступный сервер.

На основном маршрутизаторе, в интерфейсе, который смотрит во внешнюю сеть, прописываем «белый» IP. В нем происходит настройка NAT. На интерфейсе, который смотрит наружу, прописываем команду: «ip nat outside», а на интерфейсы, которые смотрят внутрь, «ip nat inside».

Также создаем Access-list, где с помощью команды «permit» добавляем наши подсети. В команде «permit» используется «wildcard mask», поэтому после IP-адресов прописываем: «0.0.0.255».

### Настройка TFTP

Настройка TFTP сервиса была произведена во вкладке Services, где его необходимо включить, и, для удобства, удалить предварительно сгенерированные в нем файлы.

## Тестирование сети

### Проверка работоспособности сети

Проверяем каждую подсеть утилитой «ping». Каждый VLAN проверяем от маршрутизатора и до внешнего сервера.

```
Router#ping 192.168.22.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.22.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms

Router#
```

Рисунок 9 - ping от маршрутизатора к конечному пользователю

```
Router#ping 213.234.20.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 213.234.20.1, timeout is 2 seconds:
!...!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms

Router#
```

Рисунок 10 - ping от маршрутизатора к внешнему маршрутизатору

### Проверка работоспособности сети

Открываем на Router 1 консоль, где выполнены следующие команды

```
1 Router>enable
2 Router#show flash
3
4 System flash directory:
5 File Length Name/status
6 3 5571584 pt1000-i-mz.122-28.bin
7 2 28282 sigdef-category.xml
8 1 227537 sigdef-default.xml
9 [5827403 bytes used, 58188981 available, 64016384 total]
10 63488K bytes of processor board System flash (Read/Write)
11
12 Router#copy flash tftp
13 Source filename []? pt1000-i-mz.122-28.bin
14 Address or name of remote host []? 192.168.10.1
15 Destination filename [pt1000-i-mz.122-28.bin]? temp.file
16
17 Writing pt1000-i-mz.122-28.bin ...!!!!!!!!!!!!!!!!!!!!!!!!!!!!
18 [OK - 5571584 bytes]
19
20 5571584 bytes copied in 0.147 secs (8684467 bytes/sec)
```

Рисунок 11 - загрузка файла по TFTP



1. Командой `enable` был совершен переход в привилегированный режим (можно заметить по символу решетки);
2. Командой `show flash` было выведено содержимое флеш-памяти (в данном случае это необходимо для тестовой загрузки по TFTP);
3. Командой `copy flash tftp` сообщаем о начале загрузке файла по TFTP, где далее указывается файл(ы), TFTP-сервер для загрузки, а также новое имя файла(ов).

На TFTP-сервере, в настройках TFTP появится выбранный ранее файл с указанным именем.

## **Вывод**

В ходе выполнения данной курсовой работы был получен опыт по работе в Cisco Packet Tracer.

Построение и настройка были выполнены с помощью встроенных инструментов, которые в общем виде имитируют реальное оборудование. В каждой подсети были разные варианты проектирование, для разнообразия задач. Вариативность задач помогла закрепить все основные навыки, полученные при изучении Cisco Packet Tracer.

Решения, созданные Cisco Packet Tracer, более легковесны как в настройке, так и в проектировании.

Отличительной особенностью является то, что за любым пакетом можно наблюдать по шагам, что может помочь в определении ситуации из-за чего сеть может работать некорректно.

К недостаткам Cisco Packet Tracer можно отнести лишь то, что все действия ограничены, то есть установить на устройство какое-либо ПО или сервис, которого нет в Cisco Packet Tracer, не предоставляется возможным. Также отсутствует возможность работать с конкретными операционными системами.