

Министерство науки и высшего образования Российской Федерации
Муромский институт (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(МИ ВлГУ)**

ОСНОВЫ АДМИНИСТРИРОВАНИЯ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ В CISCO PACKET TRACER

Практикум

Текстовое электронное издание

Учебно-методический центр МИ ВлГУ
Муром 2021

© Астафьев А.В.
составление, 2021

© МИ ВлГУ, 2021

УДК 004.77
ББК 32.972.5

Составитель:

Астафьев А.В., к.т.н., доцент.

Ответственный за выпуск:

заведующий кафедрой физики и прикладной математики,
доктор технических наук Орлов Алексей Александрович

Основы администрирования вычислительных сетей в Cisco Packet Tracer: Практикум для студентов / сост. Астафьев А.В. [Электронный ресурс]. – Электрон. текстовые дан. (). - Муром.: МИ ВлГУ, 2021. - 1 электрон. опт. диск (CD-R). – Систем. требования: процессор x86 с тактовой частотой 500 МГц и выше; 512 Мб ОЗУ; Windows XP/7/8/10; видеокарта SVGA 1280x1024 High Color (32 bit); привод CD-ROM. - Загл. с экрана.

Практикум содержит сведения, необходимые для выполнения практических работ по дисциплине «Сети электронных вычислительных машин» Тематика работ направлена на приобретение студентами знаний и навыков, необходимых для освоения общепрофессиональных и специальных дисциплин.

Текстовое электронное издание

Минимальные системные требования:

Компьютер: процессор x86 с тактовой частотой 500 МГц и выше; ОЗУ 512 Мб;
10 Мб на жестком диске; видеокарта SVGA 1280x1024 High Color (32 bit);
привод CD-ROM.

Операционная система: Windows XP/7/8/10.

Программное обеспечение: Adobe Acrobat Reader версии 6 и старше.

© Астафьев А.В., составление, 2021
© МИ ВлГУ, 2021

Оглавление

Практическая работа №1 «Установка Cisco Packet Tracer. Простейшая сеть. Коммутаторы»	4
Практическая работа №2 «Основы Cisco IOS»	12
Практическая работа №3 «Технология Vlan»	21
Практическая работа №4 «Коммутаторы 3 уровня»	25
Практическая работа №5 «Коммутаторы 3 уровня. Часть 2»	31
Практическая работа №6 «Маршрутизаторы»	37
Практическая работа №7 «Маршрутизация»	43
Практическая работа №8 «Протокол DHCP»	48
Практическая работа №9 «Технология NAT»	59

Практическая работа №1 «Установка Cisco Packet Tracer. Простейшая сеть. Коммутаторы»

Цель работы: приобрести навыки построения простейших сетей и использования коммутаторов с использованием пакета Cisco Packet Tracer.

Теоретическая часть

Packet Tracer — симулятор сети передачи данных, выпускаемый фирмой Cisco Systems. Позволяет делать работоспособные модели сети, настраивать (командами Cisco IOS) маршрутизаторы и коммутаторы [1].

Интерфейс программы Cisco Packet Tracer

При открытии программы Cisco Packet Tracer запускается главное окно, интерфейс которого представлен на рисунке 1.

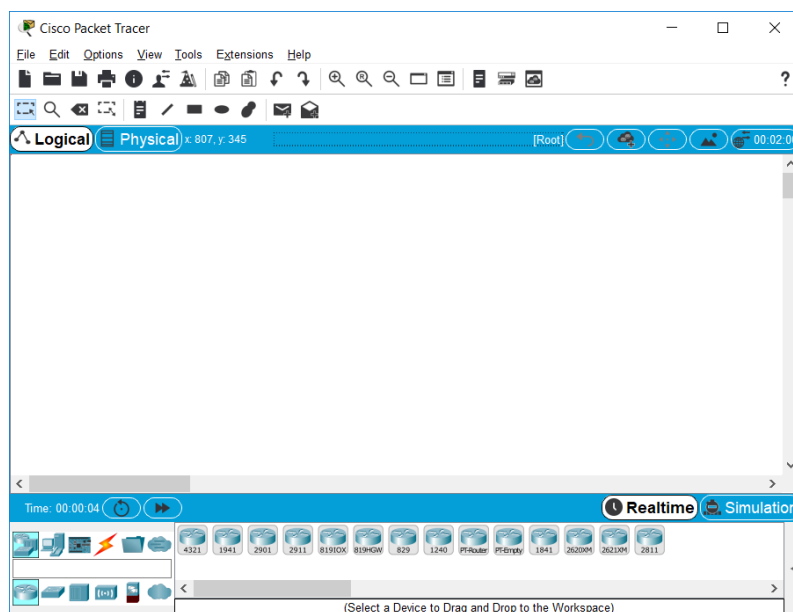


Рисунок 1 - Интерфейс программы Cisco Packet Tracer

В верхней части главного окна программы Cisco Packet Tracer располагается стандартный функционал для создания, сохранения и редактирования файлов, печати, масштабирования и т.д. Его внешний вид представлены на рисунке 2.



Рисунок 2 - Главное меню программы Cisco Packet Tracer



Сетевые устройства	Оконечные устройства	Компоненты	Соединения	Смешанное	Многопользовательские
--------------------	----------------------	------------	------------	-----------	-----------------------



Под простейшей сетью будем понимать сеть, связывающую 2 компьютера между собой. Для построения такой сети в Cisco Packet Tracer потребуется:

- На первом этапе необходимо разместить 2 компьютера (рис. 5).



На следующем этапе необходимо соединить компьютеры с помощью патч-корда (рис. 6). Для соединения устройств одного уровня модели OSI необходимо использовать перекрестный кабель (cross-over). Для соединения устройств разных уровней модели OSI (например, компьютер – коммутатор) необходимо использовать прямой кабель (straight-through).

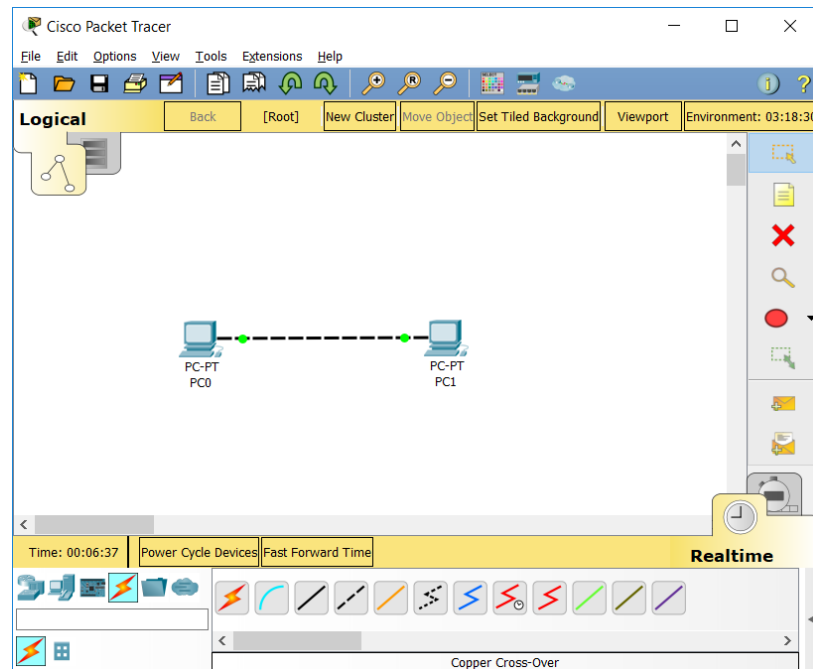


Рисунок 6 – соединение компьютеров

Для обеспечения работоспособности сети необходимо произвести настройку сетевых параметров устройств. Для этого необходимо открыть пункт «IP Configuration» и указать соответствующие адреса. Например, 192.168.1.1 для PC0 и 192.168.1.2 для PC1 (рис. 7).

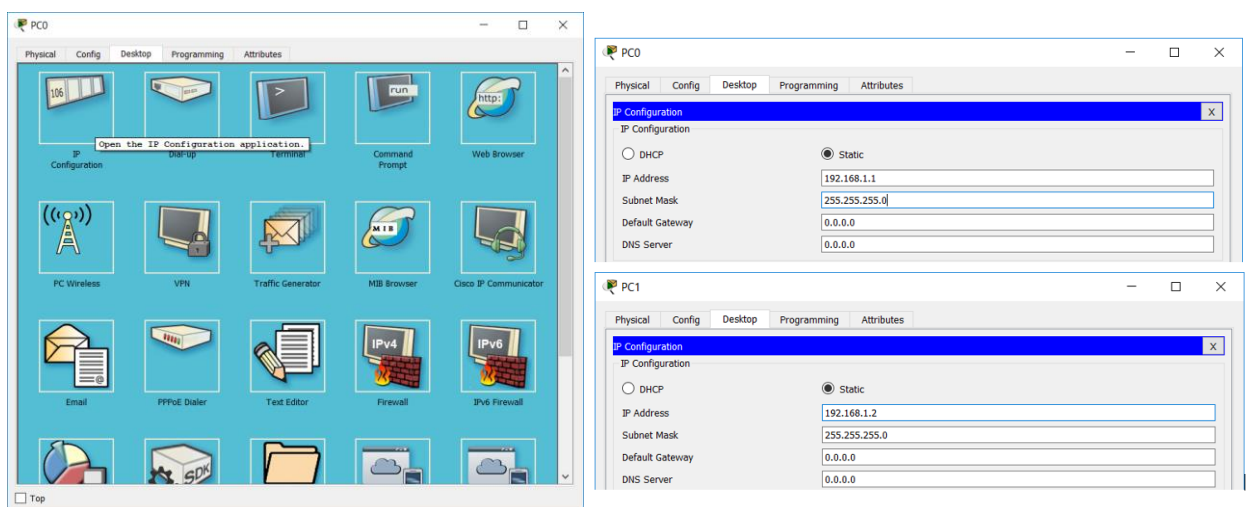


Рисунок 7 – настройка адресов компьютеров

Для проверки работоспособности сети можно воспользоваться утилитой ping. Для это открыть пункт «Command Prompt». Если отклик получен, то связь есть (рис. 8).

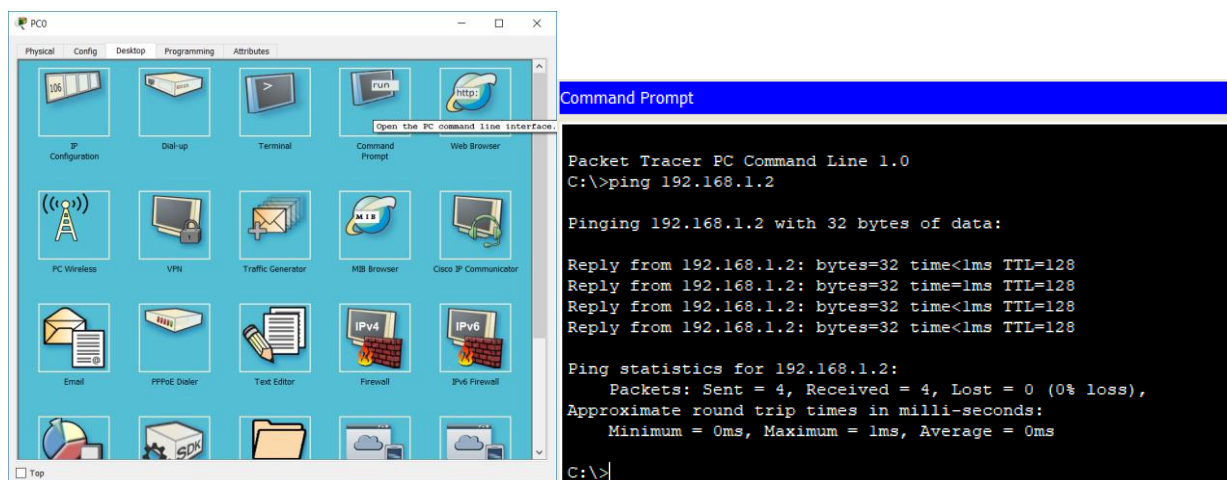


Рисунок 8 – проверка работоспособности сети утилитой ping

Сетевой концентратор (также хаб от англ. hub — центр) — устройство для объединения компьютеров в сеть Ethernet с применением кабельной инфраструктуры типа витая пара. В настоящее время вытеснены сетевыми коммутаторами [2].

Сетевой коммутатор (жарг. свитч, свич от англ. switch — переключатель) — устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети. Коммутатор работает на канальном (втором) уровне модели OSI. Коммутаторы были разработаны с использованием мостовых технологий и часто рассматриваются как многопортовые мосты. Для соединения нескольких сетей на основе сетевого уровня служат маршрутизаторы (3 уровень OSI) [3].

В отличие от концентратора (1 уровень OSI), который распространяет трафик от одного подключённого устройства ко всем остальным, коммутатор передаёт данные только непосредственно получателю (исключение составляет широковещательный трафик всем узлам сети и трафик для устройств, для которых неизвестен исходящий порт коммутатора). Это повышает производительность и безопасность сети, избавляя остальные

сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались [3].

Организация сети с использованием концентратора

В Cisco Packet Tracer сетевым коммутатором является устройство Hub-PT (раздел «Hubs» - «Generic»). Для примера добавим в схему коммутатор, 4 компьютера и соединим их прямым кабелем по портам типа Fast Ethernet. Адреса компьютеров установим как 192.168.1.1, 192.168.1.2, 192.168.1.3, 192.168.1.4 соответственно (рис. 9).

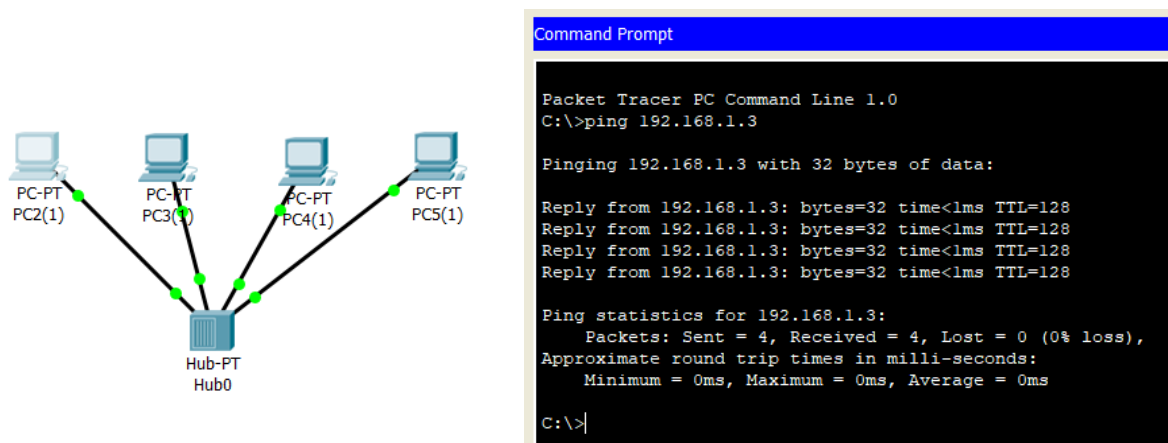


Рисунок 9 – построение сети с использованием хаба

Для визуализации работы воспользуемся возможностью симуляции. Для этого необходимо перейти в закладку «Simulation» и нажать кнопку «Auto capture / Play».

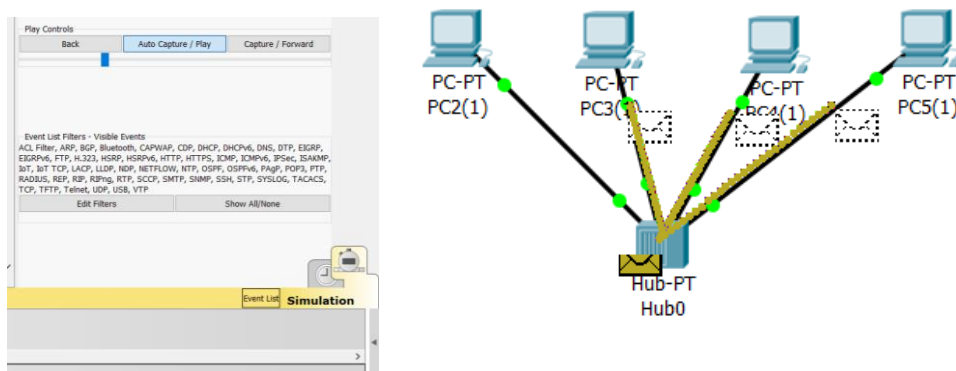


Рисунок 10 – симуляция работы сети

Чтобы смоделировать передачу пакета необходимо нажать кнопку «Simple PDU» и сказать передатчик и приемник. После этого запустить процесс симуляции (рис.11).

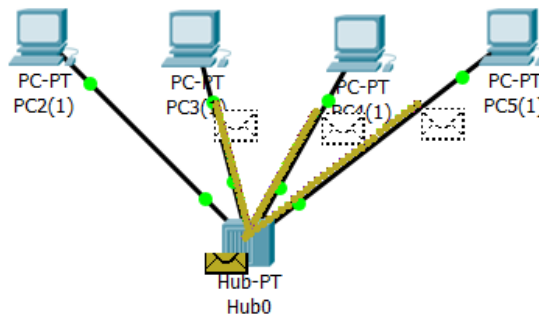
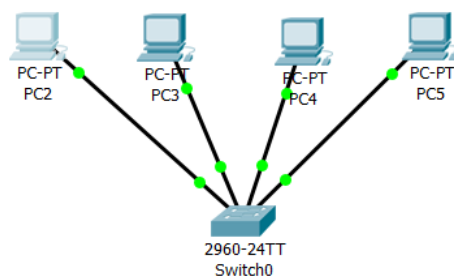


Рисунок 11 – симуляция передачи пакета

В Cisco Packet Tracer сетевым концентратором является устройство 2960. Для примера добавим в схему концентратор 2960, 4 компьютера и соединим их прямым кабелем по портам типа Fast Ethernet. Адреса компьютеров установим как 192.168.2.1, 192.168.2.2, 192.168.2.3, 192.168.2.4 соответственно (рис. 12).



```

Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

Reply from 192.168.2.4: bytes=32 time<1ms TTL=128
Reply from 192.168.2.4: bytes=32 time<1ms TTL=128
Reply from 192.168.2.4: bytes=32 time<1ms TTL=128
Reply from 192.168.2.4: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>|

```

Рисунок 12 – построение сети с использованием коммутатора

Чтобы смоделировать передачу пакета необходимо нажать кнопку «Simple PDU» и сказать передатчик и приемник. После этого запустить процесс симуляции (рис.13).

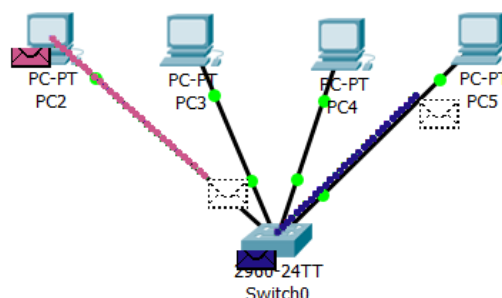


Рисунок 13 - симуляция передачи пакета

Из проведенных экспериментов видно, что при использовании концентратора пакет от отправителя приходит на все остальные устройства, а в случае с коммутатором – только на нужный.

Практическая часть

1. Ознакомиться с теоретической частью.
2. Реализовать 2 простейшие сети с адресами компьютеров согласно варианту, из таблицы 1.
3. Проверить работоспособность сетей.
4. Реализовать 2 сети, используя концентратор и коммутатор с адресами компьютеров согласно варианту из таблицы 2.
5. Проверить работоспособность сетей.
6. Смоделировать процесс передачи пакета.
7. Результаты работы представить в виде отчета.

Таблица 1 – адреса компьютеров

Вариант	PC0	PC1	PC2	PC3
1	172.22.1.1	172.22.1.2	192.168.100.1	192.168.100.2
2	172.22.2.1	172.22.2.2	192.168.110.1	192.168.110.2
3	172.22.3.1	172.22.3.2	192.168.120.1	192.168.120.2
4	172.22.4.1	172.22.4.2	192.168.130.1	192.168.130.2
5	172.22.5.1	172.22.5.2	192.168.140.1	192.168.140.2
6	172.22.6.1	172.22.6.2	192.168.150.1	192.168.150.2
7	172.22.7.1	172.22.7.2	192.168.160.1	192.168.160.2
8	172.22.8.1	172.22.8.2	192.168.170.1	192.168.170.2
9	172.22.9.1	172.22.9.2	192.168.180.1	192.168.180.2
10	172.22.10.1	172.22.10.2	192.168.190.1	192.168.190.2

Таблица 2 – адреса компьютеров

Вариант	Количество компьютеров в сети	Маршрут передачи	Адрес подсети
1	4	1-3	192.168.1.0
2	5	2-5	192.168.2.0
3	6	3-6	192.168.3.0
4	4	4-1	192.168.4.0
5	5	5-3	192.168.5.0
6	6	6-2	192.168.6.0
7	4	3-2	192.168.7.0
8	6	5-2	192.168.8.0
9	5	3-5	192.168.9.0
10	5	4-5	192.168.10.0

Практическая работа №2 «Основы Cisco IOS»

Цель работы: приобрести навыки работы в операционной системе Cisco IOS с использованием пакета Cisco Packet Tracer.

Теоретическая часть

Cisco IOS (от англ. Internetwork Operating System — Межсетевая Операционная Система) — программное обеспечение, используемое в маршрутизаторах и сетевых коммутаторах Cisco. Cisco IOS является многозадачной операционной системой, выполняющей функции сетевой организации, маршрутизации, коммутации и передачи данных [4].

В Cisco IOS есть специфичный интерфейс командной строки (command line interface, CLI), который был скопирован многими другими сетевыми продуктами. Интерфейс IOS предлагает набор многословных команд, согласно выбранному режиму и уровню привилегий пользователя. Global configuration mode предоставляет возможность для изменения настроек системы и сетевых интерфейсов [4].

Подключение к консоли

Возможные способы подключения:

1. Консольный кабель.
2. Протокол Telnet/SSH.
3. Web-интерфейс.
4. Специализированное программное обеспечение (IME, CSM, SDM).

В Cisco Packet Tracer реализован механизм подключения к оборудованию по консольному кабелю. Для этого необходимо добавить в сеть компьютер, коммутатор и соединить их консольным кабелем (Console), выбрав на компьютере порт RS232, а на коммутаторе – Console (рис. 1).



Рисунок 1 – соединение компьютера и коммутатора консольным кабелем

Далее, для подключения к консоли коммутатора, на компьютере необходимо зайти в пункт «Terminal», согласиться с настройками по умолчанию и нажать «ОК». После этого откроется консоль коммутатора (рис. 2).

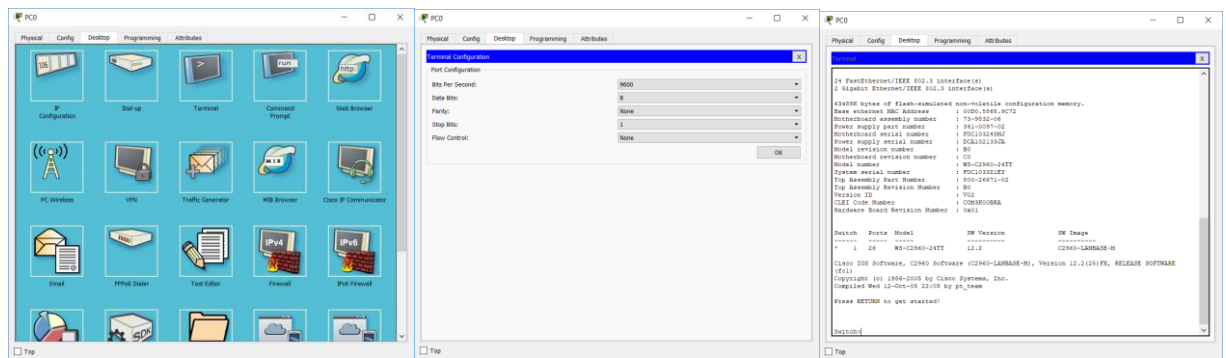


Рисунок 2 – подключение к консоли коммутатора

Помощь по командам консоли IOS можно получить введя команду ? (рис. 3).

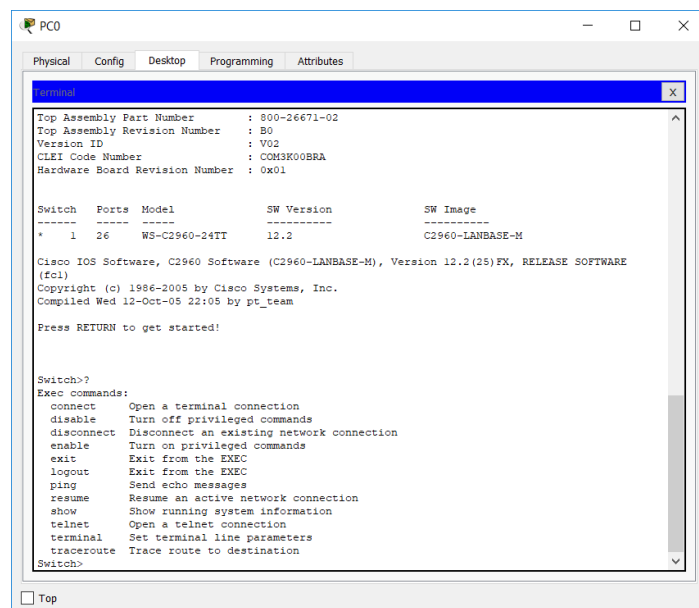


Рисунок 3 – описание команд IOS

Задание пароля для входа в привилегированный режим

Работа в IOS разделяется на несколько режимов. Для входа в привилегированный режим используется команда:

enable

После чего строка ввода будет начинаться не с Switch>, а с Switch# (рис. 4).



Рисунок 4 – вход в привилегированный режим

Использование режимов работы организовано для обеспечения безопасности. Если заново запросить описание команд, то можно увидеть, что их стало больше (рис. 5).

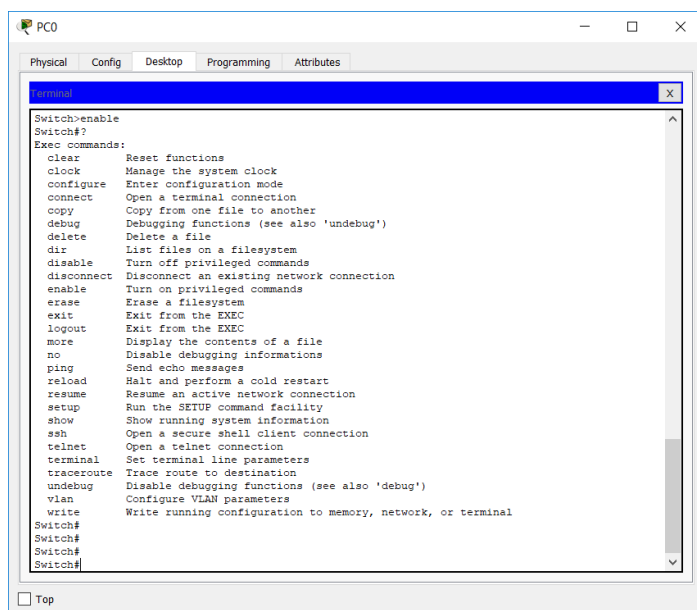


Рисунок 5 – список команд привилегированного режима

Для выхода из привилегированного режима используется команда:

disable

После чего строка ввода будет опять начинаться с Switch>, а не с Switch#.

В привилегированном режиме можно посмотреть текущую конфигурацию устройства. Для этого необходимо выполнить команду:

show running-config

или

show run

Результат представлен на рисунке 6.

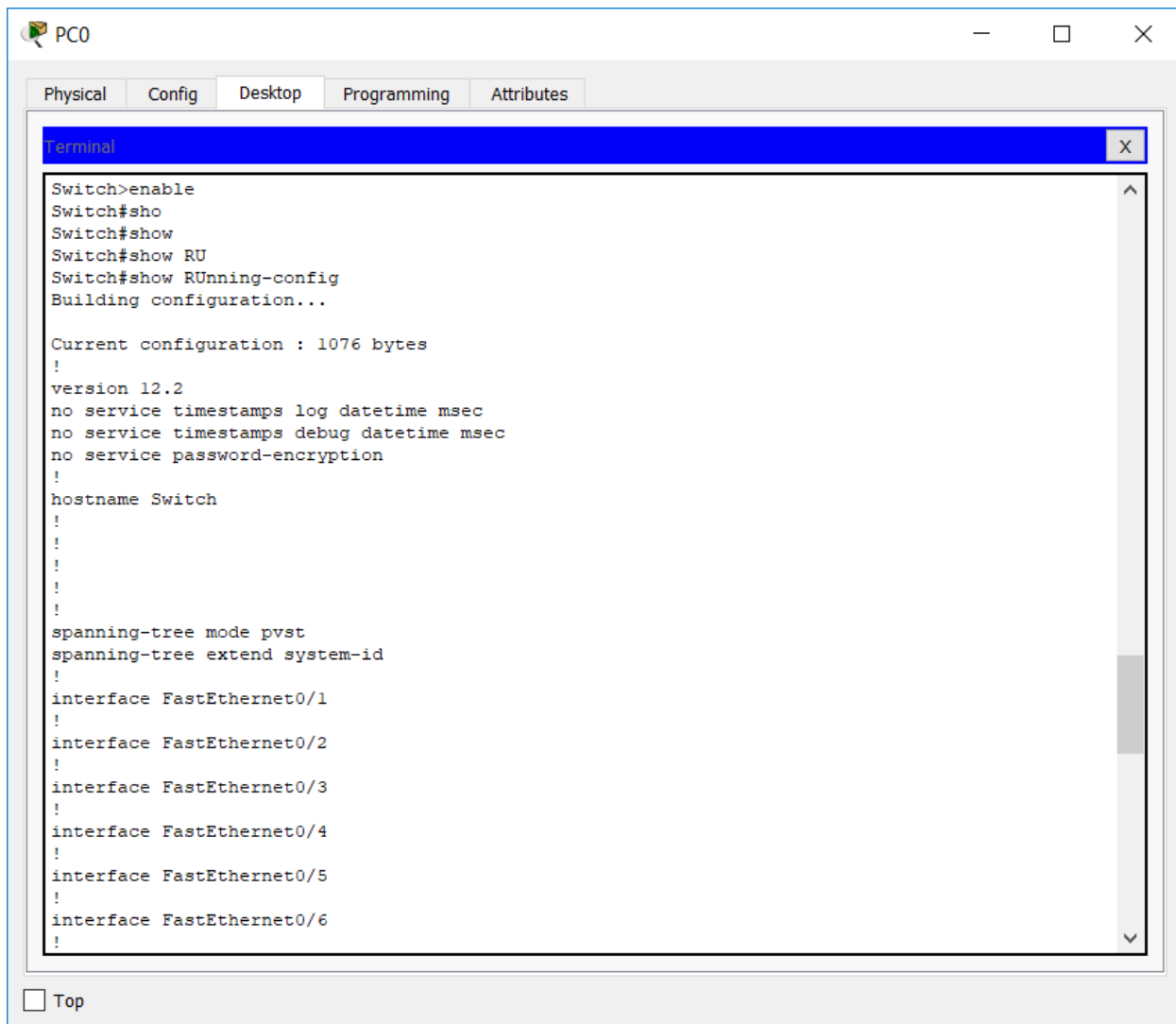


Рисунок 6 – просмотр текущей конфигурации

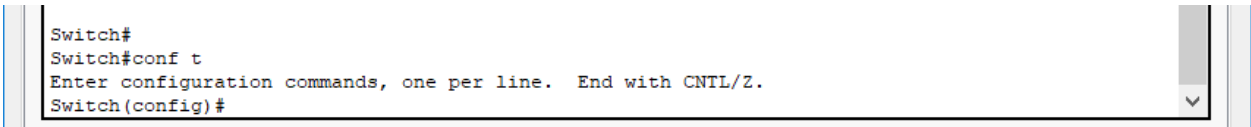
Помимо привилегированного режима в IOS существует режим глобального конфигурирования. Для входа в этот режим необходимо выполнить команду:

configure terminal

или ее сокращенную версию

conf t

После входа в режим глобального конфигурирования начала строки Switch# поменяется на Switch(Config)# (рис. 7).



```
Switch#
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

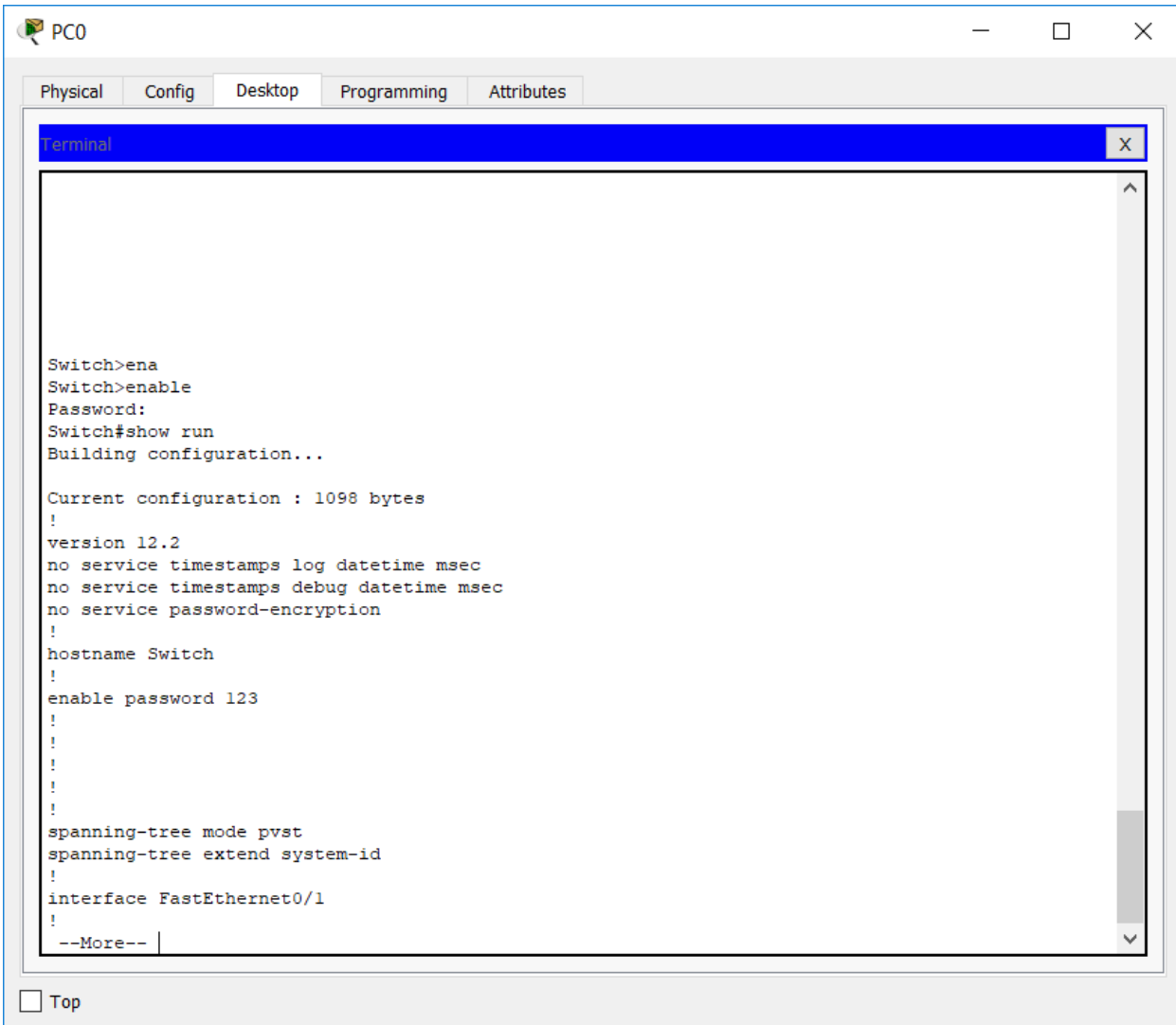
Рисунок 7 – вход в режим глобального конфигурирования

Чтобы установить пароль для входа в привилегированный режим нужно выполнить следующую команду:

enable password [new_password]

где new_password – это новый пароль.

Однако, использование этой команды организует хранение пароля в открытом виде и при просмотре конфигурации его можно увидеть (рис. 8).



```
PC0
Physical Config Desktop Programming Attributes
Terminal
Switch>ena
Switch>enable
Password:
Switch#show run
Building configuration...

Current configuration : 1098 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
enable password 123
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
--More--
```

Рисунок 8 – открытое хранение пароля

Для шифрования пароля необходимо воспользоваться следующей конструкцией:

```
conf t
service password-encryption
```

После этого пароль будет храниться в зашифрованном виде (рис. 9).

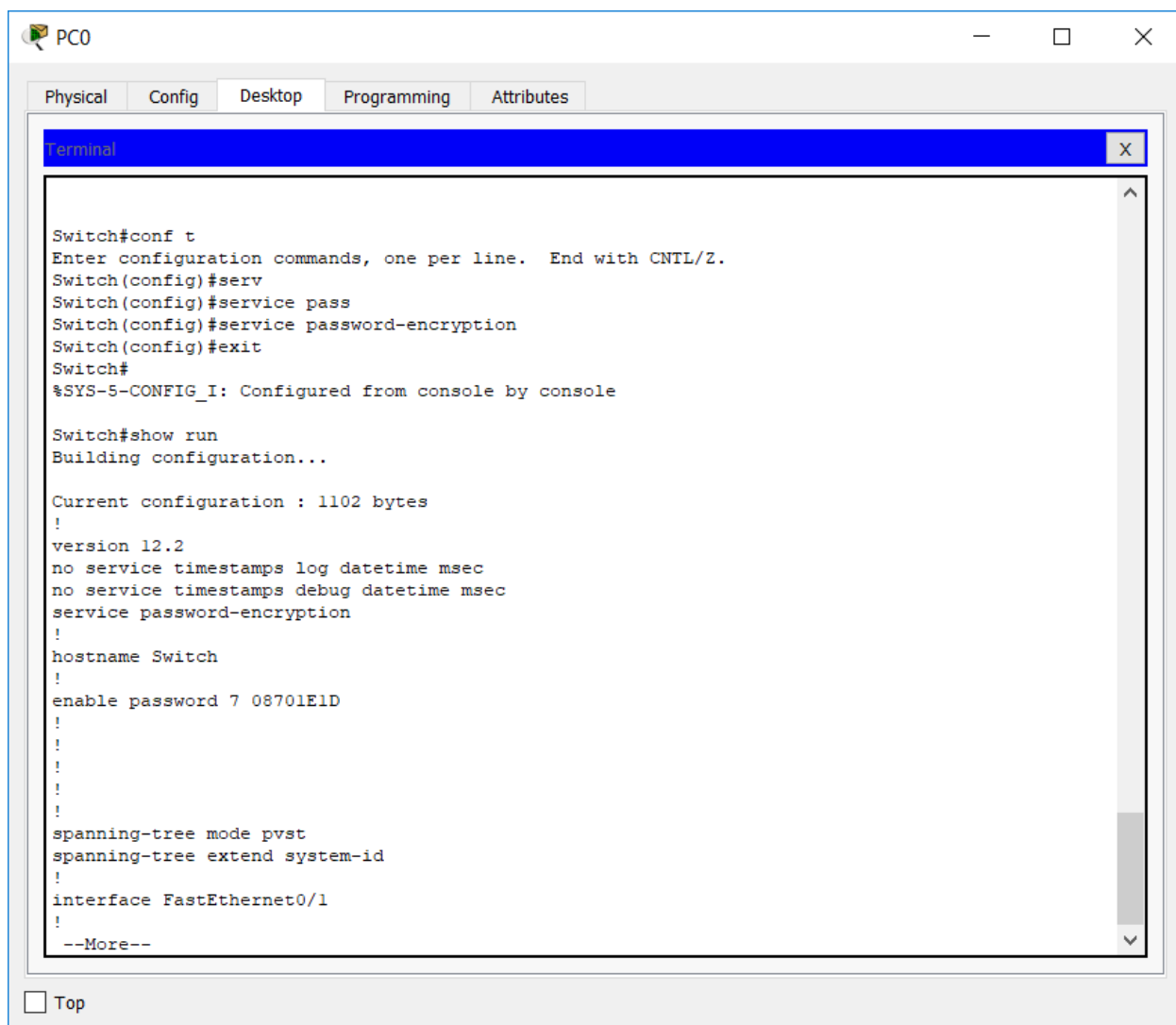


Рисунок 9 – хранение пароля в зашифрованном виде

Еще одним способом задания пароля является команда:

```
enable secret[new_password]
```

где new_password – это новый пароль.

При использовании данной команды пароль изначально будет храниться в зашифрованном виде и иметь более высокий приоритет (рис. 10).

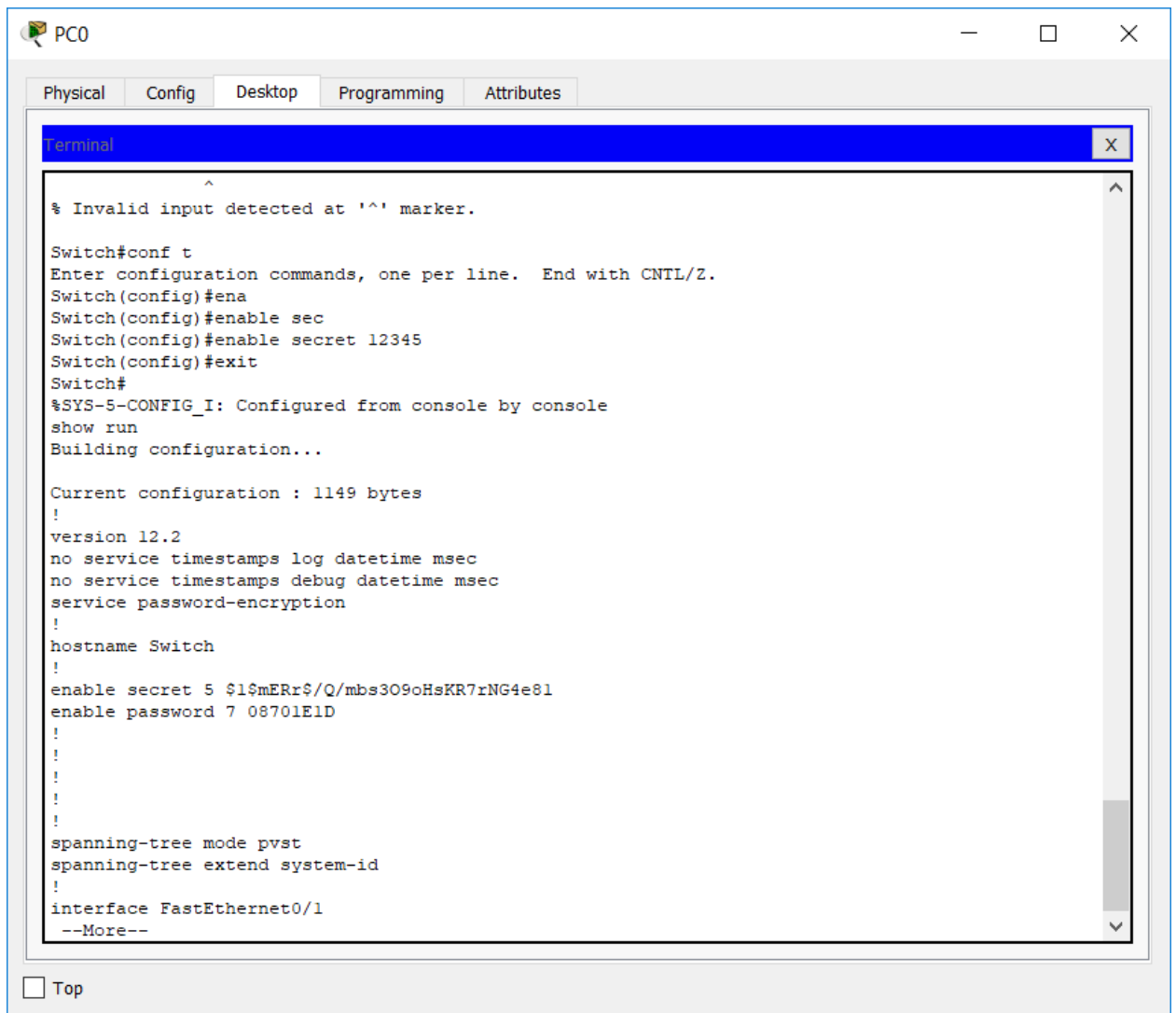


Рисунок 10 – хранение пароля в зашифрованном виде

Создание пользователя

Для создания пользователя используется следующая команда:

```
username [user_name] [privilege [1-15] secret[new_password]
password[new_password]]
```

где [user_name] – имя пользователя, privilege [1-15] – уровень привилегий, где 15 максимальный уровень, [new_password] – новый пароль.

Далее необходимо установить авторизацию при подключении к консоли. для этого необходимо зайти в режим терминальных линий:

```
line console 0
```

```
login local
```

Задание IP-адреса устройства

Задание IP адреса происходит с использованием четвертого режима работы операционной системы IOS – режим интерфейса. По умолчанию на устройствах Cisco существует интерфейс Vlan 1 (рис. 11).



Рисунок 11 – интерфейс Vlan1

Для задания IP адреса необходимо перейти в режим интерфейса с помощью команд:

```
conf t
interface Vlan 1
ip address [new_IP] [new_mask]
no shutdown
```

Настройка протокола telnet для доступа к консоли производится с использованием следующих команд:

```
conf t
line vty 0 4
transport input telnet
login local
```

Для сохранения конфигурации используется команда

```
wr mem
```

Для проверки работоспособности протокола telnet необходимо подключиться к устройству **с использованием обычного сетевого провода с персонального компьютера** и воспользоваться командой

```
telnet [IP_address]
```

Практическая часть

1. Ознакомиться с теоретической частью.
2. Построить сеть из компьютера и сетевого устройства. Произвести подключение по консольному кабелю.

3. Задать пароль на вход в привилегированный режим.
4. Создать пользователя для входа в консоль Логин указать как группа + фамилия студента.
5. Установить IP адрес устройства согласно шаблону:
192.168.[номер_по_журналу].[255%номер_по_журналу+1].
6. Активировать работу протокола telnet и проверить возможность подключения.
7. Результаты работы представить в виде отчета.

Практическая работа №3 «Технология Vlan»

Цель работы: приобрести навыки разделения сети на части с использованием пакета Cisco Packet Tracer.

Теоретическая часть

VLAN (аббр. от англ. Virtual Local Area Network) — топологическая («виртуальная») локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным членам группироваться вместе, даже если они не находятся в одной физической сети. Такая реорганизация может быть сделана на основе программного обеспечения вместо физического перемещения устройств [5].

Рассмотрим пример создания двух vlan в сети из 4 компьютеров (рис. 1).

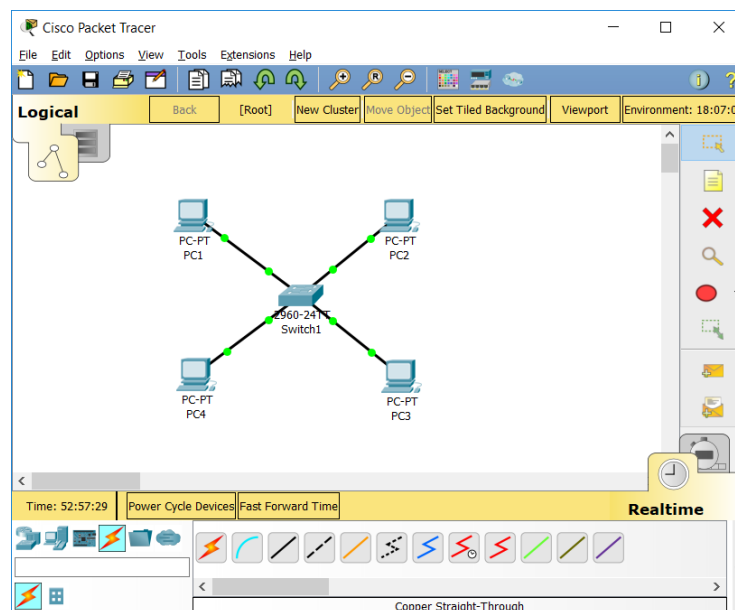


Рисунок 1 – сеть из 4 компьютеров

Предположим, что компьютеры PC1 и PC4 относятся к одной сети (например, отдел договоров), а компьютеры PC2 и PC3 – к другой (например, отдел кадров). Тогда разделение сетей можно представить в виде рисунка 2.

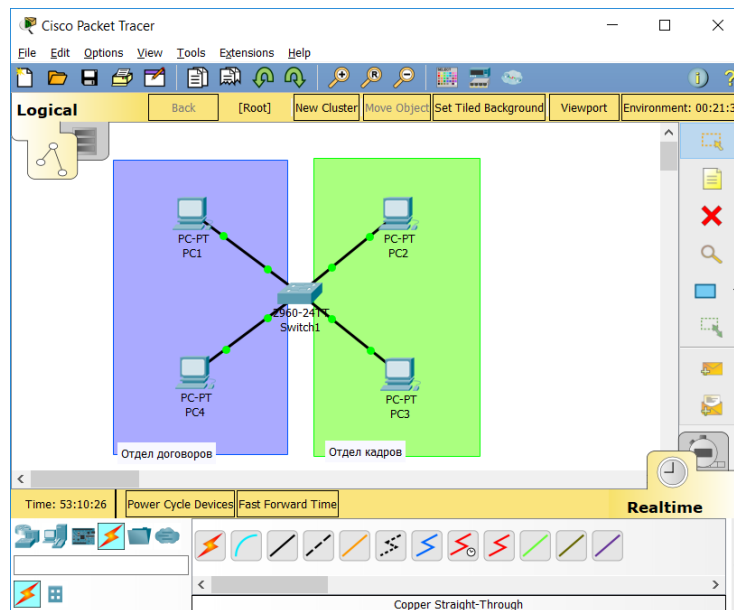


Рисунок 2 – разделение компьютеров по подсетям

Для разделения компьютеров сначала необходимо определить vlan'ы. Для этого в консоли коммутатора необходимо прописать следующие команды:

```
enable  
conf t  
vlan [номер_vlan'a]  
name [имя_vlan'a]
```

После создания vlan'ов необходимо определить какие интерфейсы будут к ним относиться. Для этого необходимо выполнить следующие команды:

```
interface fastEthernet 0/[номер_порта]  
switchport mode access  
switchport access vlan [номер_vlan'a]
```

Проверить правильность настройки можно введя в привилегированном режиме команду:

```
show vlan
```

В результате ее выполнения система покажет настройки vlan'ов (рис. 3).

VLAN Name	Status	Ports
1 default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/11, Fa0/12, Fa0/15, Fa0/16, Fa0/19, Fa0/20, Fa0/23, Fa0/24
2 otddog	active	Gig0/1, Gig0/2
3 otdkad	active	Fa0/1, Fa0/4
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddiuser-default	act/unsup	
1005 trnet-default	act/unsup	

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode
1 enet	100001	1500	-	-	-	-	-
2 enet	100002	1500	-	-	-	-	-
3 enet	100003	1500	-	-	-	-	-
1002 fddi	101002	1500	-	-	-	-	-

Рисунок 3 – отображение настройки vlan'ов

Для завершения настройки необходимо задать IP адреса компьютерам. Рекомендуется адресацию vlan'ов производить различными сегментами, так, чтобы номер сегмента совпадал с номером vlan'a. Например, для vlan 2 ip-адреса 192.168.2.1 и 192.168.2.2, для vlan'a 3 ip-адреса 192.168.3.1 и 192.168.3.2.

Допустим, что произошло объединение компаний и соответствующие отделы объединились, оставаясь физически удаленными друг от друга. Тогда структура сети может выглядеть так, как показано на рисунке 4.

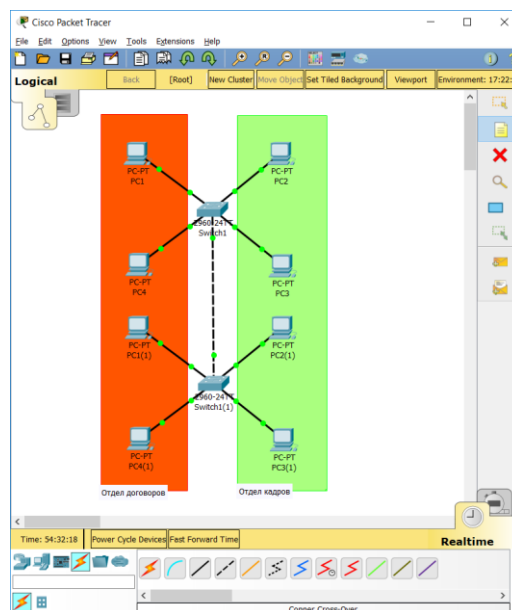


Рисунок 4 – структура сети после объединения

Настройка портов второго маршрутизатора производится аналогично. Далее нужно настроить связь между коммутаторами с использованием технологии trunk-портов. Для этого нужно произвести настройка интерфейсов подключения коммутаторов с помощью следующих команд:

```
enable
conf t
interface [интерфейс_подключения]
switchport mode trunk
switchport trunk allowed vlan [номера_vlan'ов]
```

Настройка производится на всех коммутаторах.

Практическая часть

1. Ознакомиться с теоретической частью.
2. Спроектировать 2 сети в соответствии с вариантом из таблицы 1.
3. Сети по vlan'ам в соответствии с заданием.
4. Произвести проверку работоспособности vlan'ов. Результат подтвердить скриншотами.
5. Результаты работы представить в виде отчета.

Таблица 1 – варианты заданий

№	Сеть с одним коммутатором			Сеть с двумя коммутаторами		
	Количество vlan'ов	Количество компьютеров	Ip- адреса	Количество vlan'ов	Количество компьютеров	Ip- адреса
1	3	8	172.22.vlan.0	4	12	168.77.vlan.0
2	4	6		3	14	
3	3	8		4	12	
4	4	6		3	14	
5	3	8		4	12	
6	4	6		3	14	
7	3	8		4	12	
8	4	6		3	14	
9	3	8		4	12	
10	4	6		3	14	

Практическая работа №4 «Коммутаторы 3 уровня»

Цель работы: приобрести навыки работы с коммутаторами третьего уровня с использованием пакета Cisco Packet Tracer.

Теоретическая часть

Коммутаторы третьего уровня.

Обычный коммутатор "прозрачен" для компьютеров сети, не имеет собственных MAC-адресов портов и захватывает все кадры, приходящие на порт, независимо от их адреса назначения, для последующей коммутации. Классический коммутатор 3-го уровня, подобно обычному коммутатору, захватывает все кадры своими портами независимо от их MAC-адресов, однако порты коммутатора 3-го уровня имеют и собственные MAC-адреса. Если захваченный кадр направлен на MAC-адрес какого-либо компьютера в сети, то пакет коммутируется. Если захваченный кадр направлен на MAC-адрес порта коммутатора, то пакет маршрутизируется. Коммутатор 3-го уровня может поддерживать динамические протоколы маршрутизации, такие как RIP или OSPF, а может полагаться на статическое задание маршрутов или на получение таблицы маршрутизации от другого маршрутизатора [8].

Практическая часть

Рассмотрим пример, когда компьютеры подключены к маршрутизатору третьего уровня (Cisco 3560) напрямую (рисунок 1). Необходимо разделить сеть на 3 сегмента.

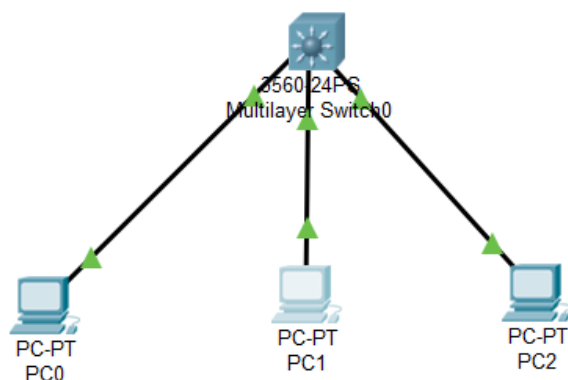


Рисунок 1 – пример сети

Внешний вид маршрутизатора Cisco 3560 представлен на рисунке 2.



Рисунок 2 – внешний вид маршрутизатора Cisco 3560

Для решения поставленной задачи необходимо сначала создать 3 vlan'а.

Для этого на маршрутизаторе необходимо ввести команды (рисунок 3):

```
en
conf t
vlan 2
name VLAN2
exit
vlan 3
name VLAN3
exit
vlan 4
name VLAN4
exit

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name VLAN2
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name VLAN3
Switch(config-vlan)#exit
Switch(config)#vlan 4
Switch(config-vlan)#name VLAN4
Switch(config-vlan)#exit
Switch(config)#
```

Рисунок 3 – создание трех vlan'ов

Далее необходимо определить порты, в которые подключаются определённые vlan'ы. Для этого на коммутаторе необходимо ввести следующие команды (рисунок 4):

```
en
conf t
interface fa0/1
switchport mode access
switchport access vlan 2
exit
interface fa0/2
```

```
switchport mode access
switchport access vlan 3
exit
```

```
interface fa0/3
switchport mode access
switchport access vlan 4
exit
```

```
Switch(config)#
Switch(config)#int fa0/1
Switch(config-if)#swit
Switch(config-if)#switchport made ac
Switch(config-if)#switchport mode ac
Switch(config-if)#switchport mode access
Switch(config-if)#swi
Switch(config-if)#switchport ac
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#int fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 4
Switch(config-if)#exit
Switch(config)#
```

Рисунок 4 – настройка портов

Чтобы проверить корректность настройки можно использовать в привилегированном режиме команду (рисунок 5):

```
show run
```

```
!
!
!
interface FastEthernet0/1
 switchport access vlan 2
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/2
 switchport access vlan 3
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/3
 switchport access vlan 4
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
--More-- |
```

Рисунок 5 – проверка настроек портов

Далее необходимо назначит IP-адреса для созданных сегментов. Для этого на маршрутизаторе необходимо выполнить следующие команды:

```
en
conf t
int vlan 2
ip address 192.168.2.1 255.255.255.0
exit
int vlan 3
ip address 192.168.3.1 255.255.255.0
exit
int vlan 4
ip address 192.168.4.1 255.255.255.0
exit
```

Чтобы проверить корректность настройки можно использовать в привилегированном режиме команду (рисунок 6):

```
show run

!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
interface Vlan2
mac-address 0002.1644.4401
ip address 192.168.2.1 255.255.255.0
!
interface Vlan3
mac-address 0002.1644.4402
ip address 192.168.3.1 255.255.255.0
!
interface Vlan4
mac-address 0002.1644.4403
ip address 192.168.4.1 255.255.255.0
!
--More--
```

Рисунок 6 - проверка настроек IP адресов

Также необходимо назначить IP адреса машин в сети. Машине PC0 – 192.168.2.2, PC1 – 192.168.3.2, PC2 – 192.168.4.2. Корректность настройки можно проверить командой ping. В настоящее время компьютеры каждого сегмента должны иметь доступ к соответствующему IP адресу коммутатора (рисунок 7).

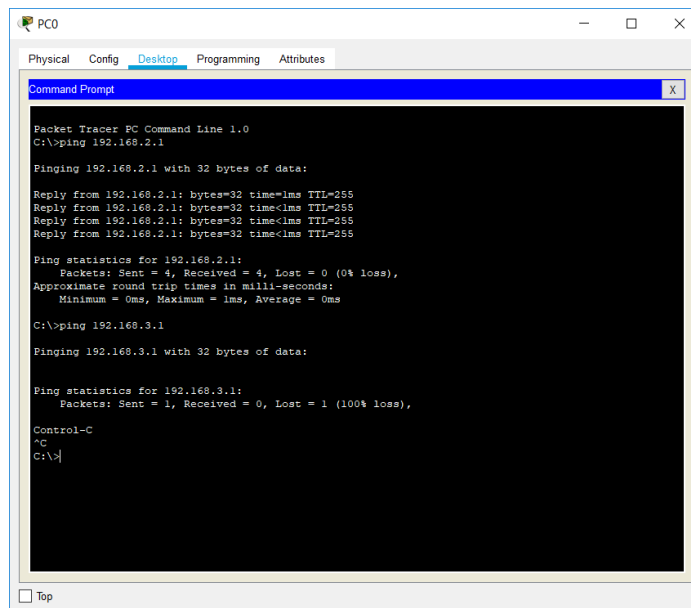


Рисунок 7 – проверка работы сети

Для того, чтобы организовать межсетевое взаимодействие необходимо указать на каждом компьютере IP адрес шлюза (поле «Default Gateway»). А также включить функцию маршрутизации на коммутаторе с помощью команд:

en
conf t
ip routing

После проведения настроек было организовано межсетевое взаимодействие между тремя сегментами (Рисунок 8).

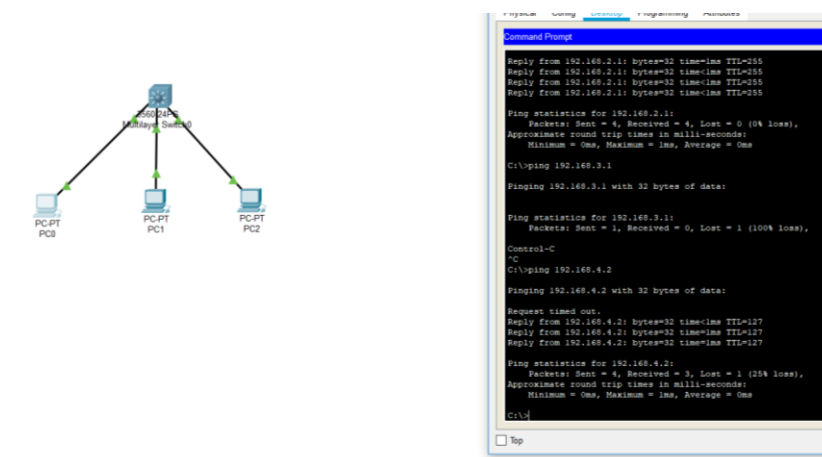


Рисунок 8 – проверка связи между сегментами (PC0 -> PC2)

Практическая часть

1. Ознакомиться с теоретической частью.

2. Построить сеть в соответствии с заданием из таблицы 1.
3. Организовать межсетевое взаимодействие.
4. Проверить связь между сегментами. Результаты подтвердить скриншотами.
5. Результаты работы представить в виде отчета.

Таблица 1 – варианты заданий

№	Количество сегментов	Начальный адрес подсетей
1	2	10.10.0.0
2	3	20.20.0.0
3	4	30.30.0.0
4	2	40.40.0.0
5	3	50.50.0.0
6	4	60.60.0.0
7	2	70.70.0.0
8	3	80.80.0.0
9	4	90.90.0.0
10	2	100.100.0.0

Практическая работа №5 «Коммутаторы 3 уровня. Часть 2»

Цель работы: приобрести навыки работы с коммутаторами третьего уровня и уровня доступа с использованием пакета Cisco Packet Tracer.

Практическая часть

Зачастую бывает так, что к коммутатору 3 уровня (коммутатору уровня распределения) подключены коммутаторы уровня доступа (рисунок 1). Например, коммутатор Switch0 обслуживает один этаж здания, а коммутатор Switch1 – другой. Предположим, что Switch0, PC0, PC1, PC2 – это отдел продаж 1 этажа, а Switch1, PC3, PC4, PC5 – отдел продаж 2 этажа.

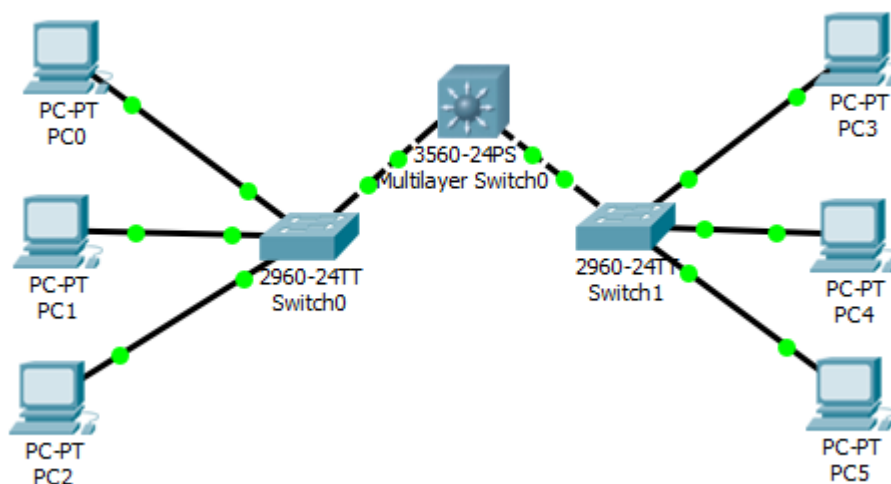


Рисунок 1 – пример локальной сети

Допустим PC0 и PC 3 – руководство отделов продаж и их необходимо вынести с отдельную подсеть, а остальные компьютеры должны иметь связь между собой. Таким образом необходимо организовать 2 VLANa, как показано на рисунке 2.

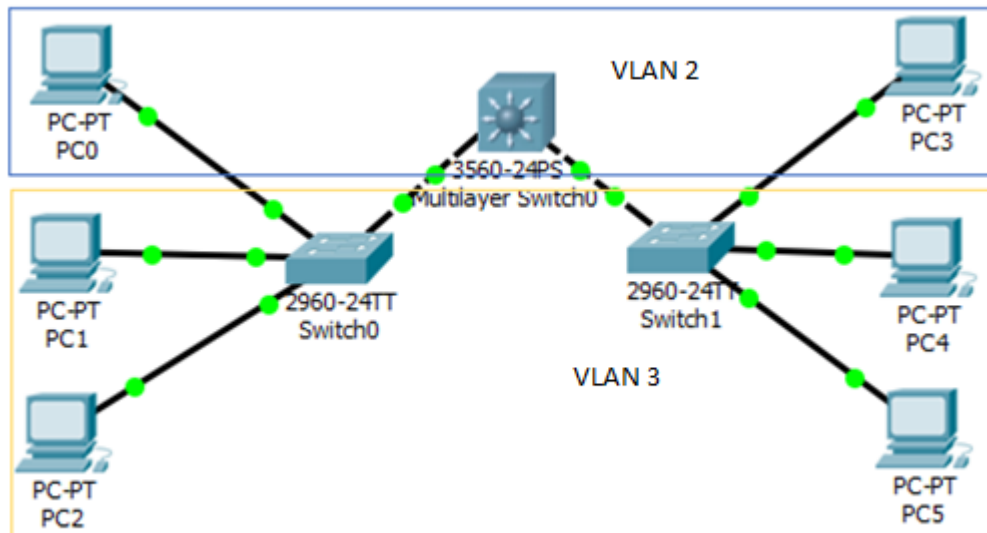


Рисунок 2 – пример сети с разделением на сегменты

Для начала настроим коммутаторы Switch0 и Switch1. Для того, чтобы определить PC0 и PC3 во VLAN 2 необходимо выполнить следующие операции:

```
en
conf t
int fa0/[номер_интерфейса_к_которому_подключен_PC]
switchport mode access
switchport access vlan [номер_vlan]
```

В результате PC0 и PC3 должны оказаться во 2 VLAN по настройкам коммутаторов Switch0 и Switch1.

Для добавления компьютеров PC1 и PC2 во VLAN 3 можно использовать команду `int range`. Тогда настройка будет выглядеть следующим образом:

```
en
conf t
int range fa0/[диапазон]      (например int range fa0/2-3)
switchport mode access
switchport access vlan [номер_vlan]
```

Проверить настройки можно с использованием команды `show run` из привилегированного режима (Рисунок 3).


```

interface FastEthernet0/1
!
interface FastEthernet0/2
switchport access vlan 3
switchport mode access
!
interface FastEthernet0/3
switchport access vlan 3
switchport mode access
!
interface FastEthernet0/4
switchport access vlan 2
switchport mode access
!
interface FastEthernet0/5
!

```

Рисунок 3 – проверка настроек интерфейсов коммутатора Switch0

Произведем настройку IP-адресов абонентов как показано на рисунке 4. Заметим, что при текущей настройке сети доступ друг к другу имеют только компьютеры PC1 и PC2, а также PC5 и PC4, т.к. подключены к одному коммутатору уровня доступа и определены в один и тот же VLAN.

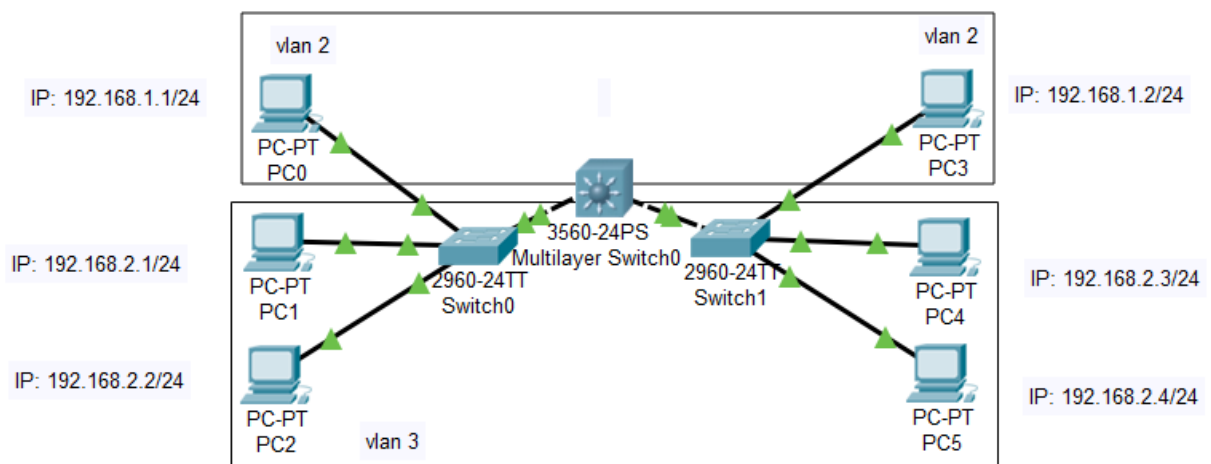


Рисунок 4 – настройка IP-адресов

Теперь необходимо настроить trunk-порты до коммутатора уровня распределения (MultiLayer Switch0).

Примечание: Для организации связи между коммутаторами уровня распределения и уровня доступа рекомендуется использовать порты типа *Gigabit Ethernet* для увеличения пропускной способности сети.

Для этого используем следующий набор команд:

```

en
conf t
int gi1/1
switchport mode trunk
switchport trunk allowed [номера_vlan]   (например: switchport trunk allowed 2,3)

```

Теперь переходим к настройке коммутатора уровня распределения (3 уровня). Сначала надо создать vlan'ы командами:

```
en
conf t
vlan [номер_vlan] (например: vlan 2)
```

Так как соединения от коммутаторов 2 уровня находятся в режиме trunk, то и соответствующие порты на коммутаторе 3 уровня установим в trunk с использованием следующих команд:

```
en
conf t
ip routing
int range gi0/[диапазон] (например: int range gi0/1-2)
switchport mode trunk
switchport trunk allowed vlan [диапазон] (например: switchport trunk allowed vlan 2,3)
switchport trunk encapsulation dot1q
exit
ip routing
```

После этого следует указать ip адреса vlan'ов с использованием следующих команд:

```
en
conf t
int vlan [номер_vlan] (например: int vlan 2)
ip address [ip-адрес] [маска] (например: ip address 192.168.1.99 255.255.255.0)
```

В итоге должна получиться локальная сеть, показанная на рисунке 5.

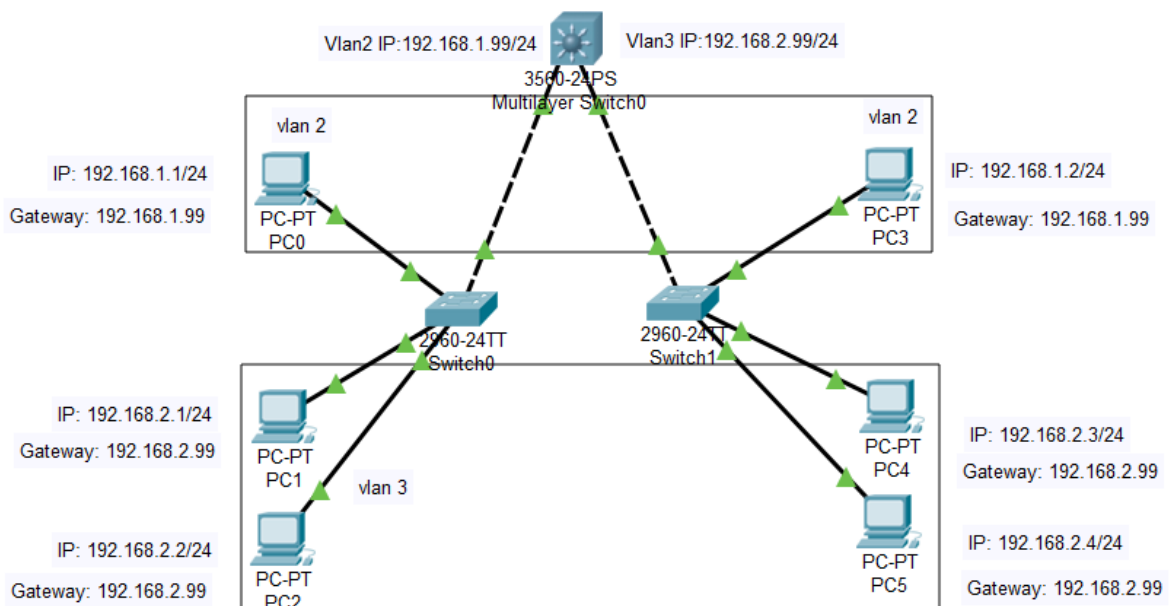
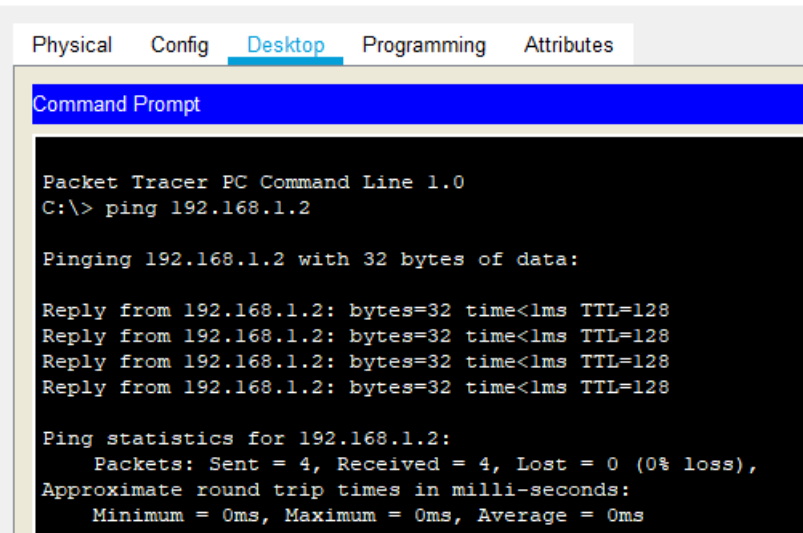


Рисунок 5 – локальная сеть с настройками

Проверим доступность компьютеров сети. Для этого проверим связь между PC0 и PC3 (рисунок 6), а также PC1 и PC5 (рисунок 7).

PC0



```
Physical  Config  Desktop  Programming  Attributes
Command Prompt

Packet Tracer PC Command Line 1.0
C:\> ping 192.168.1.2

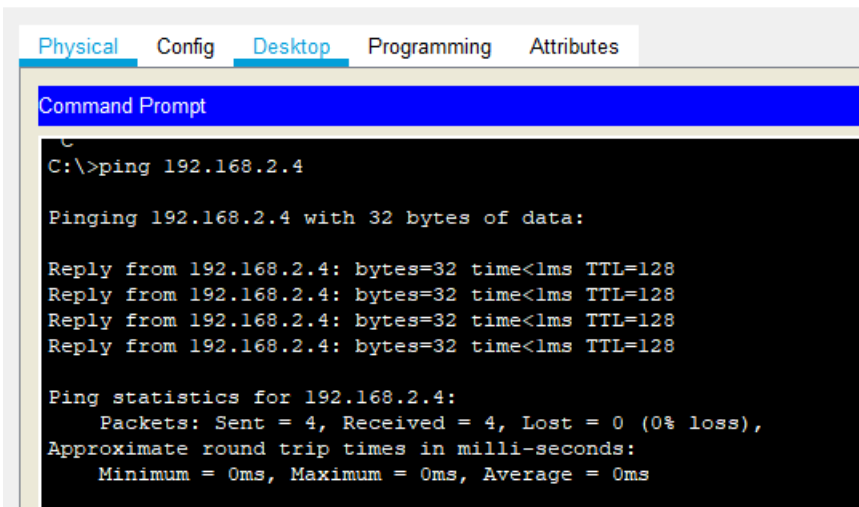
Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<lms TTL=128
Reply from 192.168.1.2: bytes=32 time<lms TTL=128
Reply from 192.168.1.2: bytes=32 time<lms TTL=128
Reply from 192.168.1.2: bytes=32 time<lms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 6 – проверка связи PC0 и PC3

PC1



```
Physical  Config  Desktop  Programming  Attributes
Command Prompt

C:\> ping 192.168.2.4

Pinging 192.168.2.4 with 32 bytes of data:

Reply from 192.168.2.4: bytes=32 time<lms TTL=128
Reply from 192.168.2.4: bytes=32 time<lms TTL=128
Reply from 192.168.2.4: bytes=32 time<lms TTL=128
Reply from 192.168.2.4: bytes=32 time<lms TTL=128

Ping statistics for 192.168.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рисунок 7 – проверка связи PC1 и PC5

Практическая часть

1. Ознакомиться с теоретической частью.
2. Построить сеть в соответствии с заданием из таблицы 1. Количество компьютеров в локальной сети не менее 10.
3. Организовать межсетевое взаимодействие.
4. Проверить связь между сегментами. Результаты подтвердить скриншотами.

5. Результаты работы представить в виде отчета.

Таблица 1 – варианты заданий

№	Количество коммутаторов уровня доступа	Количество vlan'ов	Начальный адрес подсетей
1	2	4	10.10.0.0
2	3	3	20.20.0.0
3	4	2	30.30.0.0
4	2	4	40.40.0.0
5	3	3	50.50.0.0
6	4	2	60.60.0.0
7	2	4	70.70.0.0
8	3	3	80.80.0.0
9	4	2	90.90.0.0
10	2	4	100.100.0.0

Практическая работа №6 «Маршрутизаторы»

Цель работы: приобрести навыки работы с маршрутизаторами с использованием пакета Cisco Packet Tracer.

Теоретическая часть

Маршрутизатор — специализированный компьютер, который пересылает пакеты между различными сегментами сети на основе правил и таблиц маршрутизации. Маршрутизатор может связывать разнородные сети различных архитектур. Маршрутизаторы работают на «сетевом» (третьем) уровне сетевой модели OSI, в отличие от коммутаторов (свитчей) и концентраторов (хабов), которые работают, соответственно, на втором и первом уровнях модели OSI [9].

Коммутаторы L3-уровня частично могут выполнять функции маршрутизатора, однако отличаются от них более высокой производительностью, за счет аппаратной обработки пакетов, против программной на маршрутизаторах. Дополнительно маршрутизаторы могут быть использованы как межсетевые экраны, VPN-серверы и т.д.

Практическая часть

Допустим, что в нашем распоряжении имеется небольшое предприятие с одним коммутатором и 3 персональными компьютерами, разделенные на 3 vlan'а как показано на рисунке 1.

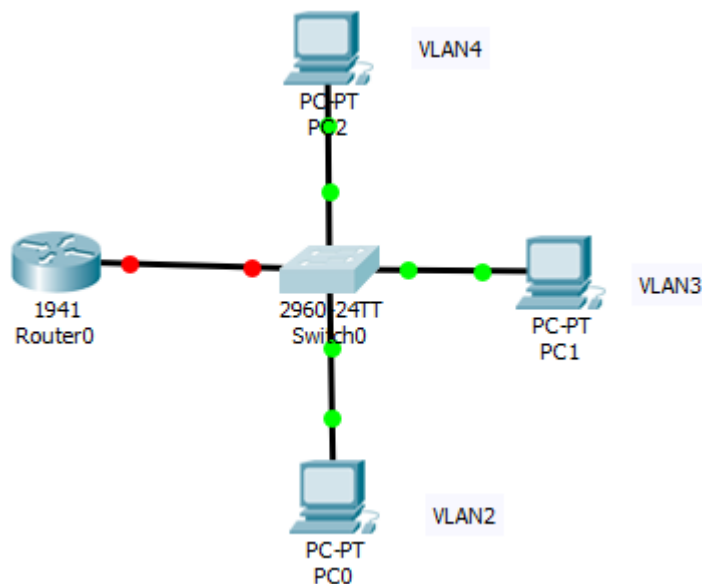


Рисунок 1 – пример сети

Для начала создадим vlan'ы на коммутаторе. Для этого выполним следующие команды:

```
en
conf t
vlan 2
name VLAN2
exit
vlan 3
name VLAN3
exit
vlan 4
name VLAN4
exit
```

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name VLAN2
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name VLAN3
Switch(config-vlan)#exit
Switch(config)#vlan 4
Switch(config-vlan)#name VLAN4
Switch(config-vlan)#exit
Switch(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Рисунок 2 – создание vlan'ов на коммутаторе

Также настроим интерфейсы коммутатора:

```
en
conf t
```

```

int fa0/1
switchport mode access
switchport access vlan 2
int fa0/2
switchport mode access
switchport access vlan 3
int fa0/3
switchport mode access
switchport access vlan 4

```

Теперь настроим trunk порт до маршрутизатора:

```

en
conf t
int fa0/4
switchport mode trunk
switchport trunk allowed vlan 2, 3, 4

```

Перейдем к настройкам маршрутизатора. В первую очередь необходимо «ПОДНЯТЬ» СВЯЗЬ.

Примечание: На коммутаторах все порты включены по умолчанию, на роутерах – выключены.

Для этого на стороне роутера произведем следующие настройки:

```

en
conf t
int gi0/0
no shutdown

```

В результате линк должен загореться зеленым (рисунок 3).

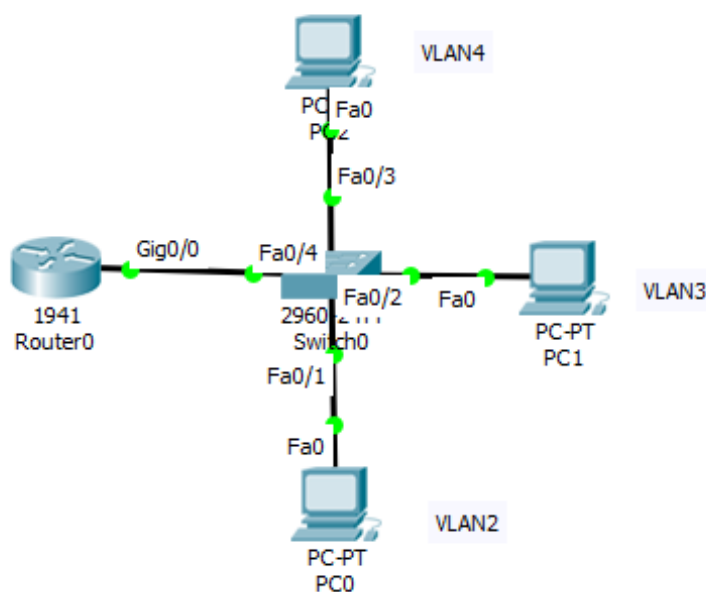


Рисунок 3 – поднятие связи с роутером

Теперь необходимо произвести дополнительные настройки интерфейса маршрутизатора. Так как подключение идет по одному интерфейсу, задать ему 3 различных настройки одновременно невозможно. Для этого реализован такой инструмент как подинтерфейсы. Для работы с подинтерфейсами используется следующая команда:

Interface [физический интерфейс].[номер подинтерфейса]

В нашем случае:

Interface gi0/0.2

Для настройки подинтерфейса необходимо выполнить следующие команды:

*Interface gi0/0.2
Encapsulation dot1Q 2
Ip address 192.168.0.100 255.255.255.0
No shutdown*

Чтобы посмотреть корректность настройки можно использовать команду show run (рисунок 4).



```
interface GigabitEthernet0/0
  no ip address
  duplex auto
  speed auto
  !
interface GigabitEthernet0/0.2
  encapsulation dot1Q 2
  ip address 192.168.0.100 255.255.255.0
  !
interface GigabitEthernet0/0.3
  encapsulation dot1Q 3
  ip address 192.168.1.100 255.255.255.0
  !
interface GigabitEthernet0/0.4
  encapsulation dot1Q 4
  ip address 192.168.3.100 255.255.255.0
  !
interface GigabitEthernet0/1
  no ip address
  duplex auto
  speed auto
  --More--
```

Рисунок 4 – просмотр настроек роутера

Далее настроим персональные компьютеры. Для этого зададим ip-адрес, маску и шлюз (рисунок 5). Проверим доступность компьютеров из разных vlan'ов (рисунок 6).

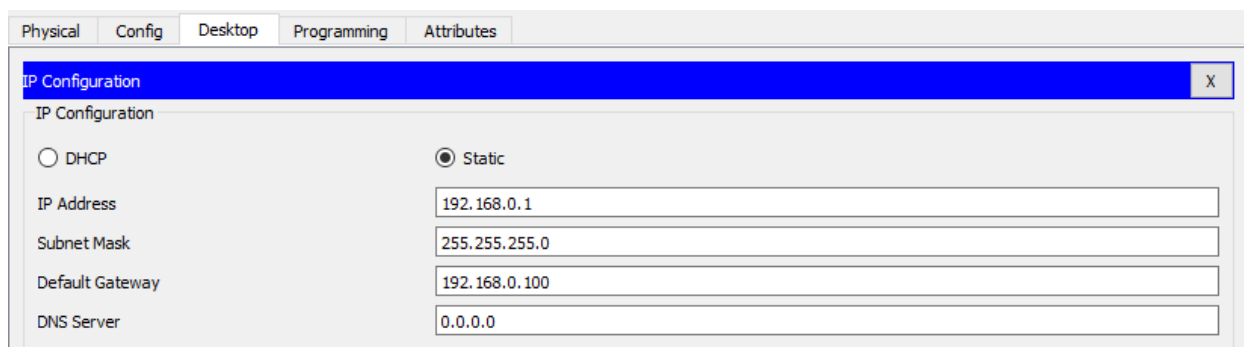


Рисунок 5 – настройка PC0

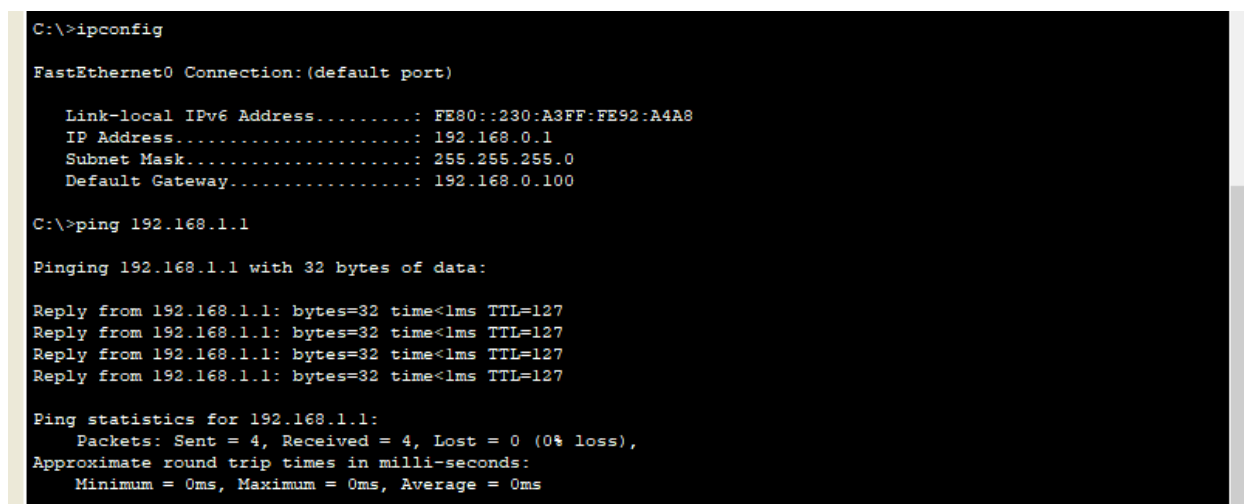


Рисунок 6 – проверка доступности компьютеров

Практическая часть

1. Ознакомиться с теоретической частью.
2. Построить сеть в соответствии с заданием из таблицы 1.
3. Организовать межсетевое взаимодействие.
4. Проверить связь между сегментами. Результаты подтвердить скриншотами.
5. Результаты работы представить в виде отчета.

Таблица 1 – варианты заданий

№	Количество персональных компьютеров	Количество vlan'ов	Начальный адрес подсетей
1	6	3	10.10.0.0
2	7	2	20.20.0.0
3	5	3	30.30.0.0
4	6	2	40.40.0.0
5	8	2	50.50.0.0

6	5	2	60.60.0.0
7	9	3	70.70.0.0
8	5	4	80.80.0.0
9	6	4	90.90.0.0
10	8	4	100.100.0.0

Практическая работа №7 «Маршрутизация»

Цель работы: приобрести навыки настройки маршрутизации с использованием пакета Cisco Packet Tracer.

Теоретическая часть

Маршрутизация (англ. Routing) — процесс определения маршрута следования данных в сетях связи [10, 11].

Маршруты могут задаваться административно (статические маршруты), либо вычисляться с помощью алгоритмов маршрутизации, базируясь на информации о топологии и состоянии сети, полученной с помощью протоколов маршрутизации (динамические маршруты) [10, 11].

Маршрутизация в компьютерных сетях выполняется специальными программно-аппаратными средствами — маршрутизаторами; в простых конфигурациях может выполняться и компьютерами общего назначения, соответственно настроенными [10, 11].

Таблица маршрутизации — электронная таблица (файл) или база данных, хранящаяся на маршрутизаторе или сетевом компьютере, которая описывает соответствие между адресами назначения и интерфейсами, через которые следует отправить пакет данных до следующего маршрутизатора. Является простейшей формой правил маршрутизации [10, 11].

Практическая часть

Допустим, что руководство попросило объединить два офиса с готовой сетевой инфраструктурой. Для примера организации статической маршрутизации возьмем сеть из предыдущей практической работы и создадим ее копию с другими ip-адресами как показано на рисунке 1 и объединим маршрутизаторы этих сетей.

В результате получается, что подсети зданий работают в штатном режиме, но связь между ними в автоматическом режиме не организуется. Необходимо настроить маршрутизацию.

Дело в том, что маршрутизатор Router0 знает о существовании только своих подсетей: 192.168.0.0/24, 192.168.1.0/24, 192.168.2.0/24, а

маршрутизатор Router1 о подсетях: 192.168.10.0/24, 192.168.11.0/24, 192.168.12.0/24.

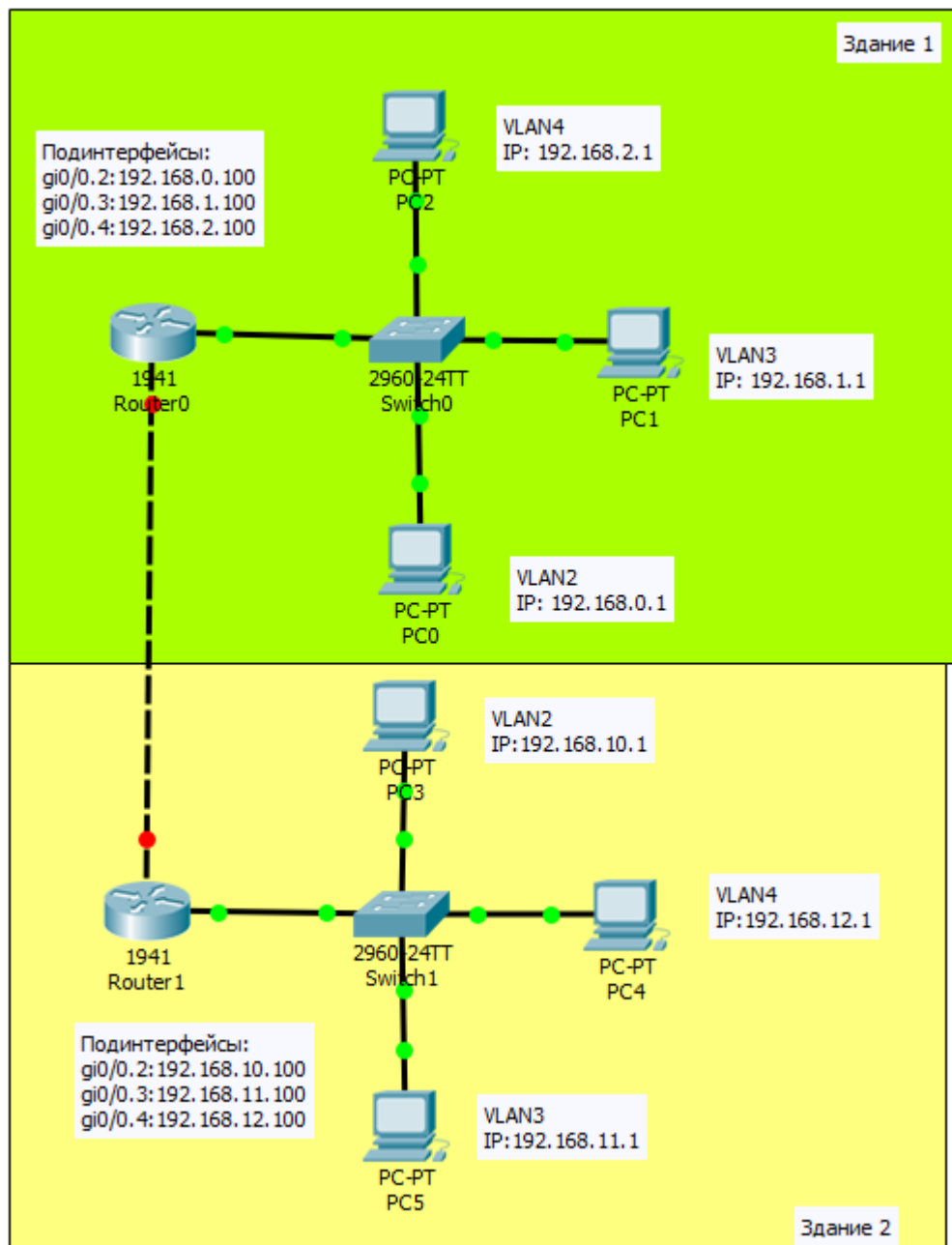


Рисунок 1 – сеть для организации маршрутизации

Для начала зададим ip адреса маршрутизаторам и поднимем связь. Для этого выполним следующие команды на обоих маршрутизаторах:

```
en
conf t
int gi0/1
no shutdown
ip address 192.168.100.1 255.255.255.0 (Для маршрутизатора Router0)
ip address 192.168.100.2 255.255.255.0 (Для маршрутизатора Router1)
```

После этого на схеме сети должна загореться связь между роутерами как на рисунке 2.

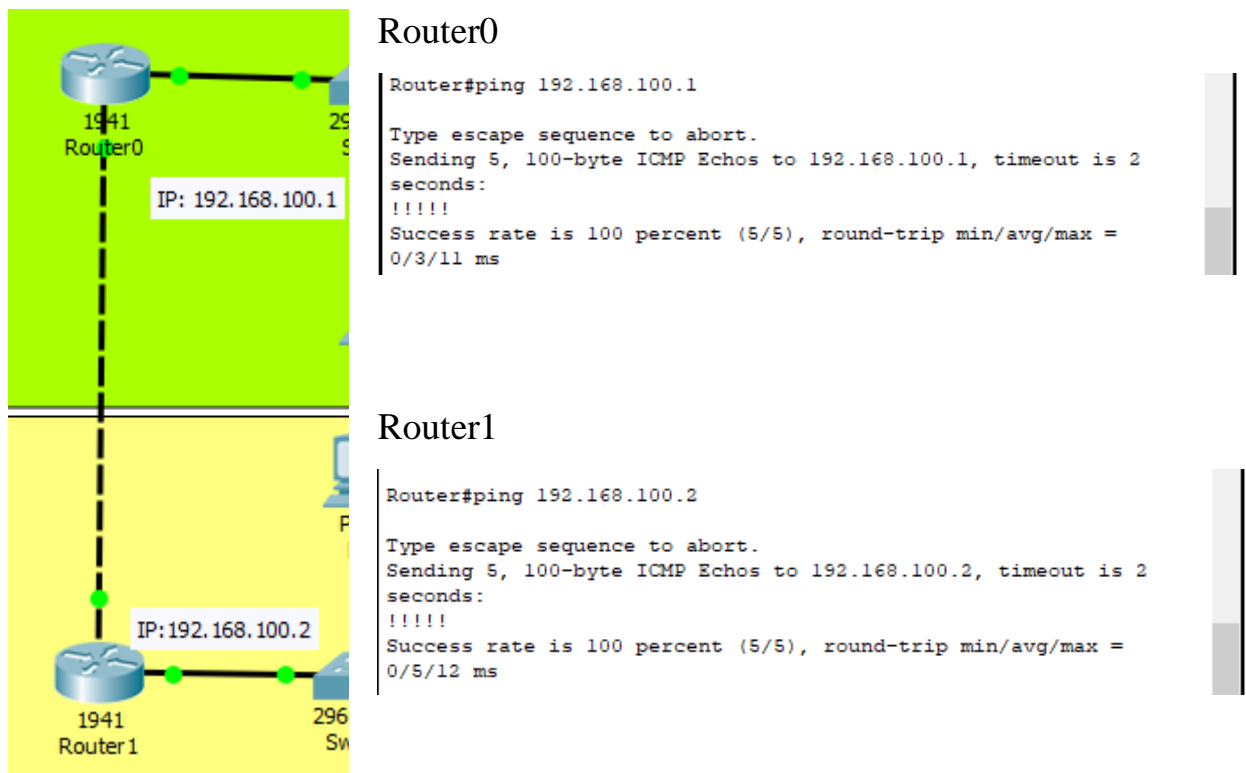


Рисунок 2 – связь между маршрутизаторами

Однако связи между компьютерами до сих пор нет, потому что отсутствуют необходимые маршруты. Чтобы посмотреть таблицу маршрутизации необходимо в привилегированном режиме ввести команду `show ip route`. Пример таблицы маршрутизации для маршрутизатора Router0 представлен на рисунке 3.

```

Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.0.0/24 is directly connected, GigabitEthernet0/0.2
L       192.168.0.100/32 is directly connected, GigabitEthernet0/0.2
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0.3
L       192.168.1.100/32 is directly connected, GigabitEthernet0/0.3
    192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, GigabitEthernet0/0.4
L       192.168.2.100/32 is directly connected, GigabitEthernet0/0.4
    192.168.100.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.100.0/24 is directly connected, GigabitEthernet0/1
L       192.168.100.1/32 is directly connected, GigabitEthernet0/1
--More--

```

Рисунок 3 – таблица маршрутизации для Router0

Символом «С» обозначаются присоединенные сети. В нашем случае это 192.168.0.0/24, 192.168.1.0/24, 192.168.2.0/24 и 192.168.100.0/24. То есть маршрутизатор знает, как передавать им пакеты.

Самым простым способом связи двух подсетей в данном случае можно свести к установке маршрута по умолчанию. Для этого в режиме глобального конфигурирования необходимо выполнить команду:

```
ip route 0.0.0.0 0.0.0.0 [interface-name] | [IP address]
```

Так для маршрутизатора Router0:

```
ip route 0.0.0.0 0.0.0.0 192.168.100.2
```

Для маршрутизатора Router1:

```
ip route 0.0.0.0 0.0.0.0 192.168.100.1
```

Таким образом, Router0 будет перенаправлять весь трафик на неизвестные ему адреса на Router1, а Router1 на Router0.

Практическая часть

1. Ознакомиться с теоретической частью.
2. Построить сеть в соответствии с заданием из таблицы 1 с использованием 2 маршрутизаторов.
3. Организовать межсетевое взаимодействие.

4. Проверить связь между сегментами. Результаты подтвердить скриншотами.

5. Результаты работы представить в виде отчета.

Таблица 1 – варианты заданий

№	Количество персональных компьютеров	Количество vlan'ов	Начальный адрес подсетей
1	6	3	10.10.0.0
2	7	2	20.20.0.0
3	5	3	30.30.0.0
4	6	2	40.40.0.0
5	8	2	50.50.0.0
6	5	2	60.60.0.0
7	9	3	70.70.0.0
8	5	4	80.80.0.0
9	6	4	90.90.0.0
10	8	4	100.100.0.0

Практическая работа №8 «Протокол DHCP»

Цель работы: приобрести навыки настройки серверов DHCP с использованием пакета Cisco Packet Tracer.

Теоретическая часть

Ранее настройка сетевых параметров компьютеров производилась вручную. Этот подход удобен и применим в случае, если компьютеров в организации 5-10. В случае, если количество компьютеров в организации превышает 50, 100 и т.д., то определять сетевые настройки руками становится проблематичным. Для настройки такого большого количества абонентов используется протокол DHCP.

DHCP (англ. Dynamic Host Configuration Protocol — протокол динамической настройки узла) — сетевой протокол, позволяющий сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве сетей TCP/IP.

На рисунке 1 представлена схема получения сетевых настроек с использованием протокола DHCP.

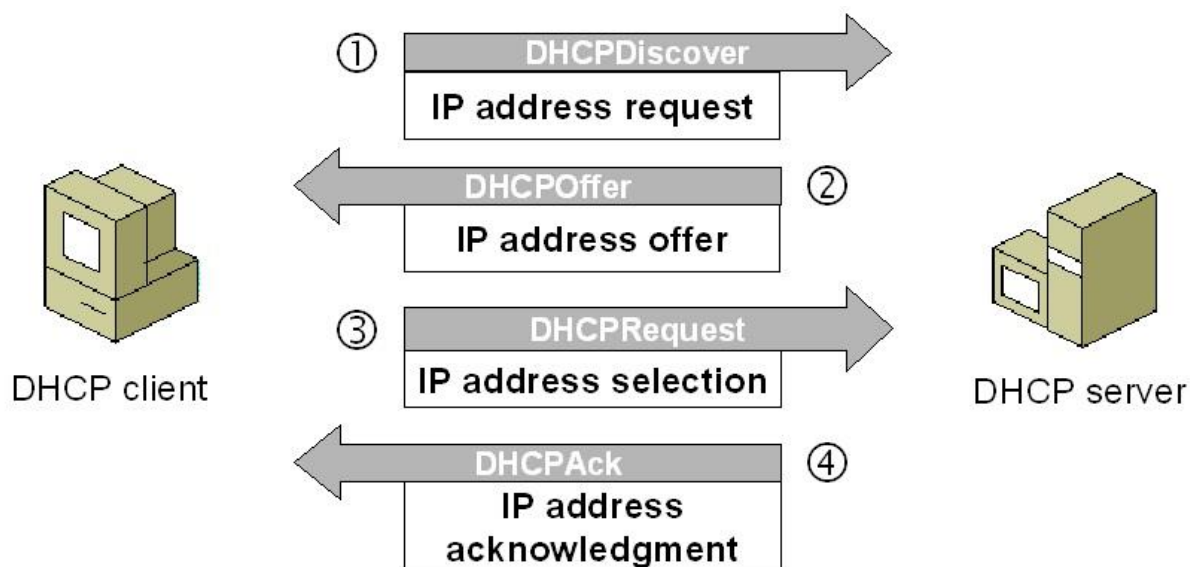


Рисунок 1 - схема получения сетевых настроек с использованием протокола DHCP

В качестве DHCP может использоваться маршрутизатор (например домашний WiFi-роутер) или специализированный DHCP-сервер (например компьютер с установленной и настроенной ОС Windows Server).

При подключении к сети абонент пытается найти DHCP-сервер и рассылает широковещательный запрос DHCPDiscover. Если в сети есть DHCP-сервер, то он принимает запрос и отвечает сообщением DHCPOffer, в которое включены предлагаемые сетевые настройки (например IP:192.168.1.30, mask:255.255.255.0). Далее клиент отправляет подтверждение в виде сообщения DHCPRequest. Сервер, в свою очередь, подтверждает операцию сообщением DHCPAck.

Практическая часть

Рассмотрим схему, где роль DHCP-сервера выполняет маршрутизатор (рисунок 2).

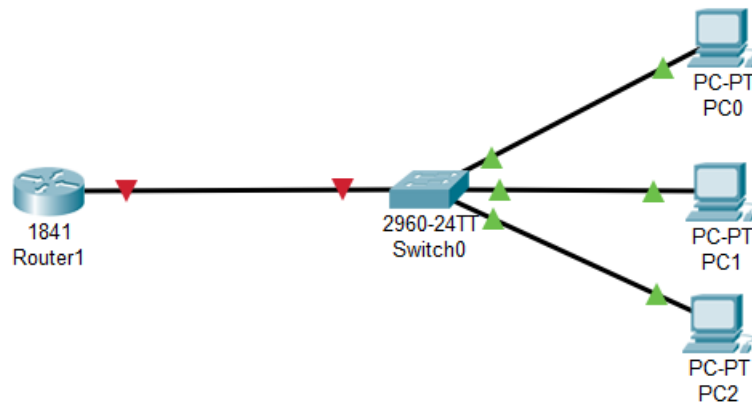


Рисунок 2 – схема сети с маршрутизатором

Переходим к настройке интерфейса, к которому подключен коммутатор Switch0. В данном случае это интерфейс FastEthernet 0/0 (Рисунок 3).

```
enable
conf t
interface fa0/0
no shutdown
ip address 192.168.1.1 255.255.255.0
exit
```

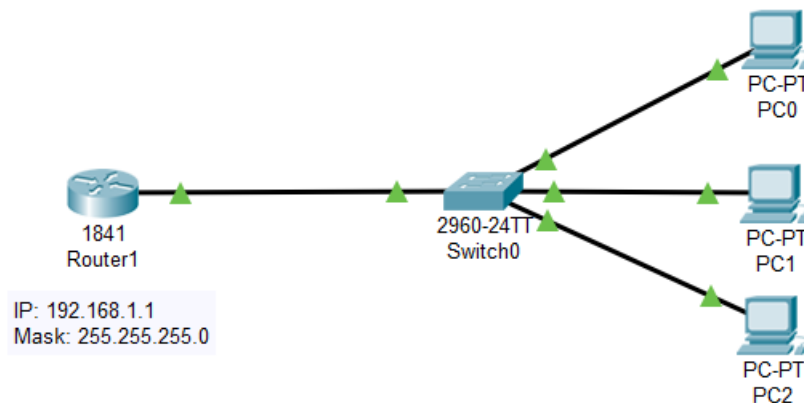


Рисунок 3 – схема с настроенным IP-адресом на маршрутизаторе

На следующем этапе необходимо создать пул адресов DHCP. Для этого необходимо использовать команду:

```
ip DHCP pool [Имя_пула]
network [ip_сети (на конце 0)] [маска_сети]
default_router [ip_маршрутизатора]
dns-server [ip_адрес_dns_сервера]
```

Настройка приведенного примера представлена на рисунке 4.

```

Router(config)#ip dhcp pool DHCP_pool
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#

```

Рисунок 4 – настройка схемы с маршрутизатором

Таким образом, все абоненты, настроенные на динамическое получение сетевых параметров получают их исходя из пула адресов. Для примера откроем настройки одного из компьютеров и изменим метод получения настроек со Static на DHCP (рисунок 5).

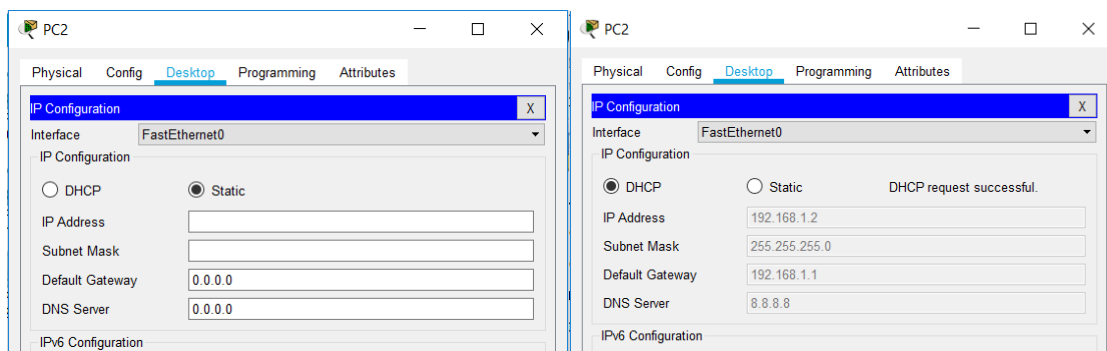


Рисунок 5 – получение динамических сетевых настроек

Еще одной полезной командой является команда исключения адреса из пула адресов:

```
ip dhcp excluded-address [ip_адрес]
```

Использование этой команды в приведенном примере возможно на ip-адресе маршрутизатора:

```
ip dhcp excluded-address 192.168.1.1
```

Таким образом маршрутизатор никогда не назначит адрес 192.168.1.1 ни одному из абонентов. Эта функция полезна еще в том случае, если в сети присутствуют сервера специального назначения (например файл-сервер). В этих случаях используются статические сетевые настройки, которые должны быть исключены из пула адресов.

Рассмотрим более сложный пример, когда сеть разделена на сегменты (рисунок 6).

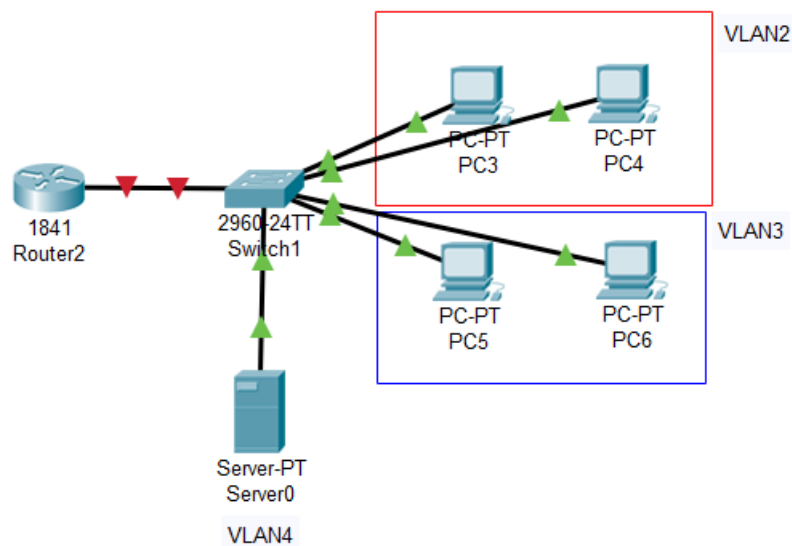


Рисунок 6 – схема сети с сегментами

Для начала создадим vlan'ы на коммутаторе Switch1 (рисунок 7).

```
Switch>
Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name VLAN2
Switch(config-vlan)#exit
Switch(config)#vlan 3
Switch(config-vlan)#name VLAN3
Switch(config-vlan)#exit
Switch(config)#vlan 4
Switch(config-vlan)#name VLAN4
Switch(config-vlan)#exit
Switch(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Рисунок 7 – создание vlan'ов

Далее разнесем компьютеры по vlan'ам (рисунок 8)/

```
Switch(config)# int range fa0/3-4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#exit
Switch(config)#int range fa0/5-6
Switch(config-if-range)#switchport mode access\
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#exit
Switch(config)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 4
Switch(config-if)#exit
Switch(config)#
```

Рисунок 8 – разнесение компьютеров по vlan'ам

Следующим этапом является прокладка настроек vlan'ов до маршрутизатора, где они и будут маршрутизироваться. Для этого необходимо порт подключения маршрутизатора к коммутатору перевести в режим trunk (в текущем примере это порт fa0/1). Этот процесс представлена на рисунке 9.

```
Switch(config)#  
Switch(config)#int fa0/1  
Switch(config-if)#switchport mode trunk  
Switch(config-if)#switchport trunk allowed vlan 2,3,4  
Switch(config-if)#exit  
Switch(config)#
```

Рисунок 9 - прокладка настроек vlan'ов до маршрутизатора.

Чтобы проверить правильность настройки можно ввести в привилегированном режиме команду show run (рисунок 9).

```
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
interface FastEthernet0/1  
  switchport trunk allowed vlan 2-4  
  switchport mode trunk  
!  
interface FastEthernet0/2  
  switchport access vlan 4  
  switchport mode access  
!  
interface FastEthernet0/3  
  switchport access vlan 2  
  switchport mode access  
!  
interface FastEthernet0/4  
  switchport access vlan 2  
  switchport mode access  
!  
interface FastEthernet0/5  
  switchport access vlan 3  
  switchport mode access  
!  
interface FastEthernet0/6  
  switchport access vlan 3  
  switchport mode access  
!  
interface FastEthernet0/7  
!  
interface FastEthernet0/8  
!
```

Рисунок 9 – проверка корректности настройки

Далее необходимо настроить соответствующий интерфейс маршрутизатора по аналогии с первым примером. Сначала необходимо включить сам интерфейс:

```
enable  
conf t  
interface fa0/0  
no shutdown
```

Следующим этапом необходимо создать подинтерфейсы для маршрутизации:

```
enable
conf t
interface fa0/0.2
encapsulation dot1Q 2
ip address 192.168.2.1 255.255.255.0
exit
```

Аналогично для других vlan'ов:

```
enable
conf t
interface fa0/0.3
encapsulation dot1Q 3
ip address 192.168.3.1 255.255.255.0
exit
```

```
enable
conf t
interface fa0/0.4
encapsulation dot1Q 4
ip address 192.168.4.1 255.255.255.0
exit
```

В итоге схема сети должна выглядеть, как это показано на рисунке 10.

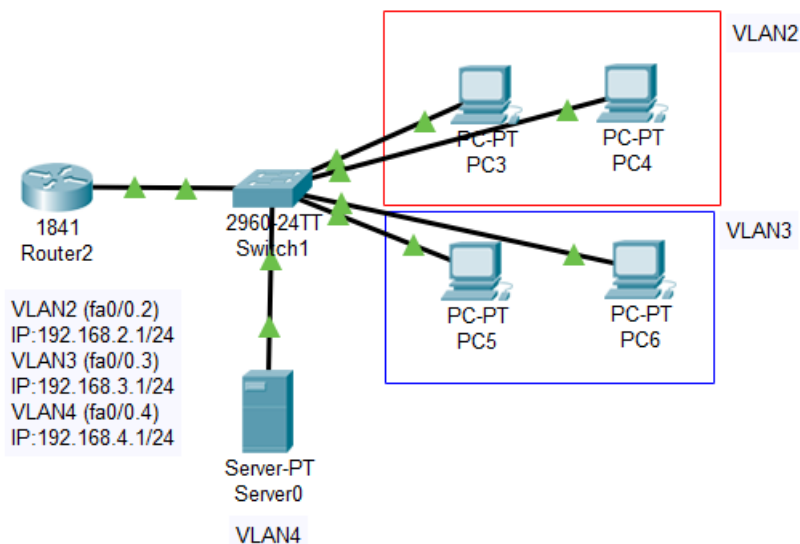


Рисунок 10 – схема сети с подинтерфейсами

Если выполнить команду `show run` из привилегированного режима то схема должна быть аналогична рисунку 11.

```
IOS Command Line Interface

!
interface FastEthernet0/0
  no ip address
  duplex auto
  speed auto
!
interface FastEthernet0/0.2
  encapsulation dot1Q 2
  ip address 192.168.2.1 255.255.255.0
!
interface FastEthernet0/0.3
  encapsulation dot1Q 3
  ip address 192.168.3.1 255.255.255.0
!
interface FastEthernet0/0.4
  encapsulation dot1Q 4
  ip address 192.168.4.1 255.255.255.0
!
interface FastEthernet0/1
  no ip address
  duplex auto
  speed auto
  shutdown
!
--More--
```

Рисунок 11 – настройки маршрутизатора

Переходим к настройке DHCP-сервера. Для начала необходимо задать его IP-адрес, например 192.168.4.2, маска: 255.255.255.0 и шлюз – IP-адрес маршрутизатора: 192.168.4.1 (рисунок 12).

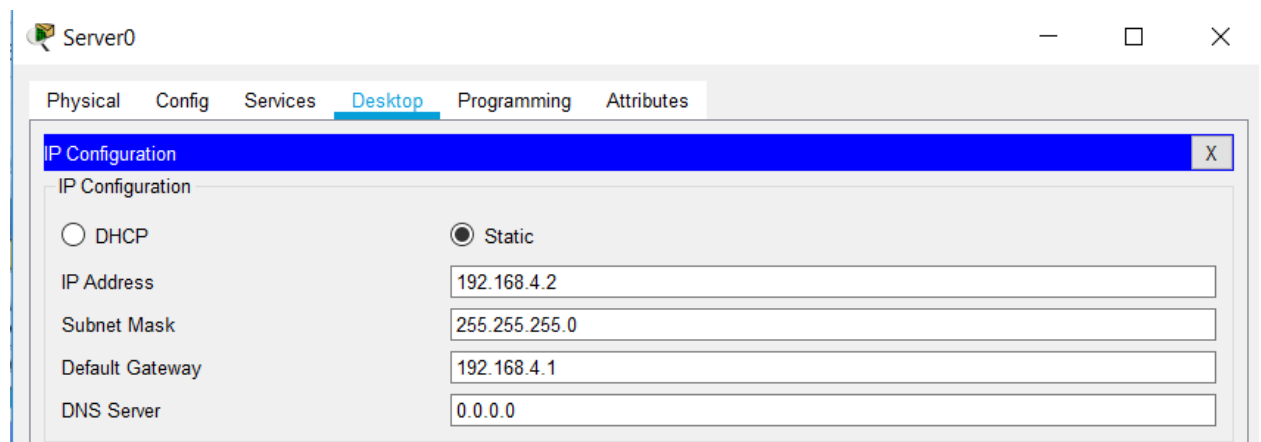


Рисунок 12 – сетевые настройки сервера

Проверим связь с маршрутизатором с помощью утилиты ping (рисунок 13).

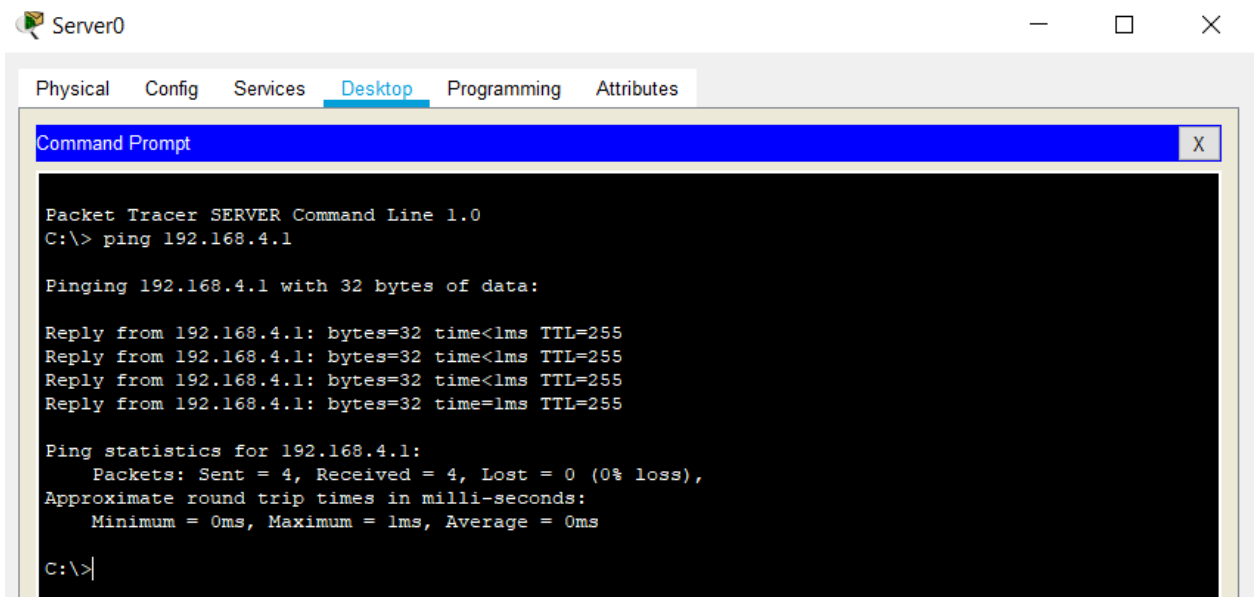


Рисунок 13 – проверка связи между маршрутизатором и сервером

Далее необходимо настроить сам DHCP-сервер. Для этого переходим на вкладку «Services» -> «DHCP» как показано на рисунке 14. Там уже присутствует пул адресов по умолчанию – «serverPool».

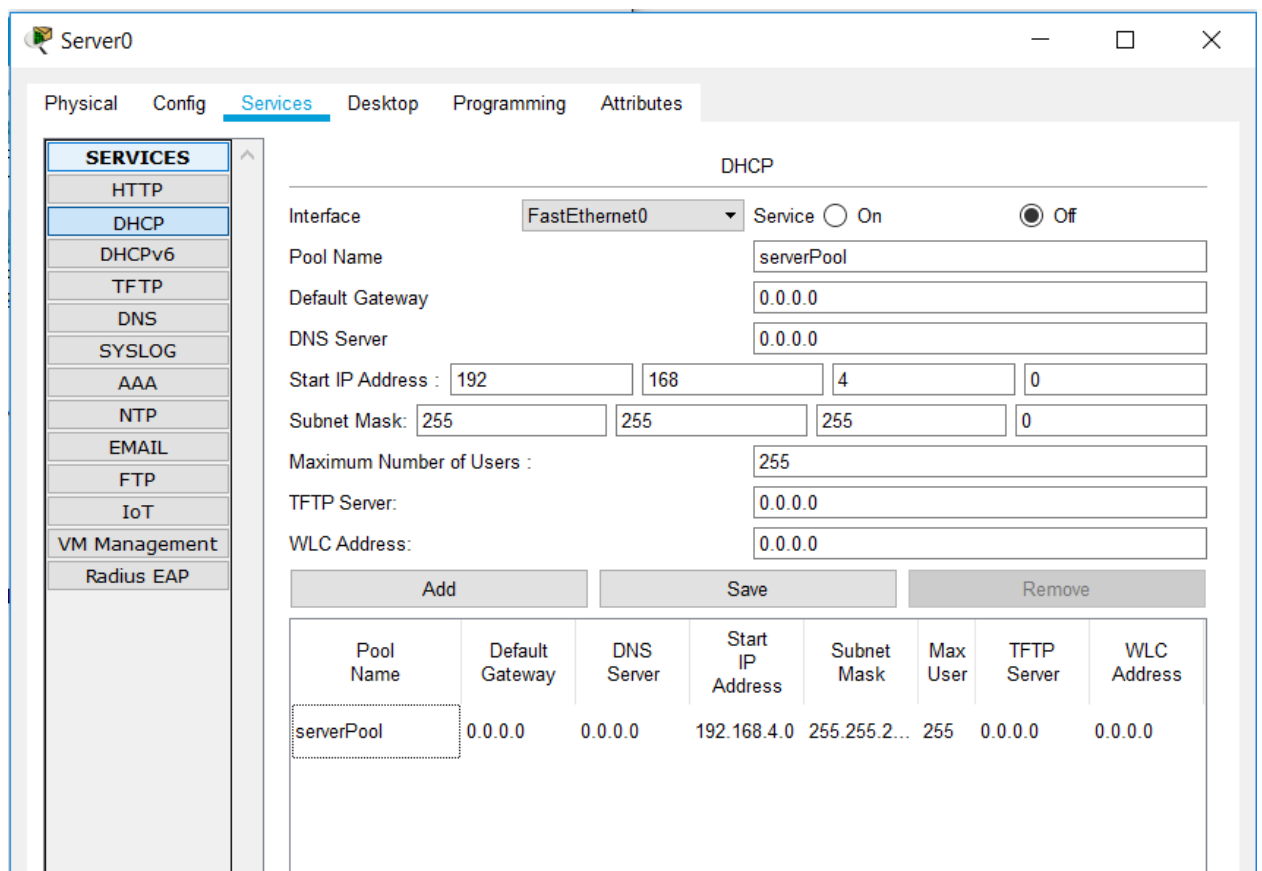


Рисунок 14 – настройки DHCP

Начнем с настройки пула адресов для VLAN2 (рисунок 15). Для этого:

1. Включаем сервис, переводя его в режим «On».
2. Задаем имя пула адресов, например «DHCP-Pool-VLAN2».
3. Указываем шлюз по умолчанию (IP-адрес маршрутизатора для данного сегмента) – 192.168.2.1.
4. Указываем адрес, с которого необходимо начать адресацию. Так как адрес 192.168.2.1 занят маршрутизатором указываем - 192.168.2.2. Маска 24 бита.
5. Добавляем пул кнопкой «Add».

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask	Max User	TFTP Server	WLC Address
DHCP-Pool-VLAN2	192.168.2.1	0.0.0.0	192.168.2.2	255.255.255.0	254	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	255	0.0.0.0	0.0.0.0

Рисунок 15 – задание пула адресов для VLAN2

Аналогично для VLAN3 и VLAN4. Однако, из-за того, что сервер DHCP и компьютеры-абоненты находятся в разных сегментах, то широковещательный запрос не пройдет. Для того, чтобы DHCP-сервер стал доступен абонентам всех сегментов необходимо организовать

перенаправление DHCP-запросов. Для этого необходимо в каждом подинтерфейсе указать ip helper-address – адрес DHCP-сервера. Для этого на коммутаторе необходимо выполнить:

enable

conf t

interface [интерфейс].[номер_подинтерфейса]

ip helper-address [IP_DHCP-сервера]

После настройки необходимо перевести абонентов на динамическое получение сетевых настроек. Если все выполнено корректно, то результат будет аналогичен рисунку 16.

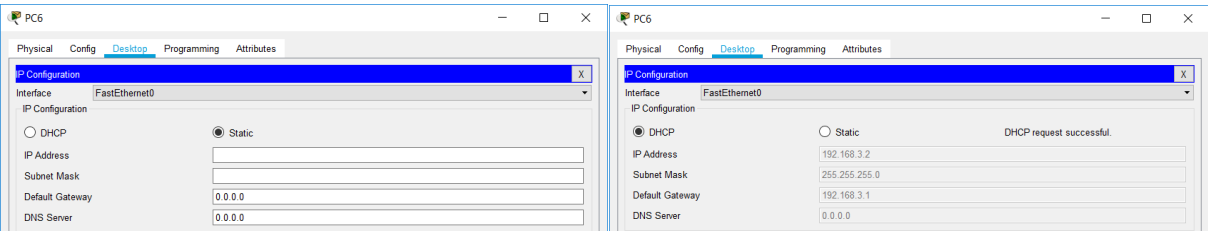


Рисунок 16 – получение сетевых настроек абонентом VLAN3

Практическая часть

1. Ознакомиться с теоретической частью.
2. Построить сеть в соответствии с заданием из таблицы 1.
3. Организовать межсетевое взаимодействие с использованием динамического распределения адресов.
4. Проверить связь между сегментами. Результаты подтвердить скриншотами.
5. Результаты работы представить в виде отчета.

Таблица 1 – варианты заданий

Пул адресов Vlan 1	Пул адресов Vlan 2	Пул адресов Vlan 3
192.168.[10*номер по списку].20-40	192.168. [10*номер по списку+1].20-40	192.168. [10*номер по списку+2].20-40

Практическая работа №9 «Технология NAT»

Цель работы: приобрести навыки настройки серверов DHCP с использованием пакета Cisco Packet Tracer.

Теоретическая часть

NAT (от англ. Network Address Translation — «преобразование сетевых адресов») — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов. Также имеет названия IP Masquerading, Network Masquerading и Native Address Translation.

Преобразование адреса методом NAT может производиться почти любым маршрутизирующим устройством — маршрутизатором[1], сервером доступа, межсетевым экраном. Наиболее популярным является SNAT, суть механизма которого состоит в замене адреса источника (англ. source) при прохождении пакета в одну сторону и обратной замене адреса назначения (англ. destination) в ответном пакете. Наряду с адресами источник/назначение могут также заменяться номера портов источника и назначения.

Существует 3 базовых концепции трансляции адресов: статическая (Static Network Address Translation), динамическая (Dynamic Address Translation), маскарадная (NAPT, NAT Overload, PAT).

1. **Статический NAT** — отображение незарегистрированного IP-адреса на зарегистрированный IP-адрес на основании один к одному. Особенно полезно, когда устройство должно быть доступным снаружи сети.

2. **Динамический NAT** — отображает незарегистрированный IP-адрес на зарегистрированный адрес из группы зарегистрированных IP-адресов. Динамический NAT также устанавливает непосредственное отображение между незарегистрированными и зарегистрированными адресами, но отображение может меняться в зависимости от зарегистрированного адреса, доступного в пуле адресов, во время коммуникации.

3. **Перегруженный NAT (NAPT, NAT Overload, PAT, маскарадинг)** — форма динамического NAT, который отображает несколько

незарегистрированных адресов в единственный зарегистрированный IP-адрес, используя различные порты. Известен также как PAT (Port Address Translation). При перегрузке каждый компьютер в частной сети транслируется в тот же самый адрес, но с различным номером порта.

Практическая часть

Рассмотрим сеть, состоящую из сервера и 3х абонентов, как показано на рисунке 1.

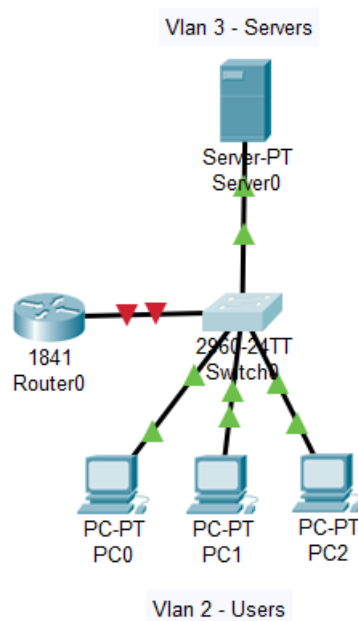


Рисунок 1 – схема сети

Для начала необходимо создать и настроить vlan'ы и определить trunk-порт. В результате настройки должны быть аналогичны приведенным на рисунке 2.

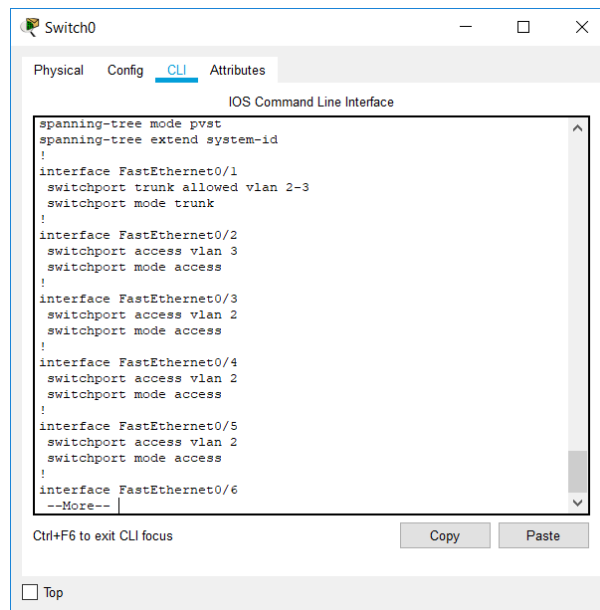


Рисунок 2 – сетевые настройки коммутатора Switch0

Далее переходим к настройкам маршрутизатора Router0. Необходимо определить подинтерфейсы для vlan'ов. Результат настройки должен быть аналогичен рисунку 3.

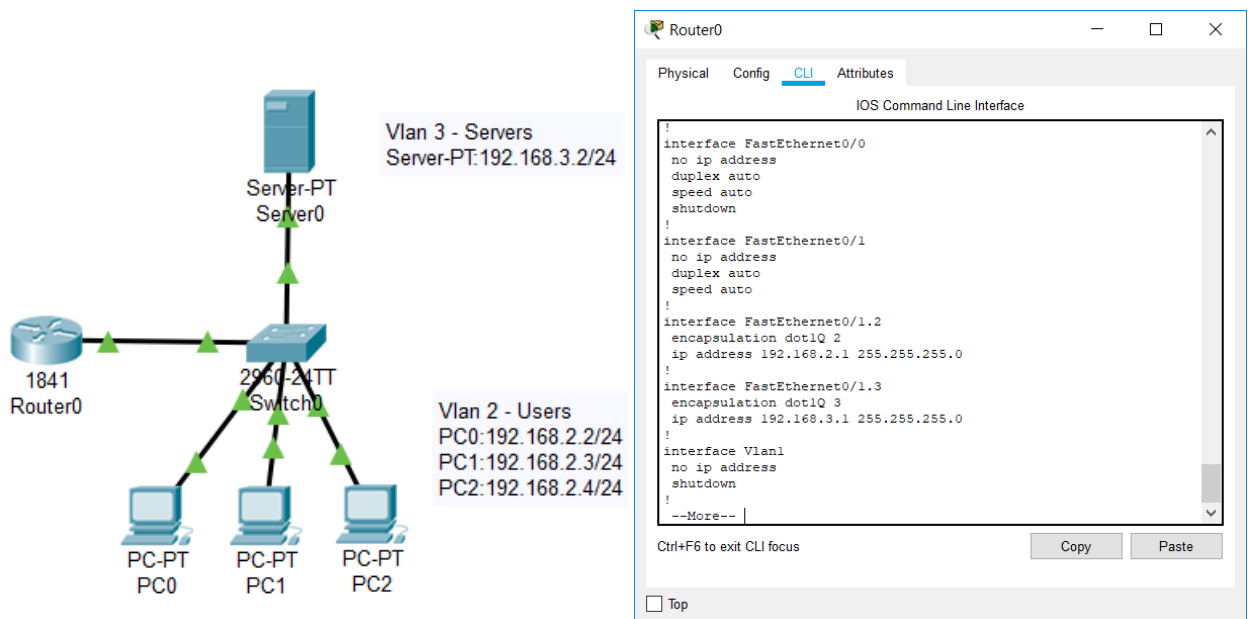


Рисунок 3 – сетевые настройки маршрутизатора

Использование технологии NAT подразумевает использование «белых» IP-адресов. Допустим, что интернет провайдер выделил один «белый» IP-адрес под нашу организацию.

Примечание: так как в Cisco Packet Tracer нет возможности подключения к интернету вместо него будем использовать еще одну сеть,

состоящую из маршрутизатора и сервера, каждый из которых имеет «белый» IP-адрес.

Настроим маршрутизатор Router2 как показано на рисунке 4.

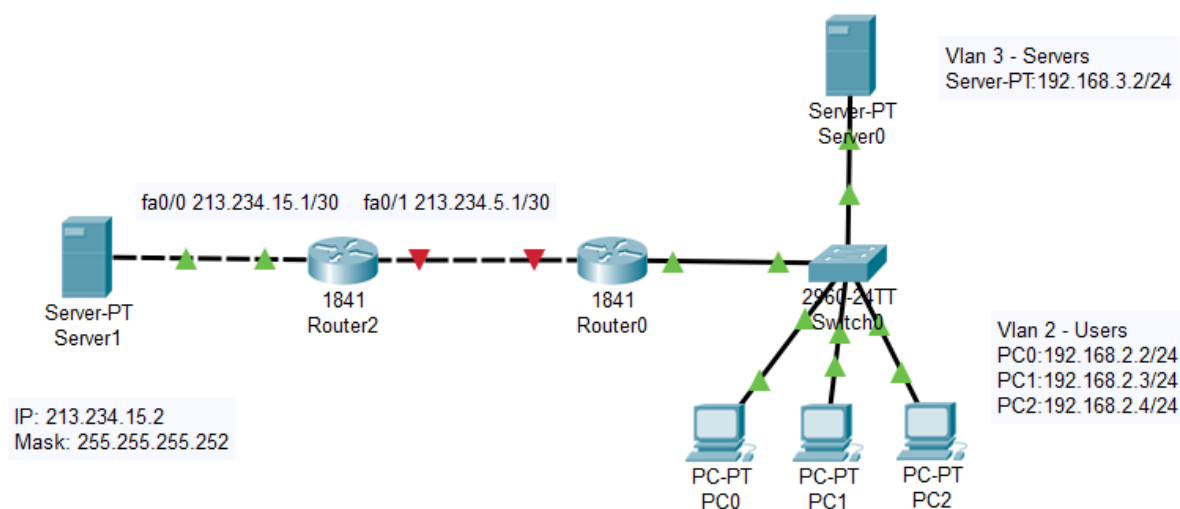


Рисунок 4 – сетевые настройки сети, эмулирующей доступ в интернет

Допустим, что провайдер выдал «белый» IP-адрес 213.234.5.2/30. Установим его на соответствующий порт локального маршрутизатора Router0.

```
enable
conf t
interface fa0/0
ip address 213.234.5.2 255.255.255.252
no shutdown
```

Также настраиваем маршрутизацию командой

```
ip route 0.0.0.0 0.0.0.0 213.234.5.1
```

Таким образом устройства Server1, Router2 и Router0 имеют доступ друг к другу, однако локальные компьютеры не имеют доступа к публичному серверу Server1, т.к. маршрутизатор Router2 не знает об их существовании. Для того, чтобы обеспечить эту связь будет использоваться технология NAT.

Первым этапом является определение сторон NAT. Для этого необходимо указать их с помощью команд:

```
enable
conf t
```

```
interface [необходимый_интерфейс]
ip nat inside или ip nat outside
```

В нашем случае расположение сторон будет таким, как показано на рисунке 5.

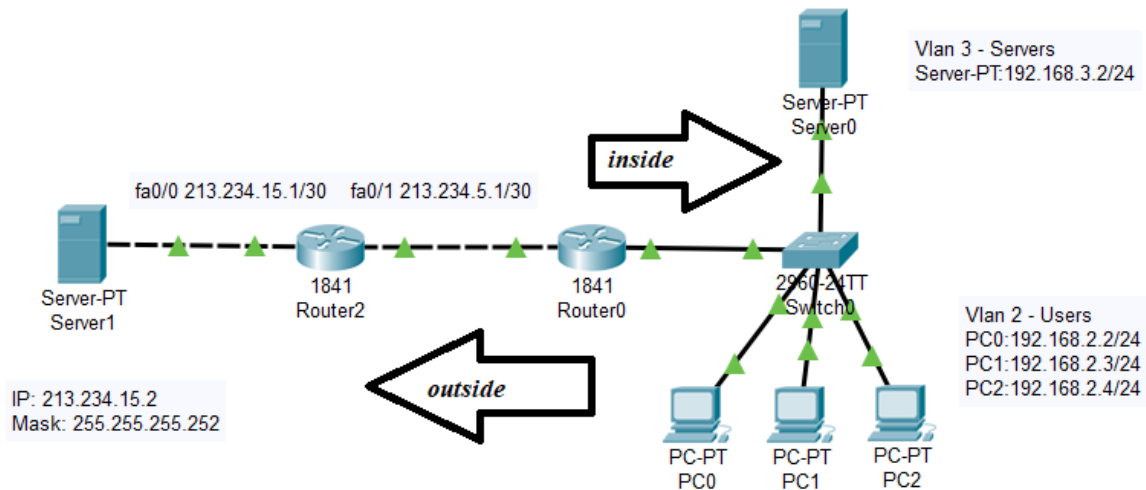


Рисунок 5 – расположение сторон NAT

Для этого выполним на маршрутизаторе Router0 следующие команды:

```
enable
conf t
interface fa0/0
ip nat outside
exit
interface fa0/1.2
ip nat inside
exit
interface fa0/1.3
ip nat inside
exit
```

После указания направления NAT необходимо создать Access List. Для этого необходимо выполнить следующие команды:

```
ip access-list standart [имя_листа]
permit [адрес_подсети] [wildcard_bits]
```

wildcard_bits – инверсия маски подсети. Например для маски 255.255.255.0 wildcard_bits будет равен 0.0.0.255.

Таким образом настройки маршрутизатора будут выглядеть следующим образом:

```
enable
conf t
ip access-list standard NATList
```

```
permit 192.168.2.0 0.0.0.255
permit 192.168.3.0 0.0.0.255
```

После выполнения всех подготовительных действий необходимо запустить саму технологию NAT с использованием следующих команд:

```
enable
conf t
ip nat inside source list NATList interface fastEthernet 0/0 overload
```

После этого компьютеры локальной сети могут иметь доступ к общедоступному серверу в интернете (рисунок 6).

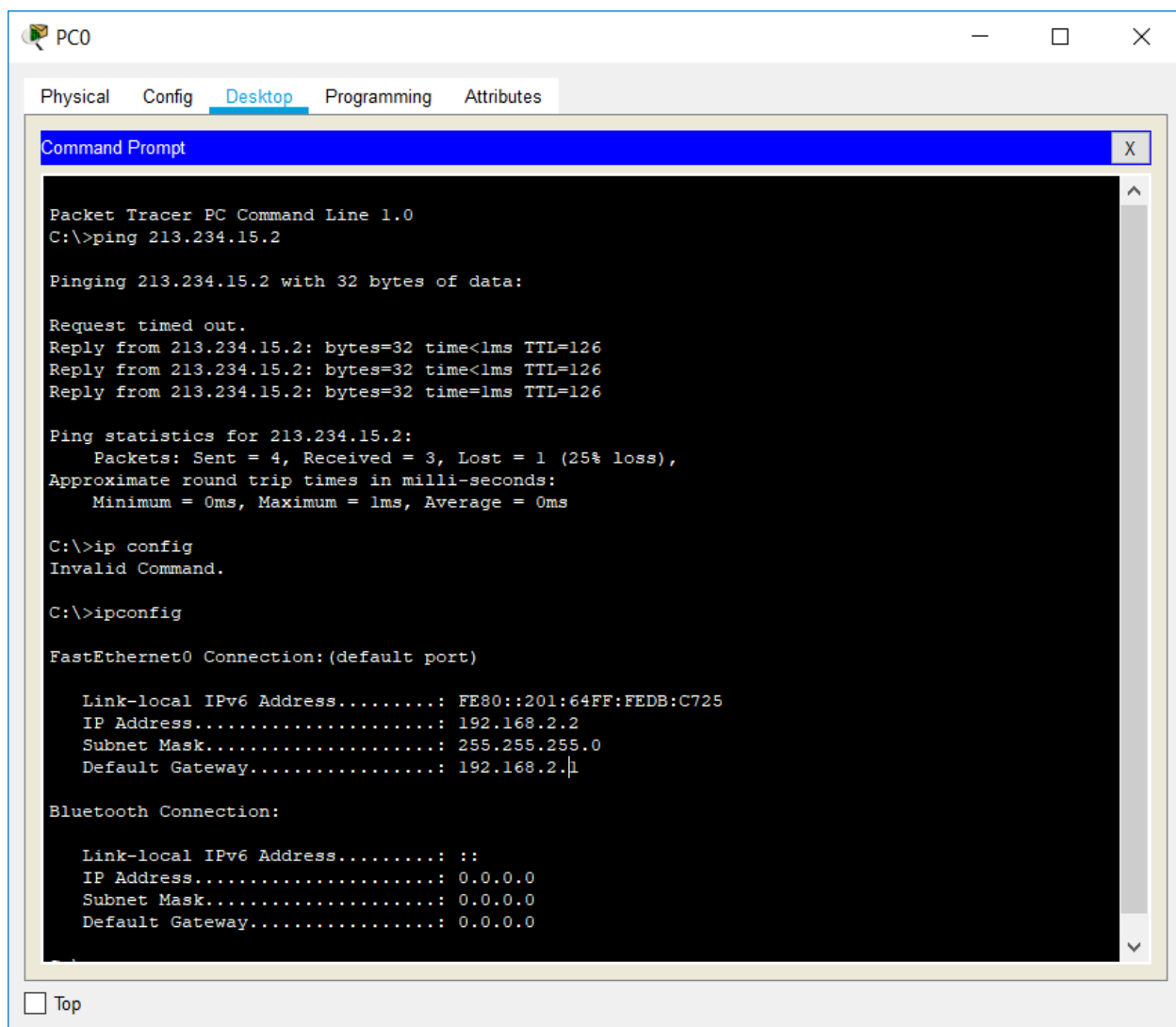


Рисунок 6 – проверка доступа абонентов к серверу

Практическая часть

1. Ознакомиться с теоретической частью.
2. Построить сеть в соответствии с теоретической частью.

3. Организовать межсетевое взаимодействие.
4. Проверить связь между сегментами. Результаты подтвердить скриншотами.
5. Результаты работы представить в виде отчета.