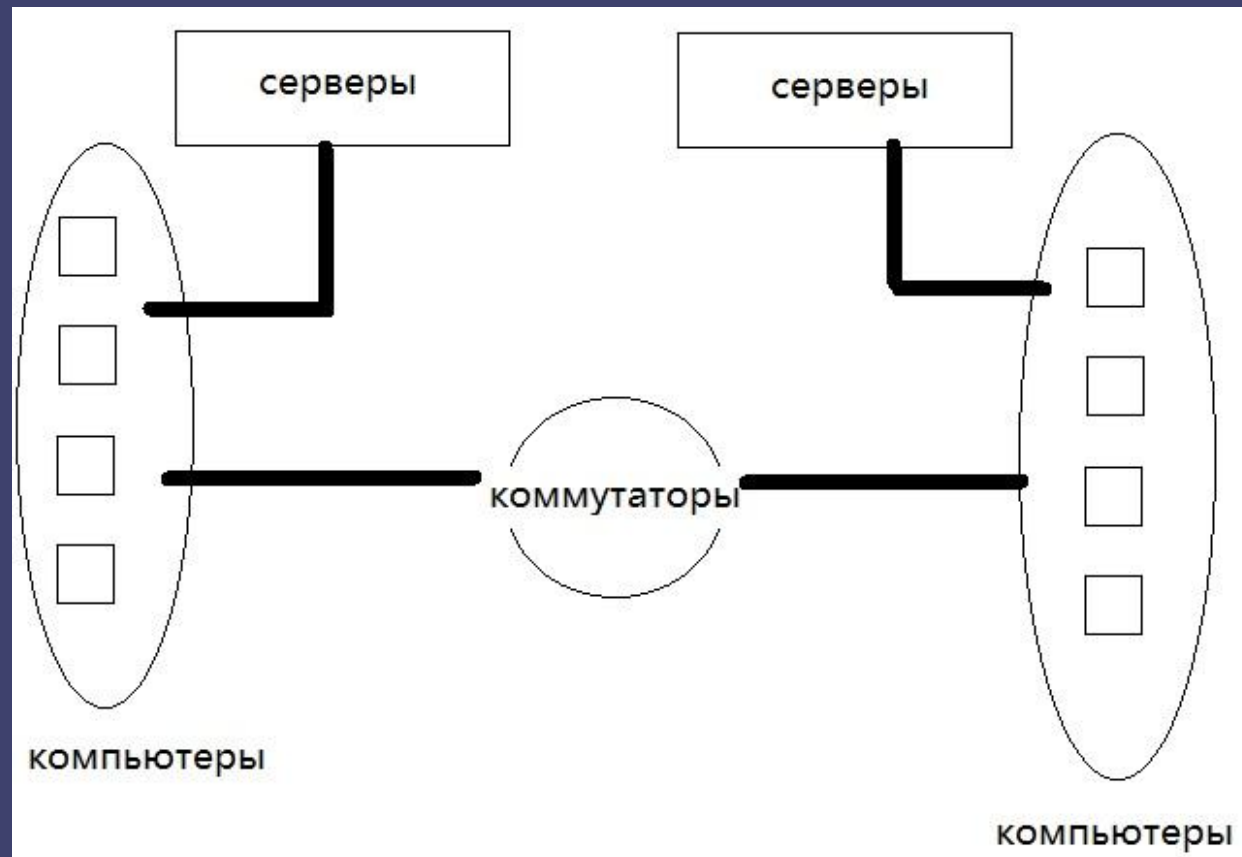




Компьютерные СЕТИ (NETWORKS)

Концептуальная схема сети



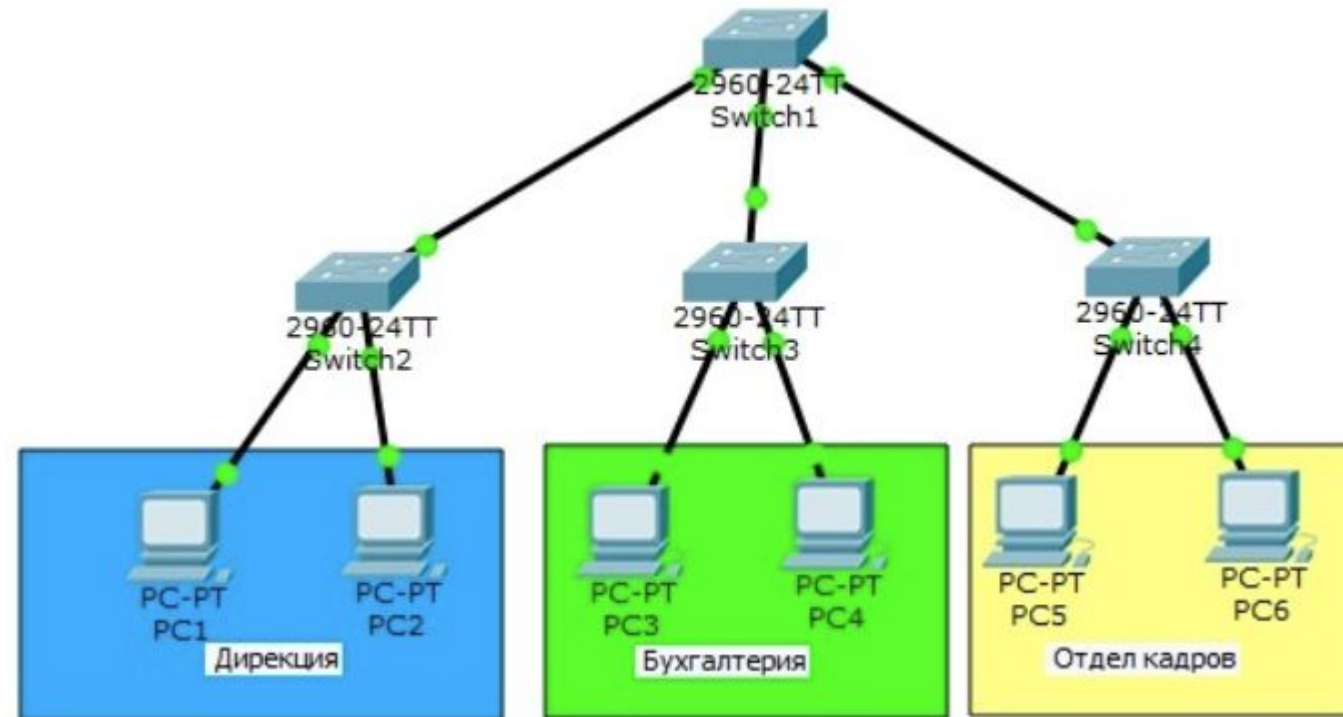
Задача:

Построить компьютерную сеть в эмуляторе Cisco Packet Tracer согласно схемы, и реализовать работу следующих технологий и протоколов:

1. VLAN
2. STP
3. DHCP
4. NAT
5. Web-сервер

VLAN (Virtual Local Area Network)

— группа устройств, имеющих возможность взаимодействовать между собой напрямую на канальном уровне, хотя физически при этом они могут быть подключены к разным сетевым коммутаторам. И наоборот, устройства, находящиеся в разных VLAN'ах, невидимы друг для друга на канальном уровне, даже если они подключены к одному коммутатору, и связь между этими устройствами возможна только на сетевом и более высоких уровнях



Зачем нужен VLAN?

Гибкое разделение устройств на группы

Как правило, одному VLAN соответствует одна подсеть. Устройства, находящиеся в разных VLAN, будут находиться в разных подсетях. Но в то же время VLAN не привязан к местоположению устройств и поэтому устройства, находящиеся на расстоянии друг от друга, все равно могут быть в одном VLAN независимо от местоположения

Уменьшение количества широковещательного трафика в сети

Каждый VLAN — это отдельный широковещательный домен. Например, коммутатор — это устройство 2 уровня модели OSI. Все порты на коммутаторе с лишь одним VLAN находятся в одном широковещательном домене. Создание дополнительных VLAN на коммутаторе означает разбиение коммутатора на несколько широковещательных доменов. Если один и тот же VLAN настроен на разных коммутаторах, то порты разных коммутаторов будут образовывать один широковещательный домен.

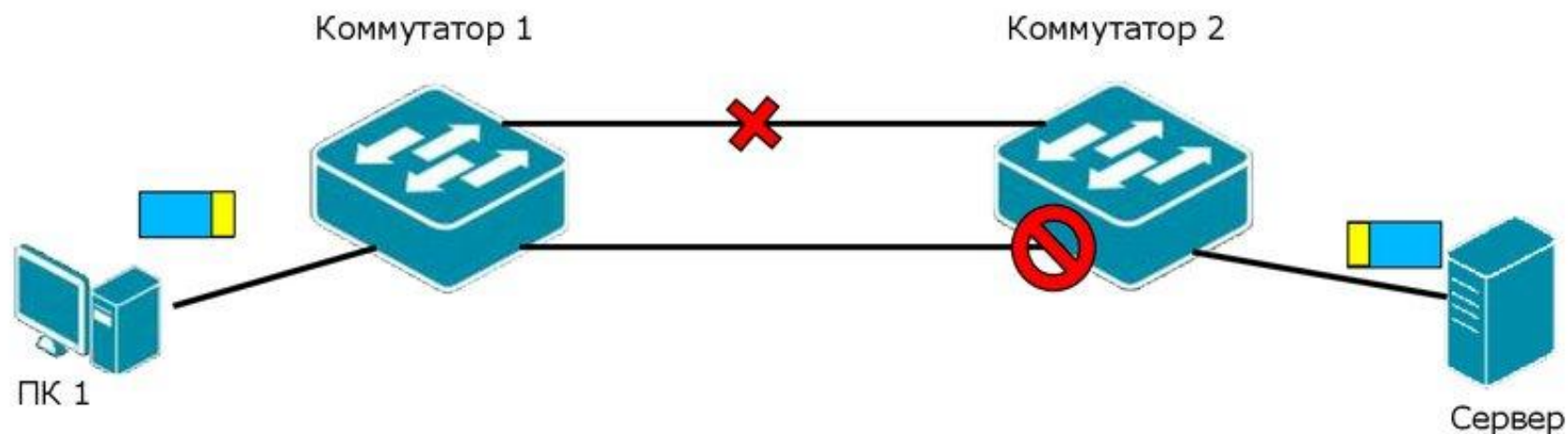
Увеличение безопасности и управляемости сети

Когда сеть разбита на VLAN, упрощается задача применения политик и правил безопасности. С VLAN политики можно применять к целым подсетям, а не к отдельному устройству. Кроме того, переход из одного VLAN в другой предполагает прохождение через устройство 3 уровня, на котором, как правило, применяются политики, разрешающие или запрещающие доступ из VLAN в VLAN.

STP (Spanning Tree Protocol) — сетевой протокол (или семейство сетевых протоколов) предназначенный для автоматического удаления циклов (петель коммутации) из топологии сети на канальном уровне в Ethernet-сетях.

Первоначальный протокол STP описан в стандарте 802.1D. Позже появилось несколько новых протоколов (RSTP, MSTP, PVST, PVST+), отличающихся некоторыми особенностями в алгоритме работы, в скорости, в отношении к VLANам и ряде других вопросов, но в целом решающих ту же задачу похожими способами. Все их принято обобщённо называть STP-протоколами.

Протокол Spanning Tree (STP)



❑ Протокол связующего дерева Spanning Tree Protocol (STP) является протоколом 2 уровня модели OSI, который:

- позволяет строить древовидные, свободные от петель, конфигурации связей между коммутаторами локальной сети;
- обеспечивает возможность автоматического резервирования альтернативных каналов связи между коммутаторами на случай выхода активных каналов из строя.

❑ В настоящее время существуют следующие версии протоколов связующего дерева:

- IEEE 802.1D Spanning Tree Protocol (STP);
- IEEE 802.1w Rapid Spanning Tree Protocol (RSTP);
- IEEE 802.1s Multiple Spanning Tree Protocol (MSTP).

DHCP (Dynamic Host Configuration Protocol/протокол динамической конфигурации узла) — это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.

NAT (Network Address Translation) — трансляция сетевых адресов. Процедура по изменению адресов в заголовках IP-пакетов при их прохождении через маршрутизатор или другое устройство.

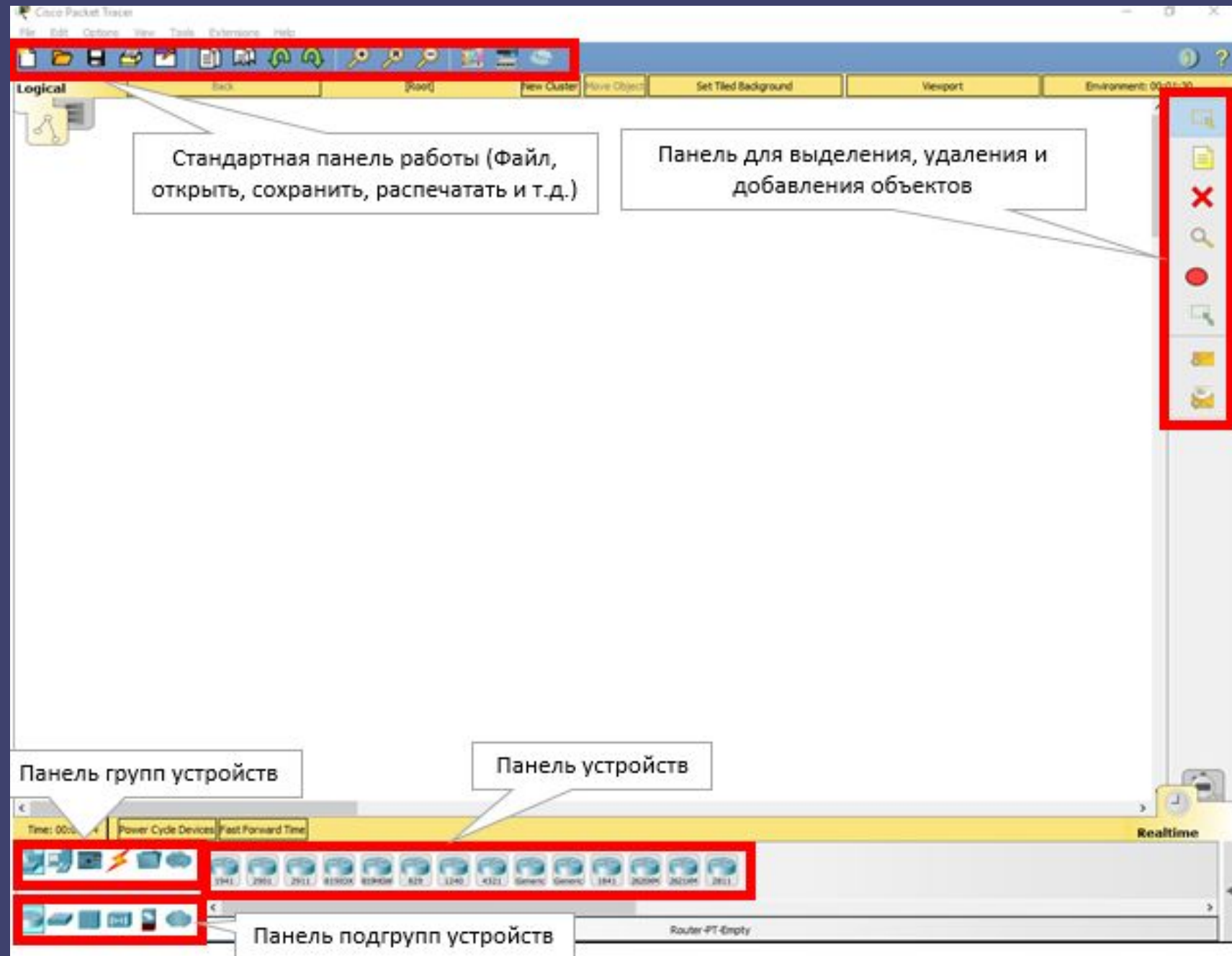
Cisco Packet Tracer – это эмулятор сети, созданный компанией Cisco. Программа позволяет строить и анализировать сети на разнообразном оборудовании в произвольных топологиях с поддержкой разных протоколов.

В ней вы получаете возможность изучать работу различных сетевых устройств:

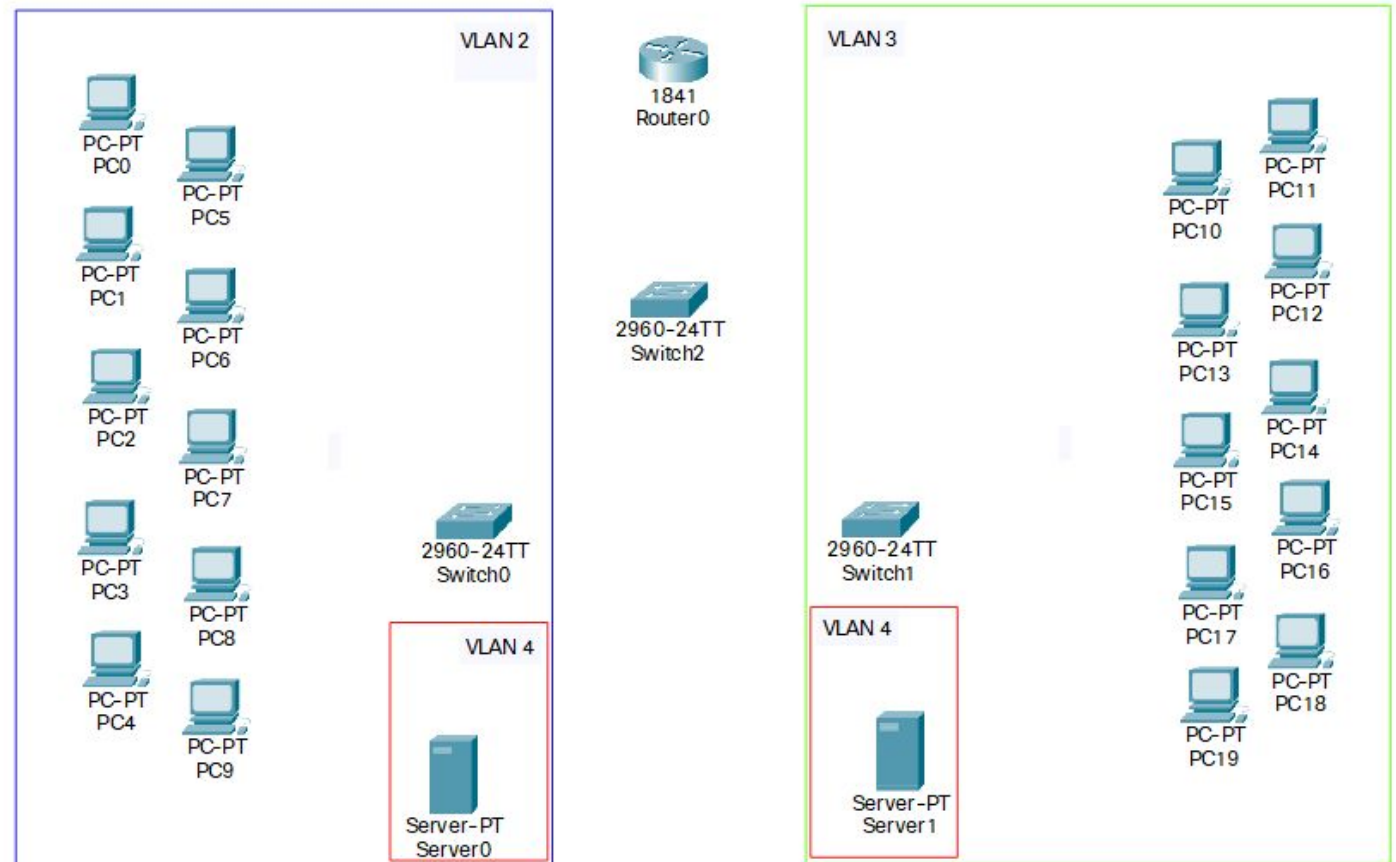
- маршрутизаторов,
- коммутаторов,
- точек беспроводного доступа,
- персональных компьютеров,
- сетевых принтеров и т.д.



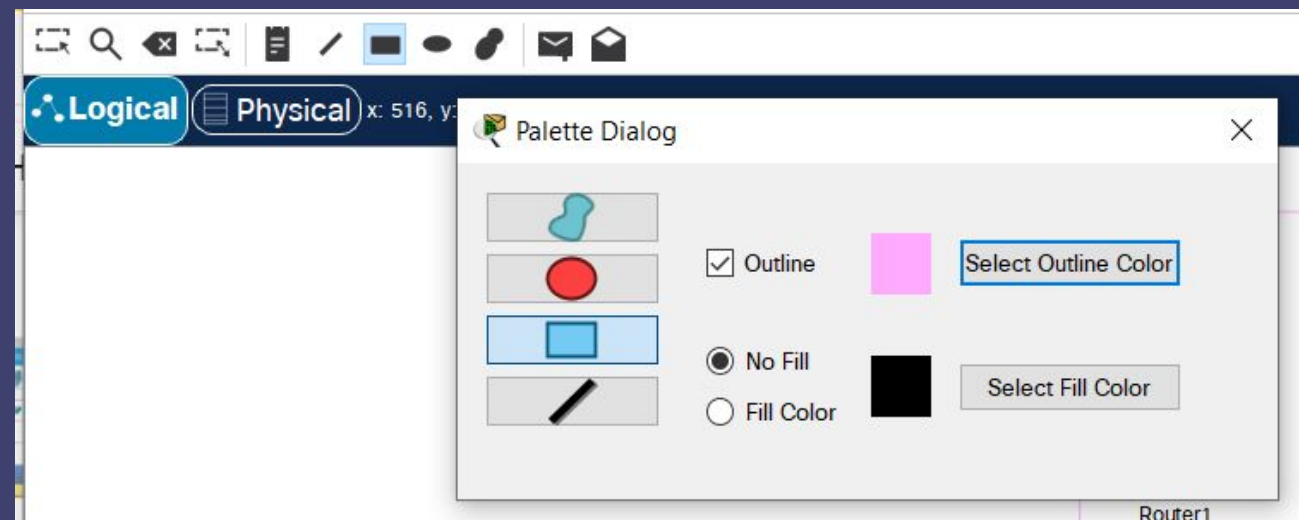
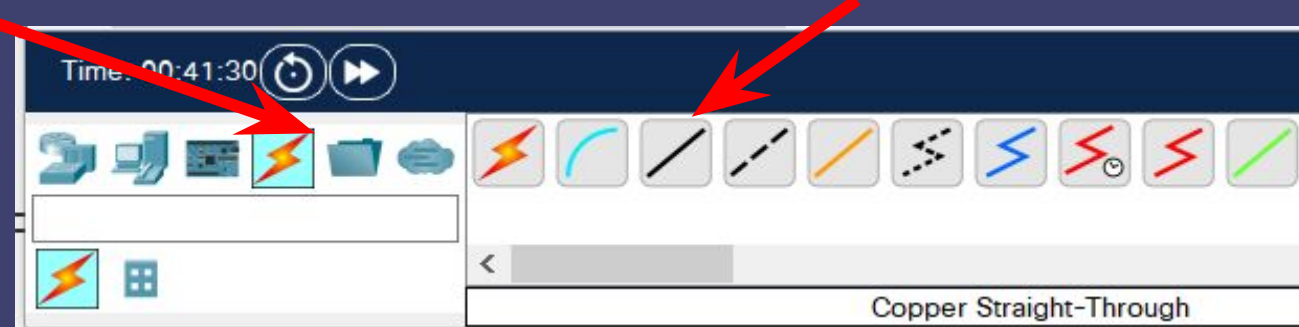
Рабочее окно Packet Tracer



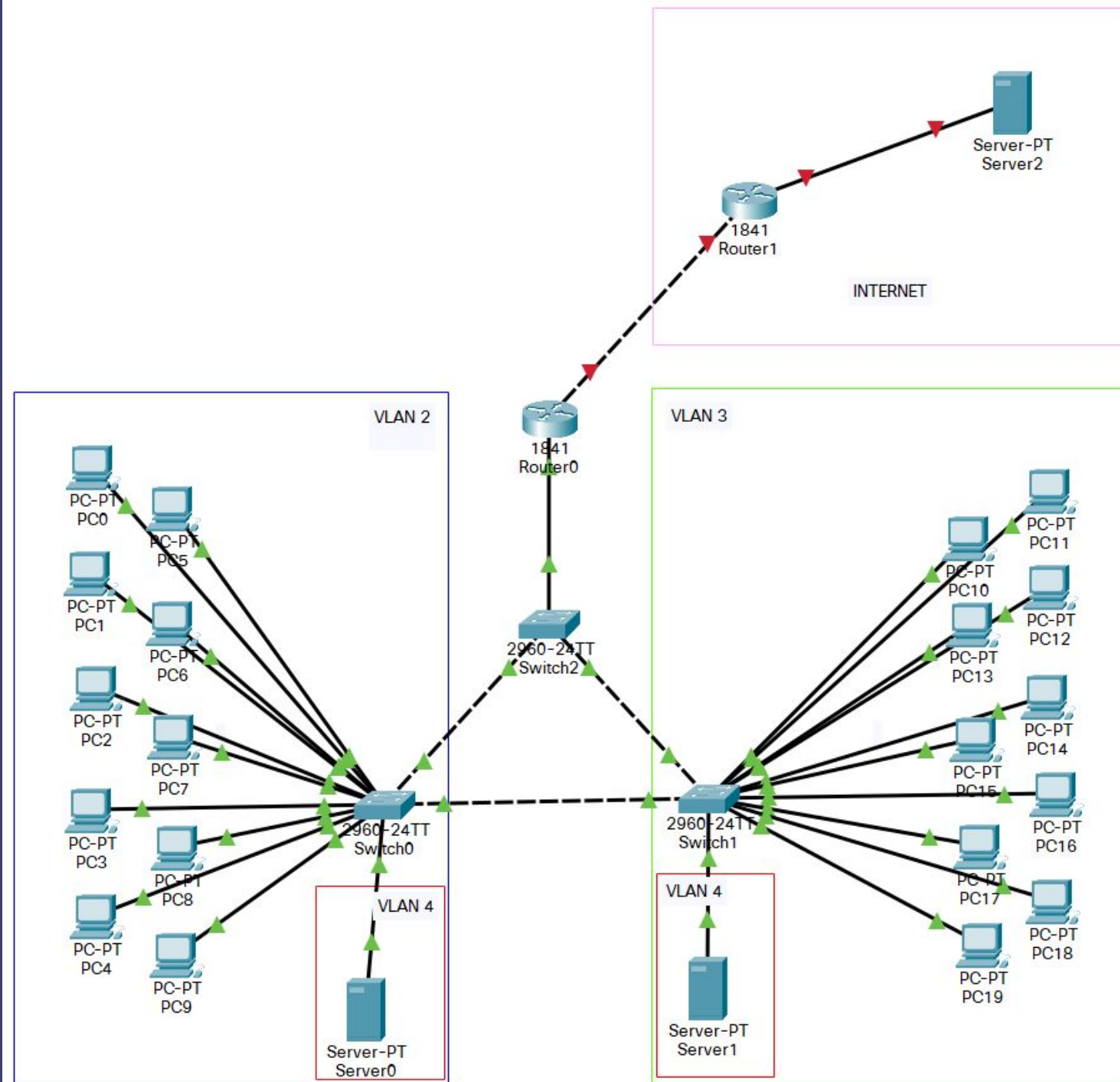
Перетаскивая из панели
оборудования нужные нам
устройства сделаем схему сети



- Выберем в панели инструментов группу “Connection” а затем в поле справа “cooper straight” кабель и соединим между компьютеры и серверы с коммутаторами, а также роутеры
- Соединим коммутаторы между собой кроссовым кабелем
- Разделим нашу схему на блоки используя панель для выделения объектов и подпишем выделенные блоки (для удобства понимания схемы)



Получилась вот такая
схема



Настроим Switch 0

```
Switch>en
```

```
Switch#conf t
```

```
Switch(config)#vlan 2
```

```
Switch(config-vlan)#name VLAN2
```

```
Switch(config)#interface range fastEthernet 0/1-10
```

```
Switch(config-if-range)#switchport mode access
```

```
Switch(config-if-range)#switchport access vlan 2
```

```
Switch(config)#Interface fastEthernet 0/24
```

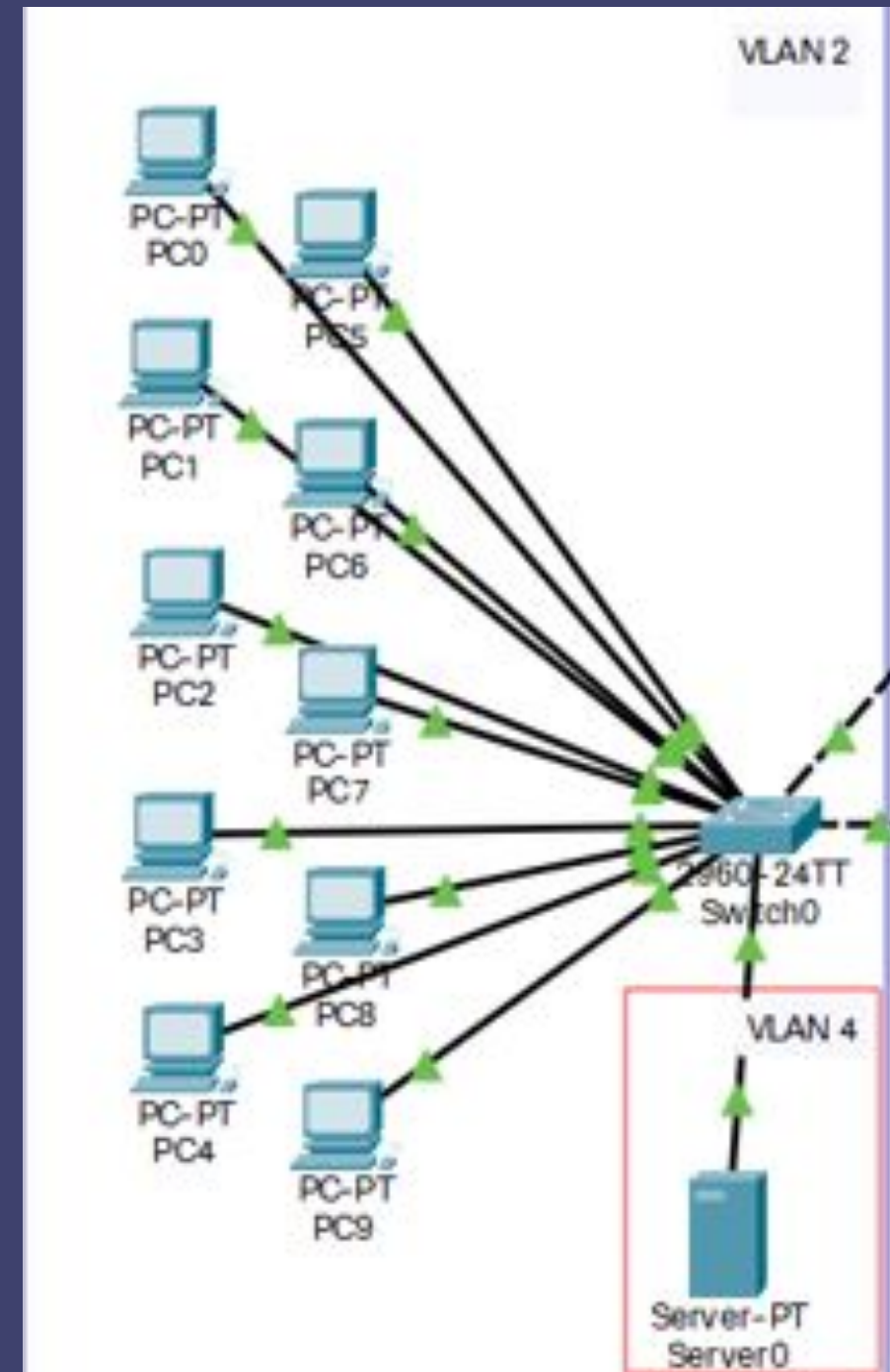
```
Switch(config-if)#switchport mode access
```

```
Switch(config-if)#switchport access vlan 4
```

```
config)#interface range fastEthernet 0/21-22
```

```
Switch(config-if-range)#switchport mode trunk
```

```
Switch(config-if-range)#switchport trunk allowed vlan 2-4
```



Настроим Switch 2

```
config)#interface range fastEthernet 0/21-22  
Switch(config-if-range)#switchport mode trunk  
Switch(config-if-range)#switchport trunk allowed vlan 2-4
```

```
config)#interface vlan 2
```

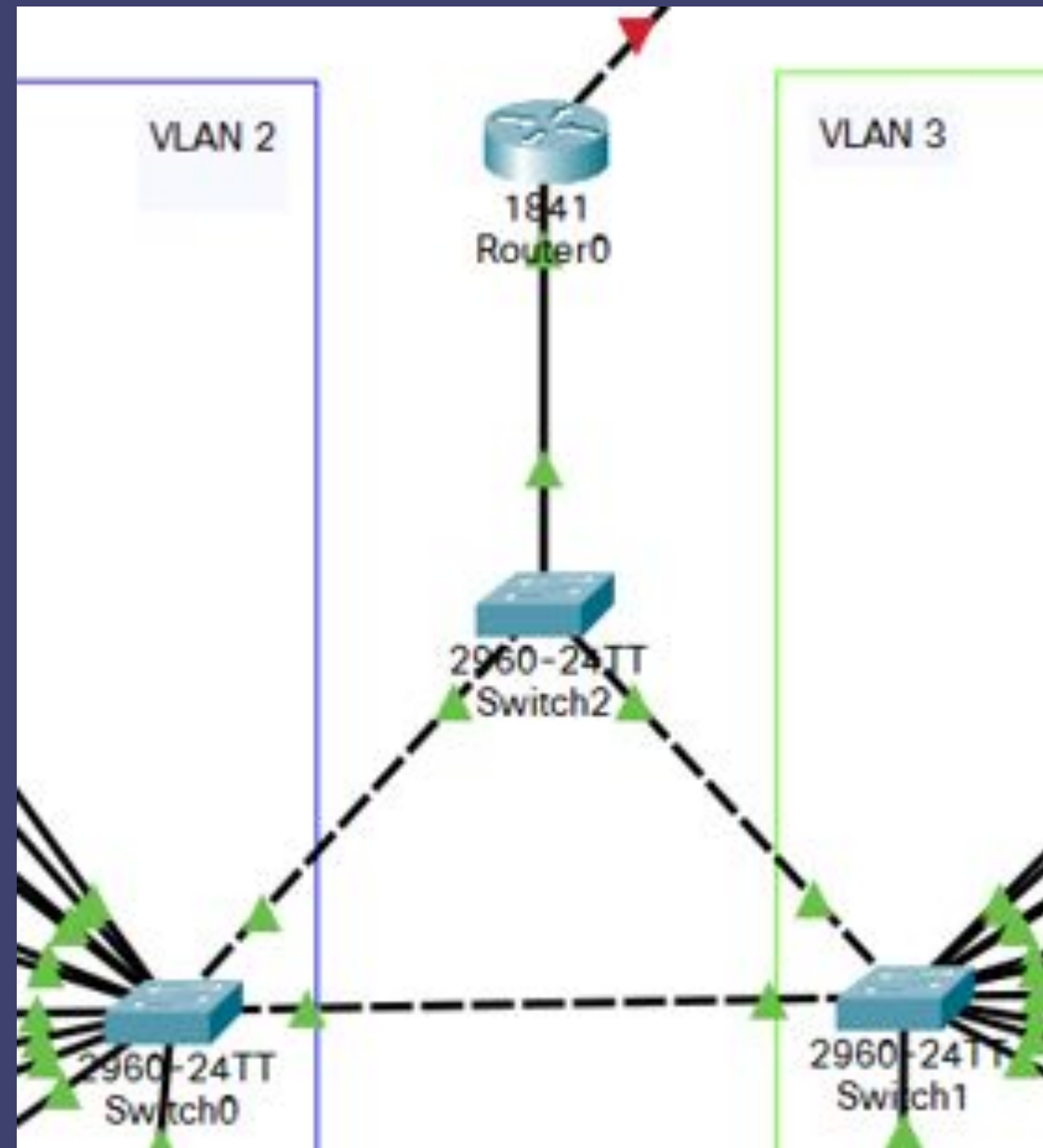
```
config)#ex
```

```
config)#interface vlan 3
```

```
config)#ex
```

```
config)#interface vlan 4
```

И если



Настроим DHCP на Server 0

Для настройки перейдём во вкладку services и выберем пункт DHCP

Настроим DHCP Сервер на выдачу IP-адресов для Vlan 2 и Vlan 3

По завершению ввода диапазона адресов, названия пула, стартового IP, и пути по умолчанию нажать кнопку ADD

Но компьютеры не получают свои адреса т.к ещё не настроен Router 0 который является ядром этой сети и через него проходят все сообщения пересылаемые в данной схеме

Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

HTTP

DHCP

DHCPv6

TFTP

DNS

SYSLOG

AAA

NTP

EMAIL

FTP

IoT

VM Management

Radius EAP

Interface

FastEthernet0

Service ☒ On

Pool Name

VLAN3

Default Gateway

192.168.3.1

DNS Server

0.0.0.0

Start IP Address :

192

168

3

Subnet Mask:

255

255

255

Maximum Number of Users :

100

TFTP Server:

0.0.0.0

WLC Address:

0.0.0.0

Add

Save

Pool Name	Default Gateway	DNS Server	Start IP Address	Subnet Mask
VLAN3	192.168.3.1	0.0.0.0	192.168.3.100	255.255.255.0
VLAN2	192.168.2.1	0.0.0.0	192.168.2.100	255.255.255.0
serverPool	0.0.0.0	0.0.0.0	192.168.4.0	255.255.255.0

Настроим Router 0

```
Router(config)#interface fastEthernet 0/0.2
```

```
Router(config-subif)#encapsulation dot1Q 2
```

```
Router(config-subif)#ip address 192.168.2.1 255.255.255.0
```

Далее настроим саб интерфейсы для других вланов и dhcp relay чтобы запросы на получение IP доходили до Server 0.

```
Router(config)#interface fastEthernet 0/0.3
```

```
Router(config-subif)#encapsulation dot1Q 3
```

```
Router(config-subif)#ip address 192.168.3.1 255.255.255.0
```

```
Router(config-subif)#ex
```

```
Router(config)#interface fastEthernet 0/0.4
```

```
Router(config-subif)#encapsulation dot1Q 4
```

```
Router(config-subif)#ip address 192.168.4.1 255.255.255.0
```

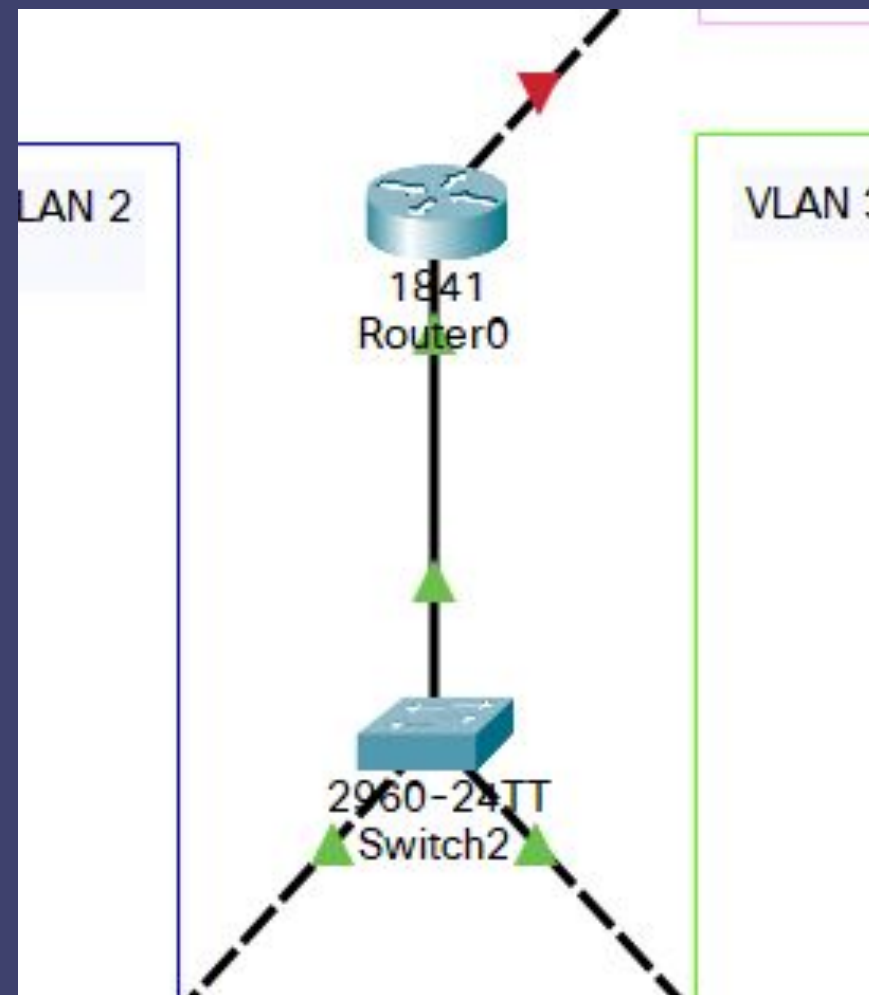
```
Router(config)#interface fastEthernet 0/0.2
```

```
Router(config-subif)#ip helper-address 192.168.4.10
```

```
Router(config-subif)#ex
```

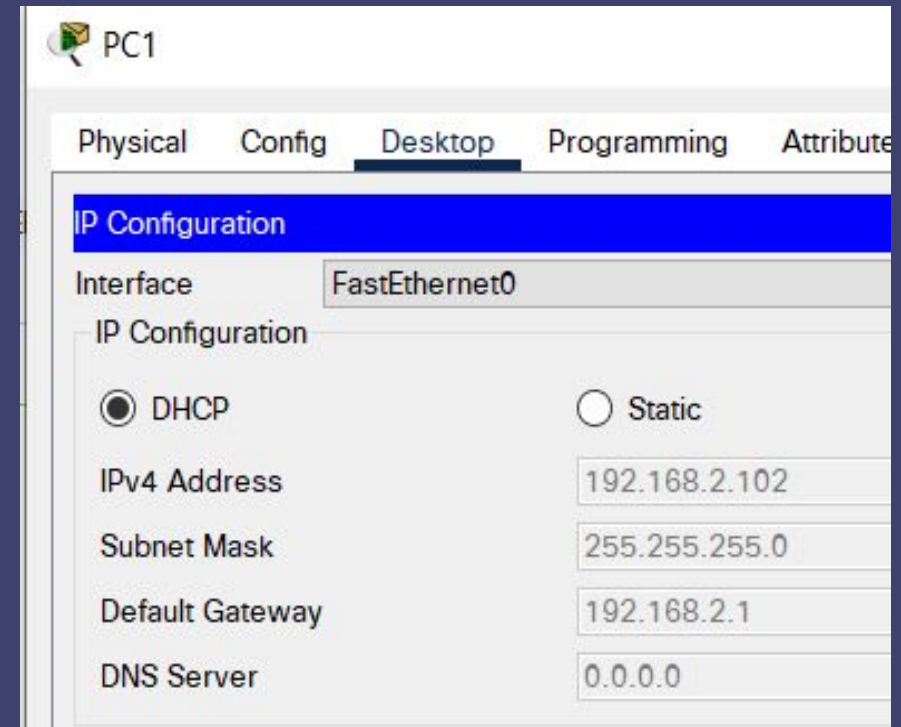
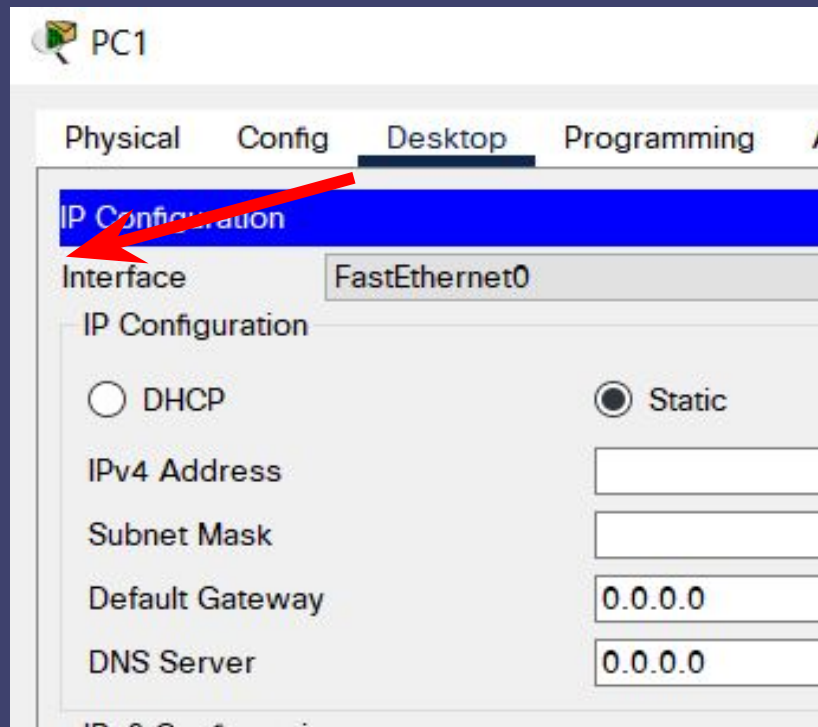
```
Router(config)#interface fastEthernet 0/0.3
```

```
Router(config-subif)#ip helper-address 192.168.4.10
```



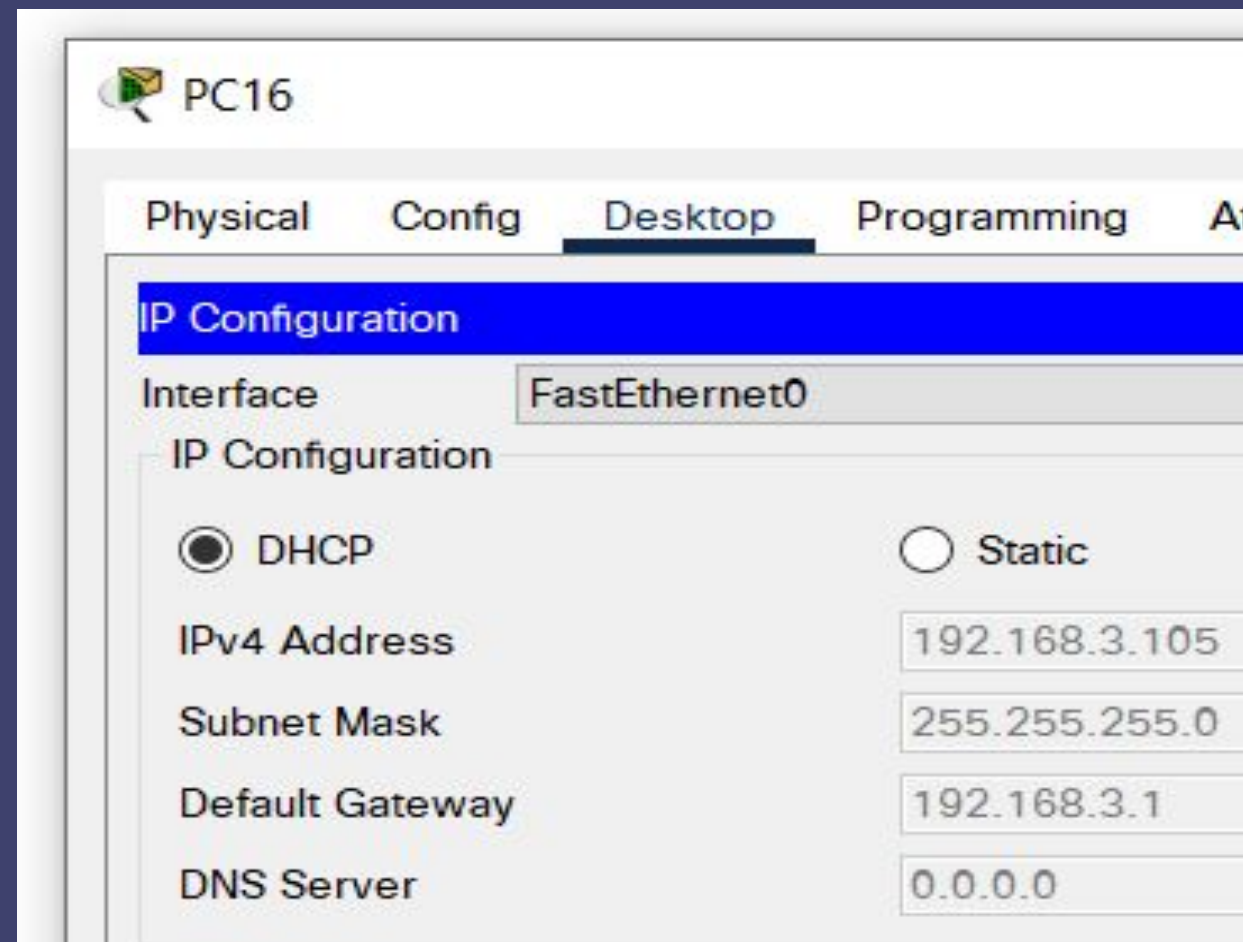
Проверим работоспособность.

Перейдём на интерфейс ПК1 и поставим ему динамическое получение IP-адреса



проверим как ip присвоится в соседнем VLAN 3, сделаем те же действия выставив галочку на пункте DHCP.

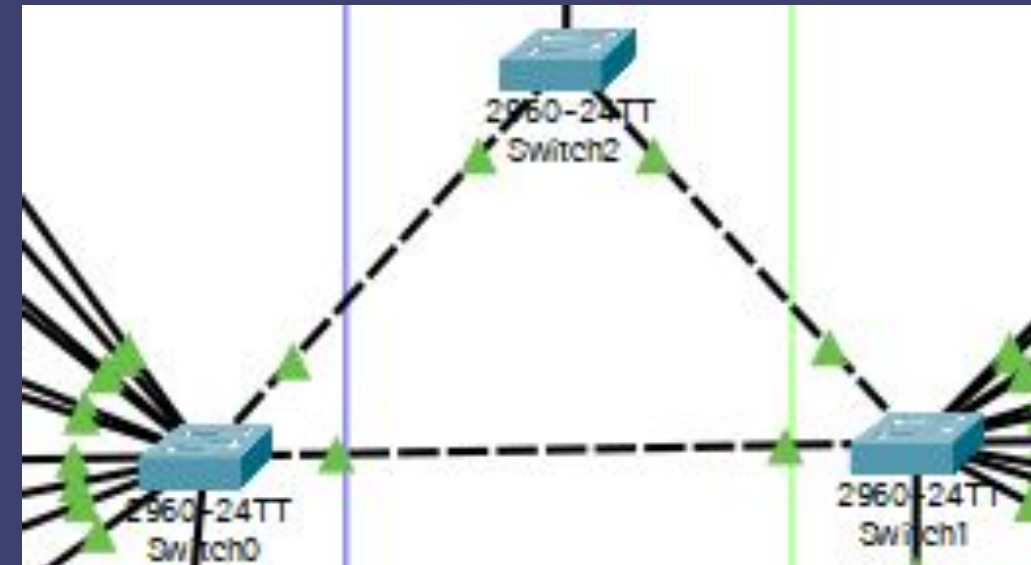
Как видно присвоение ip прошло верно



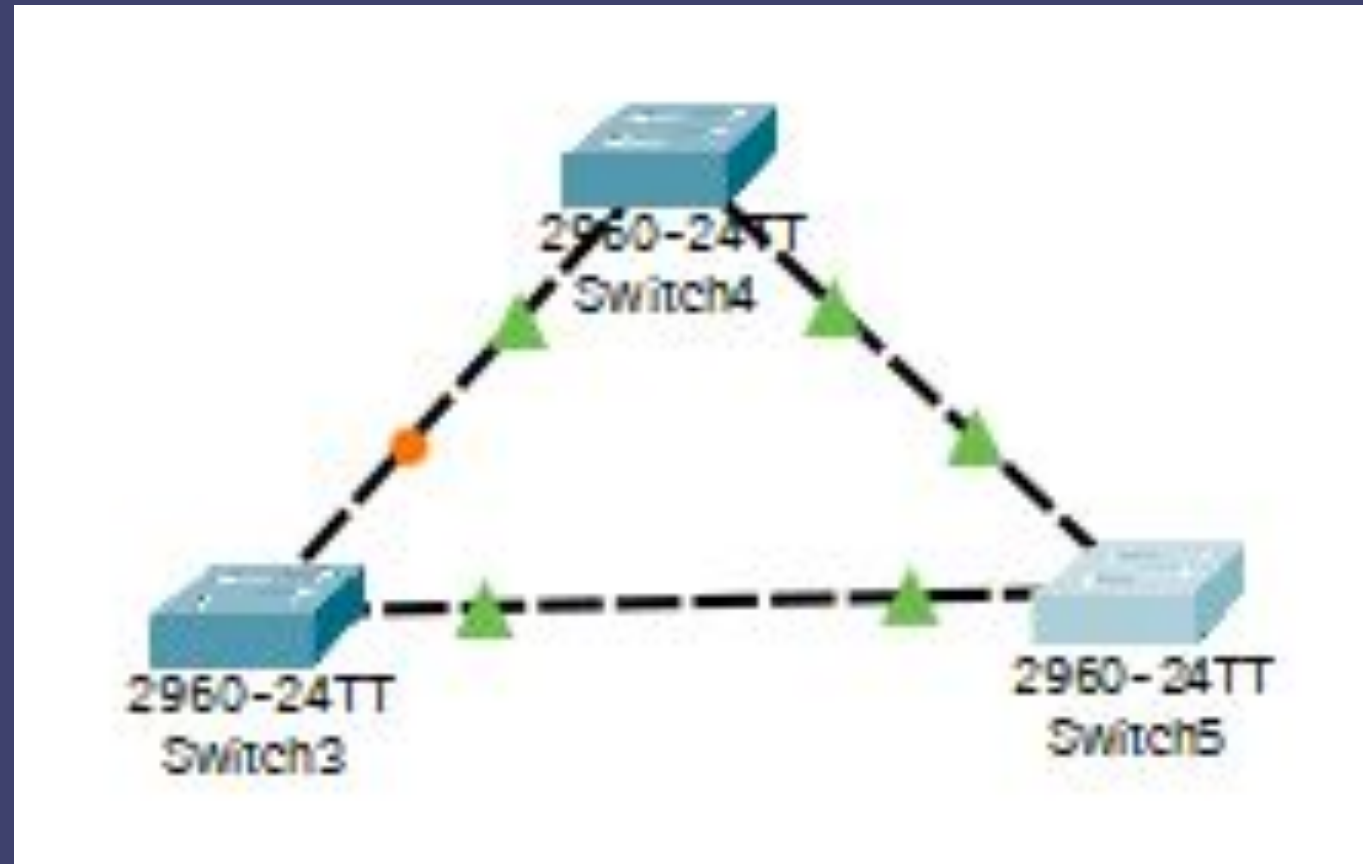
Настроим STP

Между 3-мя коммутаторами образовалась петля (но в нашем случае т.к. настроены VLAN, и протокол *PVST автоматически работает на оборудование CISCO и предотвращает появление сетевого шторма (петли нет))

***Per-VLAN Spanning Tree (PVST)** — проприетарный протокол компании Cisco Systems, который для каждого VLAN строит отдельное дерево. Он предполагает использование ISL для создания транков (тегированных портов) и позволяет порту быть заблокированным для одних VLAN и разблокированным для других.

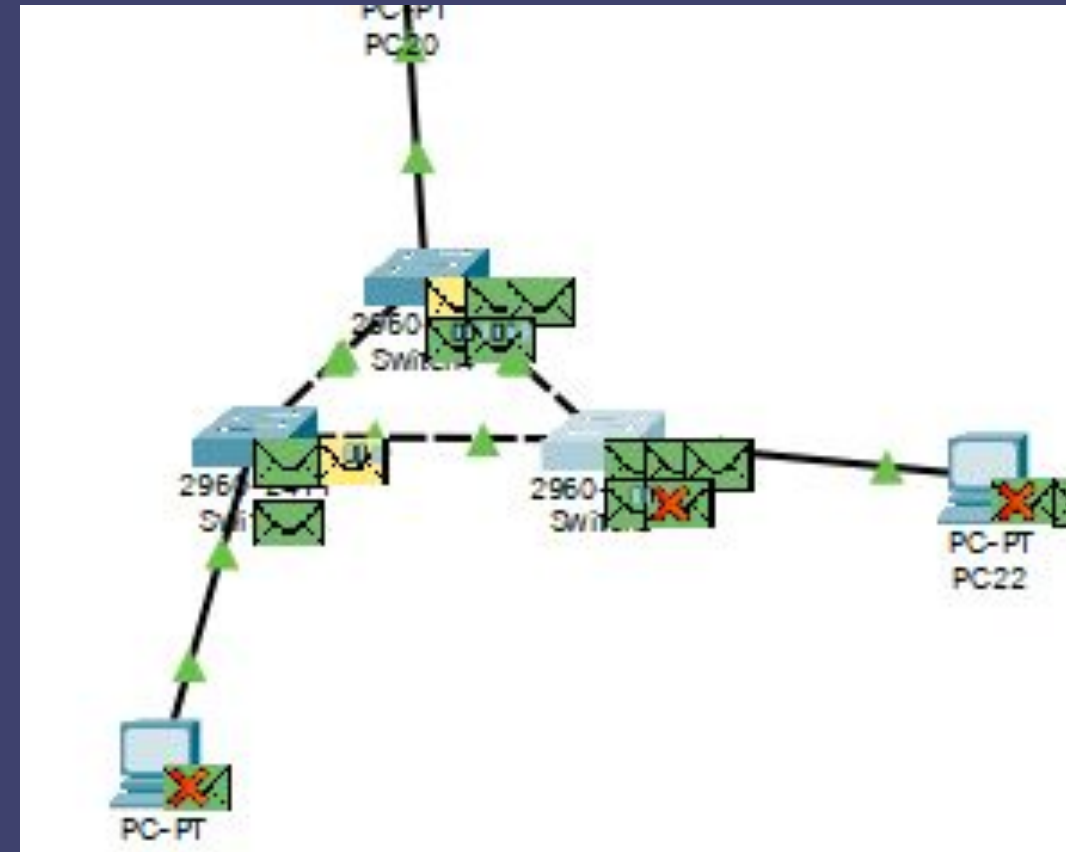


Так выглядит схема коммутаторов в которой у одного из них порт находится в заблокированном состоянии для предотвращения появления петли, которая создаст *широковещательный шторм



*Размножение широковещательных сообщений активным сетевым оборудованием приводит к экспоненциальному росту их числа и парализует работу сети.

Если принудительно выключить STP на коммутаторах то это приведёт к тому что каждое широковещательное сообщение будет дублироваться и постоянно пересылаться между всеми участниками петли что приведёт к переполнению и перегрузке сети и заметно снизит скорость передачи данных



Команда # no spanning-tree vlan X
- Для выключения алгоритма (не рекомендуется)

Роли и состояния портов

Роли портов:

- Root Port — корневой порт коммутатора
- Designated Port — назначенный порт сегмента
- Nondesignated Port — неназначенный порт сегмента
- Disabled Port — порт который находится в выключенном состоянии.

Состояния портов:

- Blocking — блокирование
- Listening — прослушивание
- Learning — обучение
- Forwarding — пересылка

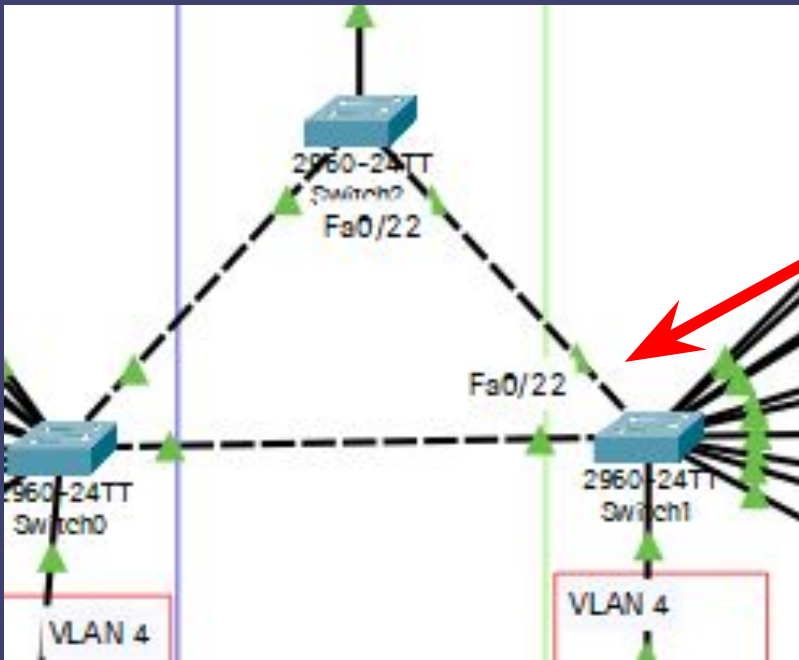
На картинке справа можно увидеть что для vlan4
данный коммутатор не является корневым
Имеет приоритет 32772
порт Fa0/21 является корневым портом т.к. смотрит в
сторону корневого коммутатора switch 0
Остальные два порта являются назначенными
И все порты могут пересылать данные

```
VLAN0004
Spanning tree enabled protocol ieee
Root ID      Priority      32772
              Address      0001.9626.E840
              Cost        19
              Port        21(FastEthernet0/21)
              Hello Time   2 sec   Max Age 20 sec   Forward Delay

Bridge ID     Priority      32772  (priority 32768 sys-id-ext 4)
              Address      0060.70D2.127D
              Hello Time   2 sec   Max Age 20 sec   Forward Delay
              Aging Time   20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0/21         Root FWD 19        128.21  P2p
Gi0/1          Desg FWD 19        128.25  P2p
Fa0/22         Desg FWD 19        128.22  P2p
```

На картинке справа настройки с switch 1
И как видно для 1 влана 22 порт находится в выключенном состоянии хотя на схеме это и не отображается
И в случае когда связь между двумя другими коммутаторам и прервётся данный линк сам поднимется и трафик пойдёт через него.



```
VLAN0001
Spanning tree enabled protocol ieee
Root ID      Priority      32769
              Address      0001.9626.E840
              Cost        19
              Port        12 (FastEthernet0/12)
              Hello Time   2 sec   Max Age 20 sec   Forward Delay 15 sec

Bridge ID     Priority      32769 (priority 32768 sys-id-ext 1)
              Address      00E0.F78A.AE1D
              Hello Time   2 sec   Max Age 20 sec   Forward Delay 15 sec
              Aging Time   20
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/12	Root	FWD	19	128.12	P2p
Fa0/21	Desg	FWD	19	128.21	P2p
Fa0/22	Altn	BLK	19	128.22	P2p

Выбор корневого коммутатора происходит по MAC адресу, чем меньше размер адреса тем больше вероятность стать корневым устройством, и чтобы по случайности менее производительное оборудование не стало корневым настроим приоритет сами используя команды :

Spanning-tree vlan X priority

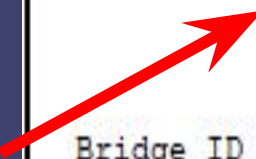
Spanning-tree vlan X root primary

Spanning-tree vlan X rapid-pvst (для включения более быстрой версии STP)

```
Switch#sh spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0001.9626.E840
             This bridge is the root
  Hello Time 2 sec    Max Age 20 sec    Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
             Address     0001.9626.E840
             Hello Time 2 sec    Max Age 20 sec    Forward Delay 15 sec
             Aging Time 20

Interface Role Sts Cost Prio.Nbr Type
-----
Fa0/12 Desg FWD 19 128.12 P2p
Fa0/22 Desg FWD 19 128.22 P2p
Fa0/21 Desg FWD 19 128.21 P2p
```

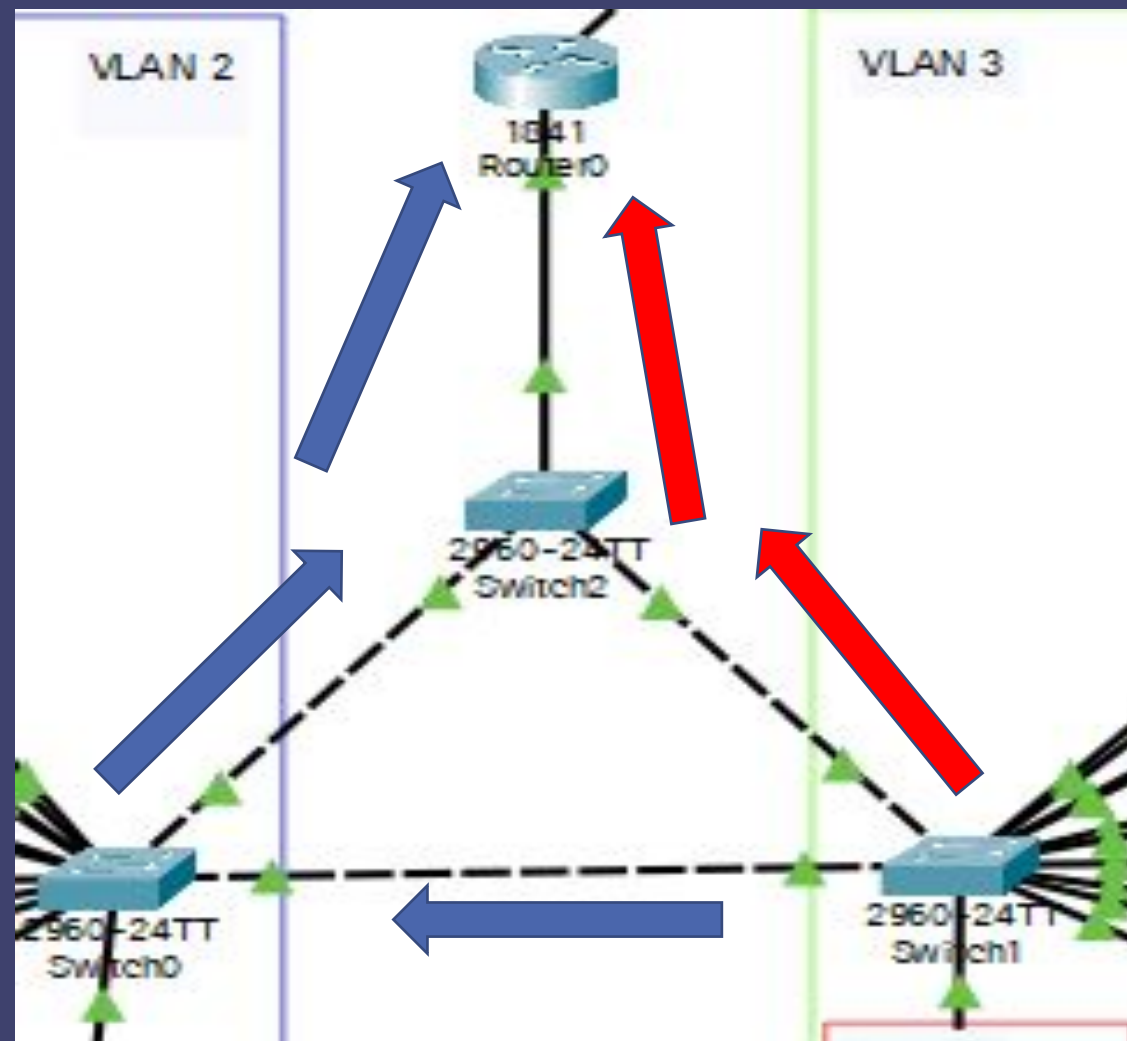


Командой #show spanning-tree можно увидеть текущие настройки, и switch 0 оказался корневым коммутатором

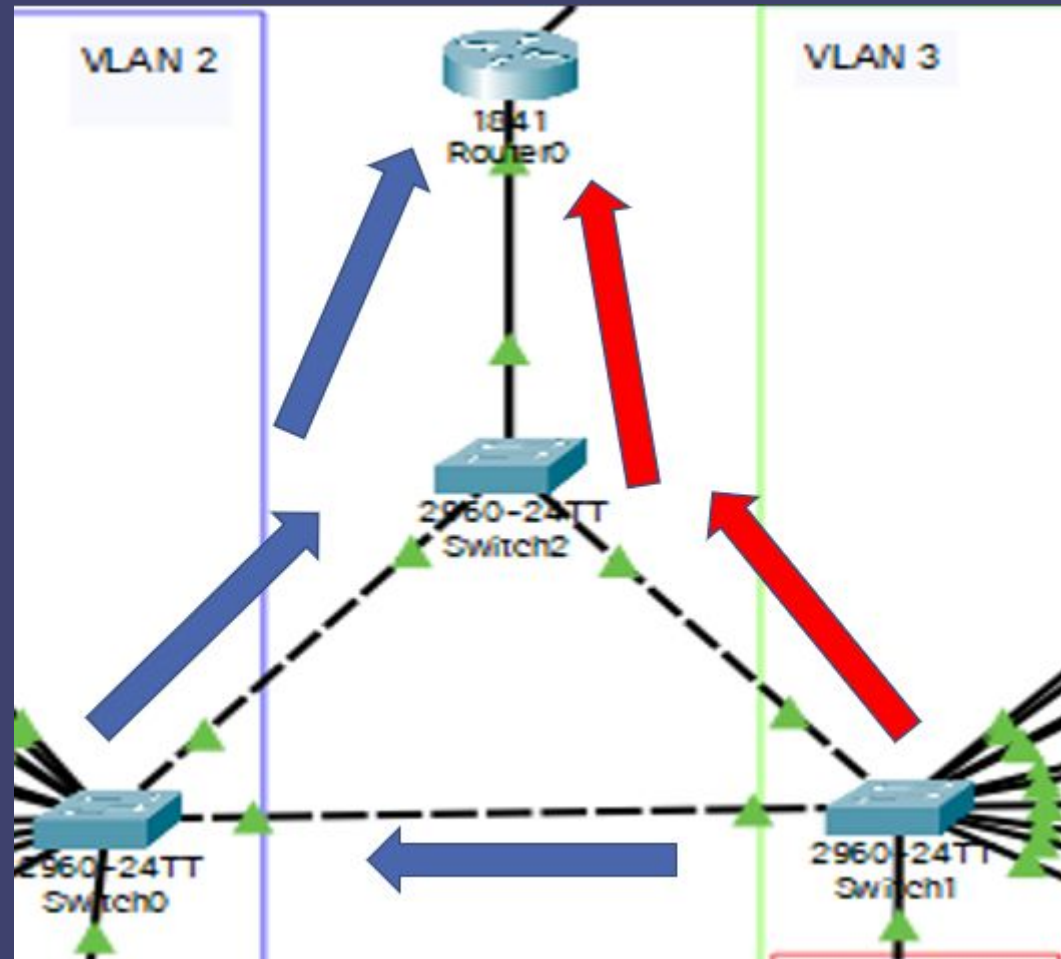
Изначально трафик 3-го VLAN следует по синим стрелкам но после присвоения приоритета трафик пойдёт по красным стрелкам, что как минимум быстрее (из последовательности пропал 1 лишний маршрут)

зададим switch 1 приоритет командой:

```
#Spanning-tree vlan 3 priority 4096
```



Проверим работу STP в деле
зайдём на любой компьютер
из vlan 3 и запустим пинг в
сторону router0 (трафик
пойдёт по красным
стрелкам, но если линия
оборвётся трафик
переключится на новую
линию и пойдёт по синим)



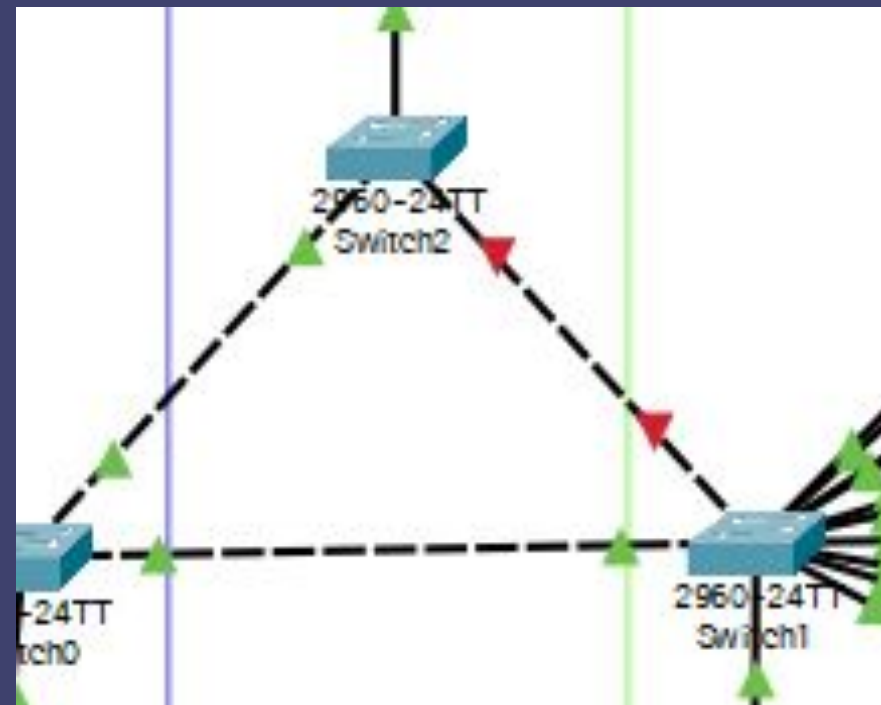
Как видно связь есть, а теперь

```
^C
C:\>ping -t 192.168.3.1

Pinging 192.168.3.1 with 32 bytes of data:

Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
Reply from 192.168.3.1: bytes=32 time=2ms TTL=255
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
```

выключим 22 порт коммутатора 1



Несколько пакетов потерялась, но вскоре связь была восстановлена, что говорит о том что STP протокол работает, но за время переключения было потеряна информация и чтобы минимизировать потери был придуман протокол RSTP (rapid STP)

```
Reply from 192.168.3.1: bytes=32 time=2ms TTL=255
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
Reply from 192.168.3.1: bytes=32 time=2ms TTL=255
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255
```

Настроим RSTP на всех свичах командой

Switch(config)#spanning-tree mode rapid-pvst

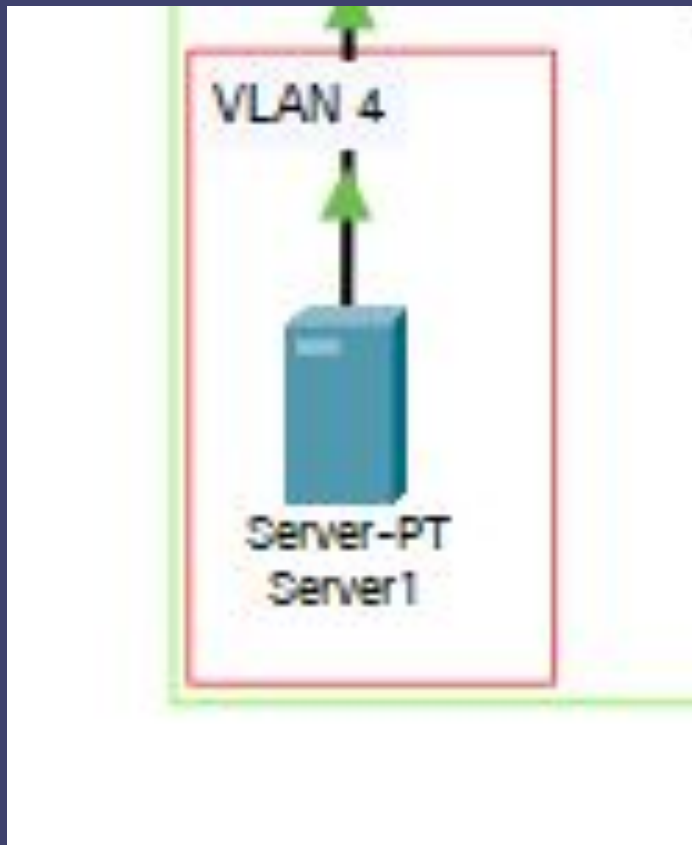
И снова выключим 22 порт

```
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255  
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255  
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255  
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255  
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255  
Request timed out.  
Reply from 192.168.3.1: bytes=32 time=1ms TTL=255  
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255  
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255  
Reply from 192.168.3.1: bytes=32 time<1ms TTL=255  
Reply from 192.168.3.1: bytes=32 time=4ms TTL=255
```

Как видно был потерян только 1 пакет

Настроим WEB-сервер на server1

Перейдём в его интерфейс во вкладку сервисов HTTP переключим кнопку на положение ON



glcal Physical x: 776, y: 831

Server1

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

HTTP

☒ On ☐ Off

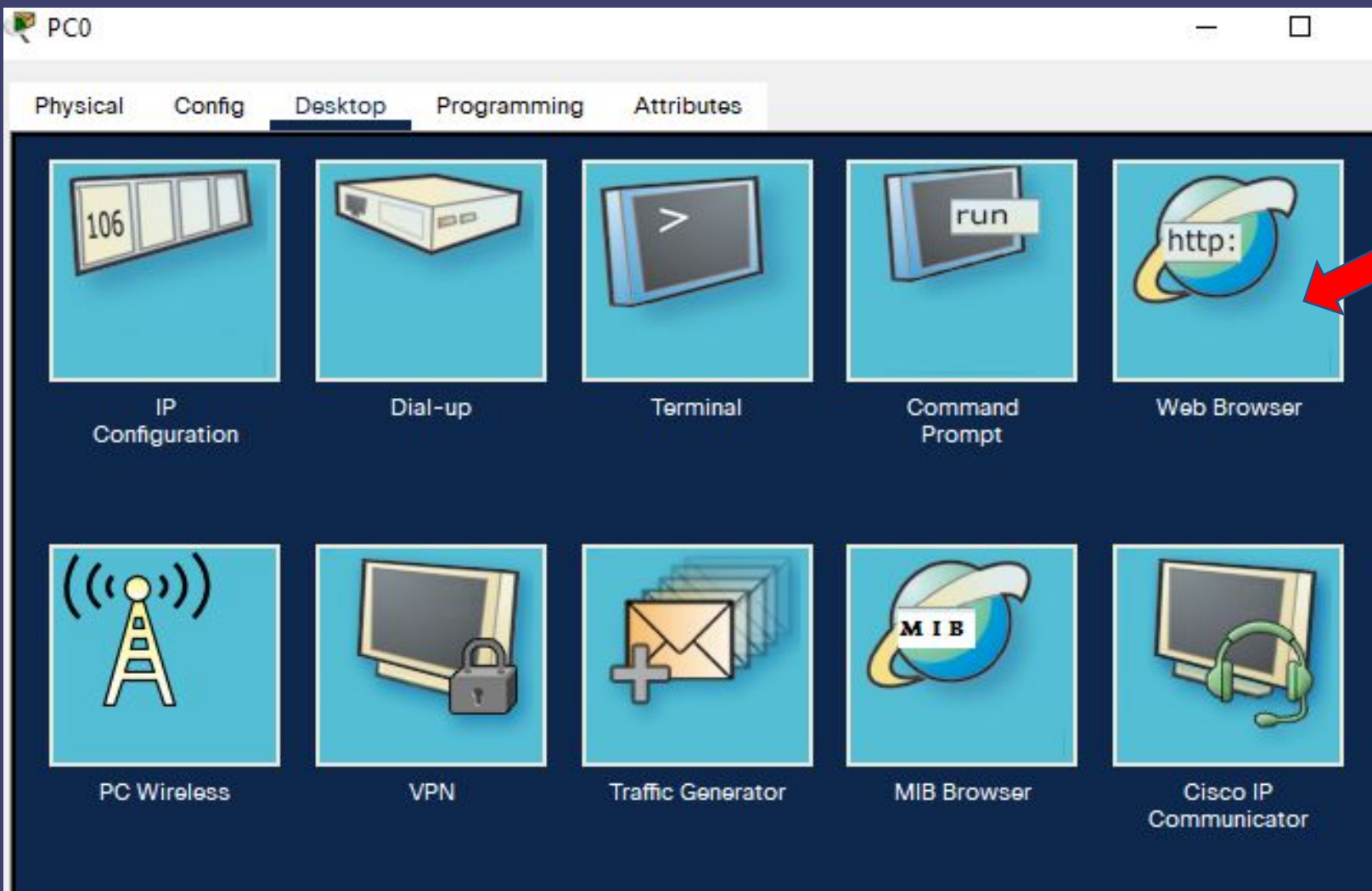
HTTPS

☒ On ☐ Off

File Manager

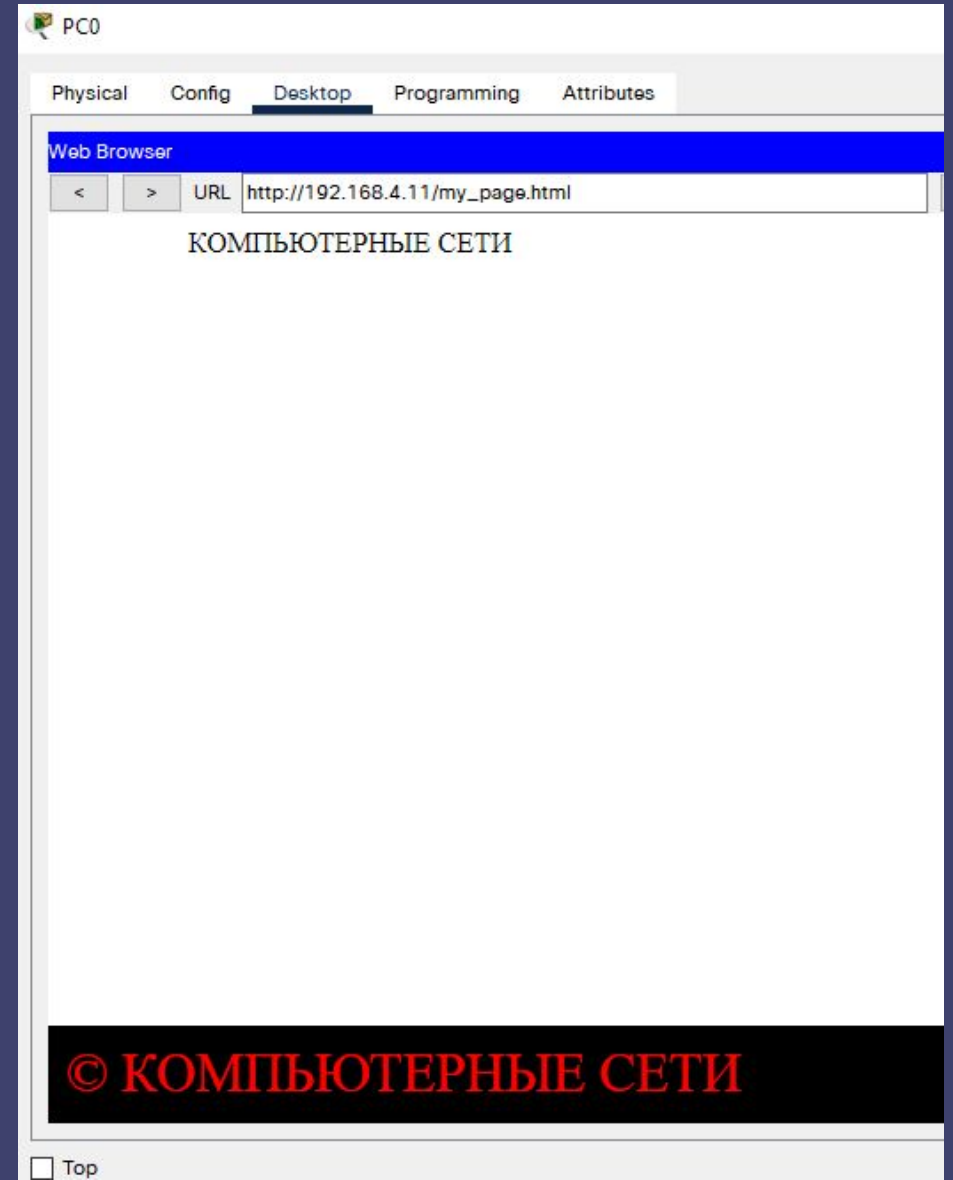
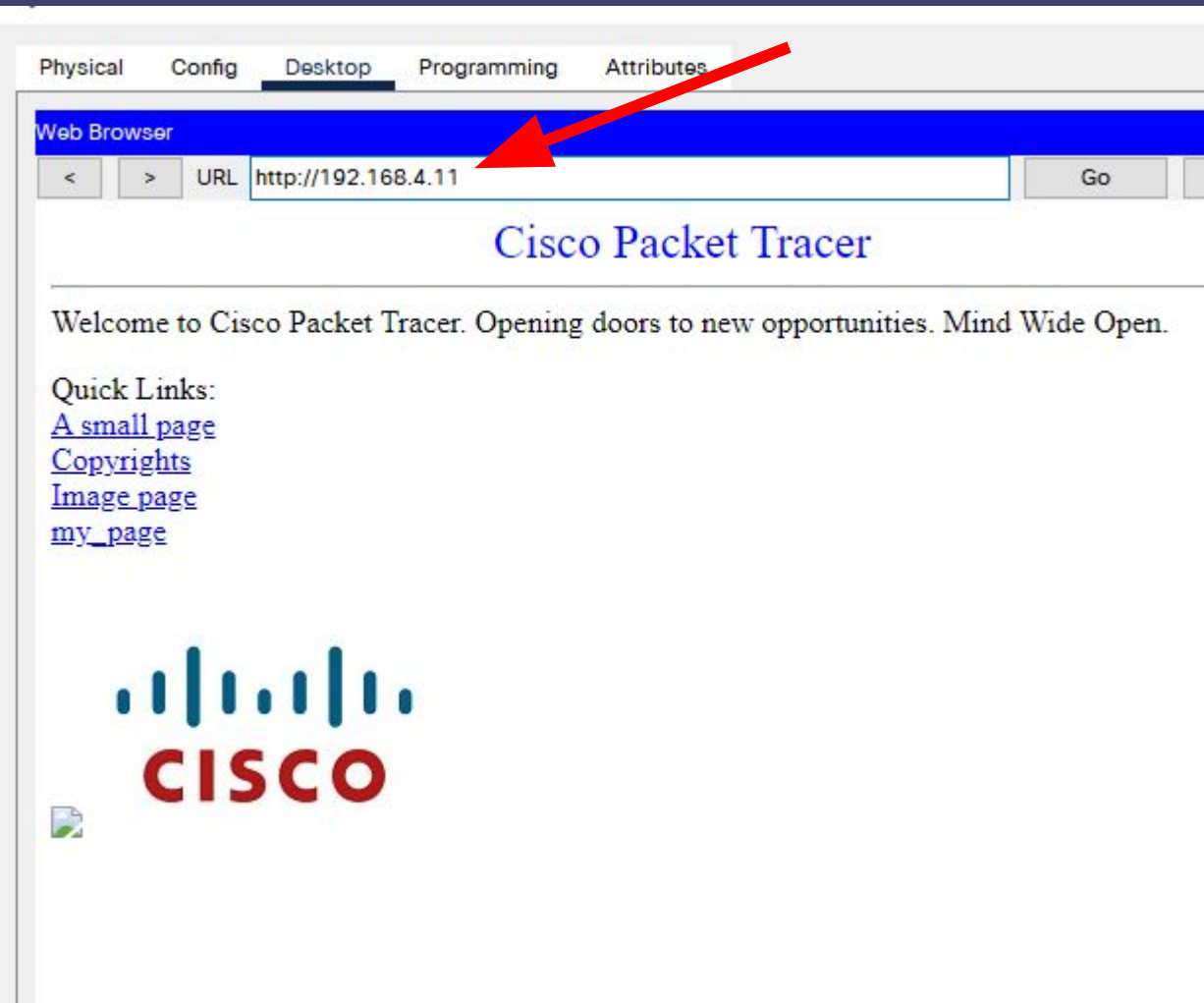
	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

Проверим его работоспособность с компьютера PC 0



Перейдём во вкладку WEB-browser
И пропишем в поисковой строке
ip адрес web-сервера

Web-сервер работает и к нему есть доступ



NAT

NAT переводит приватные адреса, в общедоступные. Это позволяет устройству с частным адресом IPv4 обращаться к ресурсам за пределами его частной сети.

NAT в сочетании с частными адресами IPv4 оказался полезным методом сохранения общедоступных IPv4-адресов. Один общедоступный IPv4-адрес может быть использован сотнями, даже тысячами устройств, каждый из которых имеет частный IPv4-адрес.

NAT имеет дополнительное преимущество, заключающееся в добавлении степени конфиденциальности и безопасности в сеть, поскольку он скрывает внутренние IPv4-адреса из внешних сетей.

Класс	Диапазоны публичных IP-адресов
A	1.0.0.0 - 9.255.255.255 11.0.0.0 - 126.255.255.255
B	128.0.0.0 - 172.15.255.255 172.32.0.0 - 191.255.255.255
C	192.0.0.0 - 192.167.255.255 192.169.0.0 - 223.255.255.255

IP-адреса для локальных сетей

Диапазоны частных (private) IP-адресов:

10.0.0.0—10.255.255.255

172.16.0.0—172.31.255.255

192.168.0.0—192.168.255.255

Настроим оборудование:

Router-Provider

```
Router#conf t
```

```
Router(config)#interface fa0/0    //fa0/0 смотрит в сторону Router0
```

```
Router(config-if)#ip address 210.224.15.1 255.255.255.0
```

```
Router(config-if)#no sh
```

```
Router#conf t
```

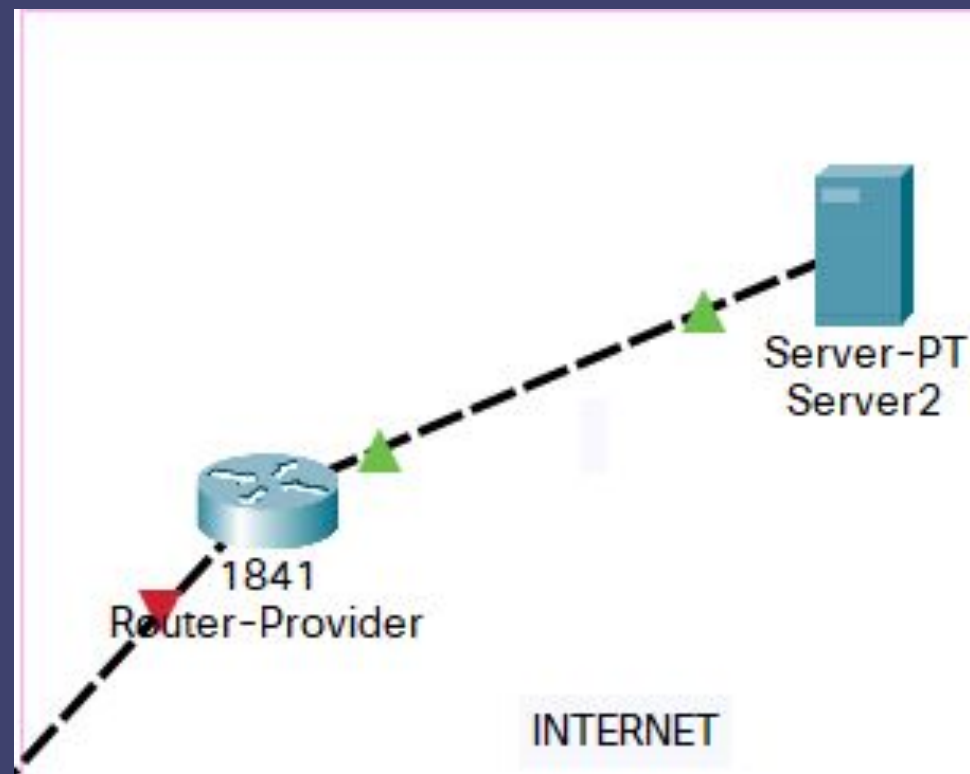
```
Router(config)#interface fa0/0    //fa0/1 смотрит в сторону Server2
```

```
Router(config-if)# ip address 215.243.165.1 255.255.255.0
```

```
Router(config-if)#no sh
```

А также задать путь по умолчанию в сторону провайдера командой

```
Router(config)#ip route 0.0.0.0 0.0.0.0 210.224.15.1
```



Пример синтаксиса команд

Определяются внешние\внутренние интерфейсы

Создаётся список доступа для адресов которые будут использоваться NAT

Команда включения PAT на внешнем интерфейсе

Настройка PAT

```
interface FastEthernet0/0
ip nat outside
interface FastEthernet0/1.2
ip nat inside
interface FastEthernet0/1.3
ip nat inside
```

```
ip access-list standard FOR-NAT
permit 192.168.2.0 0.0.0.255
permit 192.168.3.0 0.0.0.255
```

```
ip nat inside source list FOR-NAT interface FastEthernet0/0 overload
```

Настройка Static NAT

```
ip nat inside source static tcp 192.168.3.2 80 213.234.10.2 80
```

```
show ip nat translations
```


Настроим Router 0

```
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip nat outside

Router(config)#interface fastEthernet 0/0.2
Router(config-subif)#ip nat inside
Router(config-subif)#ex

Router(config)#interface fastEthernet 0/0.3
Router(config-subif)#ip nat inside
Router(config-subif)#ex

Router(config)#interface fastEthernet 0/0.4
Router(config-subif)#ip nat inside
```

Создадим аксес листы для того чтобы разрешить доступ к интернету нужным нам адресам (например разрешим компьютерам из 2-го влана доступ к сети а из 3-го нет)

```
Router(config)#ip access-list standard FOR_NAT
Router(config-std-nacl)#permit 192.168.2.0 0.0.0.255
Router(config-std-nacl)#permit 192.168.4.11 0.0.0.255 //это вэб сервер (Server1)
```

Далее пропишем команду для настройки PAT

```
Router(config)#ip nat inside source list FOR_NAT interface fastEthernet 0/1 overload
```

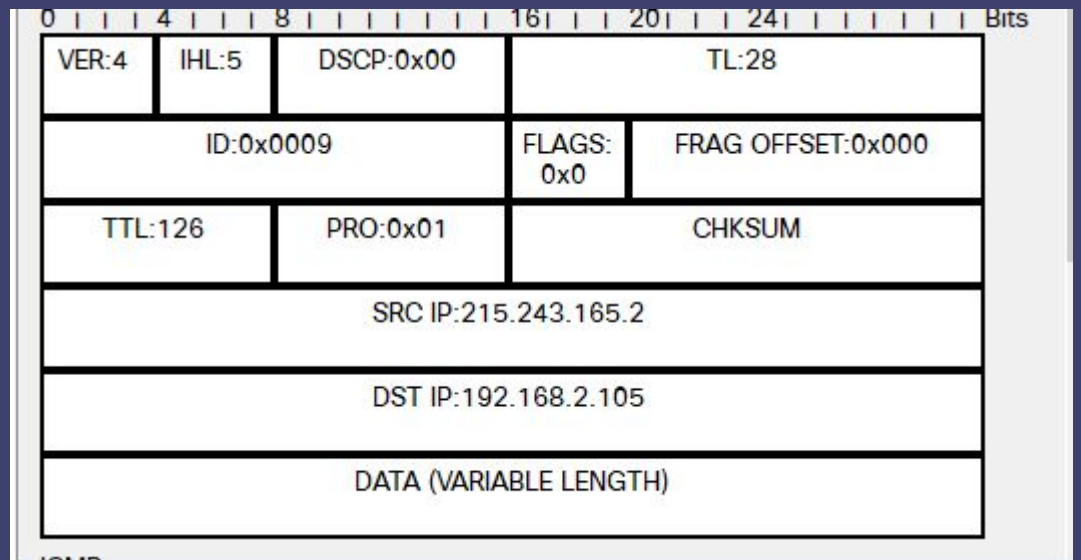
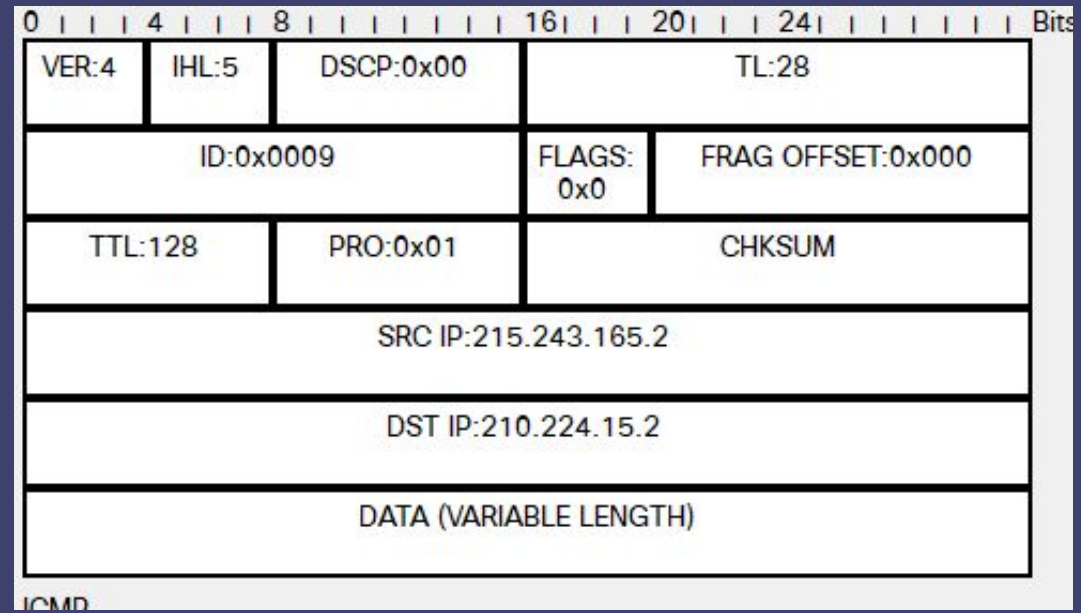
Работа NAT в действии

Отправим pdu сообщение с PC5 до Server2 и перехватим содержимое пакета до и после прохождения через Router0 при отправке и при возврате (возврат на след. слайде)

VER:4	IHL:5	DSCP:0x00	TL:28	
ID:0x0008			FLAGS: 0x0	FRAG OFFSET:0x000
TTL:255		PRO:0x01	CHKSUM	
SRC IP:192.168.2.105				
DST IP:215.243.165.2				
DATA (VARIABLE LENGTH)				

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
VER:4				IHL:5				DSCP:0x00								TL:28															
ID:0x0008												FLAGS: 0x0				FRAG OFFSET:0x000															
TTL:254								PRO:0x01								CHKSUM															
SRC IP:210.224.15.2																															
DST IP:215.243.165.2																															
DATA (VARIABLE LENGTH)																															

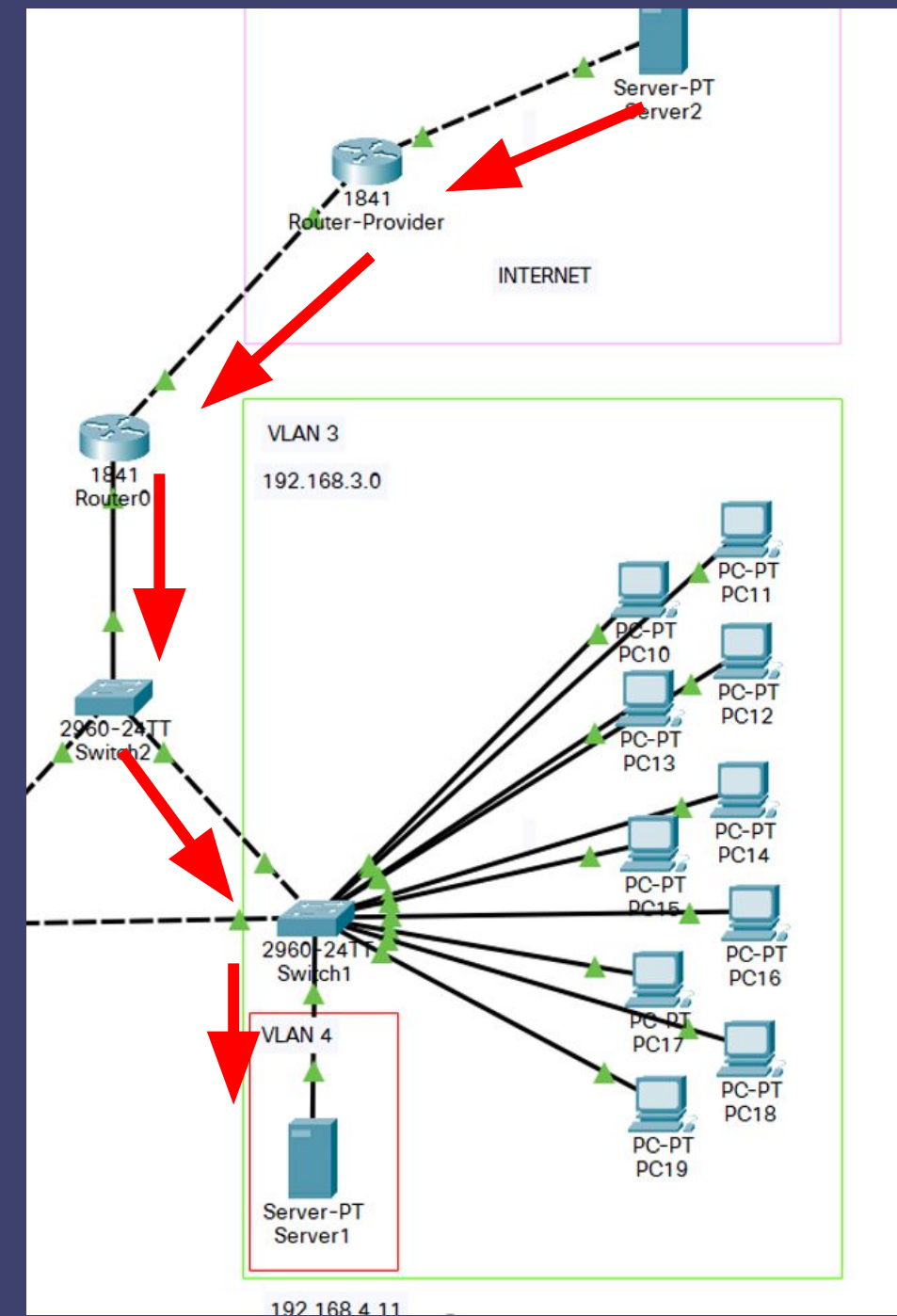
Как можно заметить при
прохождение Router 0, на
котором настроен PAT
ip-address меняется с серого
на белый и наоборот при
обратном получении пакета



Для того чтобы из интернета можно было попасть на локальный web server (Server1) нужно настроить Static NAT

Пропишем на Роутере 0 команду

```
Router(config)#ip nat inside source static tcp 192.168.4.11 80  
210.224.15.2 80
```



Проверим доступность к локальному серверу, для этого введём в строке браузера на Server2 - IP адрес принадлежащий интерфейсу fa0/1 Router0

Доступ к локальному сайту из сети открыт .

