

Лабораторная работа № 2

Изучение технологии виртуальных локальных сетей VLAN

2.1. Цель работы

Изучить и практически освоить процесс настройки технологии виртуальных локальных сетей VLAN (Virtual Local Area Network) и процесс маршрутизации между ними с использованием метода маршрутизации Router-on-a-stick. Научиться настраивать порты коммутатора в режимы access и trunk.

2.2. Задание

Ознакомиться с основными понятиями технологии виртуальных локальных сетей VLAN (Virtual Local Area Network) и методами маршрутизации между VLAN.

Собрать необходимую топологию сети, запустить и настроить виртуальное оборудование.

Согласно пунктам выполнения практической работы, сделать необходимые снимки экрана. Изучить полученную информацию и оформить ее в соответствии с требованиями раздела 6.5 (Содержание отчета).

2.3. Краткая теория

VLAN (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 ширококвещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным пользователям группироваться вместе, даже если они не находятся в одной физической сети. Такая реорганизация может быть сделана на основе программного обеспечения вместо физического перемещения устройств. Основными особенностями VLAN можно назвать его функции, а именно:

- VLAN помогает структурировать сеть;
- VLAN используется для обеспечения безопасности;
- VLAN используется для объединения;
- VLAN уменьшает количество ширококвещательного трафика.

VLAN— 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, 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.

В современных сетях VLAN — главный механизм для создания логической топологии сети, не зависящей от её физической топологии. Имеют большое значение с точки зрения безопасности, в частности как средство борьбы с ARP-spoofing.

По умолчанию на каждом порту коммутатора имеется сеть VLAN1 или VLAN управления. Сеть управления не может быть удалена, однако могут быть созданы

дополнительные сети VLAN и этим альтернативным VLAN могут быть дополнительно назначены порты.

В оборудовании Cisco используется следующая терминология портов: access port — порт, принадлежащий одному VLAN и передающий нетегированный трафик. По спецификации Cisco, access-порт может принадлежать только одному VLAN, по умолчанию это первый (нетегированный) VLAN. Любой кадр, который проходит через access-порт, помечается номером, принадлежащим этому VLAN. Trunkport — порт, передающий тегированный трафик одного или нескольких VLAN. Этот порт, наоборот, не изменяет тег, а лишь пропускает кадры с тегами, которые разрешены на этом порту. Для того, чтобы передать через порт трафик нескольких VLAN, порт переводится в режим trunk. По умолчанию в режиме trunk разрешены все VLAN.

Для назначения VLAN существуют следующие решения:

- по порту (англ. port-based, 802.1Q): порту коммутатора вручную назначается одна VLAN. В случае, если одному порту должны соответствовать несколько VLAN (например, если соединение VLAN проходит через несколько сетевых коммутаторов), то этот порт должен быть членом транка. Только одна VLAN может получать все кадры, не отнесенные ни к одной VLAN (в терминологии 3Com, Planet, D-Link, Zyxel, HP — untagged, в терминологии Cisco, Juniper — native VLAN). Сетевой коммутатор будет добавлять метки данной VLAN ко всем принятым кадрам, не имеющим никаких меток. VLAN, построенные на базе портов, имеют некоторые ограничения.

- по MAC-адресу (MAC-based): членство в VLAN основывается на MAC-адресе рабочей станции. В таком случае сетевой коммутатор имеет таблицу MAC-адресов всех устройств вместе с VLAN, к которым они принадлежат.

- по протоколу (Protocol-based): данные 3-4 уровня в заголовке инкапсулированного в кадр пакета используются, чтобы определить членство в VLAN. Например, IP-машины могут быть переведены в первую VLAN, а AppleTalk-машины во вторую. Основной недостаток этого метода в том, что он нарушает независимость уровней, поэтому, например, переход с IPv4 на IPv6 приведет к нарушению работоспособности сети.

- методом аутентификации (англ. authentication based): устройства могут быть автоматически перемещены в VLAN, основываясь на данных аутентификации пользователя, или устройства при использовании протокола 802.1X.

Маршрутизация между VLAN - это процесс, в ходе которого мы заставляем разные виртуальные локальные сети взаимодействовать друг с другом независимо от того, где присутствуют VLAN (на одном коммутаторе или на разных коммутаторах). Маршрутизация между VLAN может быть выполнена с помощью устройства 3 уровня, маршрутизатора или коммутатора 3 уровня.

Различают три способа организации маршрутизации:

- Традиционный - для каждого VLAN используется отдельный порт устройства 3-го уровня.

Для каждого VLAN на коммутаторе выделяется отдельный порт для подключения к устройству 3-го уровня. Этот порт работает в режиме доступа (access) и ему назначается конкретный VLAN. Каждый интерфейс маршрутизатора принадлежит своему VLAN и физический интерфейс маршрутизатора имеет свой IP-адрес. IP-адрес на интерфейсе маршрутизатора является шлюзом по умолчанию.

- Router-on-a-stick (ROS) - на порту маршрутизатора настраиваются подинтерфейсы, которые принадлежат разным VLAN и имеют разные IP-адреса.

В методе ROS необходимы коммутатор и маршрутизатор. Чтобы преодолеть аппаратные ограничения традиционного способа маршрутизации, используются виртуальные подинтерфейсы маршрутизаторов. Подинтерфейсы – это программные виртуальные интерфейсы, которые назначаются на физические интерфейсы. Интерфейс маршрутизатора разделяется на подинтерфейсы, которые действуют как шлюз по умолчанию для соответствующих VLAN. На каждом подинтерфейсе настраивается свой собственный IP-адрес, маска подсети и назначается свой VLAN. Это позволяет одному физическому интерфейсу одновременно быть частью нескольких логических сетей. На коммутаторе также используется один порт, который настраивается как trunk порт.

Недостатком способа ROS является использование всеми подинтерфейсами одной полосы пропускания физического интерфейса. Возможно перенасыщение канала при большом количестве хостов. Преимуществом является экономия портов на маршрутизаторе.

- Маршрутизация на основе L3 коммутатора 3-го уровня.

На L3 коммутаторах это реализуется с помощью создания виртуальных интерфейсов коммутатора Switch Virtual Interface (SVI). SVI - это логический интерфейс на многоуровневом коммутаторе, который обеспечивает обработку пакетов уровня 3 для всех портов коммутатора, связанных с этой VLAN. Для одного VLAN можно создать один SVI. SVI на L3 коммутаторе предоставляет как услуги управления, так и маршрутизации.

SVI, созданный для соответствующего VLAN, действует как шлюз по умолчанию для этого VLAN, точно так же, как вспомогательный интерфейс маршрутизатора (в технологии ROS). Если пакет должен быть доставлен в разные VLAN, т. е. маршрутизация между VLAN должна выполняться на коммутаторе уровня 3, тогда сначала пакет доставляется на коммутатор уровня 3, а затем к месту назначения, точно так же, как в процессе работы router on stick.

2.4. Порядок выполнения работы

2.4.1. Настройка портов коммутатора

Предварительная настройка сетевого оборудования

Собрать сетевую топологию согласно рисунку 2.4.1. Оборудование сети расположено на 3 этажах здания по 3-5 ПК на каждом этаже, и соединено 3 коммутаторами (Cisco 2960), соединенных между собой. Сделайте снимок экрана.

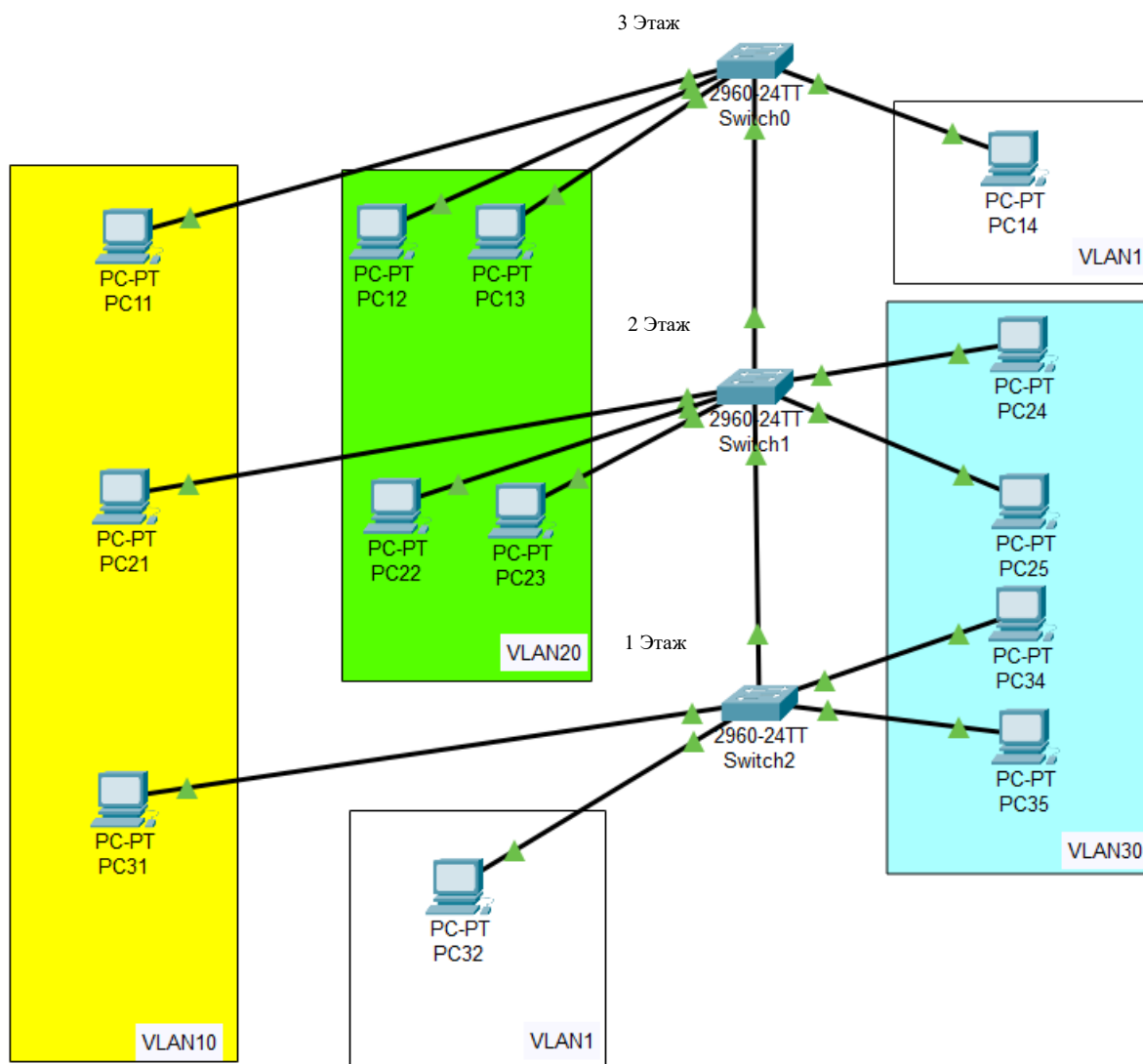


Рисунок 2.4.1. Топология сети

В практической работе предполагается создание виртуальных локальных сетей по 1-4 ПК в каждой: VLAN 1–1,3 этаж, Vlan 10 -1,2,3 этаж, Vlan 20 –2,3 этаж, Vlan30 - 1,2 этаж. При сегментировании сети лучше придерживаться правила: отдельный VLAN - отдельная сеть. Названия групп должны быть уникальными. IP-адреса назначаются в соответствии с вариантом N, где N – порядковый номер в списке учебной группы (номер в журнале). Назначьте всем устройствам сетевые адреса согласно таблице 2.4.1.

Для того чтобы назначить сетевые адреса компьютерам, один раз нажмите левой кнопкой мыши на устройстве и перейдите в закладку «Desktop», а затем нажмите на «IP Configurations». Введите IP-адрес и маску подсети в соответствующие поля, как это показано на рисунке 2.4.2 для PC11. Сделайте снимок экрана.

Таблица 2.4.1. Сетевые адреса устройств

Сетевой элемент	Интерфейс	IP-адрес	Маска	VLAN
PC11	FastEthernet0	192.168.N+10.1	255.255.255.0	10
PC21	FastEthernet0	192.168.N+10.2	255.255.255.0	10
PC31	FastEthernet0	192.168.N+10.3	255.255.255.0	10
PC12	FastEthernet0	192.168.N+20.1	255.255.255.0	20
PC13	FastEthernet0	192.168.N+20.2	255.255.255.0	20
PC22	FastEthernet0	192.168.N+20.3	255.255.255.0	20
PC23	FastEthernet0	192.168.N+20.4	255.255.255.0	20
PC24	FastEthernet0	192.168.N+30.1	255.255.255.0	30
PC25	FastEthernet0	192.168.N+30.2	255.255.255.0	30
PC34	FastEthernet0	192.168.N+30.3	255.255.255.0	30
PC35	FastEthernet0	192.168.N+30.4	255.255.255.0	30
PC14	FastEthernet0	192.168.0.1	255.255.255.0	1
PC32	FastEthernet0	192.168.0.2	255.255.255.0	1
Switch0	FastEthernet0/1	-		10
	FastEthernet0/2	-		20
	FastEthernet0/3	-		20
	FastEthernet0/4	-		1
	GigabitEthernet0/1	-		10,20
Switch1	FastEthernet0/1	-		10
	FastEthernet0/2	-		20
	FastEthernet0/3	-		20
	FastEthernet0/4	-		30
	FastEthernet0/5	-		30
	GigabitEthernet0/1	-		10,20
	GigabitEthernet0/2	-		10,30
Switch2	FastEthernet0/1	-		10
	FastEthernet0/2	-		30
	FastEthernet0/3	-		30
	GigabitEthernet0/1	-		10,30

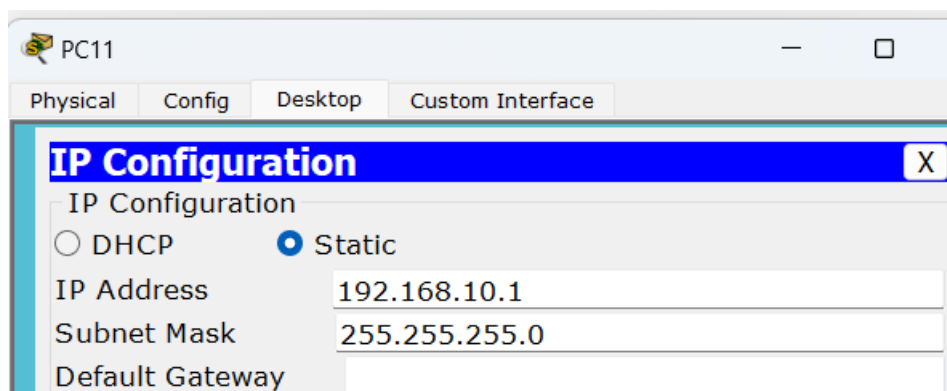


Рисунок 2.4.2. Конфигурация PC11 (для варианта 0)

Определение ПК в access-порты коммутаторов

Настроить коммутатор Switch0 Cisco 2960. Для этого один раз нажать по устройству и перейти во вкладку Command Line Interface (CLI) (для завершения команды нажать клавишу **Tab**):

Switch>**enable**

Switch#**configure terminal**

(Для упрощения ввода команд допускается ввод сокращенных команд: enable – en, configure terminal – conf t).

Создать новый VLAN10, согласно таблице 2.4.1 определить его название и назначить портам коммутатора, к которым подключены компьютеры, режим передачи трафика:

Switch(config)#**vlan 10**

Switch(config-vlan)#**name Vlan10**

Switch(config-vlan)#**exit**

Настройка портов

Switch(config)#**interface fastethernet 0/1**

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

Switch(config-if)#**switchport access vlan 10**

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

Повторить для VLAN20. Проверить правильность настроек:

Switch(config)#**vlan 20**

Switch(config-vlan)#**name Vlan20**

Switch(config-vlan)#**exit**

Switch(config)#**interface fastethernet 0/2**

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

Switch(config-if)#**switchport access vlan20**

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

Switch(config)#**interface fastethernet 0/3**

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

Switch(config-if)#switchport access vlan20

Switch(config-if)#exit

Switch#showvlan (выводит основную информацию о VLAN, рисунок 2.4.3). Сделать снимок экрана.

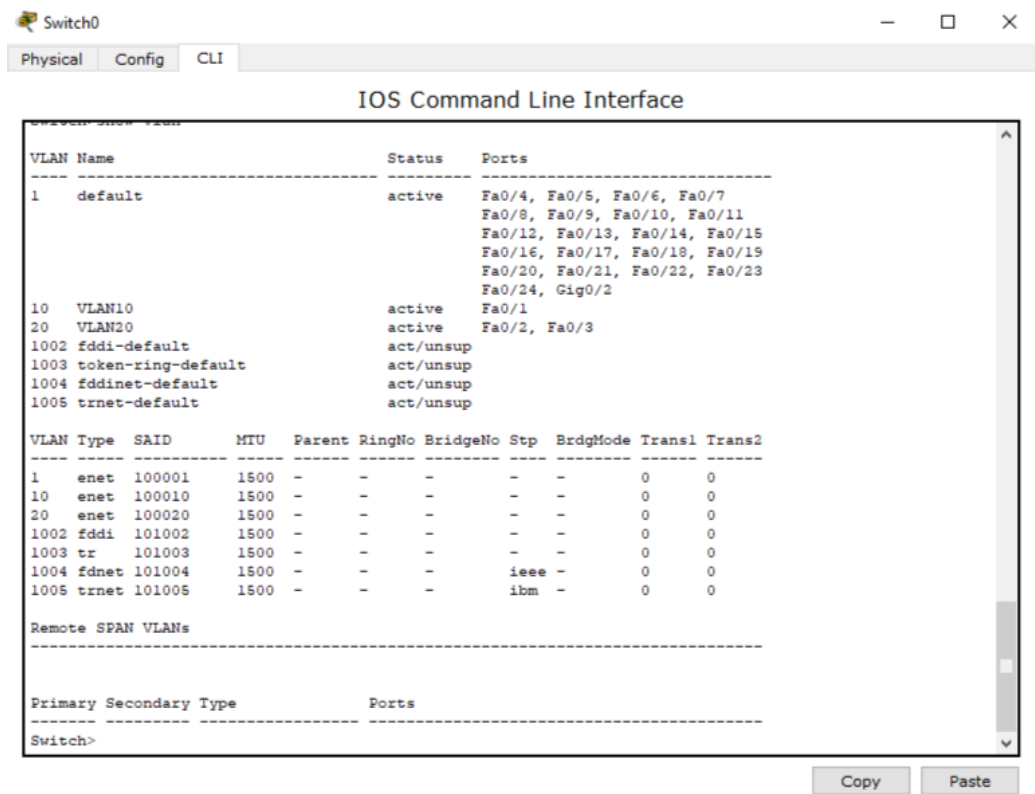


Рисунок 2.4.3. Основная информация по VLANам

Для вывода краткой информации по созданным VLAN ввести команду **Switch# show vlan brief** (рисунок 2.4.4). Сделать снимок экрана.

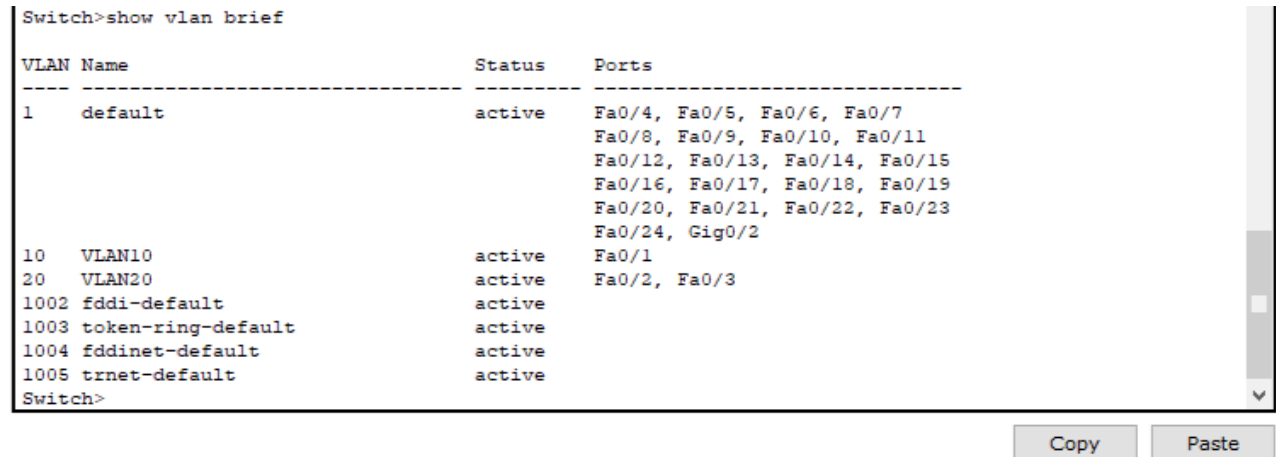


Рисунок 2.4.4. Краткая информация по VLAN

Убедиться в правильности настроек коммутатора Switch0Cisco 2960, ввести команду **show running-config** и найти в выведенной информации сведения о состоянии портов FastEthernet0/1-0/4 (рисунок 2.4.5).

Switch#show running-config

Сделать снимок экрана.

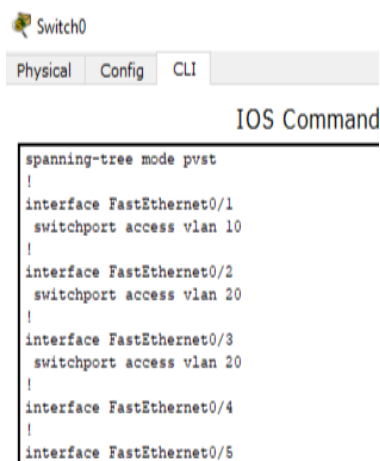


Рисунок 2.4.5. Пример настройки портов на коммутаторе Switch0

Определение trunk-портов коммутаторов

Для организации взаимодействия компьютеров, подключенных к разным коммутаторам, но находящихся в одном VLAN необходимо настроить trunk-порты (trunk-порт позволяет разбить физическое соединение на несколько сегментов). Для этого на Switch0 ввести следующие команды:

Switch#configure terminal

Switch(config)#interface GigabitEthernet 0/1

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk allowed vlan10,20 //(разрешает трафик VLAN 10 и 20)

Аналогичным способом повторите соответствующие настройки Access и Trunk портов для Switch1 и Switch2 в соответствии с таблицей 2.4.1 и внесите в отчет необходимые снимки экрана, подтверждающие правильность настроек.

Отправить простой PDU с PC11 на ПК, находящиеся в том же VLAN10 (PC21, PC31), а затем в другой VLAN20, VLAN30. Убедитесь, что ПК, расположенные в одном VLAN доступны, а в разных - нет. Сделать снимок экрана.

2.4.2. Маршрутизация между VLAN

Предварительная настройка сетевого оборудования

Соберите сетевую топологию и выполните настройку сетевого оборудования в соответствии с порядком выполнения пп.2.4.1 (рисунок 2.4.1). Добавьте на схему маршрутизатор Cisco 2901 Router0. Подключите его к коммутатору Switch2 на порт GigabitEthernet 0/2 (рисунок 2.4.6). Сделайте снимок экрана.

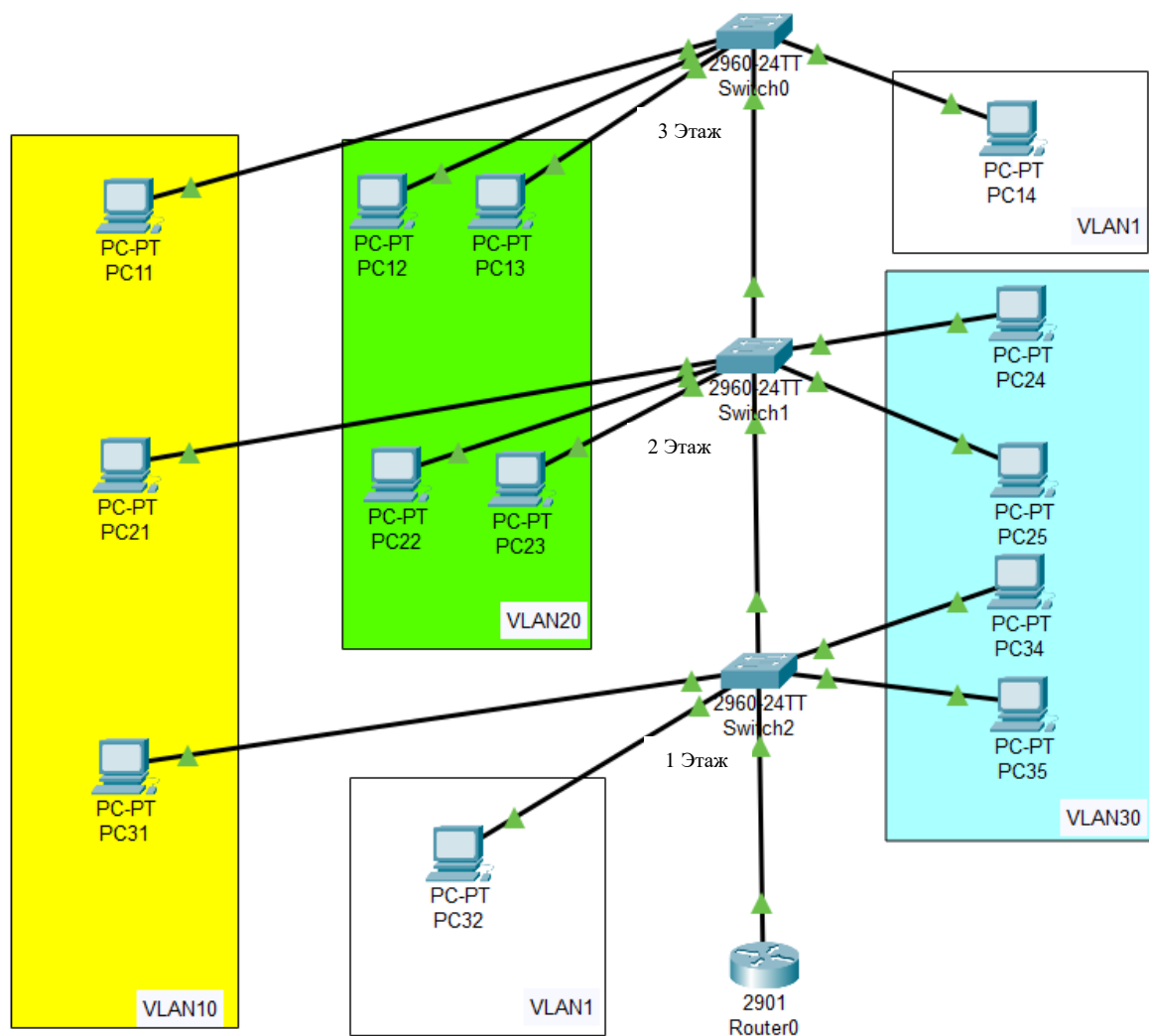


Рисунок 2.4.6. Топология сети с дополнительным маршрутизатором

В практической работе необходимо настроить маршрутизацию между VLAN.

Включить сетевой адаптер на Router0.

```
Router>enable //вход в привилегированный режим
Router#configure terminal //переход в режим конфигурирования
Router(config)#interface GigabitEthernet0/0 //настройка интерфейса GE0/0
Router(config-if)#no shutdown //включение интерфейса
```

Световая индикация статуса сетевого адаптера сменится на зеленый цвет.

Создать виртуальные подинтерфейсы (subinterface) на Router0 и настроить адресацию в соответствии с таблицей 2.4.2, где N – порядковый номер в списке учебной группы (номер в журнале).

Таблица 2.4.2. Сетевые адреса устройств

Сетевой элемент	Интерфейс	Подинтерфейс	IP-адрес	VLAN
Router0	GigabitEthernet0/0	GigabitEthernet0/0.10	192.168.N+10.254	10
		GigabitEthernet0/0.20	192.168.N+20.254	20
		GigabitEthernet0/0.30	192.168.N+30.254	30

Ввести следующие команды для настройки виртуальных интерфейсов:

```
Router(config)#interface GigabitEthernet0/0.10 //Настройка подинтерфейса VLAN10
Router(config-subif)#encapsulation Dot1Q 10
Router(config)#ip address 192.168.N+10.254 255.255.255.0 //Присвоение IP-адреса
Router(config-if)#no shutdown //Включение интерфейса
Router(config-if)#exit //Выход из конфигурирования интерфейса
```

Аналогичным способом создать и настроить для VLAN20 и VLAN30 с учетом своих адресов.

Результаты настройки Router0 проверить командой:

```
Router#show running-config
```

Пример результатов настройки интерфейса будет представлен в следующем виде:

```
interfaceGigabitEthernet0/0
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.N+10.254 255.255.255.0
!
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168. N+20.254 255.255.255.0
!
interface GigabitEthernet0/0.30
encapsulation dot1Q 30
ip address 192.168.N+30.254 255.255.255.0)
```

Сделать снимок экрана.

Настроить trunk-порт на коммутаторе Switch2.

```
Switch>enable
Switch#configure terminal
Switch(config)#interface GigabitEthernet0/2
Switch(config-if)#switchport mode trunk
```

Настроить шлюз по-умолчанию на всех PC, для каждого VLAN10, VLAN20, VLAN30 будет свой шлюз. (Для VLAN10 это будет соответствующий IP-адрес виртуального подинтерфейса192.168.N+10.254).

Проверить настройку коммутаторов Switch0, Switch1, Switch2 командой:

```
Switch#show vlan
```

Убедиться, что на каждом из них созданы все VLAN (VLAN10, VLAN20, VLAN30) (рисунок 2.4.7). В противном случае не будет проходить связь между всеми VLAN.

			Fa0/24, Gig0/2
10	VLAN10	active	Fa0/1
20	VLAN20	active	Fa0/2, Fa0/3
30	VLAN30	active	

Рисунок 2.4.7. Проверка созданных VLAN

На Trunk портах коммутаторов проверить разрешенные VLAN.

Проверьте связь между VLAN, отправив эхо-запрос или простой PDU между PC, находящимися в разных VLAN (к примеру с VLAN10 на VLAN20 или на VLAN30). Убедитесь, что все PC доступны. Сделать снимок экрана.

2.5. Содержание отчета

В индивидуальном отчёте должны быть указаны цель, задание, краткое описание выполняемых действий, представлены необходимые снимки экрана и пояснения к ним. Следует проанализировать полученные данные и описать их, дать ответы на контрольные вопросы.

2.6. Контрольные вопросы

1. Каково назначение VLAN?
2. Каковы функциональные особенности VLAN?
3. На каком уровне модели OSI взаимодействуют устройства, включенные в одну VLAN?
4. Какая терминология используется в оборудовании Cisco при назначении портов?
5. Какие решения существуют для назначения VLAN?
6. С помощью каких сетевых устройств можно осуществить маршрутизацию между VLAN?
7. Какими способами реализуется связь между VLAN?
8. Какие режимы порта устанавливаются на коммутаторе при подключении Router-on-stick?