**Практическая работа №4**

**Технология виртуальных локальных сетей vlan и протокол vtp.**

**1. Цели и задачи**

Целью данной практической работы является получение практических навыков при работе с технологией виртуальных локальных сетей (VLAN) и протоколом VTP.

Для достижения данной цели будут выполнены следующие задачи:

• изучение технологии создания виртуальных локальных сетей на коммутаторах Cisco с помощью интерфейса командной строки CLI;

• настройка интерфейсов коммутатора в режим access для связей коммутатор – узел;

• настройка интерфейсов коммутатора в режим trunk для создания VLAN-магистралей на связях коммутатор – коммутатор;

• изучение трех основных режимов протокола VTP – server, client и transparent;

• конфигурация отдельных VTP-доменов и паролей к ним.

**2. Теоретические сведения**

В данной работе будет рассмотрена возможность создания и настройки виртуальных локальных сетей. При проектировании довольно часто возникает необходимость в разделении одной сети на несколько логических блоков (например, разделение на отделы) независимо от физического расположения устройств.

В локальных сетях все устройства находятся в одном и том же широковещательном домене, это означает, что при отправке любым устройством кадра с широковещательным сообщением, копию этого кадра получат все остальные устройства. Технология VLAN (Virtual Local Area Network) позволяет помещать одни устройства в один широковещательный домен, а другие – в другой, создавая тем самым несколько широковещательных доменов. Эти широковещательные домены, создаваемые коммутаторами, называются виртуальными локальными сетями. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети.

Если VLAN-ceти используются в сетях, в которых имеется несколько соединенных коммутаторов, то в коммутаторах необходимо использовать VLАN-магистрали в сегментах, находящихся между этими коммутаторами. Создание такой магистрали приводит к тому, что в коммутаторах применяется процесс, называемый назначением тегов VLAN-ceти. С eгo помощью коммутатор-отправитель добавляет заголовок к кадру перед его отправкой по магистрали. Этот дополнительный заголовок включает поле идентификатора VLAN-ceти (VLAN ID), с помощью которого коммутатор-отправитель может ввести идентификатор VLAN-ceти, а коммутатор-получатель - определить, к какой VLАN-сети относится полученный кадр.

Таким образом, порты коммутатора, поддерживающие VLAN, можно разделить на два множества:

1. **Тегированные** порты (или транковые порты, trunk-порты в терминологии Cisco) – между ними строятся VLAN-магистрали, используются для связи коммутатор – коммутатор.

2. **Нетегированные** порты (или порты доступа, access-порты в терминологии Cisco) – для связи коммутатор – узел.

По умолчанию все порты коммутатора считаются нетегированными членами VLAN 1 (так называемый native VLAN – «родной» VLAN). В процессе настройки или работы коммутатора они могут быть перемещены в другие VLAN.

VTP (VLAN Trunking Protocol - транкинговый протокол сетей VLAN) –собственный протокол корпорации Cisco, который предоставляет средства, с помощью которых коммутаторы Cisco могут обмениваться информацией о конфигурации VLAN-ceти. В частности, протокол VTР обеспечивает передачу анонсов с информацией, позволяющей узнать о существовании каждой VLAN-ceти по ее идентификатору VLAN-ceти и имени VLAN-ceти. Но протокол VTР не анонсирует сведения о том, какие интерфейсы коммутатора относятся к той или иной VLAN-ceти.

На коммутаторах Cisco протокол VTP может работать в трёх режимах:

1. **Serve**r (режим по умолчанию):

* умеет все;
* может создавать, изменять и удалять VLAN из командной строки коммутатора;
* генерирует объявления VTP и передает объявления от других коммутаторов;
* может обновлять свою базу данных VLAN при получении информации не только от других VTP-серверов, но и от других VTP-клиентов в одном домене, если полученная конфигурация имеет более высокий номер версии;
* сохраняет информацию о настройках VLAN в файле vlan.dat во flash-памяти.

2. **Client**:

* эта роль уже ограничена;
* в этом режиме невозможно создавать, изменять и удалять VLAN - все VLAN получает и синхронизирует от сервера;
* периодически сообщает соседям о своей базе VLAN-ов;
* передает объявления от других коммутаторов;
* синхронизирует свою базу данных VLAN при получении информации от VTPсерверов или других VTP-клиентов, если полученная конфигурация имеет более высокий номер версии;
* сохраняет информацию о настройках VLAN в файле vlan.dat.

3. **Transparent:**

* независимая роль;
* возможно создавать, изменять и удалять VLAN из командной строки коммутатора, но только для локального коммутатора;
* не генерирует объявления VTP;
* если получает какое то объявление, передает дальше, но со своей базой не синхронизирует;
* сохраняет информацию о настройках VLAN в NVRAM;
* всегда использует номер версии конфигурации равный нулю.

В VTP 3-ей версии добавилась еще одна роль — **VTP Off**. Он не передает никакие объявления. В остальном работа аналогична режиму Transparent.

Если устройство использует режим сервера, это позволяет вносить изменения, добавлять или удалять VLAN. Режим клиента не позволяет вносить изменения в настройки свитча, вы можете настроить базу данных VLAN только через VTP-сервер, и она будет реплицирована на всех VTP-клиентах. Свитч в режиме transparent не вносит изменений в собственную базу данных VLAN, а просто пропускает через себя и передает изменения следующему устройству, находящемуся в режиме client. Этот режим похож на отключение протокола VTP на конкретном устройстве, превращающее его в транспортировщика информации об изменениях VLAN.

*По умолчанию все свитчи работают в режиме VTP-сервера.*

1. Процесс ввода в действие протокола VTP начинается с создания VLAN-ceти на коммутаторе, который находится в серверном режиме.

2. После этого VTP-сервер распространяет информацию об изменениях в конфигурации VLAN-ceтeй с помощью сообщений VTР, передаваемых только через VLAN-магистрали по всей сети.

3. Затем серверы и VTР-клиенты обрабатывают полученные сообщения VTР, обновляют свои базы данных с конфигурацией протокола VTР на основе этих сообщений и независимо от других передают обновления протокола VTР по своим магистралям. Процесс, в ходе которого на одном из серверов изменяется конфигурация VLAN-сетей и все остальные коммутаторы VTP усваивают новую конфигурацию, называется синхронизацией.

Серверы и клиенты VTР принимают решение о том, следует ли реагировать на полученное обновление протокола VTР и обновлять свои конфигурации VLAN ceтeй на основании того, произошло ли увеличение номера версии конфигурации базы данных VLAN-ceтeй. После каждого изменения VTP-сервером своей конфигурации VLAN-ceти этот сервер увеличивает текущий номер версии конфигурации на 1. Этот новый номер версии конфигурации отражается в сообщениях об обновлениях протокола VTР. После получения этого обновления другими коммутаторами, они обновляют свою конфигурацию VLANceтeй. Кроме того, серверы и клиенты VТР рассылают периодические сообщения VТР через каждые 5 минут на тот случай, если каким-либо вновь введенным в сеть коммутаторам потребуется информация о конфигурации VLAN-ceти. Последовательность действий при создании сети «протоколом транкинга VLAN».

**Базовые команды show коммутатора**

* ***show port-security*** – отображает все порты с включенной системой безопасности. Чтобы изучить данные конкретного интерфейса, добавьте в команду идентификатор интерфейса. В выходных данных указывается информация о максимально разрешенном количестве адресов, текущем количестве, количестве нарушений безопасности и действиях, которые необходимо выполнить;
* ***show interfaces*** – отображает все интерфейсы с данными о состоянии канала (протокола), пропускной способности, надёжности, инкапсуляции, параметрах дуплексного режима и статистике ввода-вывода;
* ***show mac-address-table*** – отображает все MAC-адреса, полученные коммутатором, в том виде, в котором они получены (динамические/статические), номер порта и сеть VLAN, назначенную порту

**3. Методические указания**

1. Для начала нужно добавить коммутатор 2960-24TT и четыре узла PC-PT на логическое рабочее пространство, а также установить соединения между коммутатором и узлами по типу «медный прямой».

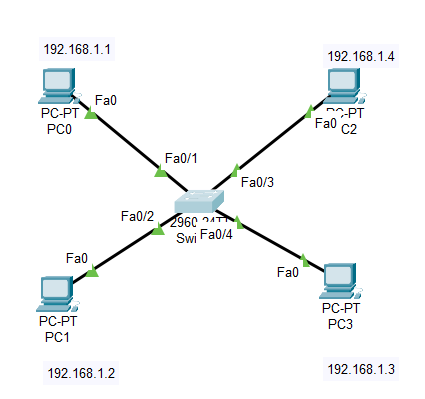
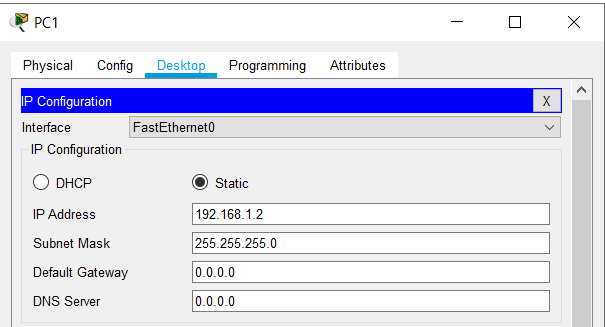
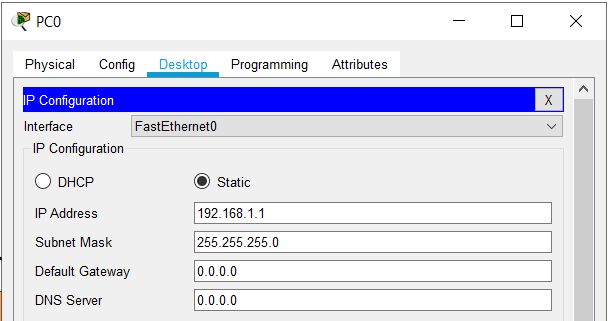
****

Рисунок 1 - Структура созданной сети

2. Для каждого узла следует настроить IP-адреса и маски подсетей.

3. Введите следующие значения в полях IP-адрес и маска подсети соответственно: 192.168.1.1 (255.255.255.0) до 192.168.1.4



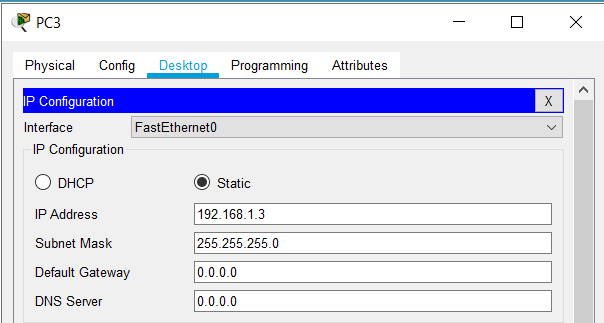
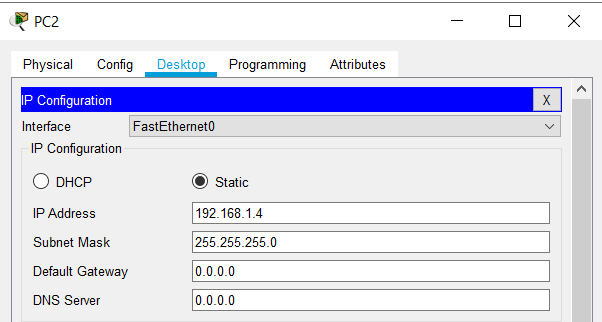


Рисунок 2 - IP конфигурации созданных ПК

4. Введите команду show vlan brief. Появится список всех VLAN на данном коммутаторе. По умолчанию все порты коммутатора принадлежат виртуальной локальной сети с номером 1.

5. Создайте VLAN с номером 2, придумайте и задайте любое имя для этой виртуальной локальной сети (например, name vlan2).

6. Добавьте два узла и в режиме конфигурации диапазона интерфейсов переведите порты в режим access.

7. С помощью команды exit вернитесь в привилегированный режим коммутатора. Возможно, придется ввести эту команду несколько раз. Посмотрите список всех VLAN (show vlan brief). Должна появиться новая строчка с именем созданного VLAN, а в столбце Ports должны быть указаны порты.

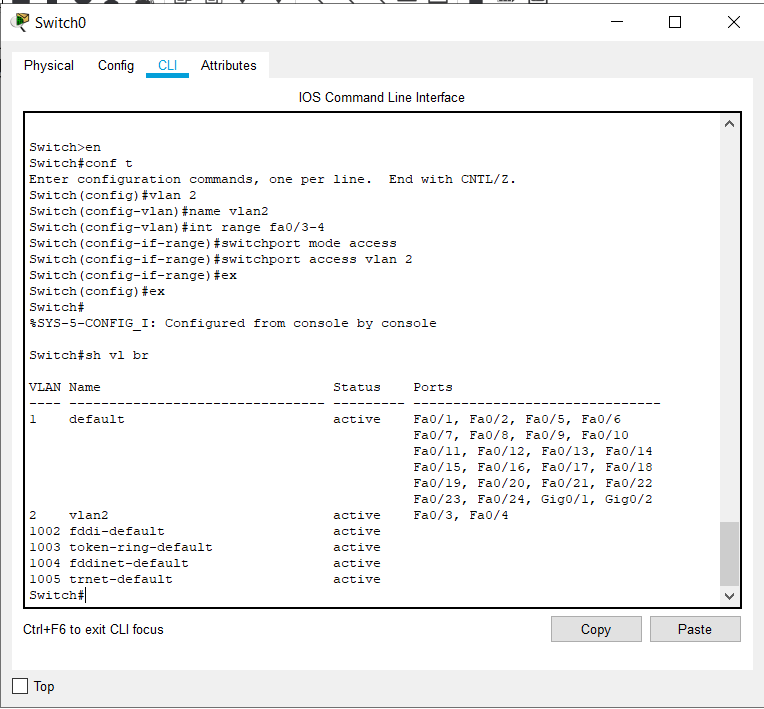
****

Рисунок 3 - Вывод команды show vlan brief

8. Проверьте связь между узлами из разных виртуальных локальных сетей. Трафик не должен проходить!

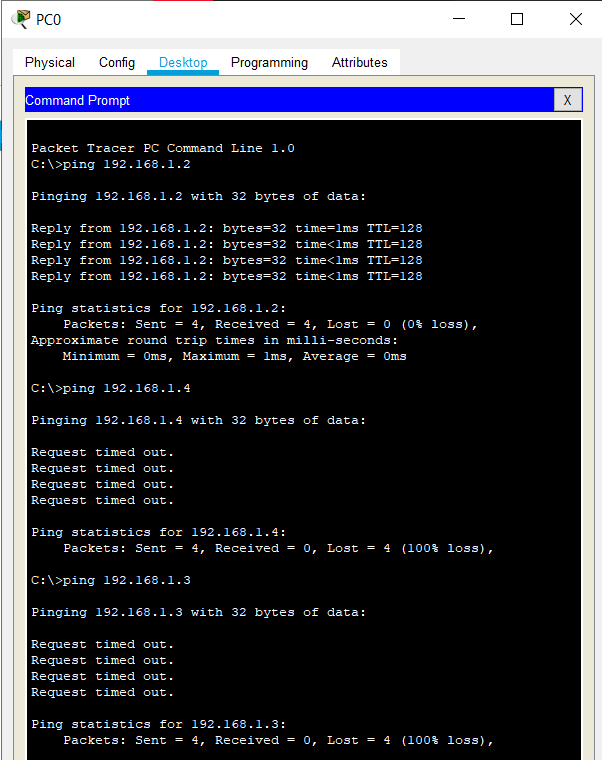
****

Рисунок 4 - Выполнение команды ping на ПК0 к ПК в разных VLAN-сетях

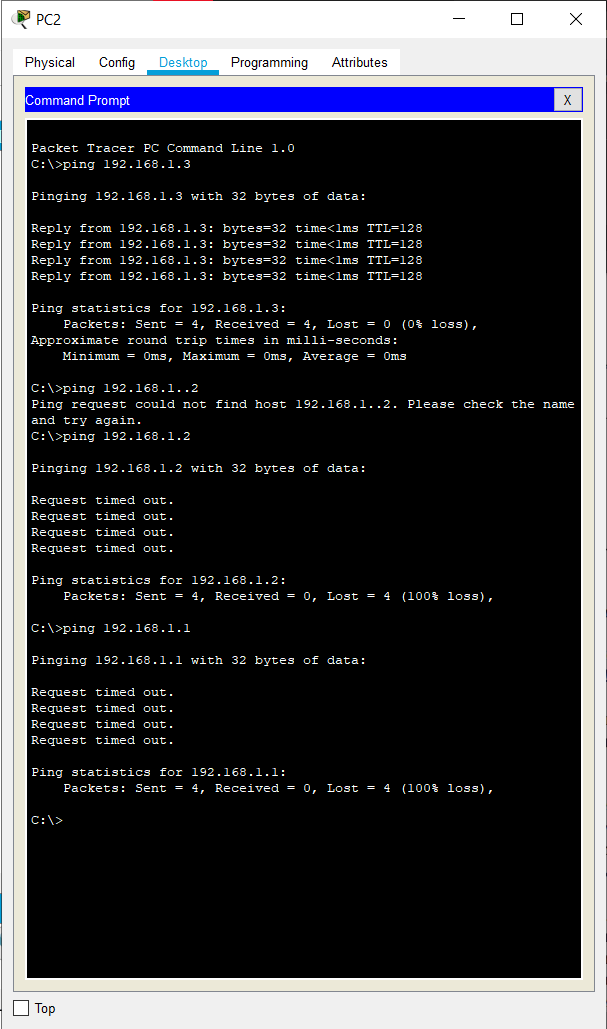
****

Рисунок 5 - Выполнение команды ping на ПК2 к ПК в разных VLAN-сетях

Предположим, что имеется задача: в одном здании на разных этажах находится два коммутатора. К каждому коммутатору подключены некоторые узлы, коммутаторы также связаны между собой. Требуется разделить сеть на два логических отдела таким образом, чтобы в каждом отделе были узлы из разных этажей.

Потребуется добавить на логическое рабочее пространство еще один коммутатор и два узла. Для настройки IP-адресов на новых узлах можно взять адреса 192.168.1.5 и 192.168.1.6, а маску подсети установить в значение 255.255.255.0. Соедините устройства (Рис. 4), используя между коммутаторами кабель «Медный перекрестный», а также интерфейс GigabitEthernet 0/1. Данный сегмент будет использоваться в качестве VLAN-магистрали, а значит, по нему будет ходить трафик из всех VLAN, поэтому логично использовать интерфейсы с высокой пропускной способностью.

По умолчанию, узлы ПК4 и ПК5 будут относиться к VLAN1, причем Коммутатор1 даже не будет знать о том, что на Коммутатор0 была созданаVLAN2. Это можно проверить, если ввести в CLI Коммутатора1 команду show vlan brief. Для синхронизации базы данных VLAN-сетей нужно настроить протокол VTP, создав для этих двух коммутаторов свой VTP-домен и пароль. Но сначала нужно установить VLAN-магистраль между двумя коммутаторами.

1. На Коммутатор0 зайдите в привилегированный режим, а затем в режим конфигурации. Введите команду interface gigabit ethernet 0/1(сокращенно - interface gi0/1).

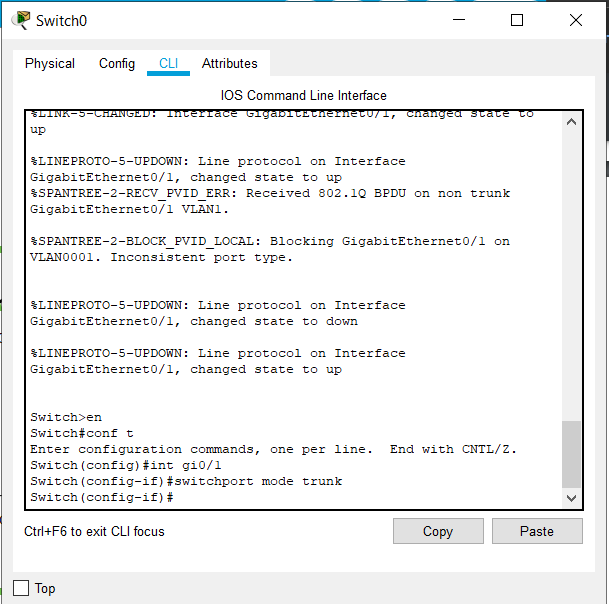
****

Рисунок 6 - Настройка порта в режим trunk на Switch0

2. Настроить порт в режим trunk, командой switchport mode trunk. Перейдите в CLI Коммутатора1 и проведите те же настройки. Таким образом, мы создаем статическую VLAN-магистраль, не используя протокол DTP.

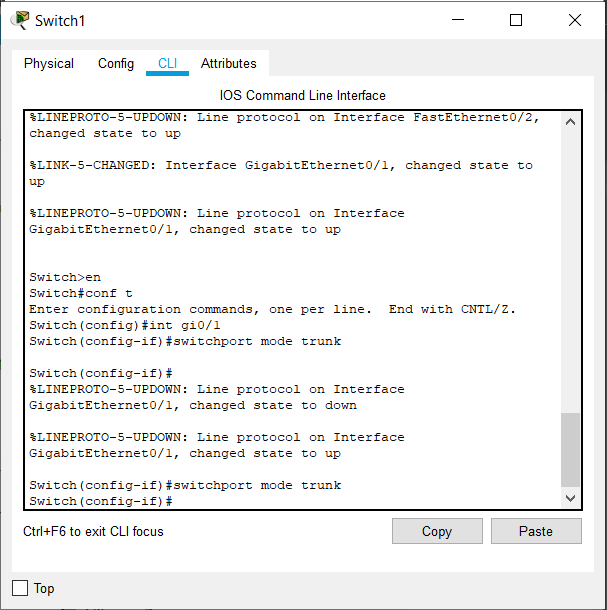
****

Рисунок 7 - Настройка порта в режим trunk на Switch1

3. Либо для создания динамической VLAN-магистрали переведите порт в режим dynamic desirable с помощью команды switchport mode dynamic desirable. Перейдите в CLI Коммутатора1 и проведите те же настройки, обратите внимание, что для динамической VLAN-магистрали можно указать режим dynamic auto.

Настройки транка проверяются с помощью следующих команд:

1. show vtp status

2. show running-config

3. show interfaces trunk

4. show interfaces [fastethernet номер\_интерфейса\ gigabitethernet\_

номер\_интерфейса] switchport

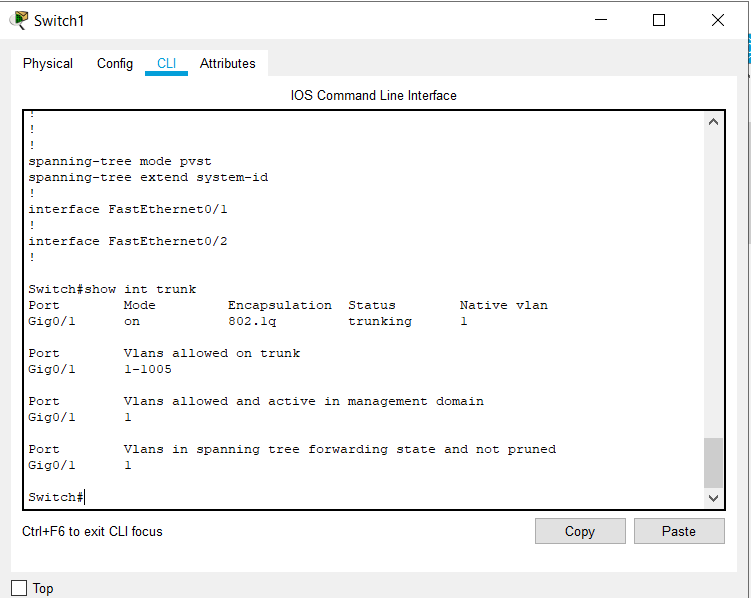
****

Рисунок 8 - Вывод команды show interfaces trunk для проверки настроек порта на Switch1

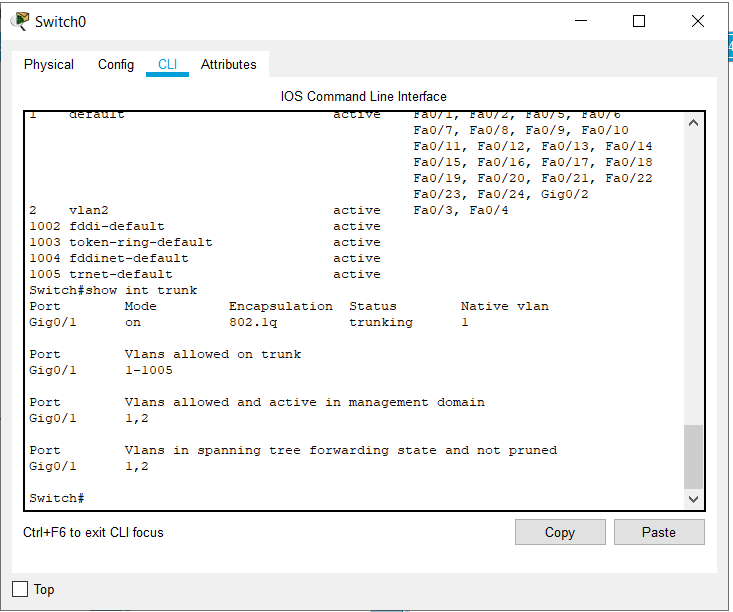
****

Рисунок 9 - Вывод команды show interfaces trunk для проверки настроек порта на Switch0

Теперь VLAN-магистраль настроена, однако в выводе команды show vlan brief на Коммутатор1 все еще не отображается созданная на Коммутатор0 VLAN2. Это происходит потому, что по умолчанию оба этих коммутатора находятся в собственных VTP-доменах. Необходимо поместить коммутаторы в один VTP-домен, для этого:

1. В CLI Коммутатора0 войдите в режим конфигурации (conf t), а затем наберите команду vtp domain <имя\_домена>. Будет установлено новое имя VTP-доменадолжно быть связано с Вашей фамилией.

2. С помощью команды vtp password<пароль\_vtp\_домена> установите пароль для домена.

3. Проверьте статус VTP-протокола, для этого используется команда show vtp status. В выводе этой команды можно посмотреть информацию о номере версии протокола VTP («VTP Version»), номере версии конфигурации («configuration revision»), максимальном числе поддерживаемых VLAN («Maximum VLANs supported locally»), числе существующих в данный момент времени VLAN («Number of existing VLANs»), роли коммутатора в VTP-протоколе («VTP Operating Mode»), а также имени VTPдомена («VTP Domain Name»).

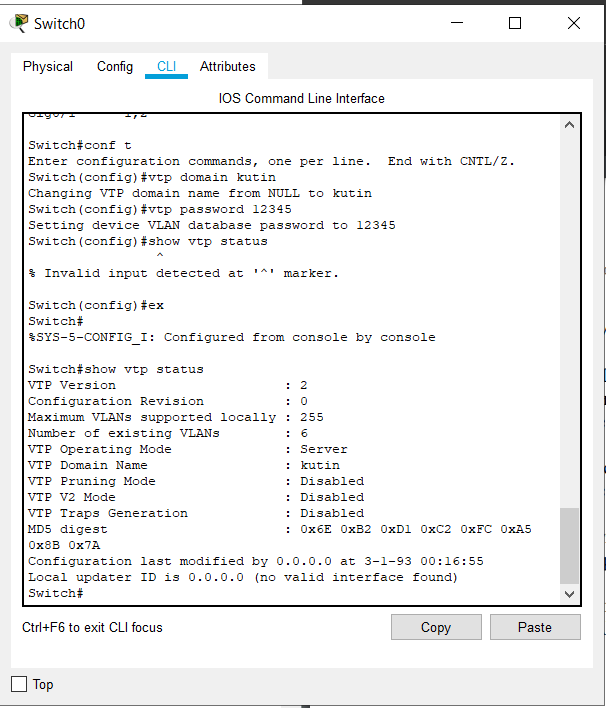
****

Рисунок 10 - Конфигурация VTP-домена на Switch0

4. Перейдите в CLI Коммутатор1. Введите команду vtp mode client для включения режима VTP-клиента. Затем продолжите настройки для включения в домен.

5. Теперь в выводе команды show vlan brief на Коммутатор1 должна появиться запись о существовании VLAN 2. Также в выводе команды show vtp status на обоих коммутаторах должен быть одинаковый номер версии конфигурации (configuration revision). Сейчас он равен 0, но он будет увеличиваться с каждым изменением VLANсетей.

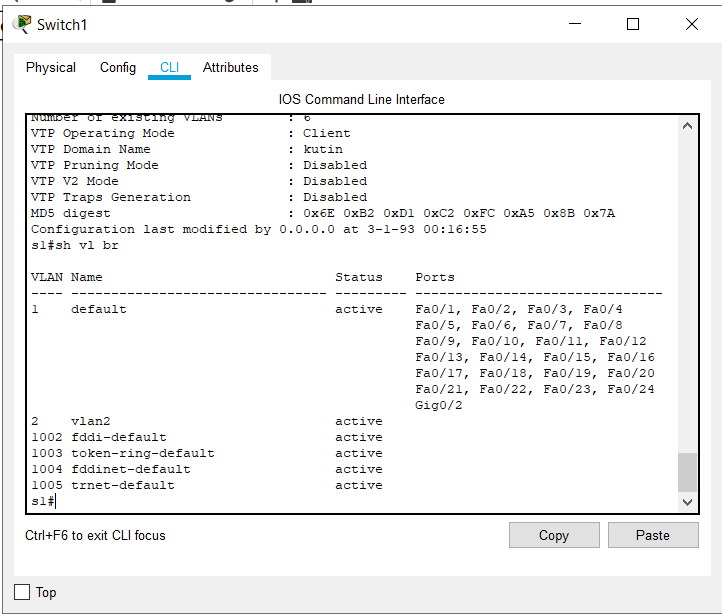
****

Рисунок 11 - Проверка настройки VTP на Switch1

6. Чтобы проверить работу VTP-протокола в деталях, перейдите в Режим Симуляции. Измените фильтры таким образом, чтобы отслеживать только трафик VTP.

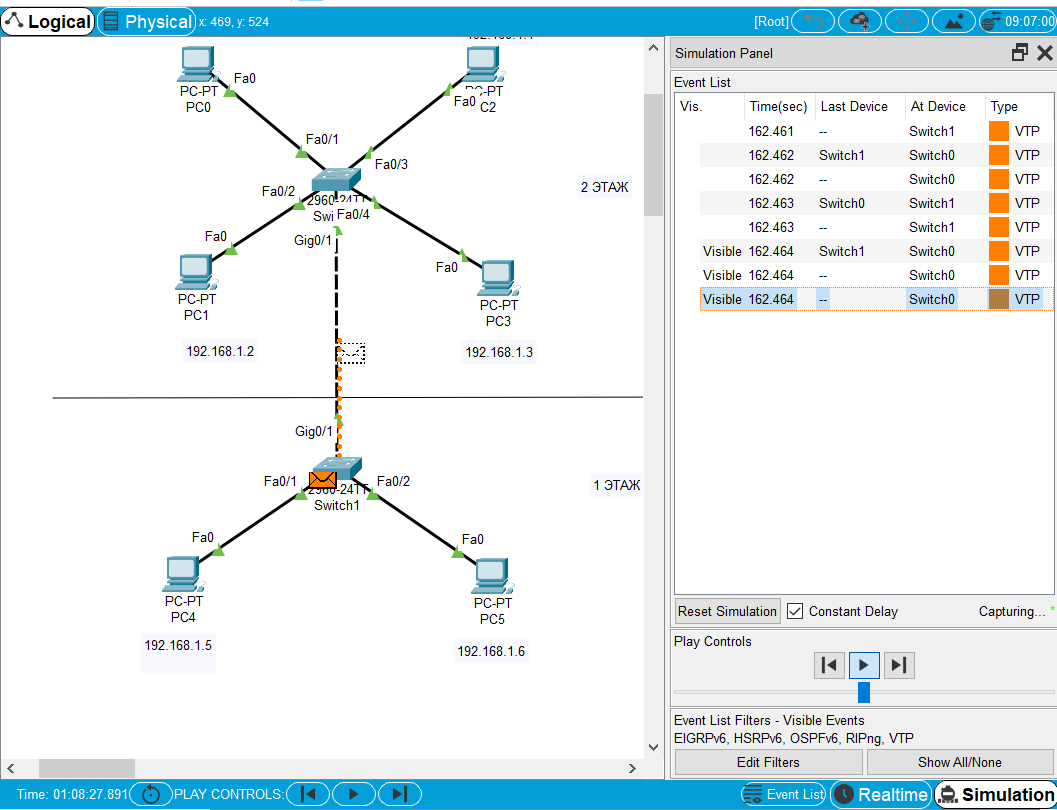
****

Рисунок 12 - Проверка работы VTP-протокола в Режиме Симуляции

7. Коммутатор0 является VTP-сервером, только он может добавлять и удалять информацию о VLAN-сетях.

8. Создайте VLAN 3 с помощью команд, изученных ранее. Поместите во вновь созданную VLAN3 новые два узла ПК6-ПК7, присоединенные к коммутатору-клиенту, и любой узел, присоединенный к коммутатору-серверу.

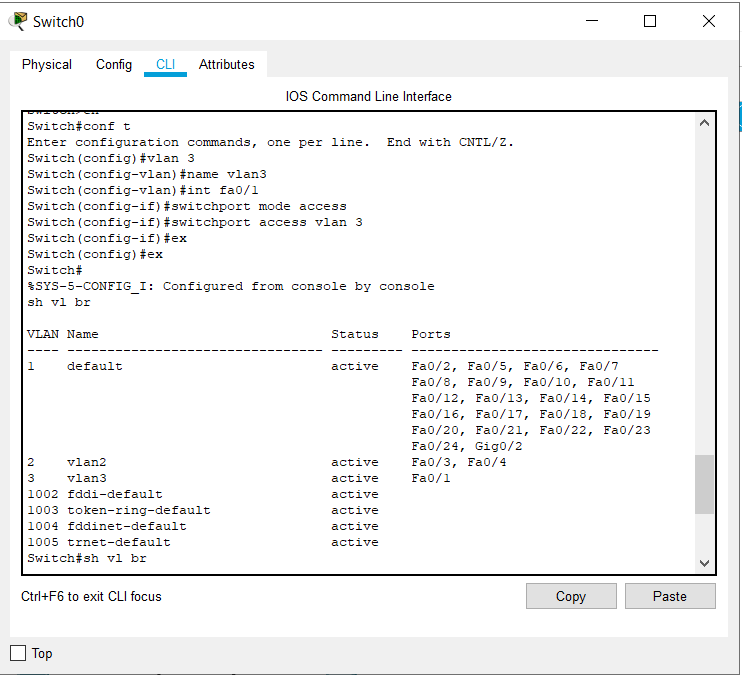
****

Рисунок 13 - Создание VLAN 3 на Switch0

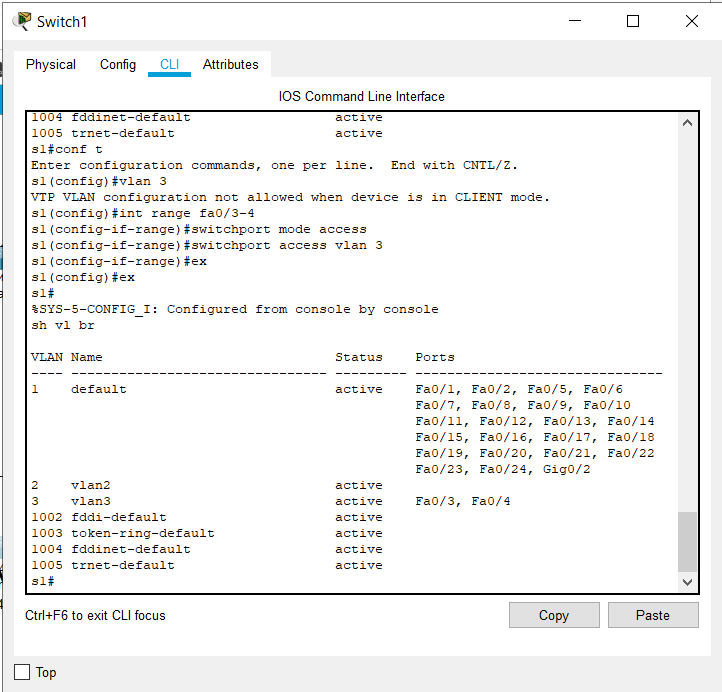
****

Рисунок 14 - Создание VLAN 3 на Switch1

9. Создайте VLAN 4. Поместите туда произвольные узлы, созданные на разных свитчах. Выделить все VLAN закрашенной областью.

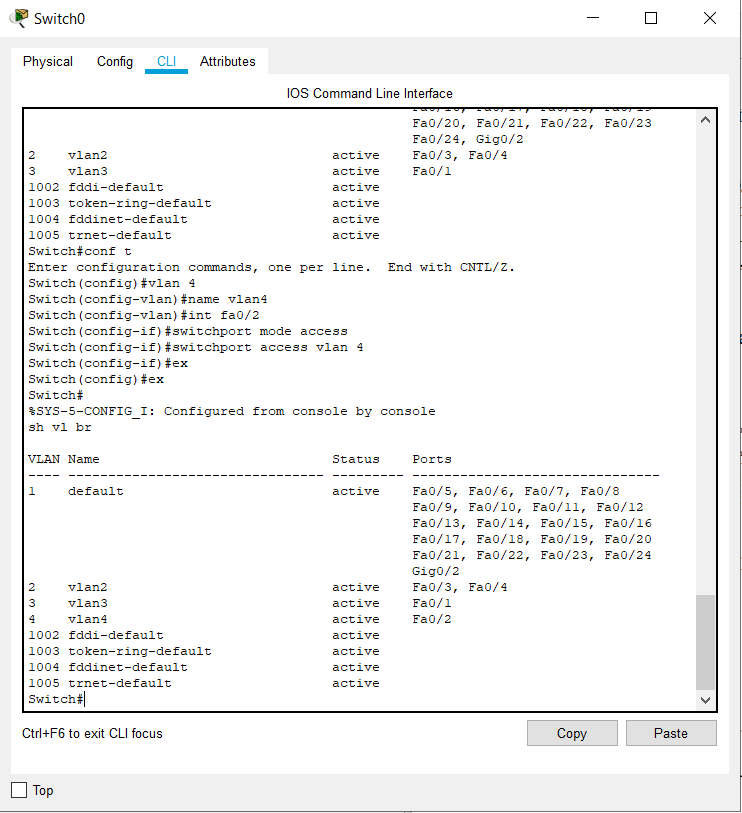
****

Рисунок 15 - Создание VLAN 4 на Switch0

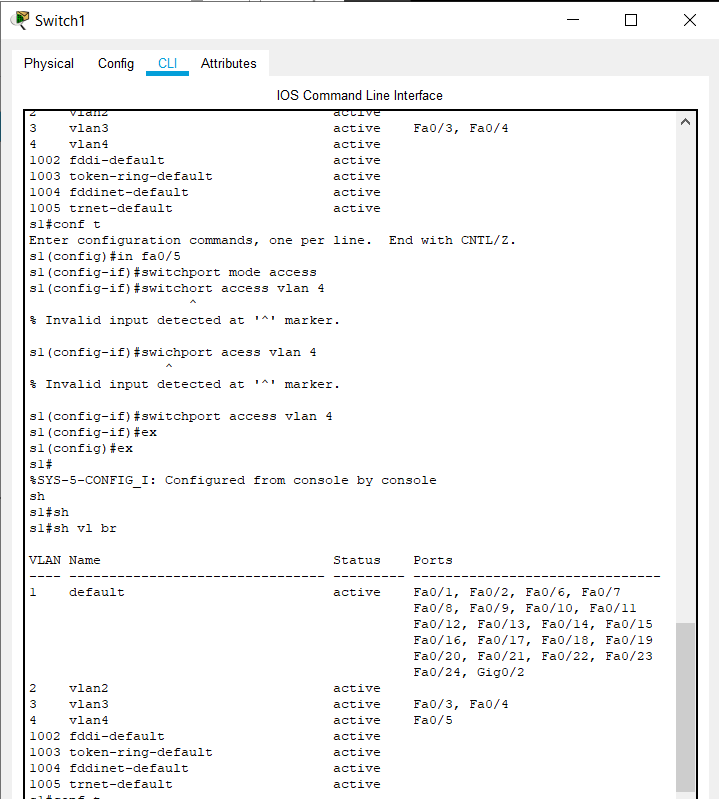
****

Рисунок 16 - Создание VLAN 4 на Switch1

10. Вернитесь в режим реального времени. При выводе команды show vtp status номер версии конфигурации должен увеличиться. Это можно заметить в строке «Configuration Revision».

11. Введите команду show vlan brief на каждом коммутаторе.

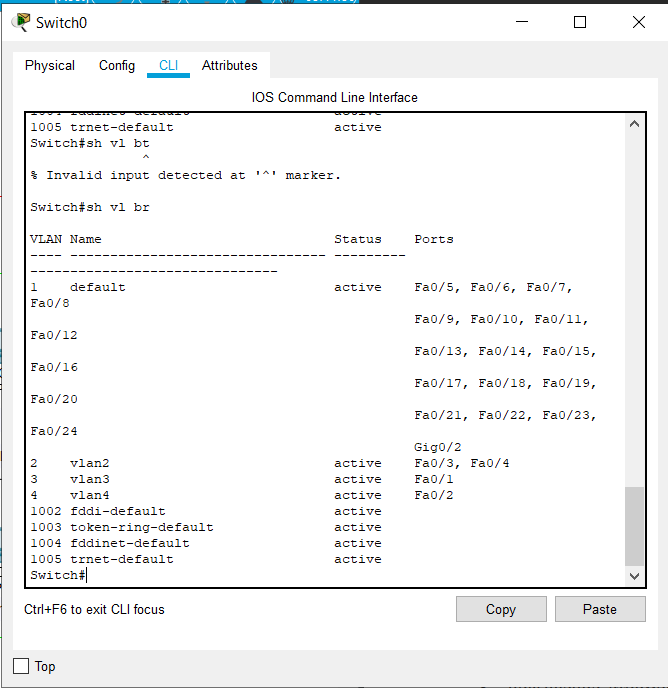
****

Рисунок 17 - Вывод команды show vlan brief на Switch0

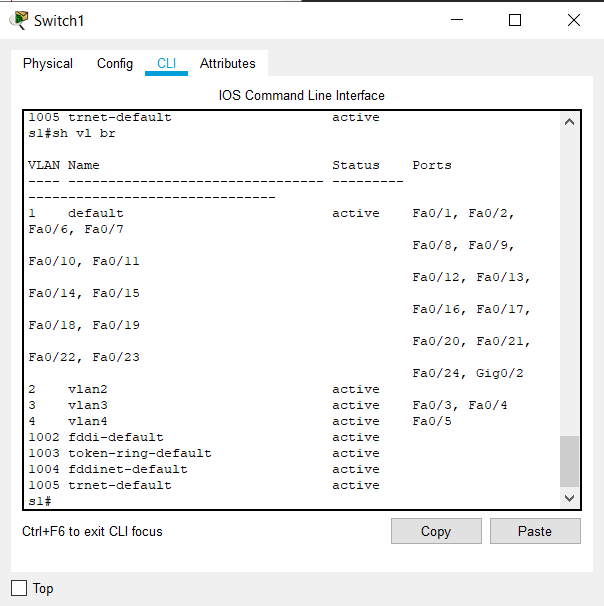
****

Рисунок 18 - Вывод команды show vlan brief на Switch1

12. Добавить третий коммутатор, работающий в режиме transparent. Создайте VLAN 5 на нем, добавьте 3 ПК.

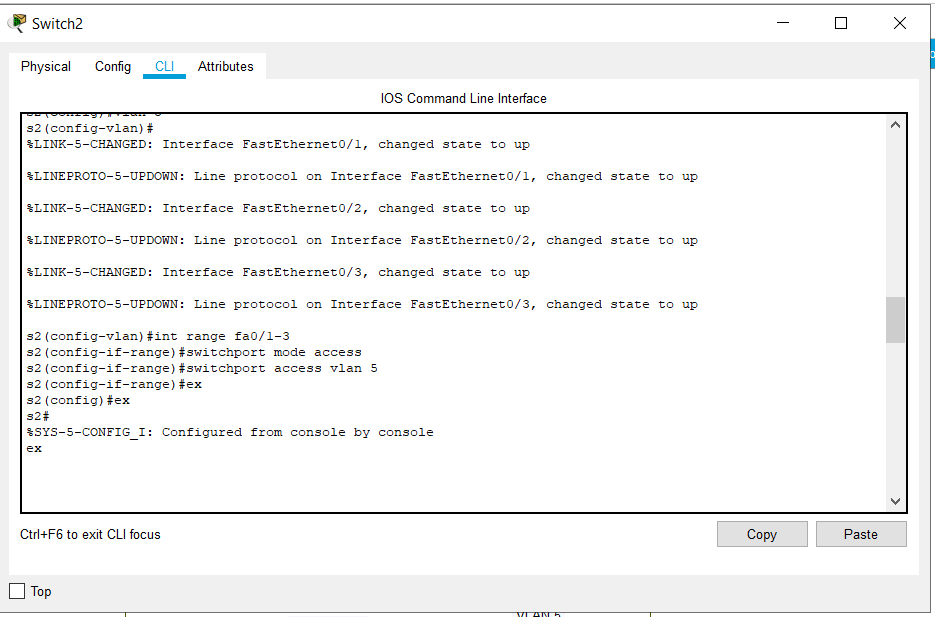
****

Рисунок 19 - Создание VLAN 5 на Switch2

13. Объясните функционирование третьего коммутатора, приведя все команды, подтверждающие его работу.

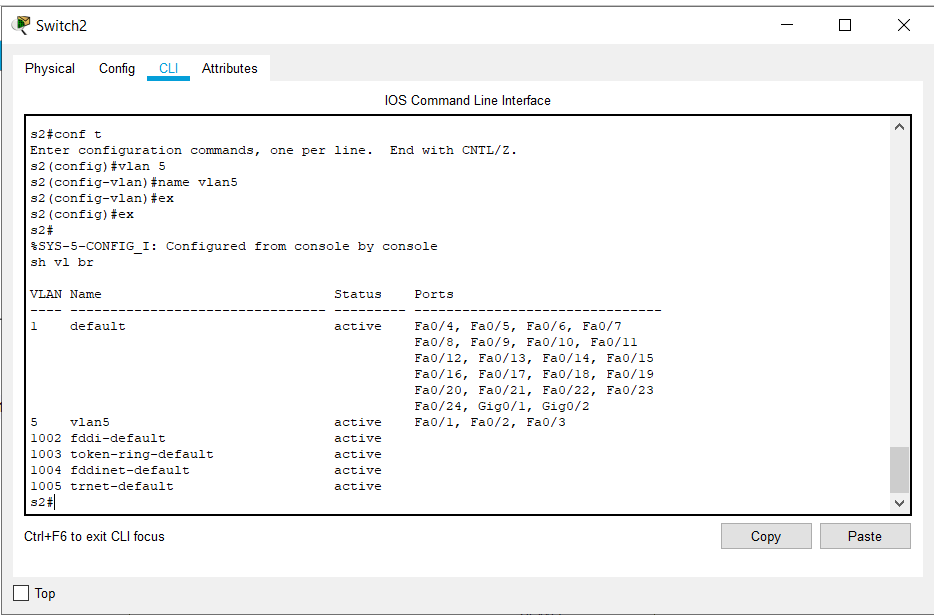


Рисунок 20 - Вывод команды show vlan brief на Switch2

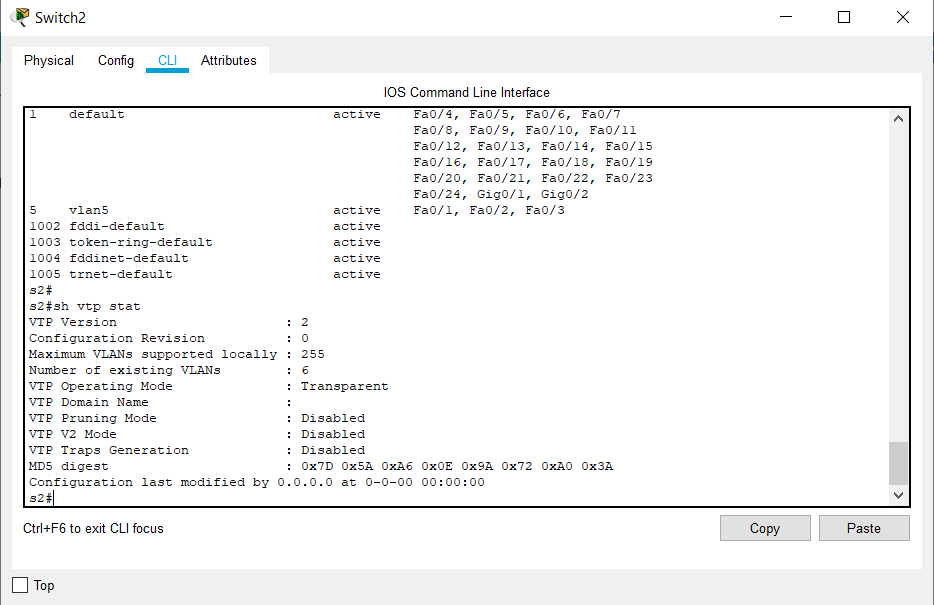
****

Рисунок 21 - Вывод команды show vtp status на Switch2

14. Все компоненты модели сети должны быть идентифицированы в соответствии с фамилией и именем студента. Все VLAN-сети выделены любой геометрической фигурой и закрашены пастельными цветами, поименованы.

15. В конце работы должна быть приведена структура сети, выделен каждый свитч, работающий в соответствующем заданию режиме и показаны рядом два окна с командами: show vtp status, show vlan brief.

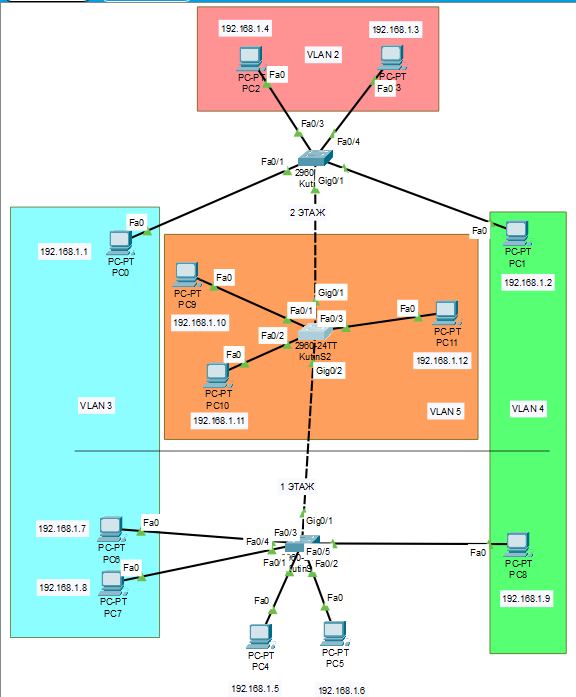
****

Рисунок 22 - Структура созданной сети

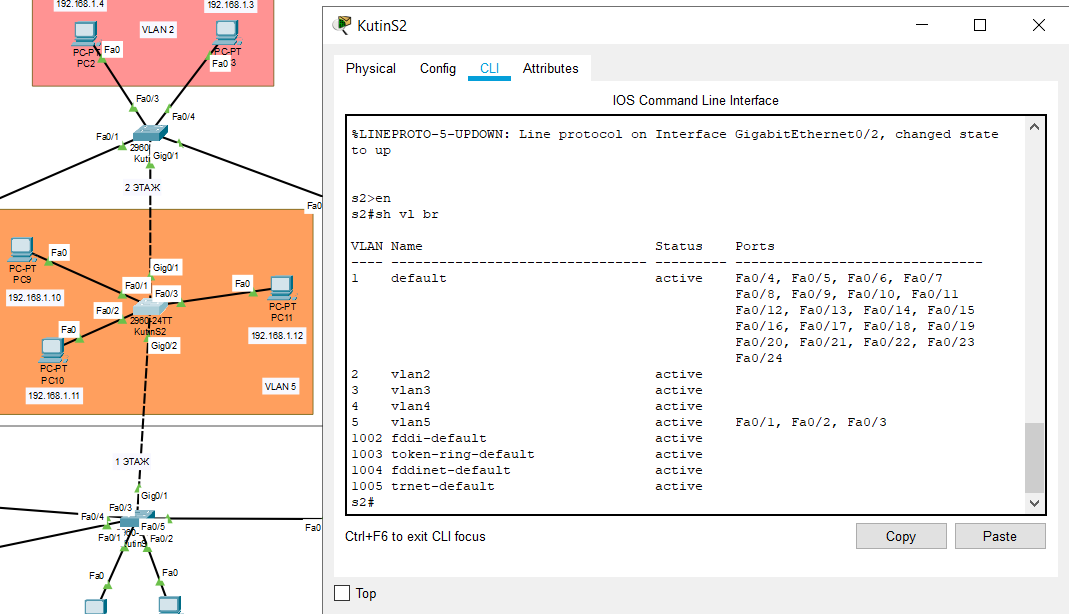
****

Рисунок 23 – Структура сети с KutinS2 и вывод команды show vlan brief

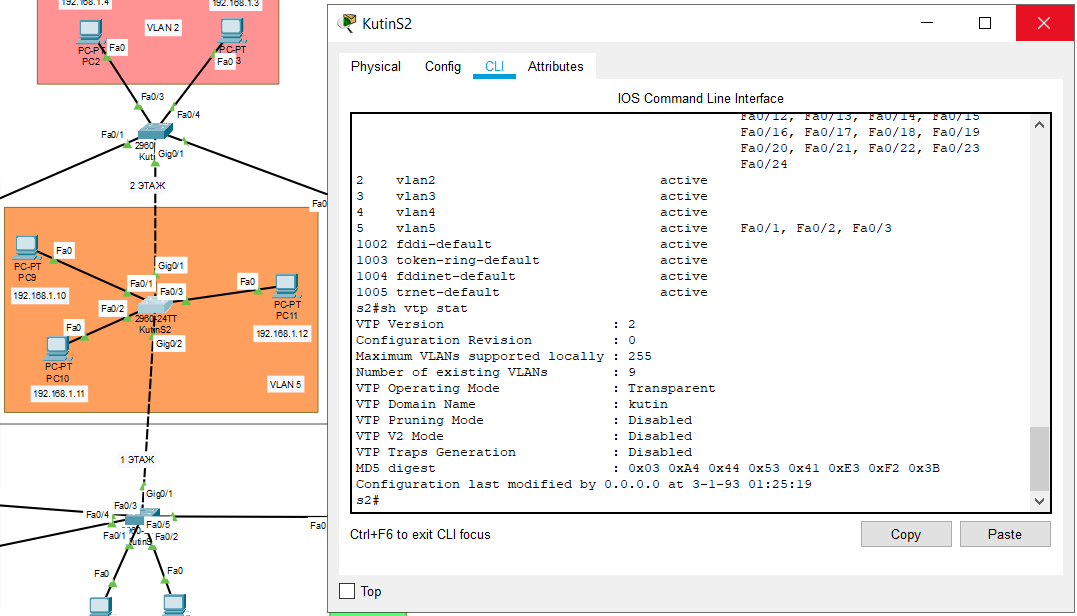
****

Рисунок 24 - Структура сети с KutinS2 и вывод команды show vtp status

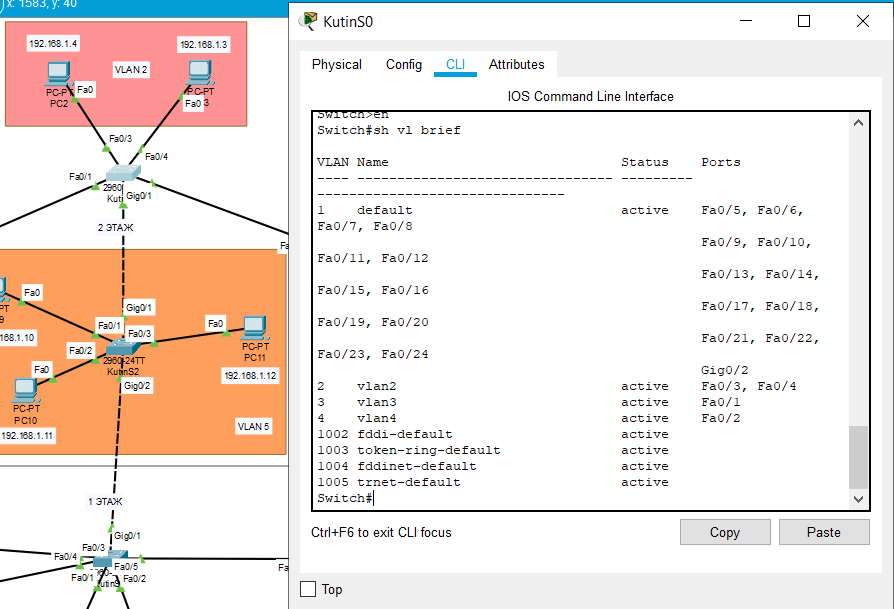
****

Рисунок 25 - Структура сети с KutinS0 и вывод команды show vlan brief

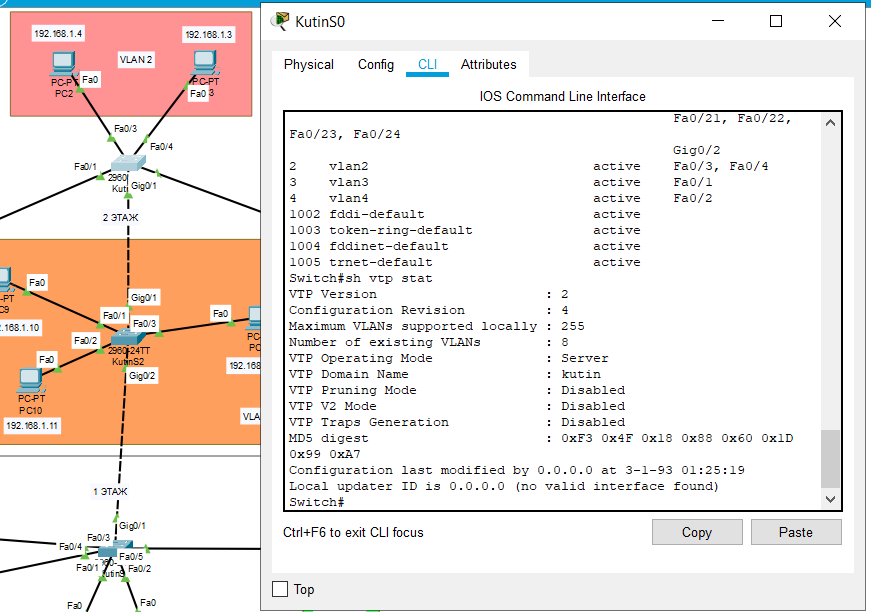
****

Рисунок 26 - Структура сети с KutinS0 и вывод команды show vtp status

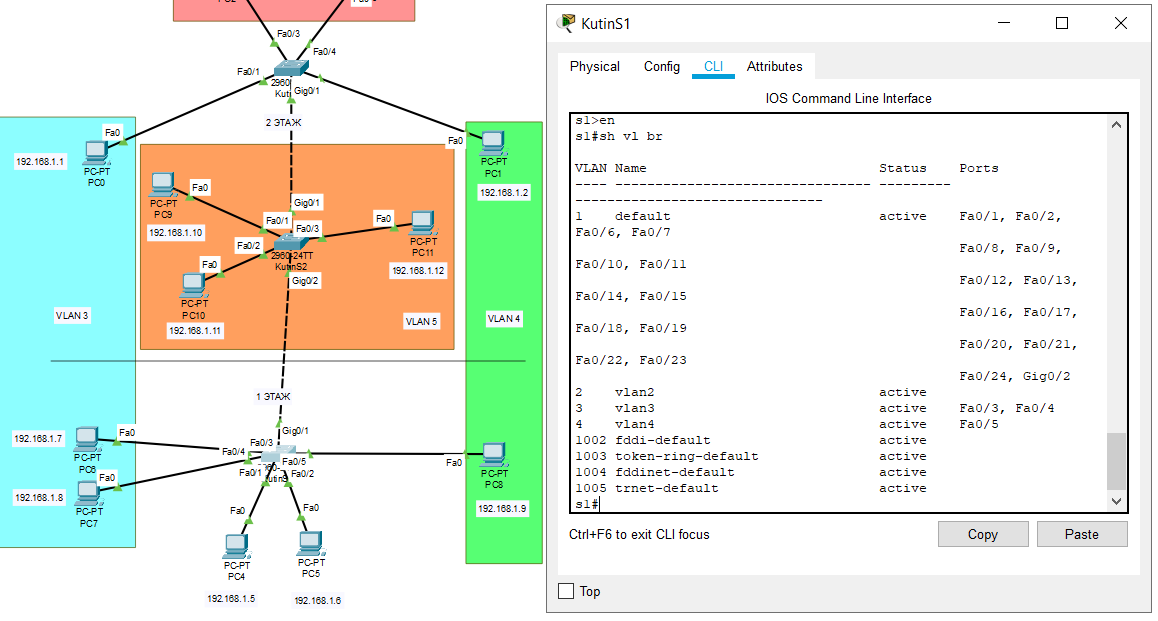
****

Рисунок 27 - Структура сети с KutinS1 и вывод команды show vlan brief

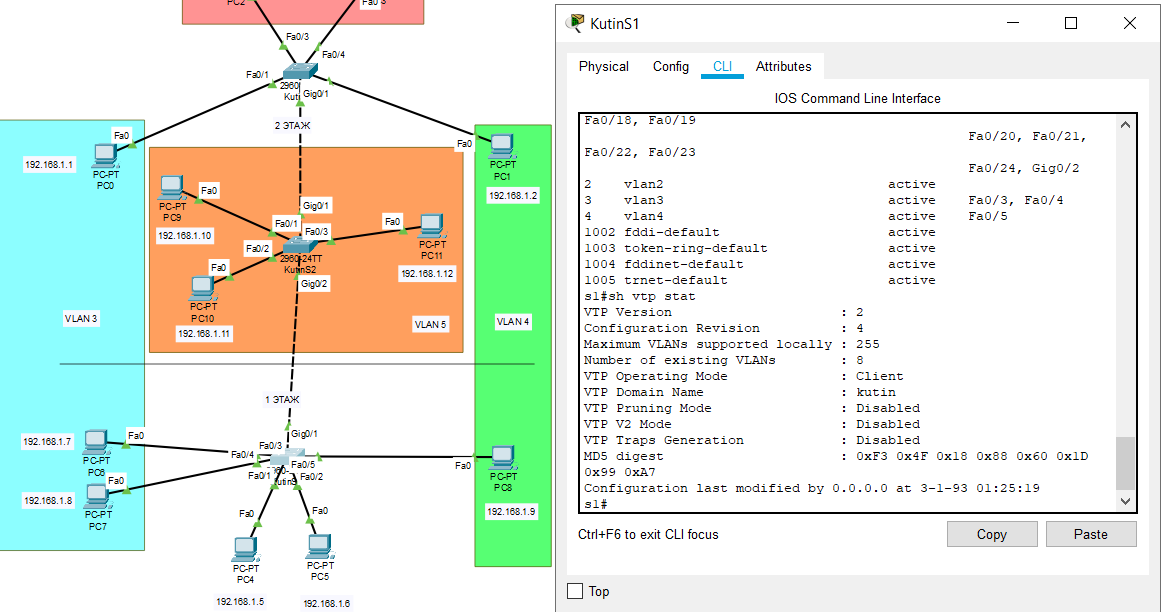


Рисунок 28 - Структура сети с KutinS1 и вывод команды show vtp status

**4. Заключение**

VTP – это отличная штука, обеспечивающая автоматическое обновление информации во всех клиентских сетевых устройствах после внесения изменений в устройство-сервер. Вам не нужно вручную вносить изменения в базу данных VLAN всех свитчей – репликация происходит автоматически.

Распределение узлов по разным виртуальным локальным сетям имеет массу преимуществ, вот некоторые из них:

* уменьшение количества широковещательного трафика в сети, это снижает издержки, которые связаны с пребыванием каждого узла в VLAN-сети;
* 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. Это позволяет создавать более гибкие проекты, в которых пользователи могут быть сгруппированы по отделам или по работающим вместе коллективам;
* достижение более высокой степени безопасности за счет выделения узлов, предназначенных для работы с конфиденциальными данными, в отдельные VLANceти;
* отделение трафика, передаваемого IР-телефонами, от трафика, передаваемого персональными компьютерами, к которым подключены эти телефоны;
* уменьшение рабочей нагрузки на средства протокола STP (SpanningTreeProtocol) путем ограничения размеров VLAN-ceти до отдельного коммутатора доступа;
* протокол VTP поддерживает систему доменных имен, с помощью которой можно создавать разные VTP-домены для разных отделов. Это позволяет иметь несколько независимых баз данных VLAN.

VLAN обеспечивают гибкость в разработке и внедрении инфраструктуры коммутируемой сети. Сети, в которых используется разделение на виртуальные локальные сети можно легко перестраивать согласно потребностям пользователей. Сети VLAN является частью любой серьезной сетевой разработки, однако необходимо понимать потребности пользователей и пути потоков информации до внедрения виртуальных сетей. Нужно тщательно взвесить преимущества использования дополнительных VLAN с точки зрения производительности и администрирования.

Однако внедрение VLAN в локальные сети также имеет следующие недостатки:

* повышение стоимости оборудования, поддерживающего VLAN. Протоколы DTP и VTP являются проприетарными разработками компании Cisco, это означает, что использование этих протоколов возможно только на оборудовании Cisco, которое по стоимости является одним из самых дорогих;
* сложность конфигурации нескольких VTP-доменов в сети.