Лабораторная работа № 5

ИЗУЧЕНИЕ ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ СЕТЕЙ

Цель работы

Изучить способы организации и назначение виртуальных локальных сетей.

Термин VLAN это сокращение от Virtual Local-Area Network и наиболее часто связан с коммутаторами. Используя VLAN, вы можете помочь себе решить технические и производственные проблемы, но они могут быть использованы на ваше усмотрение. Создание очень большого числа VLAN в вашей сети может вызвать административный ночной кошмар. Если ваша организация собирается инвестировать деньги в коммутаторы Уровня 2, которые поддерживают VLAN, используйте преимущества технологии коммутации. Коммутаторы Уровня 2 обеспечивают скорость переправления фреймов, обеспечиваемую средой передачи данных и не дает задержки, которая возникает при использовании традиционных программно-ориентированных методов коммутации при помощи маршрутизаторов. Если вы собираетесь строить коммутируемую сеть, старайтесь по возможности использовать коммутацию Канального Уровня и маршрутизацию Уровня 3 по мере надобности. Существует множество новых продуктов на рынке сетевых продуктов, которые обеспечивают маршрутизацию Уровня 3 на скорости коммутации Уровня 2, но это выходит за границы этой главы.

Каждая виртуальная сеть VLAN в сущности, создает сеть Уровня 3, которая должна быть маршрутизирована, поэтому, если вы имеете не только трафик внутри рабочей группы, вам необходимы функции маршрутизации вашей сети. Бурный рост e-mail, сетей Intranet и Internet ведет к бурному росту числа групп серверов. Серверы могут содержать общие файлы, приложения и серверы баз данных, обычно сгруппированные в выделенную сеть или сети VLAN и требует связи с пользователями, выходя за границы VLAN используя маршрутизаторы. Как напоминание, старайтесь разрабатывать вашу конфигурацию как можно более простой и гибкой. Начните с простого, затем внедряйте более комплексную конфигурацию, если существующая конфигурация не удовлетворяет вашим потребностям. Используйте VLAN для того, чтобы сделать вашу жизнь легче, а не тяжелее.

Коммутация и Виртуальные Локальные сети VLAN

Изначально коммутаторы не обеспечивали возможности создания Виртуальных Локальных сетей, так как они использовались для простой пересылки фреймов между устройствами. Рынок коммутаторов начал быстро расти, когда концентраторы коллективного доступа к среде передачи данных (hubs) начали не справляться с растущими запросами на расширение полосы пропускания сети в связи с использованием приложений клиент-сервер, обеспечивающих Графический Интерфейс Пользователя (GUI).

Ключевая разница между коммутатором и концентратором заключается в том, как они работают с фреймами. Концентратор получает фрейм, затем копирует и передает (повторяет) фрейм во все другие порты. В этом случае сигнал повторяется, в основном продляя длину сетевого сегмента до всех подключенных станций. Коммутатор повторяет фрейм во все порты кроме того, из которого этот фрейм был получен: *unicast* фреймы (адресованные на конкретный MAC адрес), *broadcast* фреймы, (адресованные для всех MAC адресов в локальном сегменте), и *multicast* фреймы (адресованные для набора устройств в сегменте). Это делает их неприемлемыми для большого числа пользователей, так как каждая рабочая станция и сервер, подключенный к коммутатору, должен проверять каждый фрейм для того, чтобы определить, адресован ли этот фрейм ему или нет. В больших сетях, с большим количеством фреймов, обрабатываемых сетевой картой, теряется ценное процессорное время. Это приемлемо для небольших рабочих групп, где передача данных имеет кратковременную "взрывную" природу.

Коммутатор работает с фреймами "с пониманием" - он считывает MAC адрес входящего фрейма и сохраняет эту информацию в таблице коммутации. Эта таблица содержит MAC адреса и номера портов, связанных с ними. Коммутатор строит таблицу в разделенной памяти и поэтому он знает, какой адрес связан с каким портом. Коммутаторы Cisco Catalyst создают эту таблицу, проверяя каждый фрейм, попавший в память, и добавляют новые адреса, которые не были занесены туда ранее. Маршрутизаторы Cisco создали эту таблицу, адресуя ее по содержимому (content-addressable memory). Эта таблица обновляется и строится каждый раз при включении коммутатора, но вы можете настраивать таймер обновления таблицы в зависимости от ваших нужд. Пример 1 показывает CAM таблицу коммутатора Catalyst 5000.

В этом примере столбец VLAN ссылается на номер VLAN, которой принадлежит порт назначения. Столбец Destination MAC ссылается на MAC адрес, обнаруженный в порту. Помните, что один порт может быть связан с несколькими MAC адресами, поэтому проверьте количество MAC адресов, которое может поддерживать ваш коммутатор. Destination Ports описывает порт, из которого коммутатор узнал MAC адрес.

Cat5500> show cam dynamic

VLAN	**Destination MAC**	**Destination Ports or VCs**
----------	----------	----------
1	00-60-2f-9d-a9-00	3/1
1	00-b0-2f-9d-b1-00	3/5
1	00-60-2f-86-ad-00	5/12
1	00-c0-0c-0a-bd-4b	4/10

Cat5500>

Рисунок 1 – Cisco CAM table

Далее, коммутатор проверяет MAC адрес назначения фрейма и немедленно смотрит в таблицу коммутации. Если коммутатор нашел соответствующий адрес, он копирует фрейм только в этот порт. Если он не может найти адрес, он копирует фрейм во все порты. Unicast фреймы посылаются на необходимые порты, тогда как multicast и broadcast фреймы передаются во все порты.

Коммутация была объявлена как "новая" технология, которая увеличивает пропускную способность и увеличивает производительность, но на самом деле коммутаторы это высокопроизводительные мосты (bridges) с дополнительными функциями. Коммутация это термин, используемый в основном для описания сетевых устройств Уровня 2, которые переправляют фреймы, основываясь на MAC адресе получателя.

Два основных метода, наиболее часто используемых производителями для передачи трафика это *cut-through* и *store and forward* .

Коммутация cut-through обычно обеспечивает меньшее время задержки, чем store-and-forward потому, что в этом режиме коммутатор начинает передачу фрейма в порт назначения еще до того, как получен полностью весь фрейм. Коммутатору достаточно того, что он считал MAC адреса отправителя и получателя, находящиеся в начале Token Ring и Ethernet фреймов. Большинство cut-through коммутаторов начинает пересылку фрейма, получив только первые 30 - 40 байт заголовка фрейма.

Store and forward копирует весь фрейм перед тем, как пересылать фрейм. Этот метод дает большую задержку, но имеет больше преимуществ. Возможности фильтрации, управления и контроля за потоком информации являются главными преимуществами этого метода. В дополнение, неполные и поврежденные фреймы не пересылаются, так как они не являются правильными фреймами. Коммутаторы должны иметь буферную память для чтения и сохранения фреймов во время принятия решения, что увеличивает стоимость коммутатора.

По мере улучшения технологий и захвата рынка новомодной технологией, начали возникать VLAN. Простейший путь понять Виртуальные сети - сравнить их с физической сетью. Физическая сеть может состоять из конечных станций, связанных маршрутизатором (или маршрутизаторами), которые используют одно физическое соединение. VLAN это логическое комбинирование конечных станций в одном сегменте на Уровне 2 и Уровне 3, которые связаны напрямую, без маршрутизатора. Обычно пользователям, разделенным физически, требуется маршрутизатор для связи с другим сегментом. Коммутаторы с возможностью построения VLAN изначально были внедрены в основных учебных городках и небольших рабочих группах. Сначала коммутация разрабатывалась по мере надобности, но сейчас это является обычной практикой внедрять коммутаторы и VLAN в настольных системах.

Каждая рабочая станция в VLAN (и только эти конечные станции) обрабатывают широковещательный трафик, посылаемый другим членам VLAN. Например, рабочие станции A, B, и C присоединены в VLAN 1. VLAN 1 состоит из трех коммутаторов Catalyst 5500. Все коммутаторы рас-

положены на разных этажах и соединены между собой опто-волокном и связаны транковым протоколом. Рабочая станция A присоединена с коммутатором A, рабочая станция B присоединена в коммутатор B и рабочая станция C присоединена в коммутатор C. Если станция A посылает широковещательный пакет, станции B и C получат этот фрейм, даже если они физически присоединены в другие коммутаторы. Рабочая станция D присоединена в коммутатор A, но объявлена в VLAN 2. Когда D посылает широковещательный пакет, станция A не увидит этот трафик, хотя она находится в том же физическом коммутаторе, но так как она находится не в той же виртуальной LAN, коммутатор не будет пересылать этот трафик на A. Помните, что VLAN работают на Уровне 2, поэтому связь между VLAN требует принятия решений маршрутизации на Уровне 3. Так же станции B и C не увидят трафик от станции D.

Виртуальные сети (VLAN) предлагают следующие преимущества:

- Контроль за широковещательным трафиком
- Функциональные рабочие группы
- Повышенная безопасность

Контроль за широковещательным трафиком

В отличие от традиционных LAN, построенных при помощи маршрутизаторов/мостов, VLAN может быть рассмотрен как широковещательный домен с логически настроенными границами. VLAN предлагает больше свободы, чем традиционные сети. Ранее используемые разработки были основаны на физическом ограничении сетей, построенных на основе концентраторов; в основном физические границы LAN сегмента ограничивались эффективной дальностью, на которую электрический сигнал мог пройти от порта концентратора. Расширение LAN сегментов за эти границы требовало использования повторителей (repeaters), устройств, которые усиливали и пересылали сигнал. VLAN позволяет иметь широковещательный домен вне зависимости от физического размещения, среды сетевого доступа, типа носителя и скорости передачи. Члены могут располагаться там, где необходимо, а не там, где есть специальное соединение с конкретным сегментом. VLAN увеличивают производительность сети, помещая широковещательный трафик внутри маленьких и легко управляемых логических доменов. В традиционных сетях с коммутаторами, которые не поддерживают VLAN, весь широковещательный трафик попадает во все порты. Если используется VLAN, весь широковещательный трафик ограничивается отдельным широковещательным доменом.

Функциональные рабочие группы

Наиболее фундаментальным преимуществом технологии VLAN является возможность создания рабочих групп, основываясь на функциональности, а не на физическом расположении или типе носителя. Традиционно администраторы группировали пользователей функционального подразделения физическим перемещением пользователей, их столов и серверов в общее ра-

бочее пространство, например в один сегмент. Все пользователи рабочей группы имели одинаковое физическое соединение для того, чтобы иметь преимущество высокоскоростного соединения с сервером. VLAN позволяет администратору создавать, группировать и перегруппировывать сетевые сегменты логически и немедленно, без изменения физической инфраструктуры и отсоединения пользователей и серверов. Возможность легкого добавления, перемещения и изменения пользователей сети - ключевое преимущество VLAN.

Повышенная Безопасность

VLAN также предлагает дополнительные преимущества для безопасности. Пользователи одной рабочей группы не могут получить доступ к данным другой группы, потому что каждая VLAN это закрытая, логически объявленная группа. Представьте компанию, в которой Финансовый департамент, который работает с конфиденциальной информацией, расположен на трех этажах здания. Инженерный департамент и отдел Маркетинга также расположены на трех этажах. Используя VLAN, члены Инженерного отдела и отдела Маркетинга могут быть расположены на всех трех этажах как члены двух других VLAN, а Финансовый департамент может быть членом третьей VLAN, которая расположена на всех трех этажах. Сейчас сетевой трафик, создаваемый Финансовым департаментом, будет доступен только сотрудникам этого департамента, а группы Инженерного и отдела Маркетинга не смогут получить доступ к конфиденциальным данным Финансового департамента. Очевидно, есть другие требования для обеспечения полной безопасности, но VLAN может быть частью общей стратегии сетевой безопасности. Показанный ниже рисунок говорит о том, как функционирование VLAN может расширить традиционные границы.

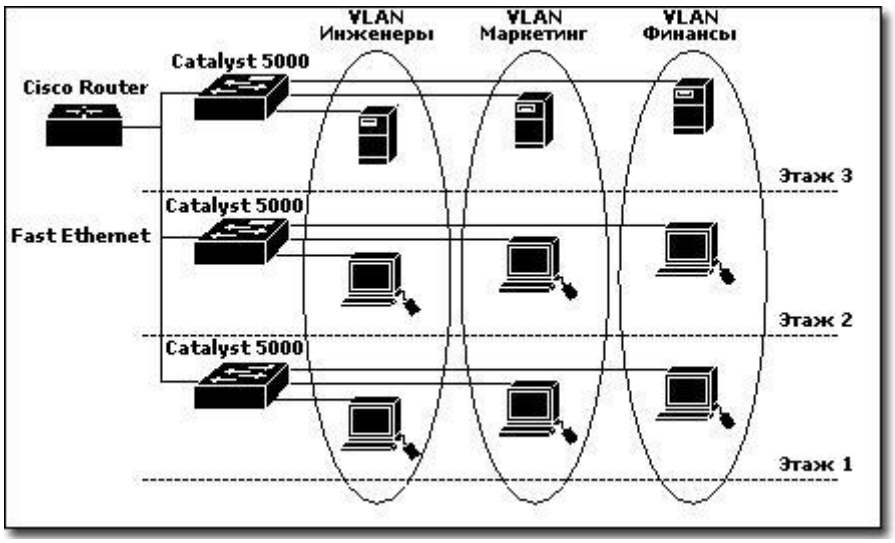

Рисунок 2

Когда VLAN объявлены для устройств, они могут быть легко и быстро изменены для добавления, перемещения или изменения пользователя по мере надобности.

Сети VLAN могут быть определены по:

- Порту (наиболее частое использование)
- MAC адресу (очень редко)
- Идентификатору пользователя User ID (очень редко)
- Сетевому адресу (редко в связи с ростом использования DHCP)

VLAN, базирующиеся на номере порта позволяют определить конкретный порт в VLAN. Порты могут быть определены индивидуально, по группам, по целым рядам и даже в разных коммутаторах через транковый протокол. Это наиболее простой и часто используемый метод определения VLAN. Это наиболее частое применение внедрения VLAN, построенной на портах, когда рабочие станции используют протокол Динамической Настройки TCP/IP (DHCP).

VLAN, базирующиеся на MAC адресах позволяет пользователям находиться в той же VLAN, даже если пользователь перемещается с одного места на другое. Этот метод требует, чтобы администратор определил MAC адрес каждой рабочей станции и затем внес эту информацию в коммутатор. Этот метод может вызвать большие трудности при поиске неисправностей, если пользователь изменил MAC адрес. Любые изменения в конфигурации должны быть согласованы с сетевым администратором, что может вызывать административные задержки.

Виртуальные сети, базирующиеся на сетевых адресах, позволяют пользователям находиться в той же VLAN, даже когда пользователь перемещается с одного места на другое. Этот метод перемещает VLAN, связывая ее с сетевым адресом Уровня 3 рабочей станции для каждого коммутатора, к которому пользователь подключен. Этот метод может быть очень полезным в ситуации, когда важна безопасность и когда доступ контролируется списками доступа в маршрутизаторах. Поэтому пользователь "безопасной" VLAN может переехать в другое здание, но остаться подключенным к тем же устройствам потому, что у него остался тот же сетевой адрес. Сеть, построенная на сетевых адресах, может потребовать комплексного подхода при поиске неисправностей.

Протокол Spanning-Tree и сети VLAN

Протокол Spanning-Tree позволяет иметь избыточные физические связи в мостовых сетях, но иметь только одно физическое соединение, пересылающее фреймы. Этот протокол переводит избыточные физические соединения с сегментом назначения в режим блокирования. Когда происходят события, изменяющие топологию сети, STP протокол производит ре-калькуляцию, какие соединения будут переправлять фреймы, а остальные останутся в заблокированном состоянии. Имеется два главных метода мостового соединения - прозрачное (transparent) и маршрутизируемое источником (source-route). STP протокол используется в прозрачном мостовом соединении для избежания

циклов в сетевых сегментах, обеспечивая также избыточность на случай неисправностей.

Прозрачное мостовое соединение в основном используется в окружении Ethernet. Этот метод возлагает ответственность за определение пути от источника к приемнику на мост. Ethernet фреймы не содержат поле RIF информации о маршруте (Routing Information Field) как, например, фреймы Token Ring, поэтому устройства просто посылают фреймы и подразумевают, что они достигнут пункта назначения. Процесс, используемый мостами для переправки фреймов, подобен тому, как работают коммутаторы Уровня 2. Прозрачное объединение проверяет входящие фреймы и запоминает MAC адрес получателя. Мост ищет этот адрес в таблице; Если он нашел его, он переправляет фрейм в соответствующий порт. Если MAC адрес не был найден, он копирует и переправляет фрейм во все порты, кроме того, из которого фрейм пришел.

Соединение, маршрутизируемое источником, используется в окружении Token Ring. Этот метод возлагает ответственность поиска устройства назначения на передающую станцию. Устройство Token Ring посылает тестовый фрейм для определения, располагается ли устройство назначения в локальном кольце. Если не было получено ответа, устройство посылает поисковый фрейм как широковещательный пакет. Широковещательный пакет пересекает сеть через другие мосты и каждый мост добавляет номер кольца и номер моста, в котором это кольцо существует пока фрейм не достигнет получателя. Комбинация номера кольца и номера моста содержится в поле RIF. Устройство-получатель отвечает на поисковый фрейм и, в конечном счете, устройство-источник получает фрейм-ответ. Теперь связи начинается с того, что каждая станция добавляет поле RIF в каждый фрейм. Соединение, маршрутизируемое источником, переправляет фреймы, основываясь на информации поля RIF, и не строит таблицу MAC адресов и портов, так как конечные устройства обеспечивают информацию о пути от источника к приемнику в поле RIF.

Для обсуждения мы рассмотрим проблему, связанную с циклами и прозрачным объединением сетей, так как это наиболее распространено сегодня. Представьте себе два сетевых сегмента, сегмент A и сегмент B с одной рабочей станцией в каждом: станция A и станция B соответственно. Два прозрачных моста присоединены к обоим сегментам A и B, создавая цикл в сети. Станция A посылает широковещательный фрейм для станции B, и оба моста считывают фрейм с их сегмента A и переправляют его в сегмент B. Оба моста связывают адрес станции A с их сегментом A в таблице адресов. Ethernet фрейм имеет адресом источника станцию A и адресом получателя широковещательный адрес. После того, как мосты переправили фрейм в сегмент B, он имеет тот же адрес отправителя и получателя, так как мосты работают на Уровне 2 и не изменяют адресов, когда переправляют фреймы. Фрейм, полученный обоими мостами в сегменте B, аккуратно переправляется назад в сегмент A, так как моты переправляют фреймы на все остальные порты. В дополнение, мосты обновляют их таблицы, связывая адрес станции A с их

интерфейсом сегмента B. Мосты будут продолжать переправлять эти фреймы снова и снова. Очевидно, что это приведет к снижению производительности сети, так как каждое устройство в сети будет обрабатывать эти фреймы снова и снова, теряя процессорное время на каждом устройстве и уменьшая пропускную способность сети. Этот пример проиллюстрирован ниже.

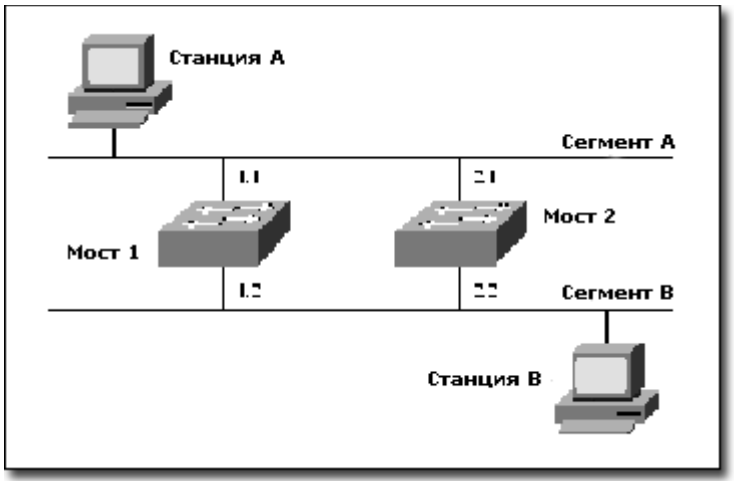

Рисунок 3

Избыточная топология с циклами

Главной причиной разработки протокола Spanning-Tree Protocol было устранение циклов в сети. Протокол Spanning-Tree гарантирует отсутствие циклов, блокируя один из портов моста ("blocking mode"), предотвращая передачу пакетов. Обратите внимание, что блокировка может быть снята, если текущий активный порт переходит в нерабочее состояние. Когда происходит изменение топологии сети, мост производит ре-калькуляцию состояния, рассылая пакеты BPDU (Bridge Protocol Data Units). При помощи BPDU, мосты обмениваются информацией, определяя, какие порты нужно блокировать.

Сейчас, когда мы понимаем основы Spanning Tree, как это относится к коммутаторам. Коммутаторы функционируют подобно мостам, поэтому каждый коммутатор принимает участие в процессе spanning-tree, если это не отключено в конфигурации. Вы должны иметь достаточно оснований для того, чтобы запретить обработку spanning tree на вашем коммутатору, так как это может вызвать серьезные проблемы. Коммутаторы гарантируют отсутствие циклов в топологии, используя алгоритм spanning-tree (STA). Алгоритм spanning-tree осуществляет топологию без циклов для каждой сети VLAN, настроенной в вашем коммутаторе. Поэтому присоединение любых сетевых устройств (кроме серверов или рабочих станций) может вызвать цикл в вашей сети, если запрещена обработка протокола spanning-tree . Главная проблема, создаваемая циклами в сети, это широковещательный шторм (broadcast storm). Это состояние сети, когда коммутаторы или мосты продолжают переправлять широковещательные пакеты во все подключенные порты; другие коммутаторы и мосты, присоединенные в ту же сеть, создавая цикл, продолжают переправлять те же фреймы назад в посылающий коммутатор или мост. Эта проблема сильно уменьшает производительность сети, так как

сетевые устройства постоянно заняты копированием широковещательных пакетов во все порты.

Настройка VLAN по умолчанию

Коммутаторы Catalyst имеют несколько VLAN, объявленных по умолчанию. Сеть VLAN 1 объявлена всегда, и все активные порты сгруппированы в нее по умолчанию. Если вам требуется добавить больше виртуальных сетей, вам нужно создать их, используя команду *SET VLAN* . VLAN 1 будет показываться, используя имя DEFAULT в любой команде *SHOW VLAN* . Дополнительно объявлены сети VLAN 1002 – 1005 для FDDI и Token Ring. Вам не нужно волноваться об удалении этих сетей, так как они являются частью конфигурации по умолчанию. В примере ниже показана такая конфигурация.

```
Cat5500> (enable) show vlan
VLAN  Name                 Status  Mod/Ports,    Vlans
-----  -------------------  -------  ------------  --------------
1     default              active  1/1-2
                                    3/1-24
                                    4/1-24
1002  fddi-default         active
1003  token-ring-default   active
1004  fddinet-default      active
1005  trnet-default        active
```

Рисунок 4

```
VLAN  Type         SAID        MTU     Parent  RingNo  BrdgNo  Stp  BrdgMode    Trans1  Trans2
--------  -------------  ----------  ---------  ---------  ----------  ----------  -----  -------------  ---------  ---------
1     enet         100001      1500    -       -       -       -    -           0       0
1002  fddi         101002      1500    -       0x0     -       -    -           0       0
1003  trcrf        101003      1500    0       0x0     -       -    -           0       0
1004  fdnet        101004      1500    -       -       0x0     -                0       0
1005  trbrf        101005      1500    -       -       0x0     -                0       0

VLAN  AREHops      STEHops     Backup  CRF
--------  -------------  ----------  ---------  ---------
1003  7            7           off

Cat5500> (enable)
```

Рисунок 5 – Просмотр сетей VLAN в Catalyst 5500

Настройка сетей VLAN через домены

Разработка любой сетевой конфигурации должна включать в себя сбор информации о потребностях пользователей для наиболее эффективного, простого и логичного использования сетевых ресурсов. Перед тем, как создавать

VLAN в ваших коммутаторах, вы должны затратить время для создания логической схемы вашей сети. Полезные вопросы, на которые стоит ответить:

- Сколько пользователей будет в каждой VLAN?
- Разделены ли VLAN физически?
- Сколько требуется усилий для создания новой VLAN?

Для обмена информацией о VLAN между коммутаторами вы должны создать транковые порты. Транковый порт это порт или группа портов, используемые для передачи информации о VLAN в другие сетевые устройства, присоединенные к этому порту и использующие транковый протокол. Транковый протокол это "язык", который коммутаторы используют для обмена информацией о VLAN. Примеры транковых протоколов - ISL и IEEE 802.1Q. Обратите внимание, что обычные порты не рекламируют информацию о VLAN, но любой порт может быть настроен для приема/передачи информации о VLAN. Вы должны активизировать транковый протокол на нужных портах, так как он выключен по умолчанию. Транковый порт это порт, предназначенный исключительно для пересылки VLAN информации используя транковый протокол. Cisco коммутаторы в основном используют протокол Inter-Switch Link (ISL) для обеспечения совместимости информации.

Для автоматического обмена информацией о VLAN через транковые порты, вам нужно настроить Cisco VLAN Trunk Protocol (VTP), который позволяет коммутаторам посылать информацию о VLAN в форме "рекламы" соседним устройствам. Передаваемая информация включает домен, номер версии, активные VLAN и другую информацию. Вы настроите сервер и, по выбору, клиентов. Преимуществом использования VTP является то, что вы можете контролировать добавление, удаление или изменение сетей VLAN в дизайне вашего коммутатора. Недостатком является ненужный трафик, создаваемый на транковых портах для устройств, которым возможно не нужна эта информация. Коммутаторы Cisco возможность ограничения VLAN информации, пересылаемой через транковый порт, используя возможность "отсечения" (pruning option). Используя VTP, вы можете гарантировать, что ваш VLAN дизайн будет распространен во все коммутаторы, использующие протокол VTP в том же домене. VTP посылает VLAN информацию через транковые порты на групповой адрес (multicast address), но не пересылает ее на обычные (не транковые) порты коммутатора.

Другая возможность - настройка коммутатора для режима прозрачной передачи и настройка каждой VLAN в каждом коммутаторе вручную. Это очень важное решение в разработке вашей сети. Если ваша сеть будет содержать много коммутаторов, содержащих много виртуальных сетей, расположенных в разных коммутаторах, возможно, имеет смысл использовать VTP. Если ваша сеть останется достаточно статической, VLAN не будут добавляться или изменяться по отношению к начальной конфигурации, прозрачное соединение может работать лучше. VTP требует использования программы сетевого управления Cisco VLAN Director для управления вашими коммутаторами. Если вы беспокоитесь об административном управлении, VTP может обеспечить решение проблемы. Вы имеете возможность установить пароль

на VTP домен для контроля изменения VLAN информации вашей сети. Дополнительно, оставив активными опции по умолчанию в ваших основных коммутаторах, вы можете контролировать процесс обновления информации. После настройки ваших коммутаторов как VTP серверов, остальные коммутаторы вашей сети могут быть настроены как клиенты, которые только получают VLAN информацию.

Настройка VTP

1. Загрузитесь в коммутатор, используя консольный порт. Если у коммутатора настроен IP адрес и маршрут по умолчанию (default route),вы можете использовать Telnet.
2. Перейдите в привилегированный режим (enable mode).
3. Объявите VTP домен, набрав команду set vtp domain *name* .
4. Вы можете разрешить режим отсечения (pruning), набрав set vtp pruning enable .
5. Вы можете установить пароль, набрав set vtp password *password* .
6. Создайте VLAN, набрав set vlan 2 .

```
Cat5500> (enable) show vtp statistics

VTP statistics:
   summary advts received 0
   subset advts received 0
   request advts received 0
   summary advts transmitted 3457
   subset advts transmitted 13
   request advts transmitted 0
No of config revision errors 0
No of config digest errors 0

VTP pruning statistics:
Trunk    Join Trasmitted Join Received Summary advts received from
                                       non-pruning-capable device
-------- --------------- ------------- --------------------------
  1/1-2  0               0             0

Cat5500> (enable)
```

Рисунок 6 – Отображение VTP статистики в коммутаторе Catalyst 5500

Результат выполнения команды SHOW VTP DOMAIN показан ниже. Имя домена задается, когда вы используете команду SET VTP DOMAIN . Локальный режим определяет режим сервера, клиента или прозрачный режим. Серверы могут обновлять VLAN информацию в VTP домене; клиенты только получают VLAN информацию. Поле Vlan-Count показывает число сетей VLAN, настроенных в коммутаторе.

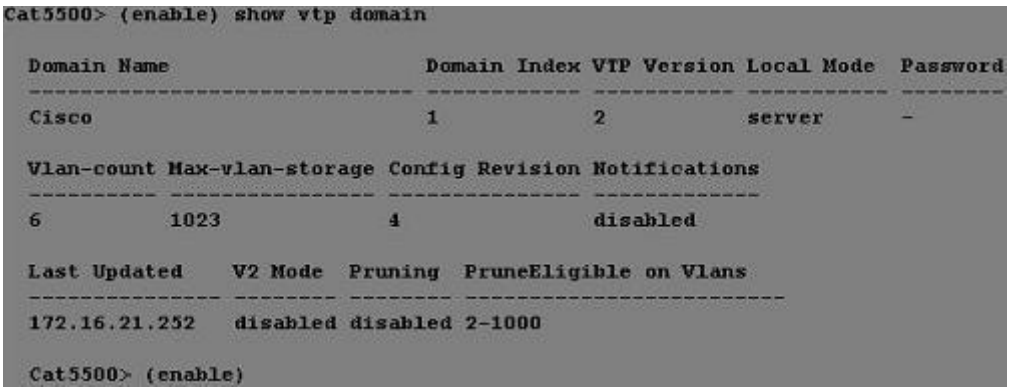

Рисунок 7 – Отображение VTP конфигурации в коммутаторе Catalyst 5500

Другой возможностью при настройке VLAN является использование дружественных имен при добавлении сетей VLAN в вашу сеть. На практике, проще использовать номера и документировать то, что вы настроили в ваших коммутаторах. Это может быть проще для пользователей, ссылаться на VLAN 1 как на Marketing VLAN, или ссылаться на VLAN 2 как на Sales VLAN. Если ваша организация решила вложить деньги в Cisco Route Switch Module (RSM), вы, возможно, захотите заняться цифровой схемой вашей VLAN. RSM это полнофункциональный Cisco маршрутизатор, устанавливаемый в коммутатора серии Catalyst 5 *x* 00. RSM не имеет внешних интерфейсных портов, потому что он имеет интерфейс на соединительной плате коммутатора Catalyst. Интерфейсы настраиваются как сети VLAN в карте RSM, и согласуется с виртуальными сетями, объявленными в вашем коммутаторе Catalyst. Для административных целей проще ссылаться на цифры, поэтому если пользователи находятся в VLAN 2, вам проще запомнить, какой интерфейс маршрутизатора нужно проверить для решения проблем. Однако если вы решили использовать дружественные имена, коммутатор Catalyst будет поддерживать и их.

Настройка сетей VLAN, используя имена

1. Загрузитесь в коммутатор, используя консольный порт. Если у коммутатора настроен IP адрес и маршрут по умолчанию (default route),вы можете использовать Telnet.
2. Перейдите в привилегированный режим (enable mode).
3. Разрешите протокол VTP версии 2, набрав **set vtp v2 enable** .
4. Объявите VTP домен, набрав **set vtp domain *name*** .
5. Переведите коммутатор в режим сервера, набрав **set vtp mode server** .
6. Вы можете разрешить режим отсечения (pruning), набрав **set vtp pruning enable** .
7. Вы можете установить пароль, набрав **set vtp password *password*** .
8. Создайте виртуальную сеть VLAN, набрав **set vlan 2 name *vlan_name* state active** .

Если вы хотите задать имя вашей VLAN, убедитесь, что вы использовали параметр NAME и имя сети VLAN на 8 шагу.

Группирование портов коммутатора в сети VLAN

Следующим шагом является назначение портов в вашу VLAN. Эта опция обеспечивает гибкость при эффективном назначении портов коммутатора в требуемую VLAN без потери портов. Предположим, вы имеете Catalyst 5500 с десятью 24-портовыми картами, всего 240 портов. Теперь предположим, что вы имеете 60 пользователей в VLAN 1 и ожидаете, что их число возрастет до 150. Также вы имеете 40 пользователей в VLAN 2 и ожидаете их рост до 8080. Вы могли бы определить точно 60 портов в VLAN 1 и 40 портов в VLAN 2, или вы можете назначить дополнительные порты в сети VLAN, учитывая их предстоящий рост.

На практике бывает легче объявить дополнительные порты в каждой VLAN и сгруппировать их по физическим картам для уменьшения бремени администрирования. Например, назначить в вашу VLAN 1 порты последовательно, начиная с порта 1 до порта 24 карты номер 3. Повторив это назначение VLAN 1 для карт 4, 5, 6, 7 и 8 вы подключите 144 точки в VLAN 1. Теперь назначьте порты с 1 по 24 карты номер 9 и повторите это для карт 10, 11 и 12 и вы будете иметь 96 портов в VLAN 2. Рисунок ниже иллюстрирует эти две VLAN и связанные с ними порты.

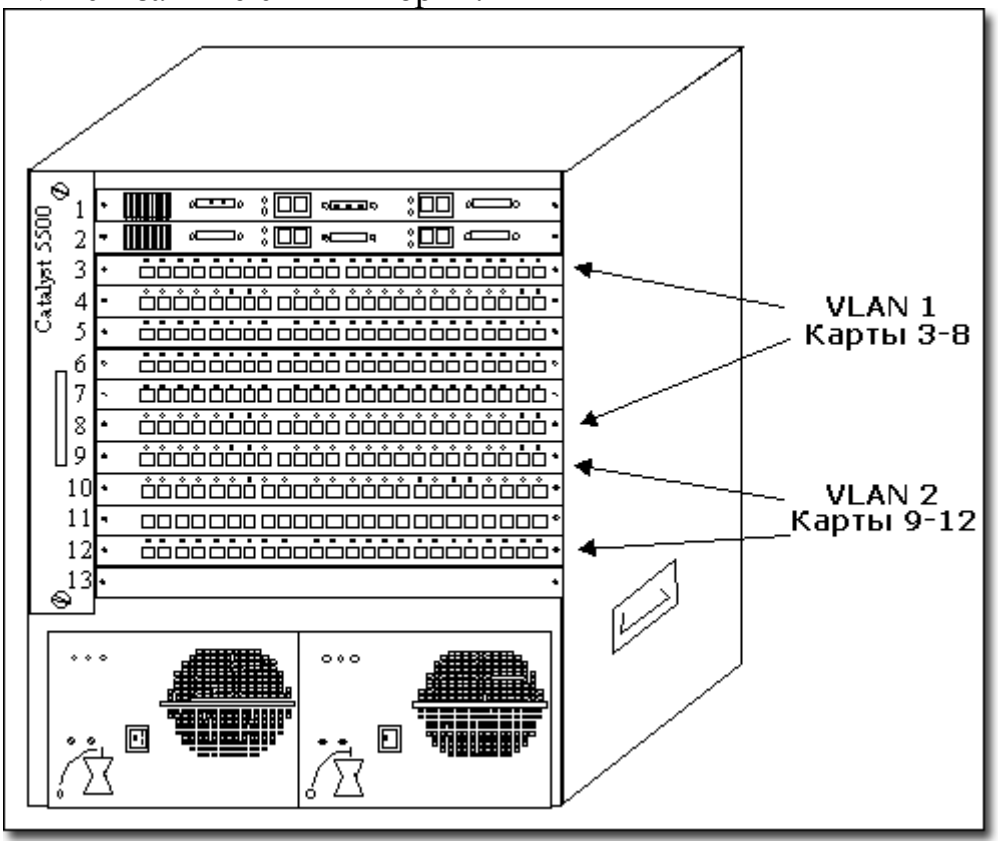

Рисунок 8

Назначение портов в VLAN

Последовательное назначение портов будет поддерживать ваши ежедневные затраты на администрирование минимальными. Что проще понять - две VLAN, назначенные последовательно в коммутаторе или разбросанные по разным картам. Например, это будет выглядеть странно, если VLAN 1 бы-

ла назначена для карт 3 – 6 и VLAN 2 для карт 7 – 8. Затем VLAN 1 добавляет 24 пользователя в карту 9. Теперь очень важно, чтобы ваша документация выросла. Что, если вы заболели, и человек без соответствующего опыта добавил пользователей в VLAN 2, но подключил их в карту, назначенную в VLAN 1. Помните: делайте все простым.

Важно обращать внимание на разные опции группирования портов коммутатора в зависимости от типа линейной карты. Catalyst 5000 24 Port 10/100 Dedicated Switch Module позволяет вам назначать каждый порт в отдельную VLAN, если необходимо. Модуль коммутатора Catalyst 5000 «24 Port 100 Mb Group Switching Module» содержит три переключаемых порта для 24 пользовательских портов. Порты 1 – 8 связаны с коммутируемым портом #1, порты 9 – 16 связаны с портом #2 и порты 17 – 24 связаны с портом #3. Поэтому вы можете объявить максимум три различных VLAN в модуле групповой коммутации. Потратьте время для изучения руководства по настройке для понимания того, какие возможности группирования портов в VLAN поддерживается картой.

Для примера, мы настроим 24-портовый 10/100 Dedicated Switch Module. Допустим, вы имеете десять карт в слотах 3 – 12, и VLAN 1 и 2 уже объявлены. Помните, что вы свободны в назначении портов для улучшений в организации - назначаем их последовательно для облегчения администрирования.

Объединение портов коммутатора в VLAN

1. Загрузитесь в коммутатор, используя консольный порт. Если в коммутаторе настроен IP адрес и маршрут по умолчанию, вы можете использовать Telnet.
2. Перейдите в привилегированный режим.
3. Назначьте порты в VLAN 1, набрав **set vlan 1 3/1-24, 4/1-24, 5/1-24**
4. Назначьте порты в VLAN 2, набрав **set vlan 2 6/1-24, 7/1-24**

Проверьте, что вы правильно настроили порты вашего коммутатора, используя команды:

```
Cat5500> (enable) show port status
 Port  Name          Status     Vlan       Level  Duplex Speed Type
 ----- ------------ ---------- ---------- ------ ------ ----- ------------
 1/1   SUP II PRIM  connected  trunk      normal full   100   100BaseFX
 1/2   SUP II PRIM  connected  trunk      normal full   100   100BaseFX
 3/1                connected  1          normal a-half a-100 10/100BaseTX
 3/2                connected  1          normal a-full a-100 10/100BaseTX
 3/3                connected  1          normal a-full a-100 10/100BaseTX
 3/4                connected  1          norm ,eltnal a-full a-100 10/100BaseTX
 3/5                notconnect 1          normal auto   auto  10/100BaseTX
 3/6                notconnect 1          normal auto   auto  10/100BaseTX
 3/7                notconnect 1          normal auto   auto  10/100BaseTX
 3/8                notconnect 1          normal auto   auto  10/100BaseTX
 3/9                notconnect 1          normal auto   auto  10/100BaseTX
 3/10               notconnect 1          normal auto   auto  10/100BaseTX
Cat5500> (enable)
```

Рисунок 9 – Показ состояния портов Catalyst 5500

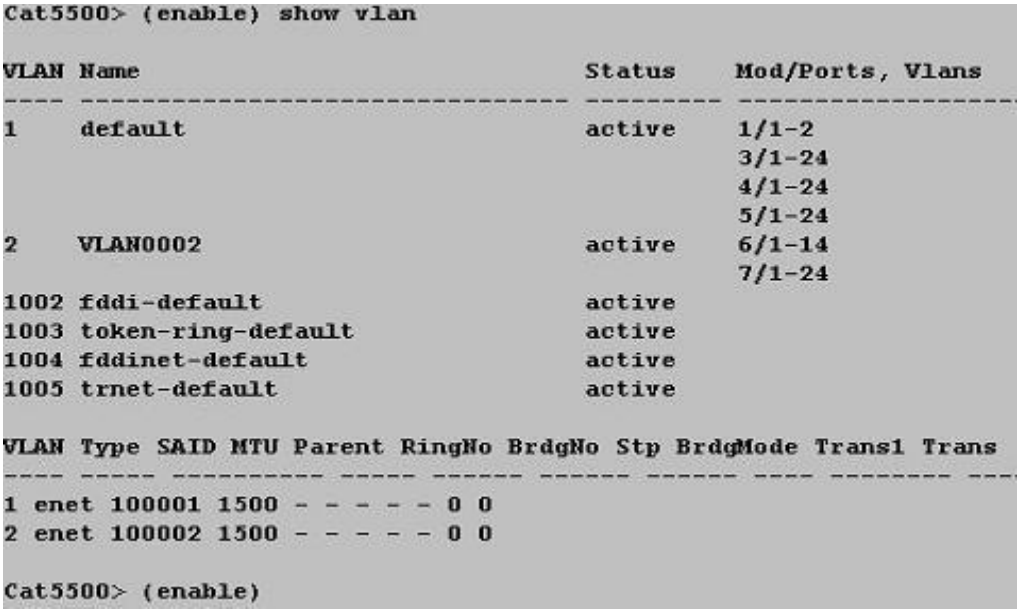

Рисунок 10 – Просмотр назначений VLAN в Catalyst 5500

После настройки портов вашего коммутатора в VLAN, вы должны рассмотреть возможность включения опции *portfast* в ваших портах для уменьшения шанса появления ежедневных проблем со связью. Помните, что коммутатор принимает участие в spanning-tree процессе; каждый порт коммутатора должен гарантировать, что он не создает цикла в сети. Например, представьте, что пользователь случайно подключил кросс-кабель в порт коммутатора, назначенный в VLAN 1 и соединил другой конец в другой порт коммутатора, также назначенный в VLAN 1. Итак, был создан цикл в сети, который теперь должен быть устранен. STA будет заботиться об этом, и на протяжении этого процесса состояние обоих портов будут изменяться при рекалькуляции. Существует пять главных состояний, в которых может находиться порт:

1. **Blocking** . Состояние всех портов по умолчанию, фреймы не переправляются портами в этом состоянии. После того, как коммутатор включен, все порты находятся в этом состоянии.
2. **Listening** . Состояние, следующее за состоянием *blocking* . Порт коммутатора так же не пересылает фреймы, но принимает участие в процессе spanning-tree для определения, нужно ли продолжать для пересылки фреймов.
3. **Learning** . Это состояние следует за состоянием *listening* . Порт коммутатора не пересылает фреймы, но готовится к переходу в состояние *forwarding* . Порт коммутатора анализирует фреймы для обучения MAC адресам.
4. **Forwarding.** Это состояние следует за состоянием *learning* . Теперь порт коммутатора пересылает фреймы и продолжает принимать участие в процессе spanning-tree . Это состояние требуется устройствам для нормального функционирования.
5. **Disabled** . Это состояние следует за состоянием *listening* . Порт коммутатора не пересылает фреймы.

Когда устройство первый раз присоединяется к порту, порт переходит из состояния blocking в состояние listening и затем в состояние learning перед тем, как начать переправлять фреймы, подразумевая, что процесс spanning-tree не нашел избыточных путей.

К счастью, Cisco обеспечивает возможность обойти этот процесс, когда устройство присоединяется к коммутатору **.** Опция *portfast* переведет порт в состояние forwarding , пропустив режимы listening и learning . По умолчанию, режим portfast отключен на всех портах. Рабочая станция или сервер, подключенные к порту с выключенным режимом portfast может сначала выглядеть как отключенный от сети. После того, как порт перейдет в состояние forwarding (после некоторого промежутка времени), устройство будет функционировать нормально. С выключенной функцией portfast, рабочая станция или сервер могут быть неспособны использовать программу ping, получить своевременно DHCP адрес или загрузиться в Novell Directory Services или сервер NetWare. Это происходит потому, что порт коммутатора не переправляет эти фреймы для запроса ping, DHCP, или загрузки в NDS. Вы можете избежать этих проблем, разрешив функцию portfast на всех портах, где подключены рабочие станции или серверы. Но будьте внимательны, так как эта команда может вызвать циклы в вашей сети.

Разрешение опции Portfast

1. Загрузитесь в коммутатор, используя консольный порт. Если в коммутаторе настроен IP адрес и маршрут по умолчанию, вы можете использовать Telnet.
2. Перейдите в привилегированный режим.
3. Разрешите режим portfast для VLAN 1, набрав команду set spantree portfast 3/1-24 enable .
4. Вы увидите следующее предупреждение :

```
Cat5500> (enable) set spantree portfast 3/1-24 enable
```

Рисунок 11

Warning: Spantree port fast start should only be enabled on ports connected to a single host. Connecting hubs, concentrators, switches, bridges, etc. to a fast start port can cause temporary spanning tree loops. Use with caution.

```
Spantree port 3/1-24 fast start enabled.
Cat5500> (enable)
```

Рисунок 12

Разрешение режима Portfast на Catalyst 5500

Далее проверьте, что вы настроили portfast правильно. Столбец Fast-Start содержит значение Enabled или Disabled . Enabled показывает, что режим fast-start включен и порт начнет переправлять фреймы, как только устройство будет присоединено и включено. Число показывает номер карты в коммутаторе. Вы также можете набрать эту же команду без номера для того, чтобы увидеть информацию portfast для всех портов.

```
Cat5500> (enable) show port span 3

   Port     Vlan Port-State    Cost  Priority Fast-Start Group
Method
   -------- ---- ------------- ----- -------- ----------
------------
   3/1      1    not-connected 100   32       enabled
   3/2      1    not-connected 100   32       enabled
   3/3      1    not-connected 100   32       enabled
   3/4      1    not-connected 100   32       enabled
   3/5      1    not-connected 100   32       enabled

   Cat5500> (enable)
```

Рисунок 13 – Проверка настройки функции portfast в Catalyst 5500

Настройка VLAN Транков

Транки используются для обмена информацией о VLAN между коммутаторами, обеспечивая тем самым возможность построения сетей VLAN, перекрывающих физические границы коммутатора. Концепция транкинга подобна протоколам маршрутизации, используемым для построения сетевой топологии. Коммутаторы используют транковые протоколы для того, чтобы определить, на какой порт посылать фреймы, если VLAN перекрывает физические границы. Используя транковый протокол, одна и та же VLAN может быть объявлена на каждом этаже 12-этажного дома. Коммутаторы Catalyst поддерживают различные транковые методы:

- **Inter-Switch Link (ISL)** Fast Ethernet (100 Mbps), Gigabit Ethernet (1000 Mbps)
- **IEEE 802.1Q** Fast Ethernet (100 Mbps), Gigabit Ethernet (1000 Mbps)
- **IEEE 802.10** Fiber/Copper Distributed Data Interface (FDDI)/(CDDI) (100 Mbps)
- **LAN Emulation** ATM (155 Mbps OC-3 and 622 Mbps OC-12)

Это всегда хорошая идея, посмотреть "Release Notes" новых версий операционной системы коммутатора, так как они включают новые функции и возможности коммутаторов. Это поможет убедиться в том, что коммутатор будет поддерживать функции, требуемые для построения вашей сети.

Далее мы кратко обсудим транковые протоколы ISL и IEEE 802.1Q и изучим команды для настройки ISL. Протоколы IEEE 802.10 и LAN Emulation выходят за границы обсуждения этой главы.

Настройка ISL Транка

ISL это танковый протокол, разработанный компанией Cisco исключительно для своих продуктов. Он позволяет устанавливать транки между коммутаторами, которые поддерживают Ethernet, FDDI, или Token Ring фреймы. Маршрутизаторы Cisco, настроенные на поддержку ICL могут понимать и осуществлять маршрутизацию между VLAN без физического подключения интерфейсных портов к каждой VLAN. Используя ISL, один Fast Ethernet

порт маршрутизатора может осуществлять маршрутизацию пакетов между двумя VLAN на коммутаторах.

Настройка ISL

1. Определите, какой порт вы будете использовать как транк.
2. Загрузитесь в коммутатор, используя консольный порт или Telnet.
3. Перейдите в привилегированный режим.
4. Настройте порт как ISL транк, используя команду **set trunk *mod_num/port_num* on** .
5. Удалите сети VLAN с транка (не обязательно), используя команду **clear trunk *mod_num/port_num vlan_num*** .
6. Добавьте сети VLAN в транк (не обязательно), используя команду **set trunk *mod_num/port_num vlan_num*** .

Проверьте правильность настройки ваших транковых портов, используя команду show trunk.

```
Cat5500> (enable) show trunk

Port     Mode         Encapsulation Status       Native vlan
-------- ------------ ------------- ------------ -----------
1/1      auto         isl           trunking     1

Port     Vlans allowed on trunk
-------- ---------------------------------------------------
1/1      1-1005

Port     Vlans allowed and active in management domain
-------- ---------------------------------------------------
1/1      1,4-5,1003,1005

Port     Vlans in spanning tree forwarding state and not pruned
-------- ---------------------------------------------------
1/1      1005

Cat5500> (enable)
```

Рисунок 14 – Проверка настройки транков маршрутизатора Catalyst 5500

Настройка Транков IEEE 802.1Q

Промышленный стандарт IEEE 802.10Q был разработан для рабочего взаимодействия систем. Он позволяет производить обмен информацией VLAN между сетевыми устройствами различных производителей. Например, коммутатор Cisco, работающий с протоколом IEEE 802.1Q может связываться с коммутатором другого производителя, так же работающим с протоколом IEEE 802.1Q. Возможности IEEE 802.1Q доступны в коммутаторах серии Catalyst версии 4.1 и выше. Проверьте руководство по настройке коммутатора для изучения команд настройки данного протокола.

Порядок выполнения работы

VLAN (аббр. от англ. Virtual Local Area Network) — логическая ("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 станциям группироваться вместе, даже если они не находятся в одной физической сети.

VLAN'ы могут быть настроены на коммутаторах, маршрутизаторах, других сетевых устройствах.

Преимущества:

1 - Облегчается перемещение, добавление устройств и изменение их соединений друг с другом.

2 - Достигается большая степень административного контроля вследствие наличия устройства, осуществляющего между сетями VLAN маршрутизацию на 3-м уровне.

3 - Уменьшается потребление полосы пропускания по сравнению с ситуацией одного широковещательного домена.

4 - Сокращается непроизводственное использование CPU за счет сокращения пересылки широковещательных сообщений.

5 - Предотвращение широковещательных штормов и предотвращение петель.

Настройка VLAN на одном коммутаторе

В данной работе рассматривается настройка VLAN на коммутаторе фирмы Cisco на его портах доступа. Создайте сеть, логическая топология которой представлена на рисунок 15. Компьютеры соединены коммутатором Cisco 2960-24TT. Имеется две подсети. В таблице 1 приведены адреса компьютеров.

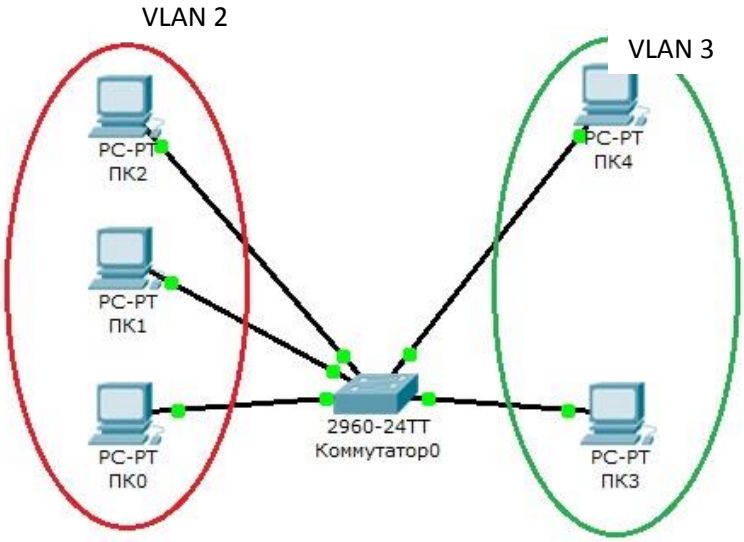

Рисунок 15 – Схема сети с одним коммутатором.

Таблица 1.

Компьютер	IP адрес	Порт коммутатора
ПК0	10.0.0.*1*/8	1
ПК1	10.0.0.*2*/8	2
ПК2	10.0.0.*3*/8	3
ПК3	192.168.0.*1*/24	4
ПК4	192.168.0.*2*/24	5

Далее будем считать, что ПК0, ПК1 и ПК2 находятся в VLAN 2, а ПК3 и ПК4 находятся в VLAN 3.

Для проверки конфигурации хоста ПК0 выполним команду ipconfig. Результат выполнения команды на рисунке 16. При желании можно выполнить аналогичную проверку на остальных хостах.

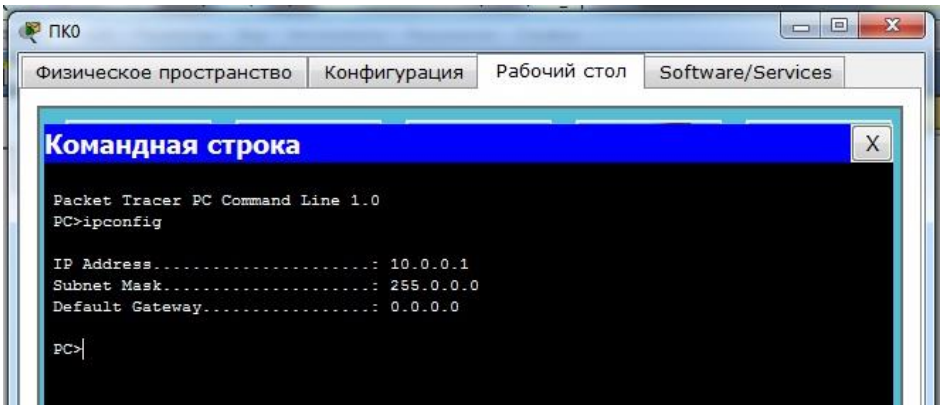

Рисунок 16 – Проверка конфигурации хоста

Проверим связность получившейся сети. Для этого пропингуем с ПК0 компьютеры ПК1 и ПК2, а с компьютера ПК3 компьютер ПК4. Если пинги проходят, то все в порядке.

Далее попробуем пропинговать с ПК0 компьютеры ПК 3 и ПК4. Как мы видим пинги не идут, поскольку компьютеры в разных подсетях.

Теперь займемся настройкой VLAN 2 и VLAN3, чтобы структурировать сети на коммутаторе и навести в них порядок.

Далее перейдем к настройке коммутатора. Откроем его консоль. Для того чтобы это выполнить в Packet Tracer дважды щелкните левой кнопкой мыши по коммутатору в рабочей области.

В открывшемся окне перейдите на вкладку CLI. Вы увидите окно консоли. Нажмите Enter,чтобы приступить к вводу команд. Информация, которая в данный момент отражена на консоли, свидетельствует о том что интерфейсы FasteEthernet0/1 – FasteEthernet0/5 успешно поднялись (то есть теперь они находятся в рабочем состоянии).

Перейдем в привилегированный режим выполнив команду **enable**:

```
Switch>en
Switch#
```

Просмотрим информацию о существующих на коммутаторе VLAN-ах (рисунок 17). Для этого выполним следующую команду:

```
Switch#sh vl br
```

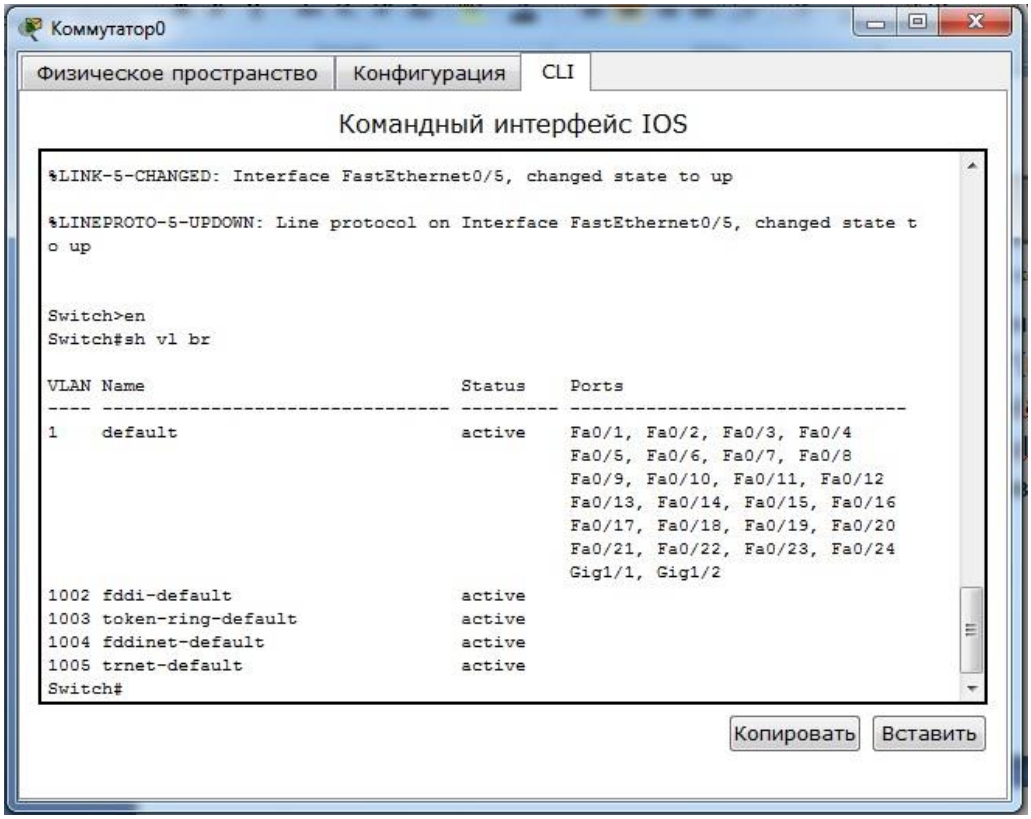

Рисунок 17 – Просмотр информации о VLAN на коммутаторе.

В результате выполнения команды на экране появится: номера VLAN – первый столбец, название VLAN - второй столбец, состояние VLAN (работает он в данный момент или нет) – третий столбец, порты принадлежащие к данному VLAN – четвертый столбец. Как мы видим по умолчанию на коммутаторе существует пятьVLAN-ов. Все порты коммутатора по умолчанию принадлежат VLAN 1. Остальные четыре VLAN являются служебными и используются не очень часто.

Для реализации сети, которую мы запланировали сделать, создадим на коммутаторе еще два VLAN. Для этого в привилегированном режиме выполните следующую команду:

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

```
Switch(config)#
```

для перехода в режим конфигурации.

Вводим команду VLAN 2. Данной командой вы создадите на коммутаторе VLAN с номером 2.

Указатель ввода Switch(config)# изменится на Switch(config-vlan)# это свидетельствует о том, что вы конфигурируете уже не весь коммутатор в целом, а только отдельный VLAN, в данном случае VLAN номер 2.

Если вы используете команду «vlan x», где x номер VLAN, когда VLAN x еще не создан на коммутаторе, то он будет автоматически создан и вы перейдете к его конфигурированию. Когда вы находитесь в режиме конфигурирования VLAN, возможно изменение параметров выбранной виртуальной сети, например можно изменить ее имя с помощью команды name.

Для достижения поставленной в задачи, сконфигурируем VLAN 2 следующим образом:

```
Switch(config)#vlan 2
Switch(config-vlan)#name subnet_10
Switch(config)#interface range fastEthernet 0/1-3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 2
```

Разберем данную конфигурацию. Как уже говорилось ранее командой VLAN 2, мы создаем на коммутаторе новый VLAN с номером 2.

Команда **name subnet_10** присваивает имя subnet_10 виртуальной сети номер 2.

Выполняя команду **interface range fastEthernet 0/1-3** мы переходим к конфигурированию интерфейсов fastEthernet0/1, fastEthernet0/2 и fastEthernet0/3 коммутатора.

Ключевое слово **range** в данной команде, указывает на то, что мы будем конфигурировать не один единственный порт, а целый диапазон портов, в принципе ее можно не использовать, но тогда последние три строки придется заменить на:

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config)#interface fastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
```

Команда **switchport mode access** конфигурирует выбранный порт коммутатора, как порт доступа (аксесс порт).

Команда **switchport access vlan 2** указывает, что данный порт является портом доступа для VLAN номер 2.

Выйдите из режима конфигурирования, дважды набрав команду **exit** и просмотрите результат конфигурирования (рисунок 18), выполнив уже знакомую нам команду **sh vl br** еще раз:

```
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#sh vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/4, Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gig1/1, Gig1/2
2    subnet_10                         active    Fa0/1, Fa0/2, Fa0/3
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

Рисунок 18 – Распределение портов на VLAN.

На коммутаторе появился еще один VLAN с номером 2 и именем subnet_10, портами доступа которого являются fastEthernet0/1, fastEthernet0/2 и fastEthernet0/3.

Далее аналогичным образом создадим VLAN 3 с именем subnet_192 и сделаем его портами доступа интерфейсы fastEthernet0/4 и fastEthernet0/5. Результат должен получиться следующим (рисунок 19):

```
Switch#sh vl br

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gig1/1
                                                 Gig1/2
2    subnet_10                         active    Fa0/1, Fa0/2, Fa0/3
3    subnet_192                        active    Fa0/4, Fa0/5
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

Рисунок 19 – Распределение портов на VLAN.

В принципе уже все готово и наша сеть настроена. Осталось лишь ее немного протестировать. Перейдите в консоль компьютера ПК0. Пропингуйте с него остальные компьютеры сети. Компьютеры ПК1 и ПК2 доступны, а компьютеры ПК3 и ПК4 не доступны. Задайте компьютерам ПК3 и ПК4 IP адреса из сети 10.0.0.0/8. Например 10.0.0.13 и 10.0.0.14. И теперь снова попробуем пропинговать с компьютера ПК0 остальные компьютеры сети. Как видим снова ничего не изменилось, хотя все пять компьютеров теоретически должны находится в одной подсети 10.0.0.0/8 и видеть друг друга, на практике они находятся в разных виртуальных локальных сетях и поэтому не могут взаимодействовать между собой.

Настройка VLAN на двух коммутаторах

Создайте сеть, логическая топология которой представлена на рисунке 20. Компьютеры соединены коммутатором Cisco 2950-24. В таблице 2 приведены адреса компьютеров.

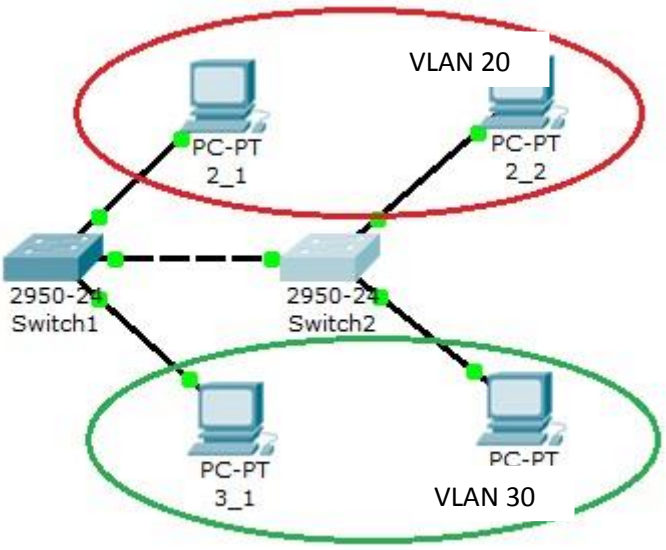

Рисунок 20 – Схема сети.

Таблица 2.

Компьютер	IP адрес	Коммутатор	Порт коммутатора	Вилан
2_1	10.0.0.1/8	Switch1	1	VLAN 20
2_2	10.0.0.3/8	Switch2	1	VLAN 20
3_1	10.0.0.2/8	Switch1	2	VLAN 30
3_2	10.0.0.4/8	Switch2	2	VLAN 30

Далее будем считать, что 2_1 и 2_2 находятся в VLAN 20, а 3_1 и 3_2 находятся в VLAN 30.

Проверим связность получившейся сети. Для этого пропингуем с 2_1 все остальные компьютеры. Поскольку пока в сети нет разделения на VLAN, то все компьютеры должны быть доступны.

Теперь займемся настройкой VLAN 20 и VLAN30, чтобы структурировать сети на коммутаторах.

Перейдите к настройке коммутатора Switch1. Откройте его консоль. В открывшемся окне перейдите на вкладку CLI, войдите в привилегированный режим и настройте VLAN 20 и VLAN30 согласно таблице 2.

Создайте на коммутаторе VLAN 20. Для этого в привилегированном режиме выполните следующую команду:

```
Switch1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

для перехода в режим конфигурации и настройте VLAN 20 и VLAN 30 следующим образом:

```
Switch1(config)#vlan 20
Switch1(config)#interface fastEthernet 0/1
Switch1(config-if-range)#switchport mode access
Switch1(config-if-range)#switchport access vlan 20
Switch1(config-if-range)#exit
Switch1(config)#vlan 30
Switch1(config)#interface fastEthernet 0/2
Switch1(config-if-range)#switchport mode access
Switch1(config-if-range)#switchport access vlan 30
```

Просмотрите информацию о существующих на коммутаторе VLAN-ах командой:

```
Switch1#sh vl br
```

У вас должен получится результат, показанный на рисунке 21.

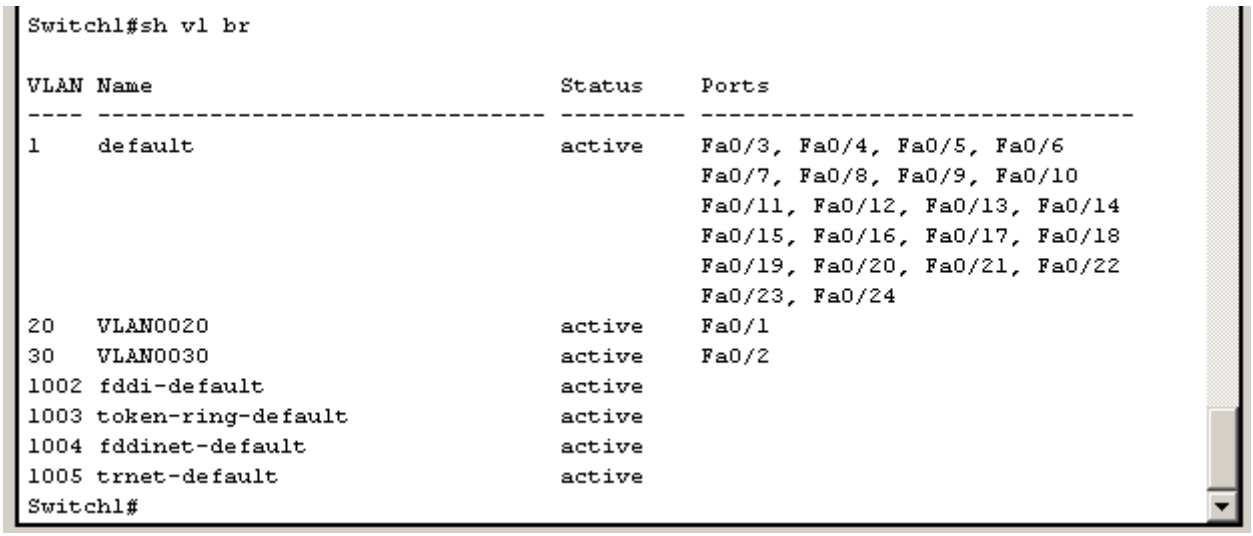

Рисунок 21 – Конфигурация Switch1

Аналогичным образом сконфигурируйте Switch2 (рисунок 22).

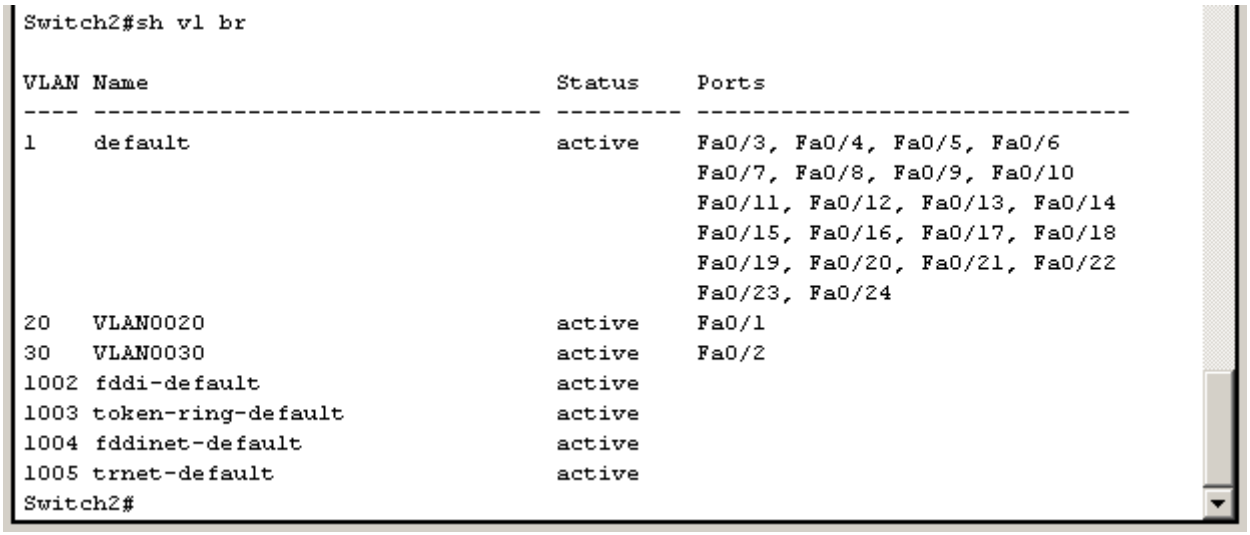

Рисунок 22 – Конфигурация Switch2

Поскольку в данный момент нет обмена информации о вилланах, то компьютеры будут пинговать только себя.

Теперь организуем магистраль обмена между коммутаторами. Для этого настроим третий порт на каждом коммутаторе как транковый.

Войдите в консоль коммутатора Switch1 и задайте транковый порт:

```
Switch1>en
Switch1#conf t
Switch1(config)#interface fastEthernet 0/3
Switch1(config)#switchport mode trunk
Switch1(config)#no shutdown
```

```
Switch1(config)#exit
```

Откройте конфигурацию коммутатора на интерфейсе FastEthernet0/3 и убедитесь, что порт транковый (рисунок 23).

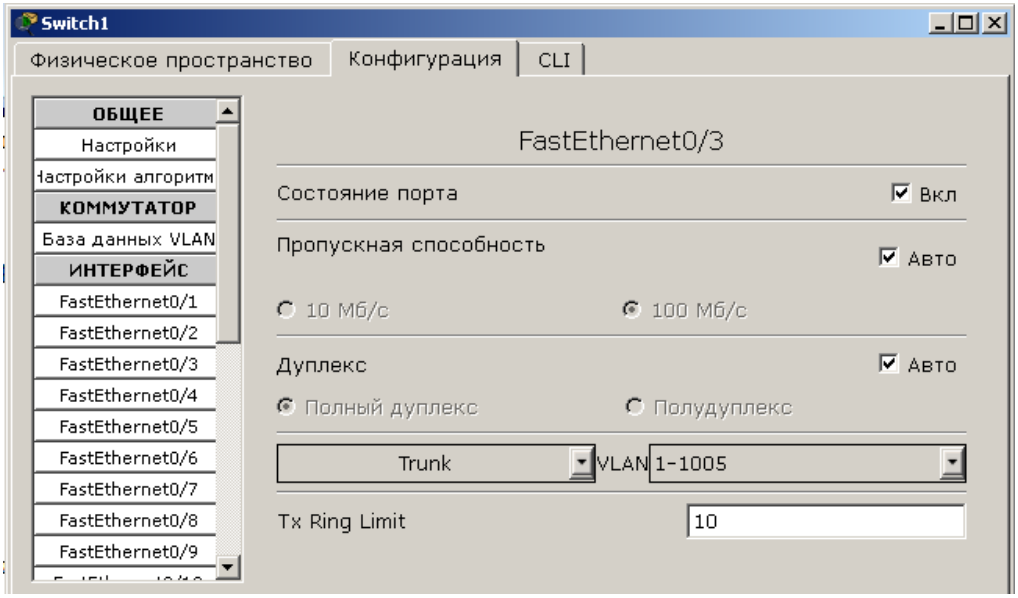

Рисунок.23 – Конфигурация интерфейса FastEthernet0/3.

На коммутаторе Switch2 интерфейс FastEthernet0/3 автоматически настроится как транковый.

Теперь компьютеры, входящие в один виллан должны пинговаться. У вас должна появиться связь между компьютерами 2_1 и 2_2, а так же между 3_1 и 3_2. Но компьютеры в другом виллане будут недоступны.