Министерство науки и высшего образования
Российской Федерации

Федеральное государственное автономное образовательное
учреждение высшего профессионального образования
«Севастопольский государственный университет»

ИССЛЕДОВАНИЕ СПОСОБОВ ПОСТРОЕНИЯ ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

Методические указания

к выполнению лабораторной работы по дисциплине

«Инфокоммуникационные системы и сети»

Для студентов, обучающихся по направлению 09.03.02
"Информационные системы и технологии" и
09.03.03. «Прикладная информатика»
по учебному плану подготовки бакалавров
дневной и заочной форм обучения

Севастополь
2021

Исследование способов построения виртуальных локальных компьютерных сетей. Методические указания к лабораторным занятиям по дисциплине «Инфокоммуникационные системы и сети» / Сост., В.С. Чернега,– Севастополь: Изд-во СевГУ, 2021 – 20 с.

Методические указания предназначены для проведения лабораторных работ по дисциплине «Инфокоммуникационные системы и сети». Целью методических указаний является помощь студентам в исследовании принципов построения виртуальных локальных сетей и работы протокола VTP. Излагаются теоретические и практические сведения необходимые для выполнения лабораторной работы, требования к содержанию отчета.

Методические указания рассмотрены и утверждены на методическом семинаре и заседании кафедры информационных систем
(протокол № ____ от «_____» _____ 2021 г.)

Рецензент: Моисеев Д.В., докт. техн. наук, проф. кафедры ИТиКС

1 Цель работы

Исследование принципов работы коммутаторов и виртуальных локальных сетей, способов конфигурации коммутаторов для построения виртуальных локальных сетей, приобретение практических навыков конфигурации коммутаторов и исследования функционирования виртуальных сетей.

2 Основные теоретические положения

2.1 Локальные и виртуальные локальные компьютерные сети

Локальные компьютерные сети (ЛКС) представляет собой такую разновидность сетей, в которой все ее компоненты, включая ЭВМ различных классов, расположены на ограниченной территории одного предприятия или учреждения и соединены через единую физическую среду. Расстояния между компьютерами локальной сети составляют от сотен метров до десятков (10…20) км. В локальных сетях сетевые компьютеры называют **рабочими станциями**. Ограниченность территории создает предпосылки для использования специфических способов передачи данных, отличных от традиционных, применяемых в глобальных сетях. Благодаря этому в ЛКС удается реализовать значительно более высокую скорость передачи (до тысяч Мбит/с) и на несколько порядков более низкую вероятность ошибок при существенно меньших затратах. Расположение локальной сети на ограниченной территории влияет также на способы административного сетевого управления, а технические характеристики ЛКС приводят к необходимости введения новых протоколов.

В настоящее время наиболее распространенным типом локальных компьютерных сетей являются сети Fast Ethernet со скоростью передачи 100 Мбит/с, построенная по древовидной (иерархической) топологии (рисунок 2.1).

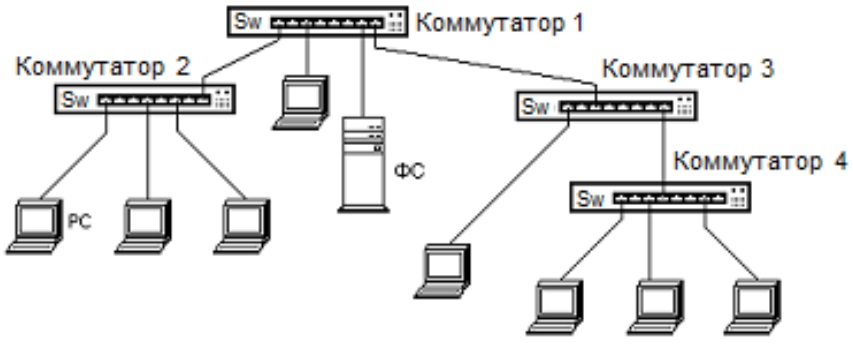

Рисунок 2.1 – Структура типовой локальной компьютерной сети Fast Ethernet

Локальная сеть строится на основе коммутаторов 2-го уровня Sw и линий связи типа витая пара. **Коммутатор** (*Switch*) представляет собой мультипроцессорный мост, способный независимо транслировать кадры между всеми парами своих портов. Благодаря этому коммутаторы, разделяя локальную сеть на под-

сети, делят единый коллизионный домен на отдельные поддомены, свободные от коллизий. Коммутатор создает соединение между своими портами по принципу "точка-точка". Поэтому компьютеры, подключенные к этим портам, имеют в своем распоряжении пропускную способность (10 или 100 Мбит/с), которую способны обеспечить соответствующие порты коммутатора.

В такой сети, если не предусмотрено никаких ограничений, каждая рабочая станция PC может осуществлять обмен информацией с любой другой PC сети или получать доступ к файл-серверу. Недостаток такой ЛКС состоит в том, что пользователи одних рабочих групп могут получить доступ к рабочим станциям пользователей других групп. Это снижает уровень безопасности сети, а также скорость доступа к общим ресурсам.

Для устранения указанных недостатков разработана технология виртуальных локальных сетей *VLAN* (*Virtual LAN*). Виртуальной локальной сетью называется совокупность узлов (рабочих станций и серверов) некоторой компьютерной сети, трафик которой, в том числе широковещательный, на канальном уровне полностью изолирован от трафика других узлов этой сети. Основное назначение *VLAN* – недопущение трафика из одной сети в другую. Это делается либо с целью увеличения реальной пропускной способности сегментов сети, или с целью защиты от несанкционированного доступа. Технология VLAN позволяет осуществить взаимодействие двух и более сетевых устройств на канальном уровне, хотя физически данные устройства, могут быть подключены к разным коммутаторам. VLAN ведут себя так же, как и физически разделённые локальные сети. То есть после разбивки сети на VLAN образуется несколько локальных сетей, которые далее возможно объединить в единое целое с помощью маршрутизации на третьем, сетевом, уровне модели OSI.

Виртуальные сети возможно создавать на основе коммутаторов из групп пользователей, основываясь на их задачах, а не по физическому расположению в сети. *VLAN* могут быть построены на базе одного или нескольких коммутаторов.

2.2 Разновидности и возможности коммутаторов

Коммутаторы по способу управления подразделяются на управляемые и неуправляемые. Неуправляемый коммутатор автоматически распределяет скорость и трафик между всеми клиентами сети. Неуправляемые коммутаторы широко используются в малых сетях с небольшим количеством (5-12) подключенных пользователей. Достоинством последних является простота в управлении и подключении.

Управляемые (программируемые) коммутаторы позволяют изменять режимы и способы коммутации путем загрузки в них управляющих программ. Управление коммутатором выполняет собственная операционная система, например Cisco IOS (*Internetwork Operating System*). Она хранится обычно в ПЗУ или флэш-памяти коммутатора. Многие управляемые коммутаторы позволяют настраивать такие функции как создание VLAN, задание качества обслуживания QoS, агрегирование и зеркалирование портов и др. Управляемые коммутаторы позволяют управлять коммутацией на канальном (втором) или сете-

вом (третьем) уровнях модели OSI. Обычно их именуют соответственно «Layer 2 Switch» или «Layer 3 Switch» сокращенно «L2 и L3 Switch». Управление коммутатором может осуществляться посредством Web-интерфейса, интерфейса командной строки (CLI), протокола SNMP и т.п. В настоящее время существуют коммутаторы и программные средства 4-го уровня, которые позволяют создавать VLAN и на базе **протоколов,** и на базе **правил**.

Все программируемые коммутаторы имеют ***консольный порт***, функции которого выполняет асинхронный интерфейс RS-232. Такой порт позволяет управлять коммутатором с персонального компьютера, который с помощью консольного кабеля соединяется с COM-портом ПЭВМ. В новых типах коммутаторов консольный порт имеет разъем RJ-45. Этот разъем можно соединить посредством специального консольного кабеля и переходника с COM-портом компьютера.

В коммутаторах имеется две разновидности портов: порты доступа (**access port**) и магистральные, транковые (**trunk port**) порты. Порт доступа принадлежит только одной виртуальной сети. Магистральный порт способен пропускать кадры многих VLAN. Чтобы коммутатор мог определить принадлежность кадра к определенной виртуальной сети, в заголовок кадра вставляется идентификатор ─ специальная метка (англ. слово **тег**) с номером VLAN. Такой кадр называется **тегированным** (помеченным). Тег добавляется коммутатором к заголовку кадра при поступлении его от рабочей станции на порт коммутатора, а при передаче кадра компьютеру, приписанному к данной виртуальной сети, тег коммутатором изымается.

2.3 Способы создания VLAN

Виртуальные сети могут создаваться на основе способа *группирования портов* коммутатора или на основе группирования MAC-адресов сетевых устройств. При использовании способа группировании портов каждый порт программным образом назначается одной из виртуальных сетей. Обмен данными в таком случае будет осуществляться только между указанными портами. Порт можно приписать нескольким виртуальным сетям, однако, в случае требований повышенной безопасности это действие не допускается. В виртуальных сетях на основе группирования MAC-адресов каждый физический адрес приписывается той или иной виртуальной сети.

Достоинством VLAN на базе портов является высокий уровень управляемости и безопасности. К недостаткам такого вида сетей следует отнести необходимость физического переключения устройств при изменении структуры отдельных сетей.

Для уменьшения количества связей между коммутаторами, на которых сконфигурированы несколько виртуальных сетей, используется одна магистральная линия. По терминологии Cisco такое соединение называется **транковым** (*Trunk*). По магистральной линии передаются друг за другом (временное мультиплексирование) кадры, принадлежащие различным VLAN.

Разделение (демультиплексирование) входящих кадров производится на основании идентификаторов виртуальных сетей, которые включаются (инкапсулируются) в кадры Ethernet. Способ маркировки виртуальных сетей и формат Ethernet-кадров регламентируется международным стандартом **IEEE 802.1Q**. Корпорация Cisco разработала собственный протокол маркирования (тегирования) VLAN, который получил название «межкоммутаторный канал» ISL (*Inter Switch Link*). Современные коммутаторы Cisco поддерживают оба протокола. В соответствии со стандартом IEEE 802.1Q к кадру Ethernet добавлен специальный маркер ***Tag*** (тег) виртуальной сети размером в четыре байта. Эти 32 тегових бита содержат информацию о принадлежности кадра Ethernet к конкретной VLAN и о его приоритете. Процедура добавления информации о принадлежности к 802.1Q VLAN в заголовок кадра называют маркированием (тегированием) кадра (*Tagging*), а извлечение маркера — *Untagging*.

Изменение структуры кадра Ethernet привело к нарушению совместимости со всеми традиционными устройствами Ethernet, ориентированными на старый формат кадра. Это связано с тем, что данные 802.1q размещаются перед полем с информацией о длине полезной нагрузки (или типе протокола). Традиционное сетевое устройство в процессе анализа заголовка не обнаружит эту информацию на обычном месте. На его месте располагается "маркер" виртуальной сети (рисунок 2.2). Новое поле состоит из тэга (маркера) протокольного идентификатора **TPID** (*Tag Protocol Identifier*) и тега управляющей информации **TCI** (*Tag Control Information*). Поле TPID имеет длину два байта и содержит фиксированный код 0x8100, который информирует, что кадр содержит тег протокола 802.1Q/802.1P. Поскольку это число больше максимальной длины кадра *Ethernet* (1500), то сетевые карты *Ethernet* будут интерпретировать его как тип, а не как длину кадра. Структура полей управляющей информации TCI изображена в нижней части рисунка 2.2

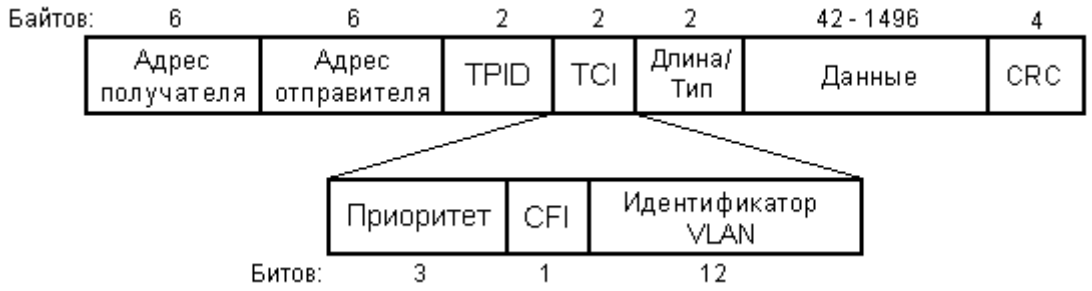

Рисунок 2.2 - Формат кадра Ehternet с меткой виртуальной сети

Трехбитовое поле "**Приоритет**" позволяет задавать 8 уровней приоритета передаваемых кадров и тем самым выделять *трафик реального времени*, *трафик со средними требованиями* и трафик, для которого *время доставки не критично*. Это открывает возможность использования сети Ethernet для задач управления и обеспечения качества обслуживания (QoS) при транспортировке мультимедийных данных. Наивысший уровень приоритета имеют кадры управления сетью, следующий приоритет задается кадрам передачи голосового тра-

фика, а следующий, более низкий уровень, установлен для видеоданных. Остальные уровни предназначены для маркировки данных с разными требованиями по задержке доставки пакетов.

Однобитовое поле **CFI** (*Canonical Format Indicator*) зарезервировано для обозначения кадров сетей других типов (Token Ring, FDDI), передаваемых по магистрали Ethernet. Значение CFI=1 является указанием того, что в поле данных содержится кадр сети *Token Ring* (Стандарт IEEE 802.5).

Поле "**Идентификатор VLAN**" VID (*VLAN Identifier*) длиной 12 бит определяет, какой виртуальной сети принадлежит кадр. 12-битовое поле позволяет коммутаторам разных производителей создавать до 4096 общих виртуальных сетей. Обычно виртуальные сети с номерами VID0 и VID4095 не используются.

Управление виртуальными локальными сетями по умолчанию осуществляется через VLAN1 (*Default VLAN*). Поэтому при конфигурировании коммутатора, как минимум, один порт должен относиться к VLAN1, чтобы можно было управлять коммутатором. Все остальные порты коммутатора могут быть назначены другим виртуальным сетям. Кадры первой VLAN обычно не тегируются. Такую виртуальную сеть называют «родной» VLAN (native vlan).

Сети VLAN обладают теми же свойствами, что и физические локальные сети, за исключением того, что VLAN являются логическими, а не физическими сетями. Поэтому конфигурирование сетей VLAN может выполняться безотносительно к физическому расположению устройств. Широковещательный, многоадресный и одноадресный трафики отдельно взятой VLAN отделены от трафика других VLAN.

Концепция VLAN, помимо решения проблемы с широковещательным трафиком даёт также ряд дополнительных преимуществ: формирование локальных сетей не по месту расположения ближайшего коммутатора, а по принадлежности компьютеров к решению той или иной производственной задачи; создание сети по типу потребляемого вычислительного ресурса и требуемой серверной услуги (файл-сервер, сервер баз данных). VLAN позволяют вести различную политику безопасности для разных виртуальных сетей; переводить компьютер из одной сети в другую без осуществления физического перемещения или переподключения.

Таким образом, технология VLAN обеспечивает следующие преимущества:

- улучшается производительность сети;
- экономятся сетевые ресурсы;
- упрощается управление сетью;
- снижается стоимость сети;
- улучшается безопасность сети.

Во всех современных коммутаторах VLANы реализованы в соответствии со стандартом 802.1Q.

2.4 Членство в сети VLAN

Сеть VLAN обычно создается администратором, который приписывает ей порты коммутатора. Сеть, созданная таким способом, называется статической виртуальной локальной сетью (static VLAN).

Статические сети VLAN являются типичным способом формирования виртуальных сетей и отличаются высокой безопасностью. Присвоенные сети VLAN порты коммутаторов всегда сохраняют свое действие, пока администратор не выполнит новое присваивание портов. Этот тип VLAN легко конфигурировать и отслеживать, причем статические VLAN хорошо подходят для сетей, где контролируется перемещение пользователей. Существуют программы сетевого управления, облегчающие выполнение рутинной процедуры присваивание портов. Однако подобные программы использовать не обязательно.

Динамические сети VLAN. Членство в динамических VLAN может устанавливаться динамически на магистральных интерфейсах коммутаторов на основе протокола GVRP (GARP VLAN *Registration Protocol*). Протокол GARP (*Generic Attribute Registration Protocol*) используется для регистрации и отмены регистрации атрибутов, таких как идентификатор виртуальной сети *VID*. Динамические сети упрощают административные задачи по их управлению и настройке. Если пользователь перемещается в другое место сети, порт коммутатора будет автоматически приписан в нужную сеть VLAN. Однако для первоначального наполнения базы данных администратору необходимо ее заполнить.

Обратите внимание, что компьютер при отправке кадров в сеть даже не догадывается, в какой VLAN он размещён. Кадры, поступающие на порт определённой VLAN, ничем не отличается от кадров другой VLAN. Иными словами, никакой информации о принадлежности трафика определённой VLAN в кадрах не содержится. Вся информация о виртуальной сети дополняется и распознается на коммутаторе. Коммутатор «знает», что компьютер, который подключен к определённому порту, находится в соответствующей VLAN и вставляет в заголовок данного кадра идентификатор (тег).

Коммутация пакетов осуществляется на основе таблицы коммутации, которая динамически составляется по мере работы коммутатора. Она представляет собой таблицу, содержащую записи о порте, соответствующем MAC-адресе устройства, а также номера VLAN. По умолчанию вначале все порты относятся к VLAN1. Пример таблицы коммутации приведен в таблице 2.1. При поиске пары MAC-адрес/порт будет сравниваться тег кадра с номером VLAN в таблице.

Таблица 2.1 – Таблица коммутации

Порт коммутатора	VLAN	MAC-адрес хоста
1	2	A
2	2	B
3	10	C
4	10	D

Для каждой новой VLAN операционной системой коммутатора создается новая таблица коммутации. Тем не менее, все базовые механизмы коммутатора остаются точно такими же, как и до разделения на VLAN, но они используются только в пределах соответствующей VLAN.

Порты коммутатора, как уже отмечалось выше, поддерживающие виртуальные подсети, делятся на две группы:

– **порты доступа** (access-ports) – к ним подключаются, как правило, конечные узлы. За каждым access-портом закреплена определённая VLAN, этот параметр называют PVID. Весь трафик, приходящий на этот порт от конечного устройства, получает метку этой VLAN, а исходящий уходит без метки. Трафик этой VLAN передается без тега. Поэтому такие порты называют нетегированными портами. На коммутаторах Cisco нетегированным порт может быть только в одной VLAN, на некоторых других коммутаторах данного ограничения нет;

– **магистральные тегированные порты** (trunk-ports). Линия связи, соединяющая транковые порты двух коммутаторов или транковый порт коммутатора с транковым портом маршрутизатора, называется магистральной или **транковой линией** (сокращенно транком, см. рисунок 2.3).

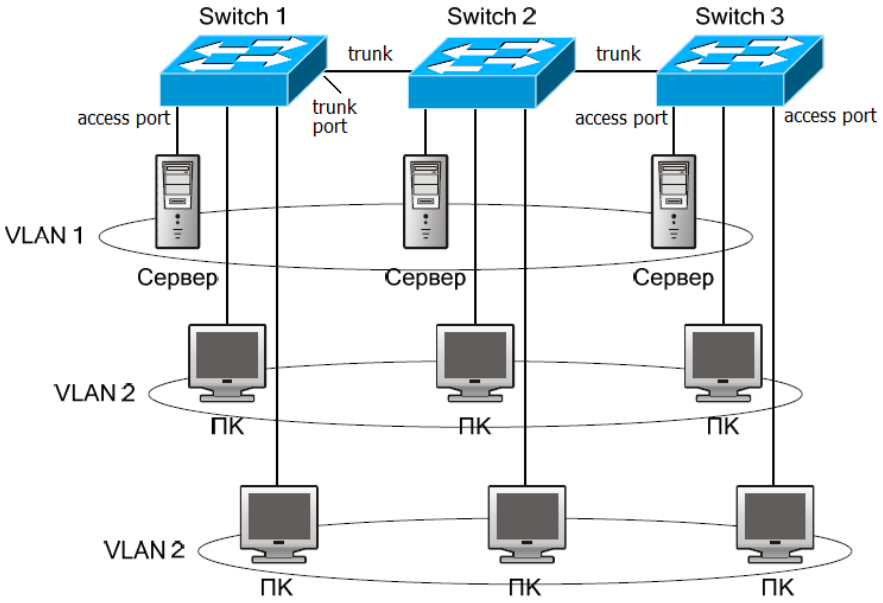

Рисунок 2.3 – Сеть VLAN, построенная на нескольких коммутаторах

По трактовой линии передаются последовательно во времени кадры нескольких различных VLAN, т.е. осуществляется временное мультиплексирование кадров. Передаваемые по этой линии кадры содержат теги, чтобы принимающая сторона (порт) могла отличить кадр, который идёт, например, в бухгалтерию, от кадра, предназначенного для ИТ-отдела. За транковым портом закрепляется целый диапазон VLAN. Без тега коммутатор не сможет различить трафик различных VLAN.

Существует «родная» native vlan, трафик которой не тегируется даже в транке. По умолчанию это VLAN 1. Можно административно переназначить

«родную» VLAN. Такое переназначение может понадобиться для совместимости с устройствами, в которых не применяется инкапсуляция по стандарту 802.1q. Например, через Wi-Fi мост нужно передать трафик 3-х VLAN, и одна из них является сетью управления. Например, если Wi-Fi-модули не поддерживают стандарт 802.1q, то управлять ими можно, только если эту VLAN настроить, как native vlan с обеих сторон.

Если порт тегирован для нескольких VLAN, то в этом случае весь нетегированный трафик будет направляться на родную VLAN (native VLAN). Если на нетегированный порт поступит тегированный кадр, то он удаляется. Обычно, по умолчанию все порты коммутатора считаются нетегированными членами VLAN 1. В процессе настройки или работы коммутатора они могут перемещаться в другие VLAN.

2.5 Построение VLAN на нескольких коммутаторах

VLAN позволяет разделять устройства на изолированные логические группы. Как правило, одной VLAN соответствует одна подсеть. Устройства, находящиеся в разных VLAN, будут находиться в разных подсетях. Но в то же время VLAN не привязана к местоположению устройств и поэтому устройства, находящиеся на некотором расстоянии друг от друга, все равно могут быть в одной VLAN, независимо от местоположения. Суть вышесказанного показана на рисунке 2.4. К первому коммутатору dsw1 подключены хосты из подсети 192.168.1.0/24, а также 192.168.2.0/24. Также к dsw1 подключен коммутатор dsw2, к которому в свою очередь подключен хост из подсети 192.168.2.0/24. Портам коммутатора, к которым подключены хосты подсети 192.168.2.0/24 назначена VLAN20, а подсети 192.168.1.0/24 – VLAN10.

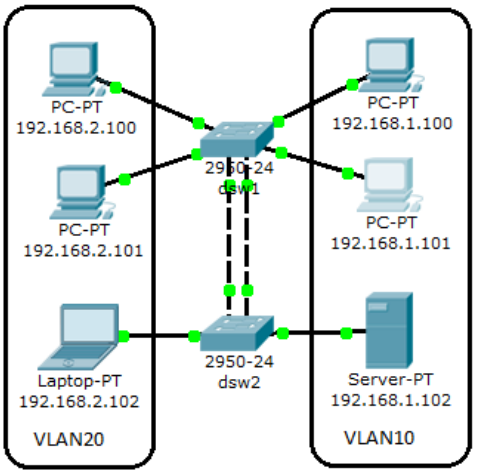

Рисунок 2.4 – Реализация нескольких VLAN на двух коммутаторах

Для того чтобы хосты 1.101 и 1.102 в VLAN 10 на коммутаторе dsw1, могли обмениваться информацией с хостами VLAN 10 добавлены две линии связи между коммутаторами, который реализуют соединение двух нетегиро-

ванных портов, находящихся в зоне видимости каждой VLAN соответственно. Однако, когда количество VLAN возрастает, то схема явно становится неэкономной, так как для каждой VLAN надо будет добавлять линию (линк) между коммутаторами для того, чтобы объединить хосты в один широковещательный сегмент. Для решения этой проблемы используются тегированные порты (рисунок 2.5).

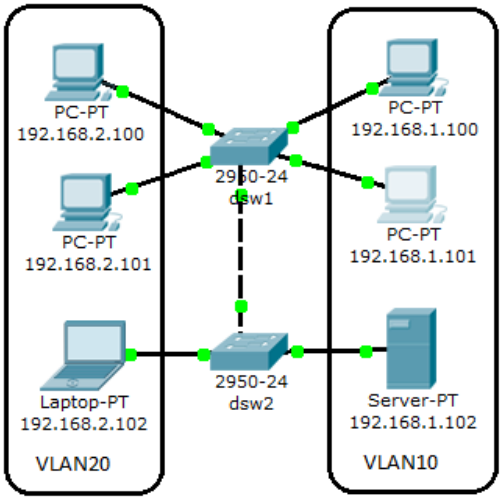

Рисунок 2.5 – Тегированный порты между коммутаторами

2.6 Особенности создания и конфигурирования VLAN

Каждой виртуальной сети должен быть присвоен свой номер. Существуют два диапазона адресов VLAN:

– стандартный диапазон VLAN – от 1 до 1000;

– расширенный диапазон VLAN – от 1025 до 4095.

На каждом коммутаторе при его изготовлении создается VLAN 1, а все интерфейсы по умолчанию относятся к ней. Процесс настройки практически идентичен для всех коммутаторов Cisco Catalyst. Создание VLAN можно осуществлять с использованием графического интерфейса (рисунок 2.6), либо с командной строки (CLI).

Создание VLAN с командной строки выполняется следующим образом.

```
switch(config)# vlan 2
switch(config-vlan)# name test
```

Просмотр информации о VLAN'ах выполняется по команде `show vlan`:

```
switch#show vlan brief
```

Пусть на коммутаторе один из портов доступа нужно отнести к VLAN 2:

```
Switch0(config)#interface fa0/1
Switch0(config-if)#switchport mode access
Switch0(config-if)#switchport access vlan 2
```

Это означает, что любой кадр, пришедший на этот интерфейс, автоматический тегируется: в него добавляется метка с номером VLAN 2.

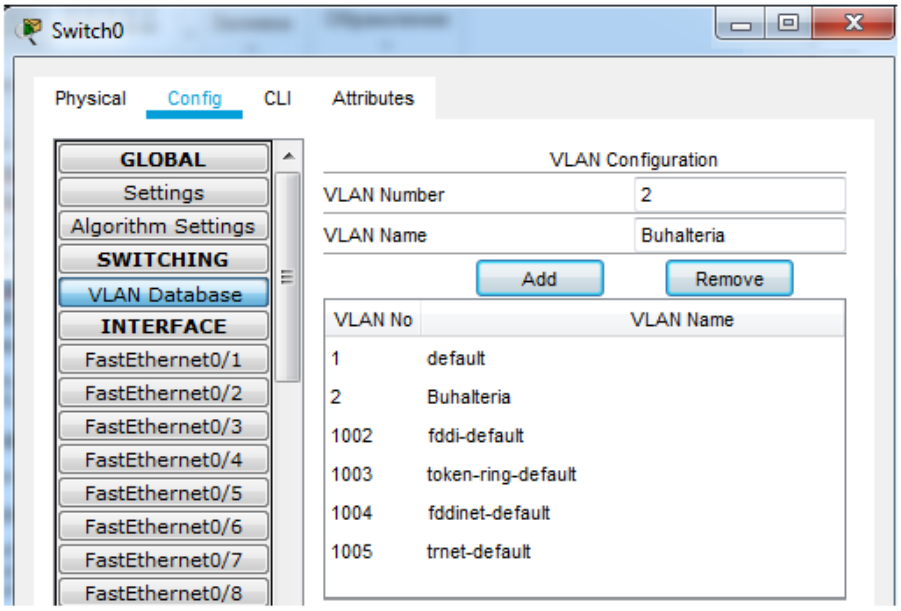

Рисунок 2.6 - Графический интерфейс при создании VLAN

Далее коммутатор ищет в своей таблице MAC-адресов среди портов, принадлежащих 2-й VLAN, порт, к которому подключено устройство с MAC-адресом получателя. Если получатель подключен к такому же access-порту, метка с кадра изымается и кадр отправляется в этот самый порт таким, каким он был изначально. То есть получателю также нет необходимости знать о существовании VLAN'ов. Если же искомый порт, является транковым, то метка (тег) в кадре остаётся.

```
Switch(config)#interface fa0/2
Switch(config-if)#switchport mode trunk
```

Если тегированный кадр поступит на access-порт, то он будет отброшен, а если нетегированный кадр поступит на trunk-порт, то он будет помещён в native VLAN. По умолчанию ею является VLAN 1. Но можно поменять её командой `switchport trunk native vlan 2`. В этом случае все кадры, помеченные 2-й VLAN, будут уходить из этого порта нетегированными, а нетегированные кадры, приходящий на этот интерфейс, помечаться VLAN 2. Кадры с тегами других VLAN останутся неизменными, проходя, через такой порт.

Оконечным узлам (компьютерам, ноутбукам, планшетам, телефонам) можно отправлять тегированные кадры и соответственно подключать их к транковым портам только если сетевая карта и программное обеспечение поддерживает стандарт 802.1q и узел может работать с тегированными кадрами. Если тегированные кадры попадут на обычный неуправляемый коммутатор или другое устройство, не понимающее стандарт 802.1q, то, скорее всего, коммутатор его отбросит из-за увеличенного размера заголовка кадра.

По умолчанию в транке разрешены все VLAN. Можно ограничить перечень VLAN, которые могут передаваться через конкретный транк. Указать перечень разрешенных VLAN для транкового порта fa0/0 можно командой:

```
switch(config)# interface fa0/0
switch(config-if)# switchport trunk allowed vlan 1-5,10,15
```

Добавление ещё одной разрешенной VLAN:

```
switch(config)# interface fa0/0
switch(config-if)# switchport trunk allowed vlan add 160
```

Удаление VLAN из списка разрешенных:

```
switch(config)# interface fa0/0
switch(config-if)# switchport trunk allowed vlan remove 160
```

Для задания или модификации параметров настройки коммутатора необходимо настроить IP-адрес для управления. Так как коммутатор является устройством второго уровня, то в нем создаётся специальный управляющий виртуальный интерфейс третьего уровня и указывается номер желаемой VLAN. Затем с ним можно работать как с обычным физическим интерфейсом.

```
switch(config)#interface vlan 2
switch(config-if)#description Management
switch(config-if)#ip address 172.16.1.2 255.255.255.0
switch(config-if)#no shutdown
```

2.7 Конфигурация виртуальных локальных сетей с использованием протокола VTP

Создание виртуальных локальных сетей при небольшом количестве коммутаторов и подключенных к ним рабочих станций обычно осуществляется администратором сети вручную путем конфигурации каждого коммутатора в отдельности. Но если коммутаторов и виртуальных сетей в организации десятки, а то и сотни, то затраты труда администратора существенно возрастают, увеличивается также и вероятность ошибок конфигурации. Для уменьшения трудовых затрат администратора и ошибок конфигурации создан протокол VTP, который используется для централизованного управления VLAN на коммутаторах.

Протокол VTP (*англ.* VLAN Trunking Protocol) – это протокол, разработанный корпорацией Cisco, который используется для обмена информацией о виртуальных сетях VLAN. VTP помогает упрощать операции с VLAN'ами в организации – добавление, удаление и изменение параметров, а также оптимизирует трафик, благодаря наличию функции ограничения широковещательного трафика `vtp pruning`.

Протокол VTP объединяет физически подключённые друг к другу коммутаторы в именованные области, называемые **доменами VTP**. В одной организации таких доменов может быть несколько. Только коммутаторы, относящиеся к одному и тому же сетевому домену, могут совместно использовать конфигурационную информацию о данной виртуальной сети.

Любой коммутатор VLAN может функционировать в *серверном, клиентском* или *прозрачном режимах*. Отличие между указанными режимами состоит в разных способах генерации конфигурационных VTP-сообщений и реакции

коммутаторов на полученные уведомления. В режиме **VTP-сервера** коммутатор автоматически рассылает через все свои магистральные порты соседним коммутаторам VTP-уведомления на групповой адрес (*multicast address*), в которых содержатся сведения о параметрах созданной на сервере виртуальной сети. Передаваемая информация включает имя домена, номер версии протокола, активные VLAN и другую информацию. Посредством таких сообщений остальные коммутаторы, входящие в одноименный домен, информируются о появлении новой виртуальной сети. Информацию, содержащуюся в VTP-сообщениях, учитывают только те коммутаторы, которые сконфигурированы в режиме сервера или клиента.

Коммутаторы Cisco, настроенные на **прозрачный** режим (transparent mode), не могут генерировать VTP-сообщения. В случае создания виртуальной сети на таком коммутаторе информация о новой VLAN остается локальной и не передается остальным коммутаторам, даже если между ними существует магистральное соединение.

В момент старта любой коммутатор виртуальной сети автоматически конфигурируется в качестве сервера. При создании, удалении или переводе сети в неактивное состояние при помощи коммутатора Cisco, находящимся в прозрачном или серверном режиме, коммутатор сохраняет конфигурационную информацию в энергонезависимой памяти и при включении питания может восстановить последнюю известную информацию. В коммутаторах-клиентах информация о всех виртуальных сетях при отключении питания теряется. Таким образом, для создания сетей VLAN коммутатор Cisco должен быть сконфигурирован администратором в режиме сервера или прозрачном режиме.

Коммутаторы Cisco позволяют передавать по магистрали трафик всех виртуальных сетей. Однако предусмотрена также возможность передавать данные только определенных сетей. Для этого в IOS коммутатора введены команды удаления и добавления сетей в магистраль.

В сети желательно иметь хотя бы один VTP-сервер, а если коммутатор один, то имеет смысл включить его сразу в режим VTP transparent. Этот режим удобен тем, что коммутатор, работающий в нём, в случае, если принимает кадр протокола VTP на любом порту, сразу передаёт этот кадр на все остальные транковые порты – т.е. просто ретранслирует этот кадр, не обрабатывая его. Этим (переключением в vtp transparent mode) заранее ликвидируется потенциальная возможность, что какой-то другой коммутатор повлияет на конфигурацию данного.

Протокол VTP в основном занимается передачей базы данных VLAN между устройствами. Делает он это в следующих случаях:

– если была изменена база данных VLAN на устройстве с ролью VTP Server (т.е. провели успешную запись – не важно, какую – добавили VLAN, удалили VLAN, переименовали VLAN), то изменение будет передано немедленно после проведения записи;

– если после последней успешной записи прошло 300 секунд.

В коммутаторах предусмотрена функция pruning. Задача функции pruning – каждый коммутатор будет «считать» фактически используемые VLAN'ы, и в случае, когда по VTP приходит неиспользуемый VLAN, уведомлять соседа, что этот трафик не имеет смысла присылать. Под этот механизм будут подпадать только первые 1000 VLAN'ов, исключая самый первый (т.е. pruning работает только для VLAN с номерами от 2 до 1001).

Базовая настройка протокола VTP выполняется следующим образом. Вначале рекомендуется начертить топологию сети, в которой предполагается применять протокол VTP. Затем нужно выбрать коммутатор, который будет сервером (ему не надо быть каким-то особо быстрым, специфической нагрузки на VTP Server нет). Если Вы не хотите использовать VTP (например, из соображений безопасности) – тогда просто переведите все устройства в режим VTP Transparent (либо off, если поддерживается оборудованием и ОС).

Настройка имени домена VTP:

```
host(config)#vtp domain имя_домена
```

Стереть имя домена штатно нельзя, только сменить.

Настройка пароля VTP:

```
host(config)#vtp password пароль
```

Пароль можно сбросить на пустой, если ввести команду `no vtp password`. Пароль VTP хранится небезопасно (у VTP Server – в файле vlan.dat, у VTP Transparent – в NVRAM), поэтому если пользуетесь VTP, делайте такой пароль, который более нигде не дублируется, т.к. получить пароль VTP – относительно несложно. Всё, от чего защищает этот пароль – это случайное добавление в сеть неправильно настроенного коммутатора. Пароль VTP не защищает передаваемую между коммутаторами информацию.

Настройка версии VTP:

```
host(config)#vtp version версия
```

Настройка VTP pruning:

Включение выполняется командой:

```
host(config)#vtp pruning
```

а выключение – `host(config)#no vtp pruning`

Настройка режима VTP:

```
host(config)#vtp mode режим
```

где режим – это `server`, `client`, `transparent` или `off`. Режим `off` получится поставить только на устройствах, поддерживающих VTPv3; на коммутаторах, которые поддерживают только VTPv1 и VTPv2 отключить протокол нельзя.

При использовании **расширенной настройки протокола VTP** следует принимать во внимание, что коммутатор, находящийся в режиме VTP Server,

хранит информацию в своей флэш-памяти. Если потенциальных мест хранения несколько, то нужное можно указать в явном виде, командой

```
host(config)#vtp file имя_файловой_системы
```

Для VTP Client и VTP Transparent это не имеет особого смысла. Также имеется возможность упростить выявление и устранение причин неисправностей, указав в явном виде интерфейс, с которого будет браться IP-адрес, отображающийся в результатах вывода команды `show vtp status`. То есть, это влияет на выбор того адреса, который будет указываться у клиентов в строчке вида

```
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

3 Описание лабораторной установки

В качестве лабораторного стенда используется персональный компьютер с установленной программой Cisco Packet Tracer. Работа с этим пакетом детально описана в предыдущей лабораторной работе.

4 Программа выполнения работы

4.1 Изучить теоретический материал, относящийся к разделу «Локальные компьютерные сети». Особое внимание следует уделить подразделу «Виртуальные локальные сети» и устройству и конфигурации коммутаторов. (Выполняется в процессе домашней подготовки).

4.2 Построить в окне эмулятора Packet Tracer локальную сеть на основе одного коммутатора. Задать узлам сети IP-адреса. Количество серверов и рабочих станций определяется вариантом задания (Приложение А.1).

4.3 Исследовать достижимость сетевых узлов путем их пингования. Результаты пингования сохранить для отчета. Этот пункт выполнить в реальном режиме и режиме симуляции.

4.4 Разделить сеть, построенную на этапе 4.2, на виртуальные сети способом группирования портов. Количество коммутаторов, виртуальных сетей и рабочих станций в виртуальных сетях определяется вариантом задания (Приложение А.2).

4.5 Исследовать пингованием достижимость сетевых узлов внутри каждой из виртуальных сетей и между виртуальными сетями. После настройки VLAN посмотреть текущую конфигурацию сети командами: show running-config, show vlan, show vlan brief, show mac address-table. Результаты пингования и просмотра конфигурации включить в отчет.

4.6 Повторить п.4.4 и 4.5 при условии, что в сети существует два коммутатора. Виртуальные сети включают компьютеры, соединенные как с первым и так и со вторым коммутаторами. Количество линий связи между коммутаторами равно количеству виртуальных сетей.

4.7 Повторить п.4.6 при использовании транковых соединений между коммутаторами.

4.8 Составить схему компьютерной сети (приложение Б) и настроить VLAN на коммутаторах в соответствии с вариантом (v – номер по списку в журнале), используя протокол VTP. Условием проверки является отсутствие связи между хостами, принадлежащими разным VLAN.

4.9 После настройки VLAN исследовать текущую конфигурацию сети командами: show running-config, show vlan, show vlan brief, show mac address-table. Результат приведите в отчет.

4.10. Оформить отчет и сделать выводы по работе.

5 Содержание отчета

1. Титульный лист.
2. Исходные данные в соответствии с индивидуальным вариантом.
3. Описание всех использованных команд.
4. Скриншоты получившихся топологий и осуществленных настроек.
5. Выводы.

6 Контрольные вопросы

1. Что такое виртуальные локальные сети и зачем они применяются?
2. Зачем применяется разбиение сети на VLAN-ы?
3. Расскажите, как функционирует неуправляемый коммутатор после включения питания.
4. Каким образом коммутатор второго уровня пересылает между портами пакеты третьего уровня ping?
5. Чем симметричный коммутатор отличается от несимметричного?
6. Что означает термин «коммутация на лету»?
7. В чем состоит отличие портов доступа от магистральных (транковых) портов?
8. Расскажите о формате кадра протокола IEEE 802.1Q?
9. Что такое «тег», зачем он нужен и где он располагается?
10. Каким образом устройство канального уровня определяет, используется ли в данном кадре протокол IEEE 802.1Q?
11. С какой целью в тег введено поле «приоритет»?
12. Что означает понятие «родная-native» VLAN?
13. С какой целью разработан протокол VTP и можно ли обойтись без его использования?
14. Каковы функции коммутаторов, работающих в серверном, клиентском или прозрачном режимах?
15. Поясните принцип работы протокола VTP?

Библиографический список

1. Бони Дж. Руководство по Cisco IOS / Дж.Бони. – М.: Изд-во «Русская редакция», 2008. – 784 с.

2. Дибров М.В. Сети и телекоммуникации. Маршрутизация в IP–сетях. В 2 ч. Часть 2: учебник и практикум для академического бакалавриата / М.В. Дибров. – М.: Изд-во Юрайт, 2019. – 351 с. https://biblio-online.ru/book/seti-i-telekommunikacii-marshrutizaciya-v-ip-setyah-v-2-ch-chast-2-437865

3. Сети и телекоммуникации: учебник и практикум для академического бакалавриата / Под ред. К.Е. Самуйлова, И.А. Шалимова, Д.С. Кулябова. – М.: Изд-во Юрайт, 2016. – 363 с.
https://biblio-online.ru/book/seti-i-telekommunikacii-432824

4. Таненбаум Э. Компьютерные сети / Э.Таненбаум. 5-е изд. – СПб.: Питер, 2012. – 960 с.

5. Хьюкаби Д. Руководство Cisco по конфигурированию коммутаторов Catalyst / Дэвид Хьюкаби, Стив Мак-Квери. – М.: Изд-во «Вильямс», 2004. – 560 с.

6. Чернега В.С. Компьютерные сети / В.С. Чернега, Б. Платтнер. – Севастополь: Изд-во СевНТУ, 2006. – 500 с.

Приложение А.1 - Таблица вариантов

Вариант	Количество PC	Количество серверов	Количество ноутбуков
1	2	2	1
2	4	1	2
3	6	1	1
4	4	2	2
5	5	1	1
6	3	3	4
7	6	2	3
8	4	3	3
9	3	3	3
10	8	2	2

Приложение А.2 - Таблица вариантов

Вариант	Количество				
	PC	серверов	ноутбуков	коммутаторов	VLAN
1	2	2	1	2	2
2	4	3	2	3	3
3	6	3	3	3	3
4	4	2	2	2	2
5	5	3	4	3	3
6	5	3	4	3	4
7	6	2	3	2	3
8	4	3	3	3	3
9	3	3	3	2	2
10	8	2	2	3	4

Приложение Б. Схема локальной компьютерной сети