Министерство науки и высшего образования
Российской Федерации
Федеральное государственное автономное образовательное
учреждение высшего образования
«Севастопольский государственный университет»

ИССЛЕДОВАНИЕ СПОСОБОВ ПОСТРОЕНИЯ ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению лабораторной работы №6
по дисциплине
«Инфокоммуникационные системы и сети»
для студентов дневного и заочного отделения по направлению
09.03.02 «Информационные системы и технологи»,
09.03.03 «Прикладная информатика»

Севастополь
2020

УДК 681.326

Методические указания к выполнению лабораторной работы «**Исследование способов построения виртуальных локальных компьютерных сетей**» по дисциплине «Инфокоммуникационные системы и сети» / сост. доц. Чернега В.С., ст.преп. Волкова А.В. – Севастополь: Изд-во СевГУ, 2020. – 22 с.

Цель указаний: 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 предназначены для выполнения лабораторных работ по дисциплине «Инфокоммуникационные системы и сети» для студентов дневной и заочной форм обучения.

Методические указания рассмотрены и утверждены на методическом семинаре и заседании кафедры «Информационные системы»

Рецензент доцент кафедры «Информационные системы»

к.т.н., доцент Кротов К.В.

СОДЕРЖАНИЕ

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).

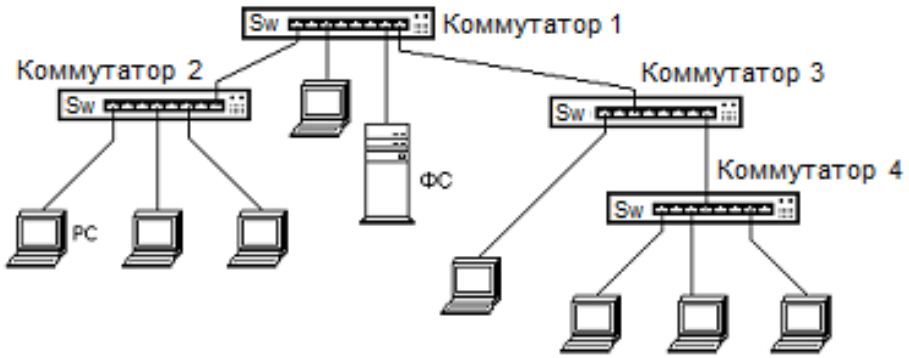

Рисунок 2.1 – Структура типовой локальной компьютерной сети Fast Ethernet

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 подсети, 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 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 сетевом (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, 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 и магистральные (транковые) порты.

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 конфигурации 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*). В магистральной линии мультиплексируются 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 VLAN, который получил название «межкоммутаторный канал» ISL (*Inter Switch Link*). Коммутаторы Cisco поддерживают оба протокола.В соответствии со стандартом IEEE 802.1Q к кадру Ethernet добавлен специальный маркер (тег) виртуальной сети (*Tag*) размером в четыре байта. Эти 32 теговых 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 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 TCI изображена в нижней части рисунка 2.2

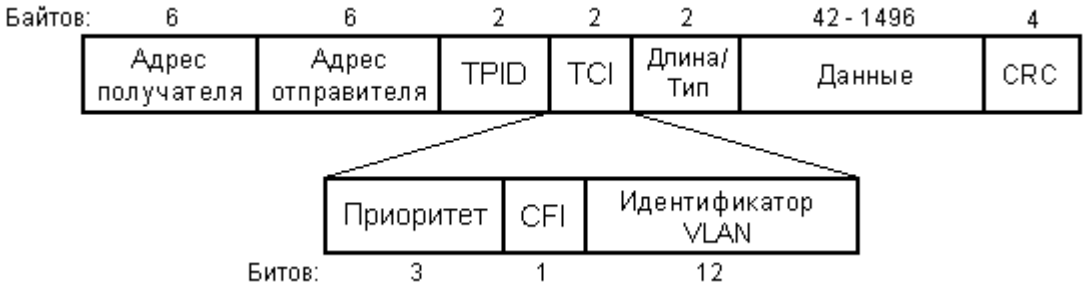

Рисунок 2.2 – Формат кадра Ehternet с меткой виртуальной сети

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 трафика, 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 указание 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 резервируются.

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.

Передача пакетов между виртуальными сетями может быть осуществлена только через маршрутизатор. Поэтому, чтобы виртуальные сети могли обмениваться

между собой пакетами каждой VLAN при конфигурировании должен быть назначен IP-адрес с соответствующей маской.

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.

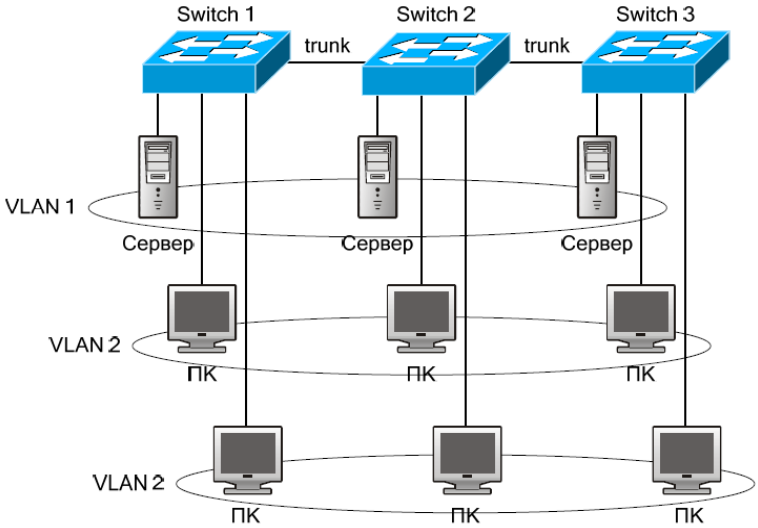

Рисунок 2.3 – Сеть VLAN, определенная логически

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.

В коммутаторах VLAN реализован в соответствии со стандартом 802.1Q.

2.3.1 Членство в сети VLAN

Сеть VLAN обычно создается администратором, который присваивает ей порты переключателя. Такой способ называется статической виртуальной локальной, сетью (static VLAN). Если администратор немного постарается и присвоит через базу данных аппаратные адреса всех хостов, переключатель можно настроить на динамическое создание сети VLAN.

Статические сети VLAN являются типичным способом формирования таких сетей и отличаются высокой безопасностью. Присвоенные сети VLAN порты переключателей 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. Программы сетевого управления помогут выполнить присваивание портов. Однако подобные программы использовать не обязательно.

Динамические сети VLAN автоматически отслеживают присваивание узлов. Использование интеллектуального программного обеспечения сетевого управления допускает формирование динамических VLAN на основе аппаратных адресов (MAC), протоколов и даже приложений. Предположим, MAC-адрес был введен в приложение централизованного управления VLAN. Если порт будет затем подключен к неприсвоенному порту переключателя, база данных управления VLAN найдет аппаратный адрес, присвоит его и сконфигурирует порт переключателя для нужной сети VLAN. Это упрощает административные задачи по управлению и настройке. Если пользователь перемещается в другое место сети, порт переключателя будет автоматически присвоен снова в нужную сеть VLAN. Однако для первоначального наполнения базы данных администратору придется поработать.

2.3.2 Коммутатор и VLAN

Компьютер при отправке трафика в сеть даже не догадывается, в каком VLAN'е он размещён. Об этом думает коммутатор. Коммутатор знает, что компьютер, который подключен к определённому порту, находится в соответствующем VLAN'е. Трафик, приходящий на порт определённого VLAN'а, ничем особенным не отличается от трафика другого VLAN'а. Другими словами, никакой информации о принадлежности трафика определённому VLAN'у в нём нет.

Однако, если через порт может прийти трафик разных VLAN'ов, коммутатор должен его как-то различать. Для этого каждый кадр трафика должен быть помечен каким-то особым образом. Пометка должна говорить о том, какому VLAN'у трафик принадлежит. Наиболее распространённый сейчас способ ставить такую пометку описан в открытом стандарте IEEE 802.1q.

2.3.3 Принцип коммутации

Внутрь фрейма после Source MAC-адреса добавляется ещё одно поле, очень грубо говоря, содержащее номер VLAN'а. Длина, выделенная для номера VLAN'а равна 12 битам, это означает, что максимальное число VLAN'ов 4096.

Кадры первого VLAN'а обычно не тегируются – он является родным VLAN'ом (native vlan). Каждый коммутатор принимает теперь решение на основе этой метки-тега (или его отсутствия).

Коммутация пакетов осуществляется с помощью 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 «1» (см. таблицу 2.1). При поиске пары MAC-адрес/порт теперь будет сравниваться тег кадра с номером VLAN'а 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

Каждая новая VLAN фактически создает новую таблицу коммутации. Тем не менее, все базовые механизмы коммутатора остаются точно такими же, как и до разделения на VLAN, но они используются только в пределах соответствующего VLAN.

2.3.4 Принадлежность VLAN

Порты коммутатора, поддерживающие VLAN'ы, (с некоторыми допущениями) можно разделить на два множества:

– нетегированные порты (access-порты, связи доступа) – к ним подключаются, как правило, конечные узлы. За каждым access-портом закреплён определённый VLAN, иногда этот параметр называют PVID. Весь трафик, приходящий на этот порт от конечного устройства, получает метку этого VLAN'a, а исходящий уходит без метки. Трафик этого VLAN передается без тега. На Cisco нетегированным порт может быть только в одном VLAN, на некоторых других коммутаторах данного ограничения нет;

– тегированные порты (trunk-порты, магистральные связи) – линия между двумя коммутаторами или от коммутатора к маршрутизатору. Внутри такой линии (транка) передаётся трафик нескольких VLAN'ов. Тут трафик уже идёт с тегами, чтобы принимающая сторона могла отличить кадр, который идёт в бухгалтерию, от кадра, предназначенного для ИТ-отдела. За транковым портом закрепляется целый диапазон VLAN'ов. Без тега коммутатор не сможет различить трафик различных VLAN'ов.

Существует native vlan. Трафик этого VLAN'a не тегируется даже в транке, по умолчанию это 1-й VLAN и по умолчанию он разрешён. Можно переопределить эти параметры. Нужен он для совместимости с устройствами, незнакомыми с инкапсуляцией 802.1q. Например, через Wi-Fi мост нужно передать 3 VLAN'a, и один из них является VLAN'ом управления. Если Wi-Fi-модули не понимают стандарт 802.1q, то управлять ими можно, только если этот VLAN настроить, как native vlan с обеих сторон.

Если порт тегирован для нескольких VLAN'ов, то в этом случае весь нетегированный трафик будет приниматься специальным родным VLAN'ом (native VLAN). Если порт принадлежит только одному VLAN как нетегированный, то тегированный трафик, приходящий через такой порт, должен удаляться. На практике это поведение обычно настраивается.

Обычно, по умолчанию все порты коммутатора считаются нетегированными членами VLAN 1. В процессе настройки или работы коммутатора они могут перемещаться в другие VLAN'ы.

2.3.5 Использование VLAN

VLAN позволяет разделять устройства на логические группы. Как правило, одному VLAN соответствует одна подсеть.

Устройства, находящиеся в разных VLAN, будут находиться в разных подсетях. Но в то же время VLAN не привязан к местоположению устройств и поэтому устройства, находящиеся на расстоянии друг от друга, все равно могут быть в одном VLAN независимо от местоположения. 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 назначен VLAN20, а подсети 192.168.1.0/24 – VLAN10.

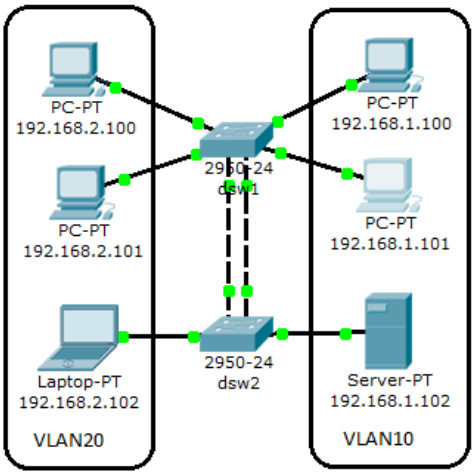

Рисунок 2.4 – Реализация нескольких VLAN

Для того чтобы хосты 1.101 и 1.102 в VLAN'е 10 на коммутаторе dsw1, могли обмениваться информацией с хостами VLAN'а 10 добавлен линк (физическое соединение) между коммутаторами, который представляет собой соединение двух нетегированных портов, находящихся в области видимости каждого VLAN'а соответственно.

Однако, когда количество VLAN возрастает, то схема явно становится очень неудобной, так как для каждого VLAN надо будет добавлять линк между коммутаторами для того, чтобы объединить хосты в один широковещательный сегмент. Для решения этой проблемы используются тегированные порты (см. рисунок 2.5).

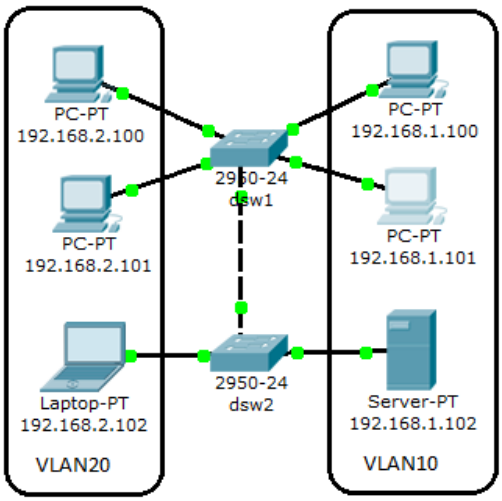

Рисунок 2.5 – Тегированный порт между коммутаторами

2.4 Изучение работы протокола VTP

Зачастую, во многих организациях существует необходимость разделения ресурсов на различные подсети (сети) с контролем доступа в них. Для таких целей есть много решений. Один из самых простых способов – создание и настройка VLAN на коммутаторах Cisco. Если надо добавить один-два VLAN, то никаких проблем это не составляет. Но что если необходимо добавить не одну виртуальную сеть, а с десяток, и это требуется сделать не на одном коммутаторе, а на 10 или даже на 100? Вводить сотни строк кода каждый раз, когда необходимо изменить присутствующие на коммутаторах VLAN? Избавиться от такой нудной и кропотливой работы поможет протокол VTP, который используется для централизованного управления VLAN на коммутаторах.

Протокол VTP является одним из самых известных протоколов, занимающихся L2-задачами. История протокола VTP достаточно продолжительна – первый раз он появляется в CatOS 2.1 (это Cisco Catalyst 2900 и 5000), после чего слегка модернизируется до второй версии и живёт очень долго. Третья версия, в которой реально много полезных изменений, вышла несколько лет назад.

2.4.1 Назначение протокола VTP

Протокол VTP (англ. VLAN Trunking Protocol) – это протокол, который используется для обмена информацией о VLAN (виртуальных сетях), протокол разработан в Cisco. Ключевое назначение протокола VTP – это обмен коммутаторов специфической базой данных с информацией о VLAN'ax. В данном процессе могут участвовать и маршрутизаторы, в случае, если у них установлена специальная карта, являющаяся мини-коммутатором (т.н. switchboard). VTP помогает упрощать операции с VLAN'ами в организации – добавление, удаление, изменение параметров, а также оптимизирует трафик, благодаря наличию функции vtp pruning. VTP 3-й версии ещё и помогает жить протоколу MST (стандарт 802.1s), плюс исправляет проблемы VTP версий 1 и 2.

Протокол VTP объединяет физически подключённые друг к другу коммутаторы (т.е. не через роутер или даже через другой свитч, но не поддерживающий VTP) в именованные области, называемые доменами VTP. В одной организации таких доменов может быть несколько, главное – чтобы они непосредственно не общались друг с другом.

2.4.2 Техническая реализация протокола VTP

Технологически протокол VTP реализован как SNAP-вложение в кадры ISL или 802.1Q. Работать может на 802.3 (Ethernet) и 802.5 (Token Ring).

Служебные данные VTP вкладываются не сразу в кадр 802.3, а после транкового заголовка. Выглядит это так:

– обычный заголовок 802.3 (Destination MAC, Source MAC, тип вложения – например, в случае 802.1Q это будет `0x8100`);

– субзаголовок LLC-уровня, содержащий код `0xAA 0xAA`, обзначающий, что далее идёт SNAP-вложение;

– субзаголовок SNAP – Subnetwork Access Protocol, показывающий, что будет разделение на субпротоколы канального уровня, а не сразу обработка уйдёт на сетевой уровень – несёт уже конкретную информацию, что вложен будет протокол, идентифицируемый как Cisco'вский протокол VTP.

А далее – уже данные самого протокола VTP, относящиеся к одному из типов сообщений – VTP summary advertisement, VTP subset advertisement, VTP advertisement request, VTP join message.

Весь трафик VTP идёт на специальный мультикастовый MAC-адрес вида `01-00-0C-CC-CC-CC`. Так как на этот же адрес, допустим, идёт и трафик протокола CDP, тоже цисковского, то используется схема разделения по SNAP-типу – для CDP он выбран `0x2000`, для VTP – `0x2003`. Это мультиплексирование канального уровня.

2.4.3 Логическая реализация протокола VTP

1. **Server** (режим по умолчанию):

– можно создавать, изменять и удалять VLAN из командной строки коммутатора;

– генерирует объявления VTP и передает объявления от других коммутаторов;

– может обновлять свою базу данных VLAN при получении информации не только от других VTP-серверов, но и от других VTP-клиентов в одном домене, с более высоким номером ревизии;

– сохраняет информацию о настройках VLAN в файле vlan.dat во flash;

– поддержка Private VLAN (VTPv3);

– возможность анонсирования VLAN из расширенного диапазона (VTPv3).

2. **Client** (устройства с Read only доступом):

– нельзя создавать, изменять и удалять VLAN из командной строки коммутатора;

– передает объявления от других коммутаторов;

– синхронизирует свою базу данных VLAN при получении информации VTP;

– сохраняет информацию о настройках VLAN в файле vlan.dat во flash;

– настройки VLAN сохраняются в NVRAM и в режиме клиента (VTPv3);

– поддержка Private VLAN (VTPv3);

– возможность анонсирования VLAN из расширенного диапазона (VTPv3).

3. **Transparent** (прозрачный):

– можно создавать, изменять и удалять VLAN из командной строки коммутатора, но только для локального коммутатора;

– не генерирует объявления VTP;

– передает объявления от других коммутаторов;

– не обновляет свою базу данных VLAN при получении информации по VTP;

– сохраняет информацию о настройках VLAN в NVRAM;

– всегда использует configuration revision number 0.

4. **Off** (отключенный, новый режим работы VTP, добавился в 3 версии):

– не передает на другие порты, полученные по транкам объявления VTP;

– в остальном аналогичен режиму Transparent.

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.

Примечание: Все настройки выплолняются только на портах в режиме *транка*.

В разных режимах VTP хранение информации о VLAN'ах реализовано различными способами:

– коммутатор с ролью VTP Server будет хранить настройки в файле vlan.dat на указанном устройстве хранения (один из flash'ей устройства);

– коммутатор с ролью VTP Transparent или VTP Off будет хранить настройки в конфигурации (это config.text, или, говоря проще, NVRAM);

– коммутатор с ролью VTP Client будет хранить настройки в оперативной памяти (их не будет видно в конфигурации или на flash).

2.4.4 Домены VTP

Домены VTP – это подмножества непосредственно подключенных друг к другу коммутаторов.

Для идентификации принадлежности устройства к домену VTP используется сравнение названия домена и хэша пароля (безусловно, не друг с другом, а между устройствами – т.е. оба этих параметра должны совпадать, чтобы VTP-устройства могли корректно общаться). Название домена VTP – это текстовая строка длиной до 32 байт (в случае, если название короче, оно добивается нулями – zero-padding), пароль – тоже текстовая строка, в чистом виде в сети не передающаяся, хранящаяся в случае работы устройства в роли VTP Server в файле vlan.dat, а в случае работы в режиме VTP Transparent – в config.text

Обратите внимание на следующие два важных момента. Первый – то, что название домена является case-sensitive, потому что строки сравниваются побайтово. Поэтому коммутаторы из домена Domain и из домена DOMAIN работать друг с другом не будут. Второй – работа с паролем. В кадрах передаётся хэш пароля, а не хэш кадра. Поэтому этот пароль нужен только для идентификации принадлежности к домену и никак не подтверждает целостность сообщения VTP. Его можно просто разово заснифить и добавлять в VTP-сообщения для придания им «легитимности».

Примечание: для успешной связи двух коммутаторов необходимо, чтобы у них были одинаковые версии протокола VTP.

Примечание: даже если Вы не используете протокол VTP как таковой по его основной задаче – синхронизации базы VLAN'ов, то Вам желательно, чтобы коммутаторы обладали одинаковыми настройками VTP в части имени домена. Причина – протокол динамического согласования транков – DTP – отправляет в ходе процедуры анонса имя VTP-домена, и в случае, если имя не совпадает, согласование не происходит. Т.е. два коммутатора, «смотрящие» друг на друга портами в режиме dynamic auto, в случае разных VTP-доменов просто не смогут согласовать транк. Решений будет несколько – отключить автосогласование (`switchport mode trunk`), отключить DTP (`switchport nonegotiate`), или выставить одинаковые имена доменов.

2.4.5 Принцип работы протокола VTP

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

– если изменилась базу данных VLAN'ов 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 (см. выше) прошло 300 секунд.

VTP версий 1 и 2 передаёт только данные по VLAN'ам с номерами от 1 до 1005 (десятибитовые номера VLAN'ов). Зато в VTPv3 это успешно решено и обмен данными про VLAN'ы охватывает весь диапазон – от 1 до 4094.

Несмотря на то, что стартовым инициатором рассылки VTP может быть только устройство с ролью VTP Server, пересылать обновление могут любые коммутаторы – т.е. устройству с ролью VTP Client совсем необязательно быть непосредственно подключённому к VTP Server. Клиент, получив от сервера рассылку с новой версией базы данных VLAN'ов, передаст её на все другие транковые порты, за которыми опять же могут быть другие VTP Client'ы (применили к себе, но отправили дальше) и VTP Transparent (не применили к себе, но отправили дальше). Ограничения стандарта 802.1D на максимальный диаметр «поля» коммутаторов здесь не действуют.

Какая база данных актуальнее определяется при помощи системы версий. У каждой базы VLAN'ов будет своя версия. В случае, если устройством получено обновление, которое старше по номеру, чем имеющаяся БД, то имеющаяся БД заменяется новой. Целиком, без всяких join/merge.

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'ов с номерами от 2 до 1001). Более того, под pruning будет подпадать только уникастовый и неизвестный мультикастовый трафик, поэтому, к примеру, BPDU протоколов семейства STP фильтроваться не будут.

Т.е. допустим, у нас есть два коммутатора – A и B. Коммутатор A имеет роль VTP Server, а B – VTP Client. Между ними – транковый канал, 802.1Q. На коммутаторе B включен vtp pruning. Допустим, на коммутаторе A в базу VLAN добавлены VLAN 10 и VLAN 20. Соответственно, коммутатор A уведомит по протоколу VTP своего соседа – B – о новой ревизии базы VLAN'ов. Сосед B добавит эти VLAN'ы в базу и теперь, когда подключенный к коммутатору A клиент, например, передаст броадкаст в VLAN'е 10, этот броадкаст дойдёт и до коммутатора B. Невзирая на то, что у коммутатора B может вообще не быть ни одного порта и интерфейса в VLAN 10, а также не быть других транков (т.е. трафик 10-го VLAN'а коммутатору B совсем не нужен). Вот в данном случае механизм pruning сможет сэкономить полосу пропускания канала между коммутаторами A и B просто не отправляя трафик неиспользуемого VLAN'а коммутатору B.

2.4.7 Устранение неисправностей (troubleshooting) протокола VTP

Неисправностей в VTP может быть очень много. Рассмотрим основные из них.

Проверка каналов между коммутаторами:

– проверьте физическую доступность интерфейсов;

– проверьте корректность режима дуплекса и скорости;

– проверьте, что корректно согласовался транк;

– проверьте, совпадают ли native vlan'ы.

Проверка настройка VTP:

– коммутаторы должны быть непосредственно подключены друг к другу;

– должен быть хотя бы один VTP Server;

– версии VTP, а также имя домена и пароль должны быть идентичны у всех устройств.

Проблема добавления нового коммутатора: заключается в следующем: новый коммутатор при добавлении делает следующее – он слушает трафик VTP и при получении первого же advertisement берёт из него настройки (имя домена и пароль). Дефолтная настройка коммутатора – это режим VTP Server (т.е. когда Вы достаёте коммутатор из коробки, Вы сразу можете на нём создавать VLAN'ы, в случае VTP Client это было бы невозможно).

Соответственно, возможна неприятная ситуация. Состоит она в том, что можно взять коммутатор, заранее его сконфигурировать, внеся больше изменений, чем есть сейчас в инфраструктурном VTP, задать правильные параметры домена и подключить к сети. Тогда коммутатор своей базой затрёт существующую. Почему так произойдёт и как это может быть? Рассмотрим подробнее.

Вы покупаете новый коммутатор и вводите его в эксплуатацию. Отдельно от других, которые работают в VTP. Ну, вот так сложилось – допустим, в филиале организации его ставите, где он не является непосредственно подключенным к другим коммутаторам. Начинаете с ним работать. Работаете интенсивно – добавляете на него VLAN'ы, удаляете их, переименовываете. Каждое действие плюсует единицу к revision number. Вдруг через некоторое время возникает ситуация – филиал закрывается. Коммутатор перевозят в основной офис, и Вы подключаете его к другим. И тут выясняется следующее. У данного коммутатора ревизия численно выше, чем у местного VTP Server. Имя домена и пароль совпадают. Как только транк поднимается, новый коммутатор выстреливает advertisement, который начинают слушать все остальные коммутаторы и ретранслировать дальше. Это штатный функционал – Вы не можете ограничить получение VTP-данных только от одного, «правильного» сервера. Соответственно, эта волна накрывает все коммутаторы в режиме Client и тот, который в Server. Это тоже штатное поведение – VTP Server, получив VTP-данные с большим номером ревизии, чем у себя, перезаписывает свою базу. И всё, Вы имеете большие проблемы – вместо Вашей базы VLAN'ов у Вас на всех коммутаторах та, которая была в филиале.

Чтобы избежать этого, можно поступить по-разному. Например, не делать у этого коммутатора имя домена и пароль, как в основной VTP-сети. Но можно и проще – ведь чтобы этого всего не произошло, надо просто сбросить номер ревизии. Для этого достаточно переименовать домен у коммутатора в какое-нибудь временное название и после вернуть назад. Ревизия сбросится. После не забудьте включить режим VTP Client.

Примечание: Именно из-за этой ситуации использование VTP в production-сети с высоким уровнем безопасности является нежелательным. Злоумышленник может провести достаточно простую атаку – ему хватит доступа к транковому порту и возможности отправить, допустим, VTP-уведомление о том, что пришла база с версией 10000 и одним VLAN'ом, и всё – вся VTP-инфраструктура примет это как нормальное положение вещей и остальные VLAN'ы пропадут. Поэтому в безопасных сетях все коммутаторы работают в VTP transparent, где такая ситуация невозможна в принципе.

3 ОПИСАНИЕ ЛАБОРАТОРНОЙ УСТАНОВКИ

3.1 Принцип работы VLAN

1. От компьютера отправляется пакет другому компьютеру этой же сети. Этот пакет инкапсулируется в кадр, и пока никто ничего не знает о VLAN'ах, поэтому кадр уходит, как есть, на ближайший коммутатор.

2. У каждого VLAN'а есть номер. Существуют два типа VLAN:

– стандартный диапозон VLAN – от 1 до 1000;

– расширеный диапозон VLAN – от 1025 до 4096.

На каждом коммутаторе существует VLAN 1, все интерфейсы по умолчанию относятся к нему. Процесс настройки практически идентичен для всех коммутаторов Catalyst.

Сначала необходимо создать VLAN и задать ему имя:

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

Просмотр информации о VLAN'ах:

```
switch# show vlan brief
```

3. На коммутаторе необходиимый порт отметим как член 2-го VLAN'а командой:

```
switch(config)#interface fa0/1
switch(config-if)#description “I am using simple frames”
switch(config-if)#switchport mode access
switch(config-if)#switchport access vlan 2
```

Это означает, что любой кадр, пришедший на этот интерфейс, автоматический тегируется: на него вешается ленточка с номером VLAN'а. В данном случае с номером 2.

Далее коммутатор ищет в своей таблице MAC-адресов среди портов, принадлежащих 2-му VLAN'у, порт, к которому подключено устройство с MAC-адресом получателя.

3. Если получатель подключен к такому же access-порту, то ленточка с кадра отвязывается, и кадр отправляется в этот самый порт таким, каким он был изначально. То есть получателю также нет необходимости знать о существовании VLAN'ов.

4. Если же искомый порт, является транковым, то ленточка на нём остаётся.

```
Switch(config)#interface fa0/2
Switch(config-if)#description “I am using tagged frames”
Switch(config-if)#switchport mode trunk
```

Если тегированный кадр прилетит на access-порт, то он будет отброшен.

Если нетегированный кадр прилетит на trunk-порт, то он будет помещён в native VLAN. По умолчанию им является 1-й VLAN. Но можно поменять его командой `switchport trunk native vlan 2`. В этом случае все кадры, помеченные 2-м VLAN'ом будут уходить в этот порт нетегированными, а нетегированные кадры, приходящий на этот интерфейс, помечаться 2-м VLAN'ом. Кадры с тегами других VLAN'ов останутся неизменными, проходя, через такой порт.

Конечным 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, то 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, свитч его отбросит из-за увеличенного размера кадра. Зависит от разных факторов: производитель, софт (прошивка), тип форвардинга (cut-through, store-and-forward).

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 1-2,10,15
```

Добавление ещё одного разрешенного 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
```

3.2 Сеть управления

Рассмотрим команды настройки IP-адрес для управления. Для этого необходимо создать виртуальный интерфейс и указать номер интересующего VLAN'a. А далее работать с ним, как с самым 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
```

3.3 Базовая настройка протокола VTP

Первым делом необходимо нарисовать топологию сети, в которой собираетесь применять протокол VTP. Посмотрите, какие версии протокола поддерживаются устройствами (обычно везде есть VTPv2). Выберите устройство, которое будет сервером (ему не надо быть каким-то особо быстрым, специфической нагрузки на VTP Server нет, ему лишь желательно обладать максимальным uptime – временем бесперебойной работы). 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:

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

Стереть имя домена штатно нельзя, только сменить.

Настройка пароля VTP:

```
switch(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, например, случайное добавление в сеть неправильно настроенного коммутатора и последующие проблемы. Пароль VTP не защищает передаваемую между коммутаторами информацию.

Настройка версии VTP:

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

Настройка VTP pruning:

Включение выполняется командой:

```
switch(config)#vtp pruning
```

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

Настройка режима VTP:

```
switch(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.

3.3.1 Расширенная настройка протокола VTP

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, пишущийся 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
```

Примечание: Если в выводе команды `show vtp status` ниже этой строчки есть что-то вида `Local updater ID is 0.0.0.0 (no valid interface found)`, то на устройстве нет рабочих IPv4-интерфейсов, и данная команда не имеет смысла – надо

вначале сделать хотя бы один интерфейс, с которого можно будет забрать IP-адрес для идентификации VTP-устройства.

Делаться это будет такой командой:

```
host(config)#vtp interface интерфейс
```

где *интерфейс* – это, например, `loopback 0`.

4 ПРОГРАММА И МЕТОДИКА ВЫПОЛНЕНИЯ РАБОТЫ

1. Изучение работы протокола VTP. По умолчанию коммутаторы являются серверами. Если коммутатор в серверном режиме отправляет обновление с номером версии, превышающим текущий номер версии, все коммутаторы изменят свои базы данных в соответствии с новым коммутатором.

Настройте протокол VTP между коммутатором **Switch-Server** и **Switch-Client1**. Затем добавьте коммутаторы **Switch-Transparent** и **Switch-Client2** и настройте их соответствующим образом (см. рисунок 4.1). При любом изменении таблицы VLAN необходимо просматривать текущую конфигурацию протокола VTP коммутаторов с помощью команды `show vtp status`.

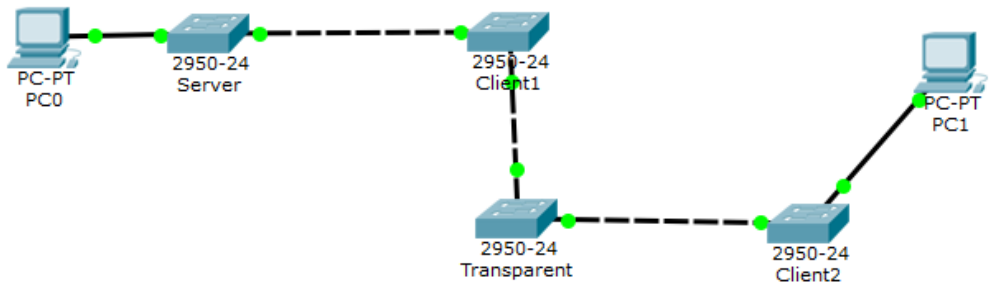

Рисунок 4.1 – Изучение работы протокола VTP

Задание на настройку:

– настроить на коммутаторах соответствующие режимы VTP;

– VLAN, которые создаются на Switch_Server, должны присутствовать и на коммутаторах Switch_Client1 и Switch_Client2 (хотя они там не создавались);

– хосты PC0 и PC1 должны ping-овать друг друга;

Примечание: скорее всего при проверке ping между хостами PC0 и PC1 ничего не произойдет. Это может быть связано с тем, что Switch_Transparent находится в режиме VTP Transparent и он не принимает во внимание сообщения от VTP Server, а лишь транслирует их дальше. По этой причине, он не сможет пропустить VLAN хостов PC0 и PC1 через себя, так как его просто нет, и хосты не получат сетевую доступность. Поэтому, надо добавить этот VLAN вручную на Switch_Transparent.

2. Настройка VLAN. Реализовать схему, представленную на рисунке 4.2 и настроить VLAN на коммутаторах в соответствии с вариантом (v – номер по списку в журнале) и используя протокол VTP (как Вы считаете, какой коммутатор должен

остаться в режиме сервера?). Условием проверки является отсутствие связи между хостами, принадлежащими разным VLAN.

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

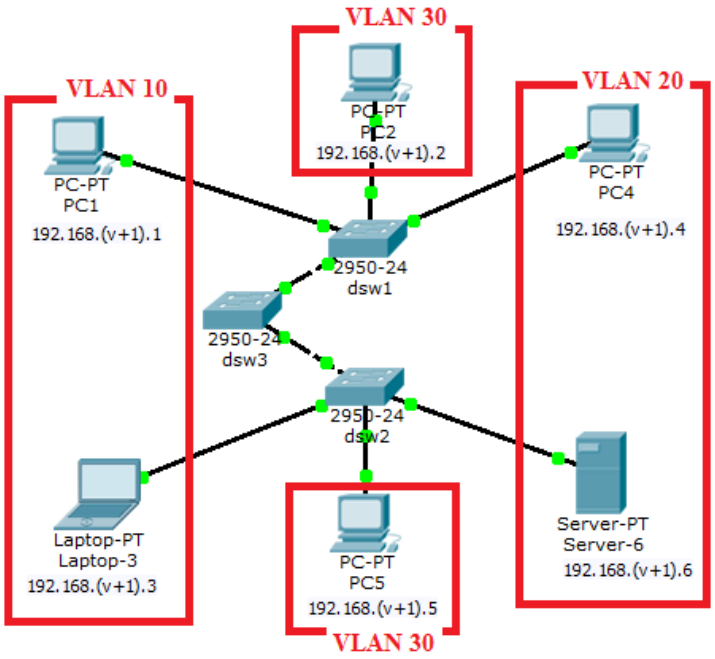

Рисунок 4.2 – Изучение работы протокола VTP

5 СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист.
2. Цель и программа лабораторной работы.
3. Исходные данные в соответствии с индивидуальным вариантом.
4. Скриншот с топологией локальной сети.
5. Команды и скриншоты этапов настройки локальной сети.
6. Скриншоты результатов тестирования сети.
7. Выводы.

6 КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое виртуальные локальные сети и зачем они применяются?
2. Зачем применяется разбиение сети на VLAN-ы?
3. Что такое магистральные (trunk) порты и порты доступа (access)?
4. Что такое interVLAN routing?
5. Способы организации interVLAN routing?
6. Зачем использовать протокол VTP?
7. 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.