Лабораторная работа № 7 Изучение виртуальных локальных сетей (VLAN). Конфигурирование VLAN на одном коммутаторе.

**Цель работы:** Изучение общих принципов работы виртуальных сетей VLAN, назначен6ие и особенности построения VLAN на одном коммутаторе при помощи эмулятора CISCO Packet Tracer.

**Оборудование:** Персональный компьютер, включенный в сеть IP, Microsoft Windows, приложение CISCO Packet Tracer

# Основные сведения

CISCO Packet Tracer - это визуальное моделирование сетей на основе оборудования CISCO: маршрутизаторов (1841, 2620XM, 2621XM, 2811), коммутаторов (2950-24, 2950Т, 2960), концентраторов, повторителей, беспроводных точек доступа (маршрутизатор Linksys WRT300N), компьютеров. Использование многих параметров: настройка IP-адреса и маски подсети на проводной и беспроводной сетевой карте (статического, динамического DHCP), настройка подключения к устройствам через консоль в терминале, работа в командной строке, веб-браузере), серверов (HTTP, DHCP, TFTP, DNS), эмуляция WAN (DSL-модемы, кабельные модемы, Frame Relay), принтеров, IP-телефонов, многопользовательское облако. ***Каждый тип оборудования включает в себе пустое шасси и ряд модулей, которые можно установить.*** Конфигурирование и настройка данного оборудования через виртуальную консоль CLI в операционной системе IOS, через графическое отображение в окне (имени устройства, конфигурационного файла, сетей VLAN, интерфейсов (дуплексности, скорости, MAC-адреса, IP-адреса, маски подсети), статической и динамической маршрутизации).

# Виртуальные сети (Virtual LAN)

**Коммутаторы –** это устройства канального уровня, которые позволяют соединить несколько физических сегментов локальной сети в одну большую сеть. Коммутация локальных сетей обеспечивает взаимодействие сетевых устройств по выделенной линии без возникновения коллизий, с параллельной передачей нескольких потоков данных. Коммутаторы локальных сетей обрабатывают кадры на основе алгоритма прозрачного моста (transparent bridge) IEEE 802.1D, который применяется в основном в сетях Ethernet. При включении питания коммутатор начинает изучать расположение рабочих станций всех пРисунокоединенных к нему сетей путем анализа МАС-адресов источников входящих кадров.

Адреса изучаются динамически. Это означает, что, как только будет прочитан новый адрес, то он сразу будет занесен в **контентно-адресуемую память (content-addressable memory, САМ).** Каждый раз, при занесении адреса в таблицу коммутации, ему пРисунокваивается временной штамп. Это позволяет хранить адреса в таблице в течение определенного времени. При обращении по этому адресу, он получает новый временной штамп. Адреса, по которым не обращались долгое время, из таблицы удаляются.

Коммутатор использует таблицу коммутации для пересылки трафика. Когда на один из его портов поступает пакет данных, он извлекает из него информацию МАС-адрес приемника и ищет этот МАС-адрес в своей таблице коммутации. Если в таблице есть запись, ассоциирующая МАС-адрес приемника с одним из портов коммутатора, за исключением того, на который поступил кадр, то кадр пересылается через этот порт. Если такой ассоциации нет, кадр передается через все порты, за исключением того, на который он поступил. Это называется лавинным распространением (flooding). Широковещательная и многоадресная рассылка выполняется также путем лавинного распространения. С этим связана одна из проблем, ограничивающая применение коммутаторов. Наличие коммутаторов в сети не препятствует распространению широковещательных кадров (broadcast) по всем сегментам сети, сохраняя ее прозрачность. В случае если в результате каких-либо программных или аппаратных сбоев протокол верхнего уровня или сам сетевой адаптер начнет работать не правильно, и будет постоянно генерировать широковещательные кадры, коммутатор в этом случае будет передавать кадры во все сегменты, затапливая сеть ошибочным трафиком. Такая ситуация называется широковещательным штормом (broadcast storm).

Современные коммутаторы (Swith’s), сетевые устройства канального уровня, как правило обладают **дополнительными «интеллектуальными» функциями** и позволяют конфигурироваться и **управляться из командной строки интерфейса (command-line interface – CLI** ) с помощью консоли или Web- интерфейса.

Среди них самые распространенные и наиболее используемые дополнительные функции это:

* VLAN - Построение виртуальных локальных сетей VLAN;
* Семейство протоколов Spanning Tree IEEE 802.1d, 802.1w, 802.1s;
* Статическое и динамическое агрегирование каналов по протоколу IEEE 802.3ad LACP;
* Сегментация трафика и обеспечение качества обслуживания QoS;
* Функции обеспечения безопасности, включая аутентификацию IEEE 802.1х и функцию Port Security;
* Протоколы группового вещания;
* SNMP – управление и др.

Построение и поддержка виртуальных локальных сетей VLAN является одной из основных и часто применяемых функций используемых в сетях с коммутаторами.

Применение технологии VLAN преследует следующие цели:

* ***Уменьшение количества широковещательного трафика в сети.***

Это одна из основных задач, решаемая с помощью VLAN. Сеть, построенная на коммутаторах Ethernet, даже при значительно разветвленной топологии обязана пропускать широковещательный трафик (MAC адреса ***FF:FF:FF:FF:FF:FF***) ко всем компьютерам разных сегментов сети. Производительность сети в данные моменты значительно снижается. Создание VLAN означает разбиение сети на коммутаторах на несколько широковещательных доменов. Один и тот же VLAN на разных коммутаторах образовывает один широковещательный домен.

* ***Гибкое разделение устройств на группы.***

Как правило, одному VLAN соответствует одна IP-подсеть. Устройства, находящиеся в разных VLAN, будут находиться в разных IP-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.

* ***Увеличение безопасности и управляемости сети.***

Когда сеть разбита на VLAN, упрощается задача применения политик и правил безопасности. С VLAN политики можно применять к целым подсетям, а не к отдельному устройству. Кроме того, переход из одного VLAN в другой предполагает прохождение через устройство 3-го уровня, на котором, как правило, применяются политики, разрешающие или запрещающие доступ из VLAN в VLAN.

Виртуальной локальной сетью (Virtual LAN, VLAN) называется группа узлов сети, трафик которой, в том числе широковещательный, на канальном уровне полностью изолирован от трафика других узлов.

Это означает, что передача кадров между разными виртуальными сетями на основании MAC-адреса невозможна, независимо от типа адреса - уникального, группового или широковещательного. В то же время, внутри виртуальной сети кадры передаются по технологии коммутации, то есть только на тот порт, который связан с адресом назначения кадра. Таким образом, с помощью виртуальных сетей решается проблема распространения широковещательных пакетов и вызываемых ими следствий, которые могут развиться в широковещательные штормы и существенно снизить производительность сети.

Виртуальная локальная сеть (Virtual Local Area Network, VLAN) представляет собой коммутируемый сегмент сети, который логически выделен по выполняемым функциям, рабочим группам или приложениям, вне зависимости от физического расположения пользователей. Виртуальные локальные сети обладают всеми свойствами физических локальных сетей, но рабочие станции можно группировать, даже если они физически расположены не в одном сегменте, т.к. любой порт коммутатора можно настроить на принадлежность определенной VLAN. При этом одноадресный, многоадресный и широковещательный трафик будет передаваться только между рабочими станциями, принадлежащими одной VLAN. Каждая VLAN рассматривается как логическая сеть, т.е. пакеты, для данной VLAN будут коммутироваться коммутатором только в пределах этой VLAN.

Для того, чтобы трафик одной VLAN попадал в другую, применяются сетевые устройства 3-го уровня OSI, а именно маршрутизаторы.

Достоинством технологии виртуальных сетей является то; что она позволяет создавать полностью изолированные сегменты сети путем логического конфигурирования коммутаторов, не прибегая к изменению физической структуры.

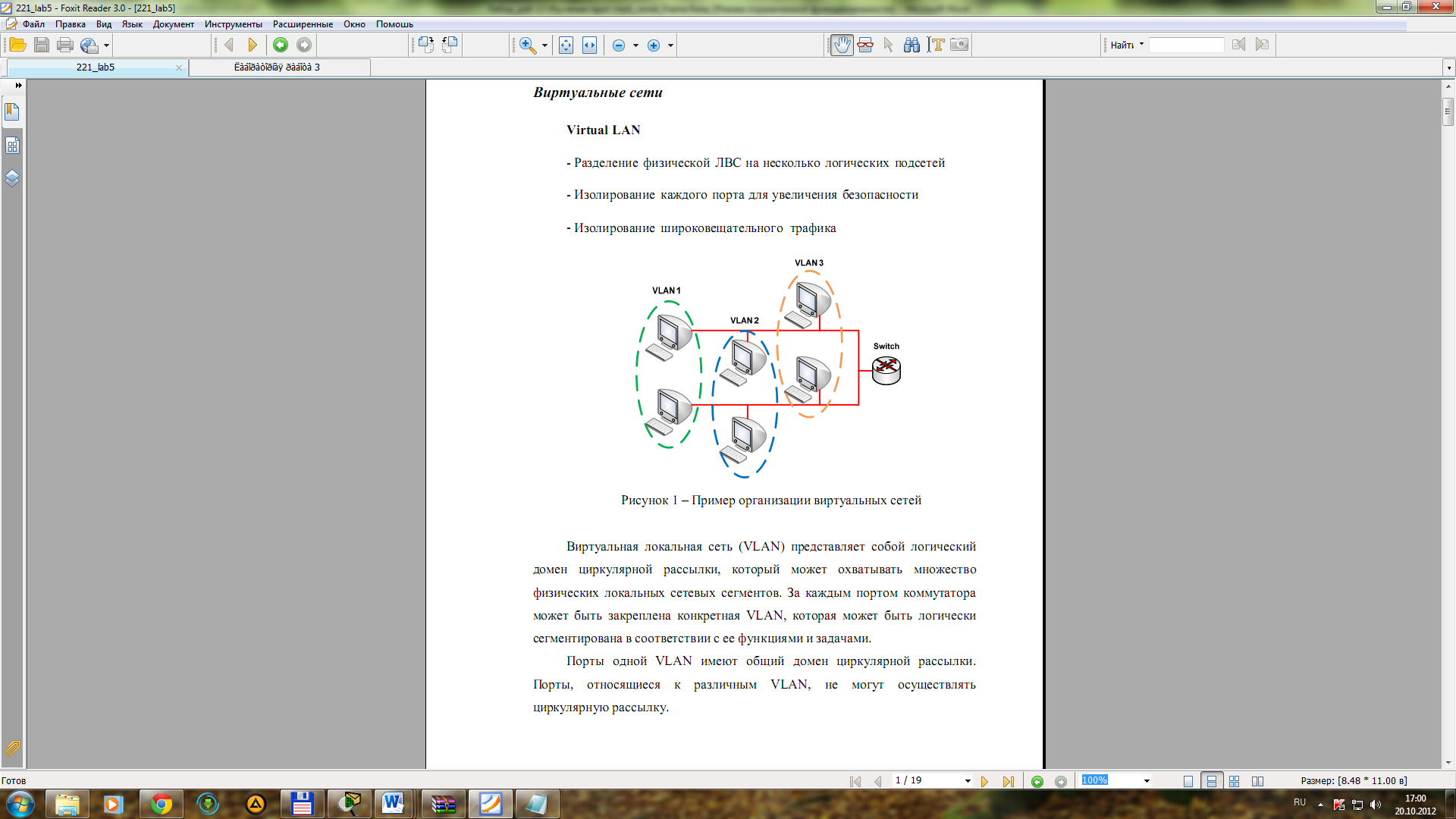


Рисунок. 7.1. Пример организации виртуальных сетей

Построение VLAN сетей могут осуществляться различными способами. В основном применяются три типа VLAN:

* VLAN на базе портов;
* VLAN на базе MAC-адресов;
* VLAN на основе меток в дополнительном поле кадра – стандарт IEEE 802.1Q;

# VLAN на базе портов на одном коммутаторе.

***(Теория и практическое выполнение в Packet Tracer)***

При использовании VLAN на базе портов, каждый порт назначается в определенную VLAN, независимо от того, какой пользователь компьютер или Hub подключены к этому порту. Это означает, что все пользователи, подключенные к этому порту, будут членами одной VLAN. Конфигурация портов статическая и может быть изменена только вручную.

***Основные характеРисуноктики VLAN на базе портов:***

**Применяются в пределах одного коммутатора**. Если необходимо организовать несколько рабочих групп в пределах небольшой сети на основе одного коммутатора, например, необходимо разнести технический отдел и отдел продаж, то решение VLAN на базе портов оптимально подходит для данной задачи.

**Простота настройки**. Создание виртуальных сетей на основе группирования портов не требует от администратора большого объема ручной работы - достаточно каждому порту, находящемуся в одной VLAN, пРисуноквоить один и тот же идентификатор VLAN (VLAN ID) .

**Возможность изменения логической топологии сети без физического перемещения станций** – достаточно всего лишь изменить настройки порта, с одной VLAN (например, VLAN технического отдела) на другую (VLAN отдела продаж) и рабочая станция сразу же получает

возможность совместно использовать ресурсы с членами новой VLAN. Таким образом, VLAN обеспечивают гибкость при перемещениях, изменениях и наращивании сети.

**Каждый порт может входить только в один VLAN**. Поэтому **для объединения** **виртуальных подсетей** – как внутри одного коммутатора, так и между двумя и более коммутаторов, **нужно использовать сетевой уровень** (третий уровень модели ISO/OSI). Один из портов каждой VLAN подключается к интерфейсу маршрутизатора, который создает таблицу маршрутизации для пересылки пакетов из одной подсети в другую, при этом IP адреса подсетей должны быть разными.

## Практическое выполнение:

### Создадим в Packet Tracer модель сети согласно Рисунок 7.1

# Для создания сети используем коммутатор cisco 2960-24PT, девять компьютеров PC-PT, один сервер Server-PT.

# Первые три PC-PT (ПК-0-ПК-2) будем считать как хосты бухгалетии –“buh”, следующие три компьютера (ПК-3-ПК-5) – компьютеры отдела продаж- “Sales”, остальные компьютеры и сервер отнесем к отделу маркетинг –“Market”.

# ПРисуноквоим IP-адреса каждому хосту и серверу согласно *следующему правилу: для ПК-0: IP –adress: 10.10.NN.G01, для ПК-1- IP –adress: 10.10.NN.G02 и т.д., для Sever-PT - IP –adress: 10.10.NN.G10. (где NN Ваш порядковый номер в журнале группы, G – порядковый номер группы, а именно - «1» для первой группы «2» для втрой группы)*

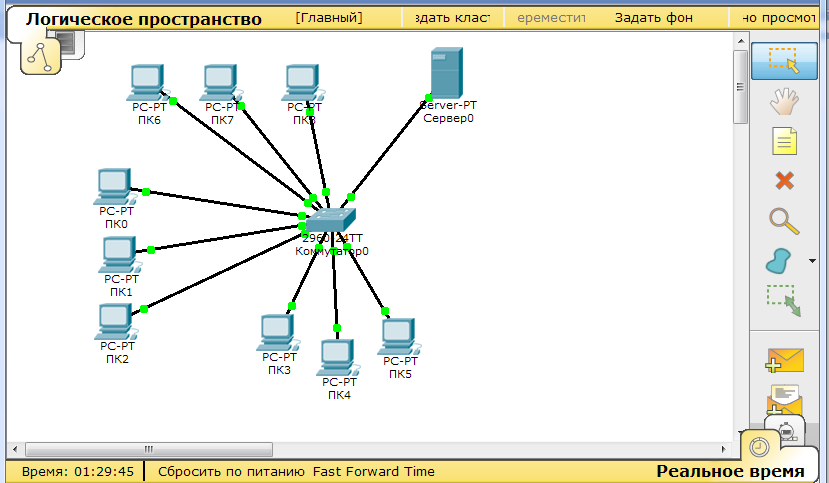
# Данные компьютеры соединить с портами коммутатора согласно таблицы, приведённой ниже: (в отчёте создать аналогичную таблицу с конкретными данными согласно вариантам)

Таблица № 7.1 Первоначальная конфигугация сети LAN.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №пп | Отдел | Компьютер | IP-адрес | № порта коммутатора |
| 1 | Бухгалтерия (Buh) | ПК-0 | 10.10.NN.101 | Fa 0/1 |
| 2 | ПК-1 | 10.10.NN.102 | Fa 0/2 |
| 3 | ПК-2 | 10.10.NN.103 | Fa 0/3 |
| 4 | Отдел продаж (Sales) | ПК-3 | 10.10.NN.104 | Fa 0/4 |
| 5 | ПК-4 | 10.10.NN.105 | Fa 0/5 |
| 6 | ПК-5 | 10.10.NN.106 | Fa 0/6 |
| 7 | Отдел маркетинга (Market) | ПК-6 | 10.10.NN.107 | Fa 0/7 |
| 8 | ПК-7 | 10.10.NN.108 | Fa 0/8 |
| 9 | ПК-8 | 10.10.NN.109 | Fa 0/9 |
| 10 | Server | 10.10.NN.110 | Fa 0/10 |

(Название – имена компьютеров можно присваивать на английском)

Рисунок 7.2. Топология сети с одним коммутатором.



Маска на каждом из компьютеров должна соответствовать 255.255.255.0

1. Проверим прохождение пакетов каждого из компьютеров к серверу и междусобой. Результат зафиксируем в отчете. (Например между ПК1 и ПК10 и ПК8)

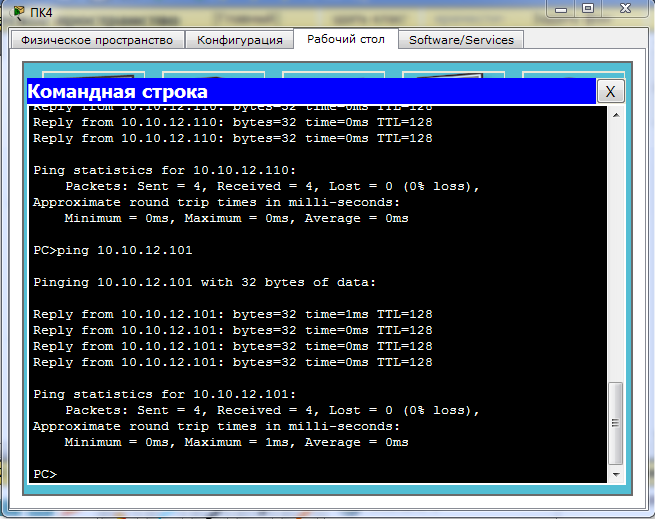
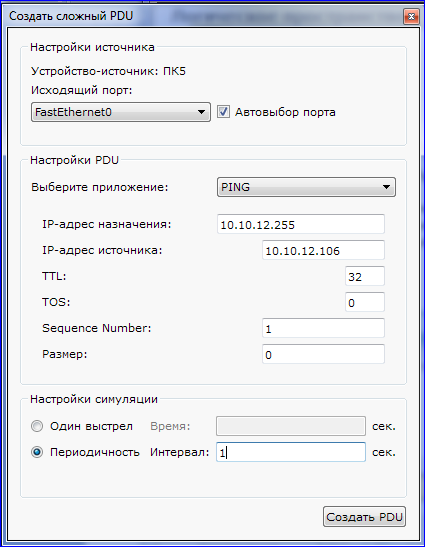


Рисунок 7.3. Прохождение тестовых пакетов между ПК-4, Server и ПК-4 и ПК-0.

1. Данная сеть являтся сетью одного адресного пространства IP адресов и одного широко-вещательного домена. Проверим данное утверждение.

Переключимся в режим симуляции и создадим комплексный PDU: щёлкнув по элементу меню “комплексное PDU” -> ; с помощью мышки перенесём его на любой компьютер. Откроется диалоговое окно с параметрами IP пакета, заполним поля диалогового окна как показано на Рисунок.7.4. в соответсвии со своими вариантами, нажимаем кнопку создать PDU.



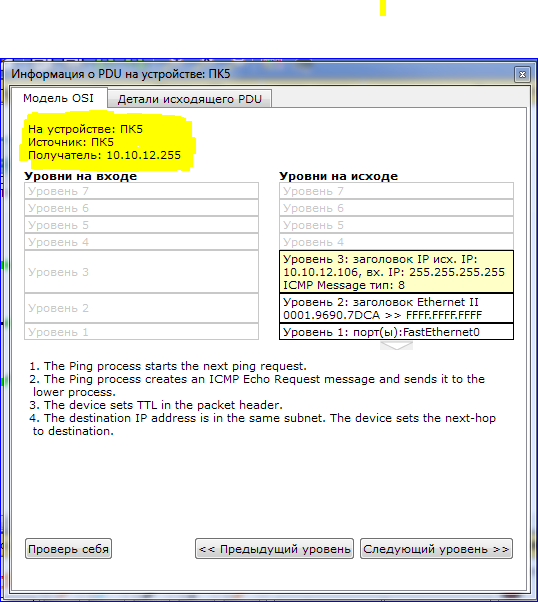
**Рис 7.4. Диалоговое окно «Создание комплексного PDU».**

IP –адрес назначения и источника заполняется в соответсвии с IP –номерами Вашего варианта и используемого компьютера. (В данном случае представлен 12 вариант первой группы и ПК-5). Последний октед IP-адреса назначения должен равняться значению 255, т.е. широко-вещательная рассылка с использованием IP протокола.



На выбранном компьютере появится сохраненный пакет, дважды щёлкнув по нему откроем информационное окно Рисунок 7.5. Проанализируйте его и сделайте Screen Shot's, сохранив в отчете. Обратите внимание на выделенные желтым цветом параметы пакета.

Рис. 7.5. Информационное окно «комплексного PDU»



Используя кнопки «Захват/Вперед» проследим прохождение пакета по сети. Здесь видно сразу, что созданный пакет распространяется на все компьютеры сети – Рисунок 7.6.

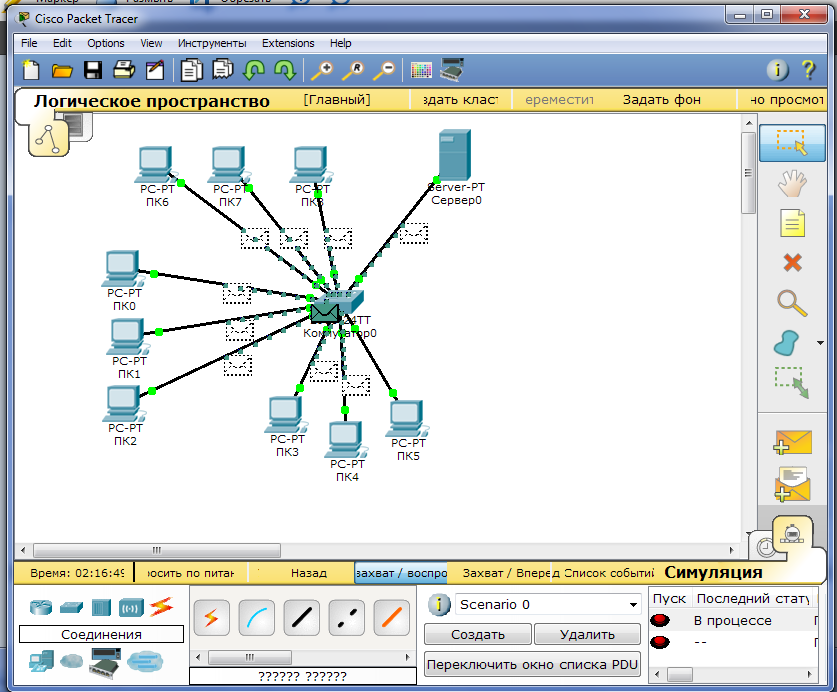


Рис. 7.6. Передача широковещательного пакета/кадра на все задействованные порты коммутатора.

1. Таким образом, данная сеть является сетью с единым широковещательным доменом.
2. Сохранить файл для отчета LR\_7\_FIO.pkt;
3. Используя возможность конфигурации коммутатора cisco 2960, разделим сеть на три виртуалные локальные сети VLAN.
4. Каждая VLAN имеет свой индентификатор- диапазон номеров 1-4096, который условно делится на «нормальный диапазон»: 1-1005 и «расширенный»: 1006-4094. Номера 1002-1005 назначаются для виртуальных сетей технологий Token Ring и FDDI.

Таблица № 7. Индентификаторы vlan, применяемые в коммутаторах CISCO

|  |  |  |  |
| --- | --- | --- | --- |
| **VLANs** | **Диапазон** | **Использование** | **Передается VTP** |
| ***0, 4095*** | ***Reserved*** | ***Только для системного использования.*** | — |
| 1 | Normal | VLAN по умолчанию. Можно использовать, но нельзя удалить. | Да |
| 2-1001 | Normal | Для VLANob Ethernet. Можно создавать, удалять и использовать. | Да |
| 1002-1005 | Normal | Для FDDI и Token Ring. Нельзя удалить. | Да |
| 1006-4094 | Extended | Только для VLANob Ethernet. | Версия 1 и 2 нет, версия 3 да |

1. Создадим три VLAN для одного коммутатора, используя статическое конфигурирование:

Создание виртуальных сетей может производиться двумя способами:

* в режиме глобального конфигурирования;
* из привилегированного режима конфигурирования по команде vlan database.

Корпорация Cisco рекомендует использовать первый способ создания VLAN’s.

Создаём VLAN, используя первый способ - в режиме глобального конфигурирования:

1. ***Используя CLI входим в привеллегированный режим:***

***Switch>enable***

1. ***Переходим в режим глобального конфигурирования:***

***Switch#conf term***

***Switch(config)#***

1. ***Создаём первую VLAN***

**Правило для выбора VLAN: IDVLAN =NN\*10+NumVLAN,**

**NN-Ваш порядковый номер по журналу**. (В примере NN=12)

***Switch(config)#vlan 121***

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

1. ***Аналогично создаем вторую и тетью VLAN’s***

***Switch(config)#vlan 122***

***Switch(config-vlan)#vlan 123***

1. ***Присвоим имена созданным VLAN's, согласно таблице 7.1., с помощью команд:***

***Switch(config)#vlan 121***

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

***Switch(config-vlan)#vlan 122***

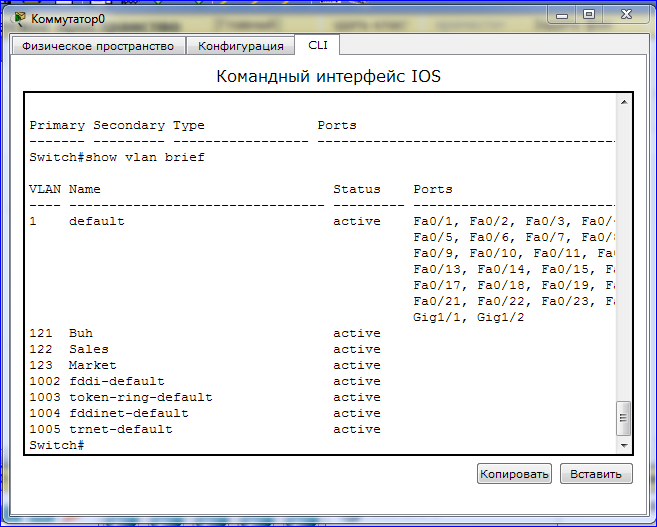
***Switch(config-vlan)#name Sales***

***Switch(config-vlan)#vlan 123***

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

1. ***С помощью команды Switch(config-vlan)#do show vlan brief посмотрим состояние виртуальных сетей и интерфейсов коммутатора Cisco на данном этапе. Аналогичную команду можно использовать в глобальном режиме:***
2. ***Для перехода в глобальный режим используем дважды команду exit и далее***

Рисунок 7.7. Состояние VLAN после первоначальной конфигурации.



***Switch(config)#show vlan brief или sh vlan brief***

1. ***Следует обратить внимание, что -все порты принадлежатVLAN 1 по умолчанию. В соответствии с исходным заданием дополняем таблицу значениями IDVLAN (Таблица 7.3.)***

Таблица № 7. Конфигурация VLAN коммутатора CISCO 2960.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №пп | Отдел | Компьютер | IP-адрес | № порта коммутатора | IDVLAN |
| 1 | Бухгалтерия (Buh) | ПК-0 | 10.10.12.101 | Fa 0/1 | 121 |
| 2 | ПК-1 | 10.10.12.102 | Fa 0/2 |
| 3 | ПК-2 | 10.10.12.103 | Fa 0/3 |
| 4 | Отдел продаж (Sales) | ПК-3 | 10.10.12.104 | Fa 0/4 | 122 |
| 5 | ПК-4 | 10.10.12.105 | Fa 0/5 |
| 6 | ПК-5 | 10.10.12.106 | Fa 0/6 |
| 7 | Отдел маркетинга (Market) | ПК-6 | 10.10.12.107 | Fa 0/7 | 123 |
| 8 | ПК-7 | 10.10.12.108 | Fa 0/8 |
| 9 | ПК-8 | 10.10.12.109 | Fa 0/9 |
| 10 | Server | 10.10.12.110 | Fa 0/10 |

1. ***Сконфигурируем порты коммутатора в соответствии с Таблицей №7.3.***

Порты в коммутаторах Cisco назначаются одной из сетей VLAN. Такие порты обеспе­чивают соединение для конечных компьютеров пользователей или узловых устройств, таких, как маршрутизатор и сервер, и называются *портами доступа к сети (access ports).* Стандартно все устройства назначаются сети VLAN 1, которая называется *стандартной сетью VLAN (default VLAN).* После создания VLAN-сети можно вручную назначить ей порт, который сможет обмениваться данными только с другими устройствами в ней, используя пару команд:

**switchport mode access** и **switchport access vlan №**

Ниже описаны необходимые действия по конфигурированию портов коммутатора для включения в состав определенной VLAN-сети.

***Выбираем порт или диапазон портов***

***Switch(config)#int range fa0/1-3 (В данном случае выбран диапазон портов для VLAN ‘”buh”)***

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

***Switch(config-if-range)#switchport access vlan 121***

***Switch(config-if-range)#end***

***Switch#***

Выполним дальнейшую конфигурацию для остальных портов; команды CLI отобразить в отчете виде Screen Shot’s

1. С помощью команды Switch#show vlan brief из глобального режима посмотрим конфигурацию vlan. Проанализируем результат и зафиксируем в отчете ввиде Screen Shot’s и анализа. (Сравните Риссунок 7.7 и Рисунок 7.8)

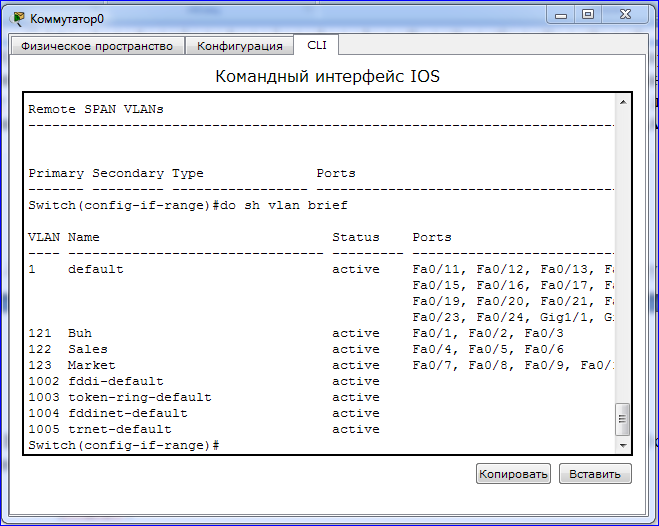
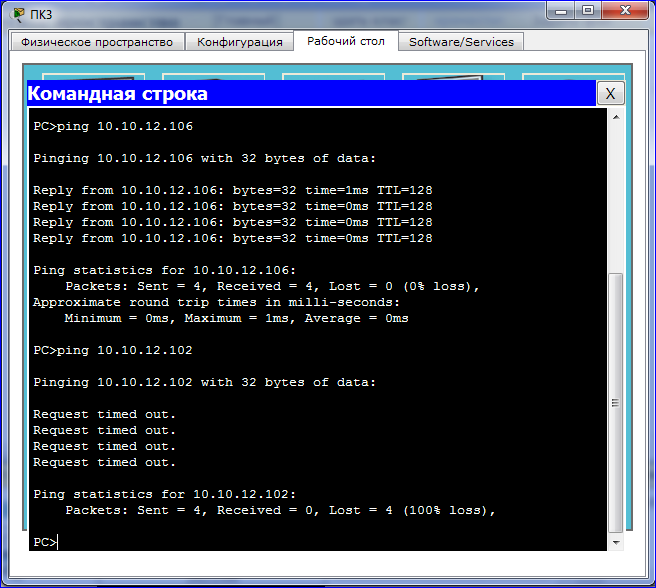


Рисунок 7.8. Состояние VLAN's после «привязки» портов.

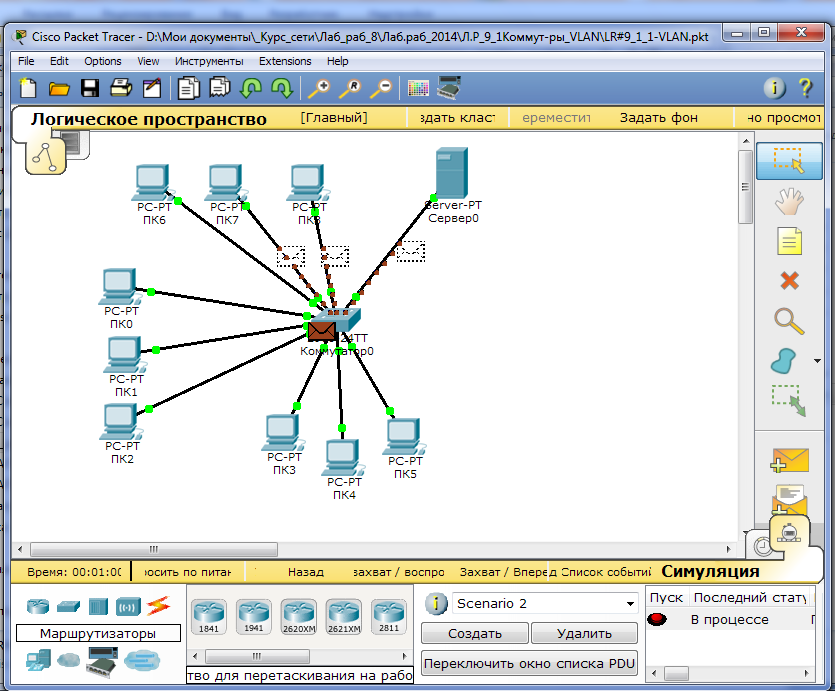
1. С помощью команды ping проверим «связанность» и доступность компьютеров в одной Vlan и в разных, результат представить виде Screen Shot's.

Рис.7.9 Проверка доступности компьютеров в одной VLAN и в разных.



1. ***Сформируем и пошлем широковещательный пакет например, в сети “Market”.***

Рис. 7.10. Продвижение широковещательного трафика в пределах одной VLAN.



В режиме симуляции воспроизвести продвижение широковещательного пакета, просмотреть «Информацию PDU на устройствах: коммутатор, компьютер», проанализируйте: результат анализа и Screen shot's сохраните в отчете.

1. В результате создания vlan's и их конфигурации, получены три изолированные локальные сети. Как правило в таких сетях IP адреса назначаются из разных подсетей. Часто придерживаются следующего правила – один из октедов IP адреса назначают равным или визуально похожим на IDVLAN. Выполним данную рекомендацию:

* ***Адресное пространство подсети «Бухгалтерия» установим второй октед IP адреса равным IDVLAN =NN\*10+1, таким образом IP адреса для VLAN “buh” , будут иметь значения: (10. VLAN\_1.12.XX):10.121.12.XX;***
* ***Адресное пространство подсети «*Отдел продаж (Sales)» *,будет равным, (10. VLAN\_2.12.XX): т.е.: 10.122.12.XX***
* ***Адресное пространство подсети « Отдел маркетинга (Market)», также поменяем второй октед: (10. VLAN\_3.12.XX): 10.123.12.XX;***

При необходимости соединить три независимые VLAN's в одну сеть можно используя сетевое устройство третьего уровня: более мощный коммутатор с функциями третьего уровня или маршрутизатор. В этом случае преимущества сетей с VLAN сохраняются: уменьшаются широковещательные домены до масштабов VLAN's, гибкое разделение хостов на функциональные группы, независимо от местоположения, более высокое обеспечение безопасности и управляемости сети.

13. Сохранить файл для отчета LR\_7-VLAN-1\_FIO.pkt;

**Контрольные вопросы*:***

1. Назовите и кратко объясните основные алгоритмы коммутаторов Ethernet.
2. Что такое «широковещательный шторм» и в каких ситуациях он возникает?
3. Что представляют собой виртуальная локальная сеть VLAN?
4. Назначение, функции и преимущества сетей VLAN?
5. Рассказать подробно создание виртуальных сетей на базе одного коммутатора.
6. Показать на примере конфигурацию VLAN на базе портов одного коммутатора!
7. Распространение широковещательного трафика до назначения VLAN и после, продемонстрировать!
8. Рассказать подробно создание виртуальных сетей на базе двух и более коммутаторов с группированием портов без тегирования. Недостаток этого метода.
9. Что означает тегирование Ethernet кадров и для сего это необходимо? Поля кадра с тегом VLAN, обозначение, назначение и краткое описание каждого поля стандарта IEEE 802.1Q.
10. Как обозначаются в терминологии Cisco тегированные порты и нетегированные порты?
11. Какие два подхода существуют при назначении в определённый VLAN?
12. Что такое агрегирование каналов? Название терминология Cisco для агрегированных и тегированных портов?
13. Что означает параллельные и не параллельные каналы при агрегировании портов?
14. Как распределяется передача кадров одного сеанса связи при агрегировании портов?
15. Какие преимущества предоставляет агрегирование портов?
16. Что такое статический trunkи для чего применяется его настройка в лабораторной работе?
17. Что такое IOS, CLI? Какие режимы поддерживаются в CLI? Какие основные команды Вы знаете?
18. Как «поднять» порт маршрутизатора?
19. Продемонстрировать команды Cisco (CLI) для тегированных и агрегированных портов!
20. Как осуществляется контроль за широковещательным трафиком в сетях VLAN?
21. Дайте определение VTP, какие функции он выполняет?
22. Для чего в коммутаторах используется режим transparent?
23. Что представляет собой interface на маршрутизаторе CISCO, какие бывают интерфейсы и sub-interface.
24. Для чего нужна маршрутизация в случае применения VLAN?
25. Привести примеры команд для настройки функции маршрутизации коммутатора Cisco 3560-24?
26. Как называется коммутатор с функциями маршрутизации?
27. Как дополнительно настраиваются хосты – компьютеры для обеспечения возможности доступа к компьютерам других VLAN?
28. Так что же дает нам применение VLAN?

Практически показать смоделированную сеть и подробно рассказать о конфигурации любого узла сети.

Изучение виртуальных локальных сетей (VLAN). Конфигурирование VLAN на одном коммутаторе