

---

# ЛАБОРАТОРНАЯ РАБОТА № 3 ИЗУЧЕНИЕ ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ СЕТЕЙ (VLAN). КОНФИГУРИРОВАНИЕ С ПОМОЩЬЮ ПРОГРАММЫ – PACKET TRACER.

**Цель работы:** Ознакомиться с принципами работы виртуальных сетей VLAN при помощи эмулятора CISCO Packet Tracer.

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

## 1. ОСНОВНЫЕ СВЕДЕНИЯ

CISCO Packet Tracer - это визуальное моделирование сетей на основе оборудования CISCO: маршрутизаторов (1841, 2620XM, 2621XM, 2811), коммутаторов (2950-24, 2950T, 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), модемного Dial-up соединения, 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).

## 2. 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 присоединенных к нему сетей путем анализа MAC-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, CAM).** Каждый раз, при занесении адреса в таблицу коммутации, ему присваивается 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 MAC-адрес приемника и ищет этот MAC-адрес в своей таблице коммутации. Если в таблице есть запись, ассоциирующая MAC-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 (Switch'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 сегодня, 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 802.1x 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 (устройства 2-го уровня модели OSI), 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 образует 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 последствий, которые могут развиваться 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.

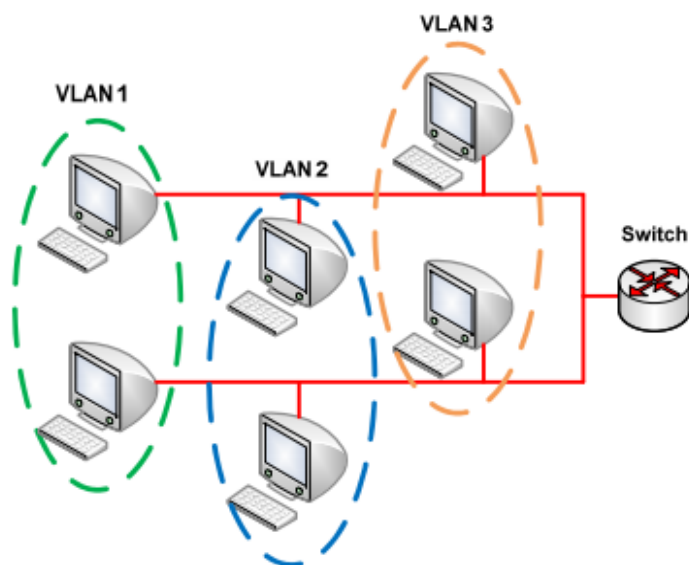


Рис. 3.1. Пример организации виртуальных сетей

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;

### 3. 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 или 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 характеристики 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, присвоить 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 коммутаторами, 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.

### 3.1 ПРАКТИЧЕСКОЕ ВЫПОЛНЕНИЕ:

#### 3.1.1 СОЗДАДИМ В PAKET TRACER МОДЕЛЬ СЕТИ СОГЛАСНО РИС 3.1

1. Для создания сети используем коммутатор cisco 2960-24PT, девять компьютеров PC-PT, один сервер Server-PT.
2. Первые три PC-PT (ПК-0-ПК-2) будем считать как hosts бухгалтерии –“buh”, следующие три компьютера (ПК-3-ПК-5) – компьютеры отдела продаж- “Sales”, остальные компьютеры и сервер отнесем к отделу маркетинг –“Market”.
3. Присвоим 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 второй группы)
4. Данные компьютеры соединить с портами коммутатора согласно таблицы, приведённой ниже: **(в отчёте создать аналогичную таблицу с конкретными данными согласно вариантам)**

ТАБЛИЦА № 3. 1 ПЕРВОНАЧАЛЬНАЯ КОНФИГУГАЦИЯ СЕТИ LAN.

№пп	Отдел	Компьютер	IP-адрес	№ порта коммутатора
1	Бухгалтерия (Buh)	ПК-0	10.10.12.101	Fa 0/1
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
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
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

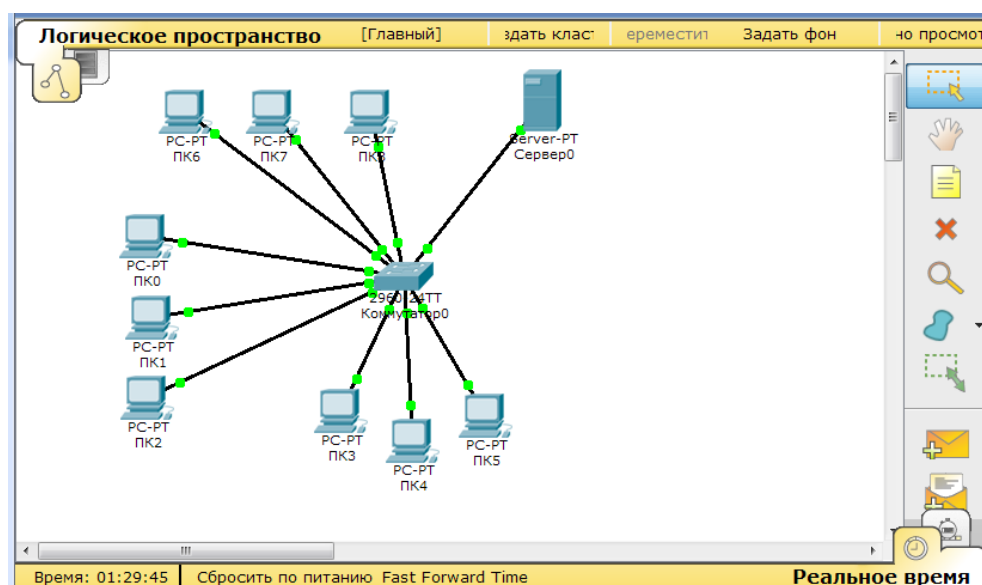


Рис 3.2. Топология сети с одним коммутатором.

Маска на каждом из компьютеров должна соответствовать 255.255.255.0

5. Проверим прохождение пакетов каждого из компьютеров к серверу и междусобой. Результат зафиксируем в отчете.

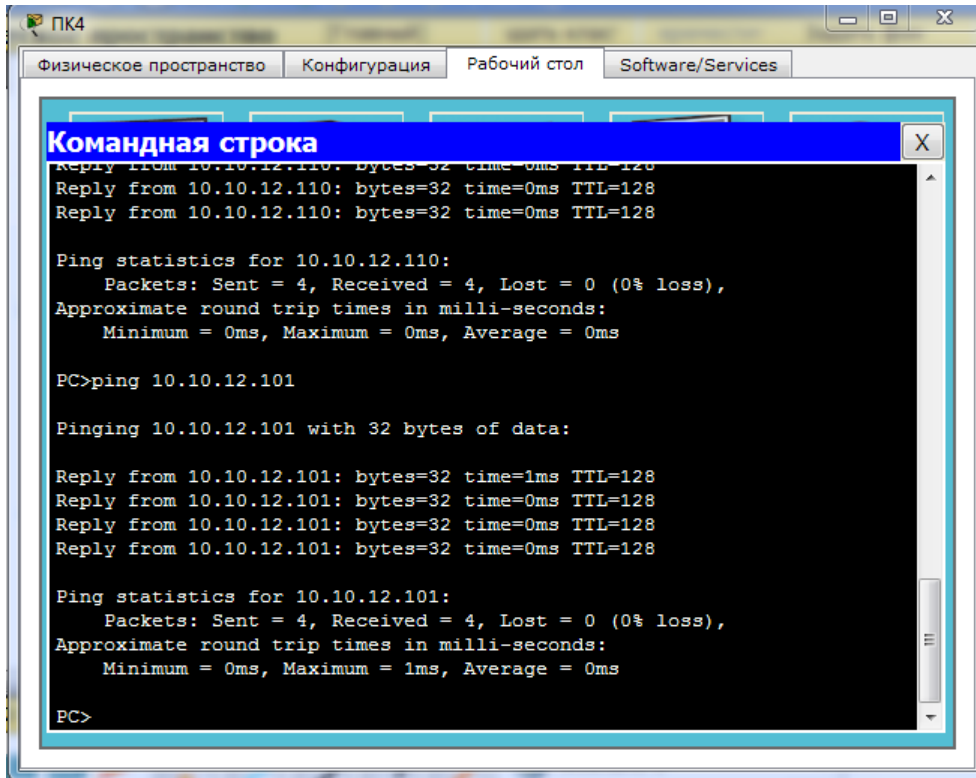



Рис 3.3. Прохождение тестовых пакетов между ПК-4, Server и ПК-4 и ПК-0.

6. Данная сеть является сетью одного адресного пространства IP адресов и одного широковещательного 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 Рис.3.4. в соответствии со своими вариантами, нажимаем кнопку создать PDU.

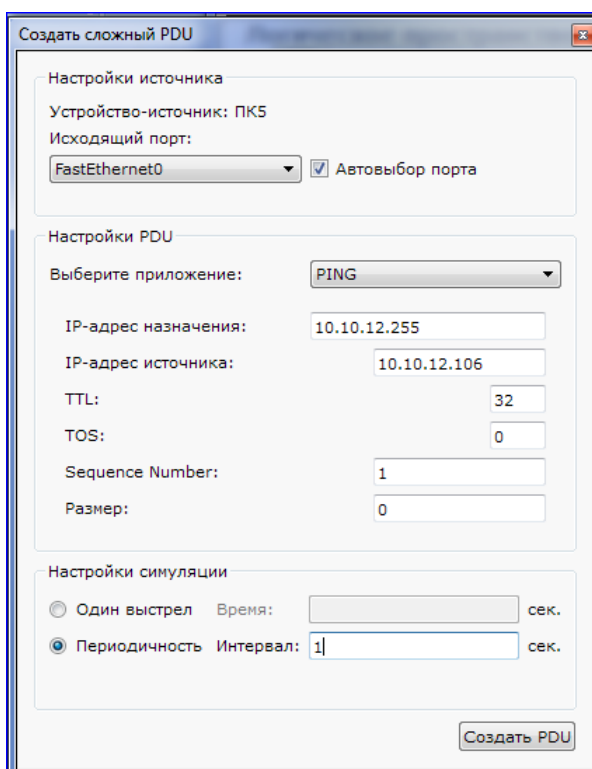


Рис 3.4. Диалоговое окно «Создание комплексного PDU».

IP –адрес назначения и источника заполняется в соответствии с IP –номерами Вашего варианта и используемого компьютера. (В данном случае представлен 12 вариант первой группы и ПК-5). Последний октет 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 Рис 3.5. Проанализируйте его и сделайте Screen Shot's, сохранив в отчете. Обратите внимание на выделенные желтым цветом параметры пакета.

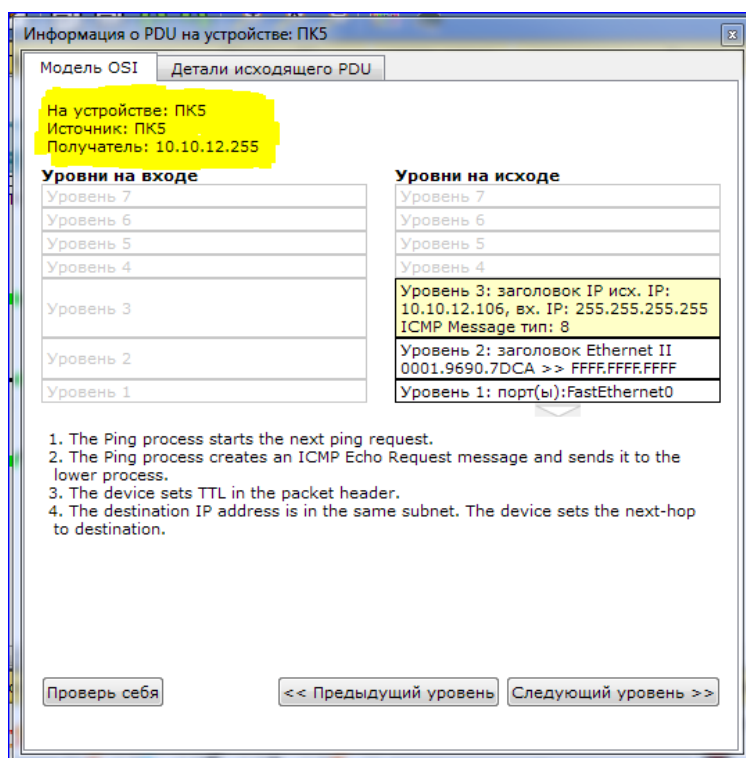


Рис. 3.5. Информационное окно «комплексного PDU»

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

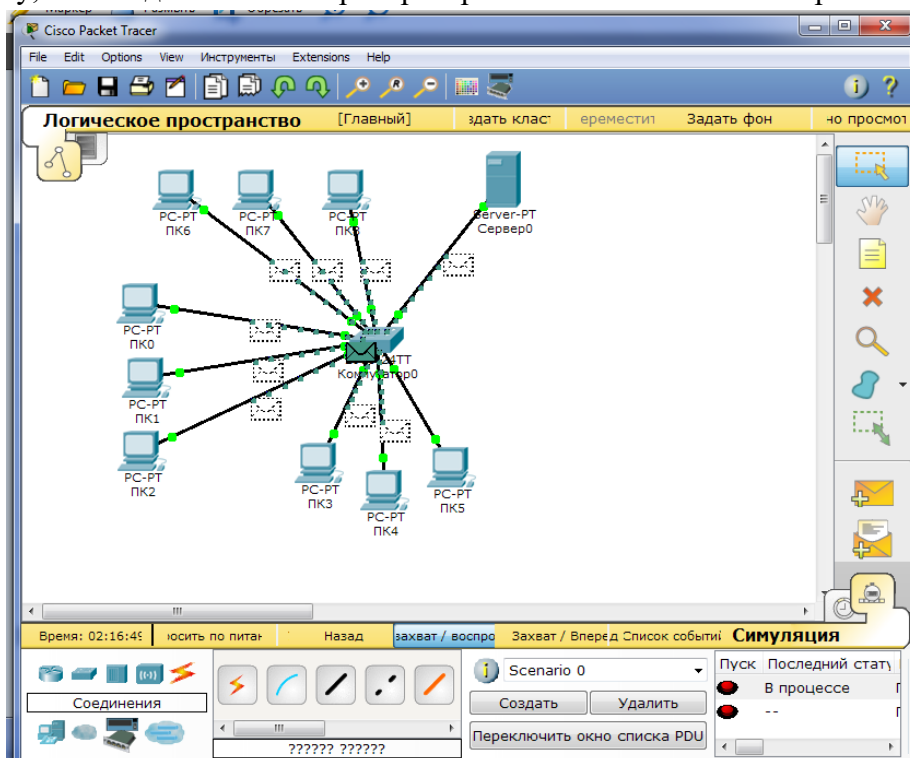


Рис. 3.6. Передача широковещательного пакета/кадра на все задействованные порты коммутатора.

7. Таким образом, данная сеть является сетью с единым широковещательным доменом.
8. Сохранить файл для отчета LR\_9-0-1\_FIO.pkt;
9. Используя возможность конфигурации коммутатора cisco 2960, разделим сеть на три виртуальные локальные сети VLAN.
10. Каждая VLAN имеет свой идентификатор- 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 № 3. 2 ИНДЕНТИФИКАТОРЫ VLAN, ПРИМЕНЯЕМЫЕ В КОММУТАТОРАХ CISCO

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

11. 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 привилегированный режим:

*Switch>enable*

2. Переходим в режим глобального конфигурирования:

*Switch#conf term*

*Switch(config)#*

3. Создаём первую VLAN

**Правило для выбора VLAN:  $IDVLAN = NN * 10 + NumVLAN$ .**

**NN-Ваш порядковый номер по журналу.**

*Switch(config)#vlan 121*

*Switch(config-vlan)#*

4. Аналогично создаем вторую и третью VLAN's

*Switch(config)#vlan 122*

*Switch(config-vlan)#vlan 123*

5. Присвоим имена созданным VLAN's, согласно таблице 3.1., 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*

6. 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:

7. Для перехода в глобальный режим используем дважды команду `exit` и далее

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

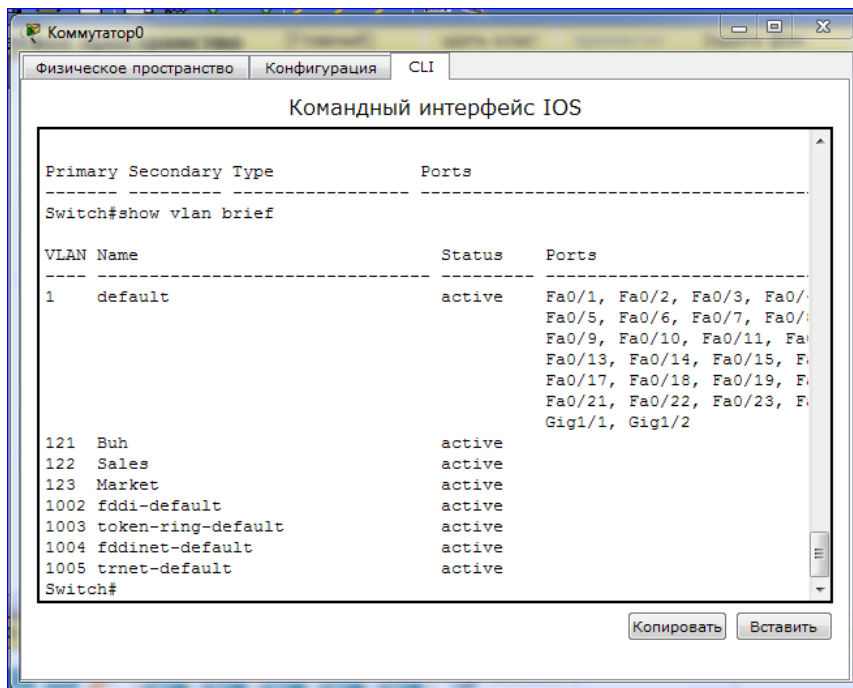


Рис 3.7. Состояние VLAN после первоначальной конфигурации.

8. Следует обратить внимание, что -все порты принадлежат VLAN 1 по умолчанию. В соответствии с исходным заданием дополняем таблицу значениями IDVLAN

ТАБЛИЦА № 3.3 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	

9. Сконфигурируем порты коммутатора в соответствии с Таблицей №3.3.

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*

*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

10. С помощью команды Switch#show vlan brief из глобального режима посмотрим конфигурацию vlan. Проанализируем результат и зафиксируем в отчете в виде Screen Shot's и анализа.

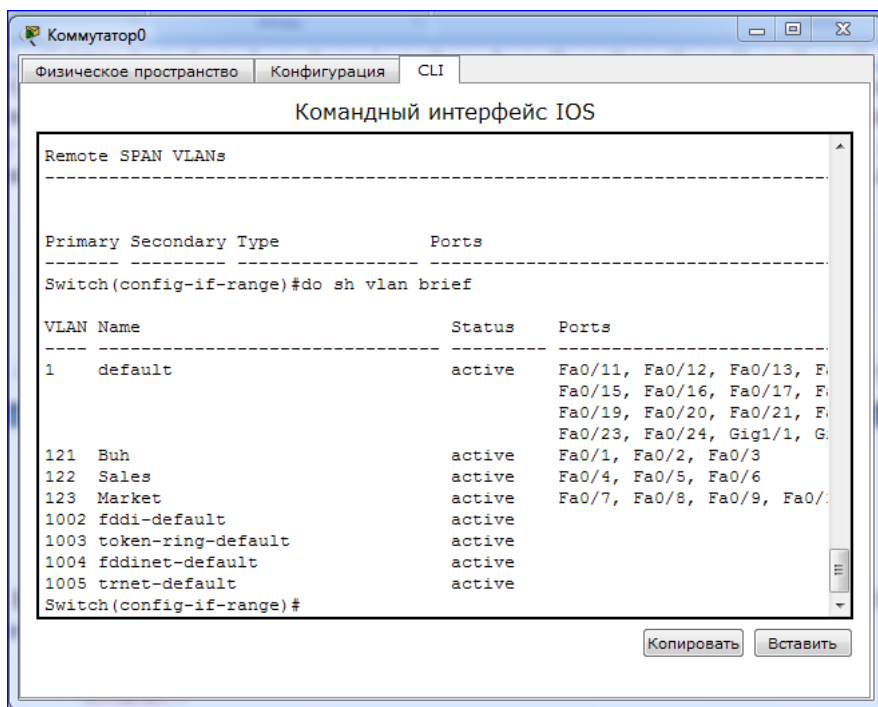


Рис 3.8. Состояние VLAN's после «привязки» портов.

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

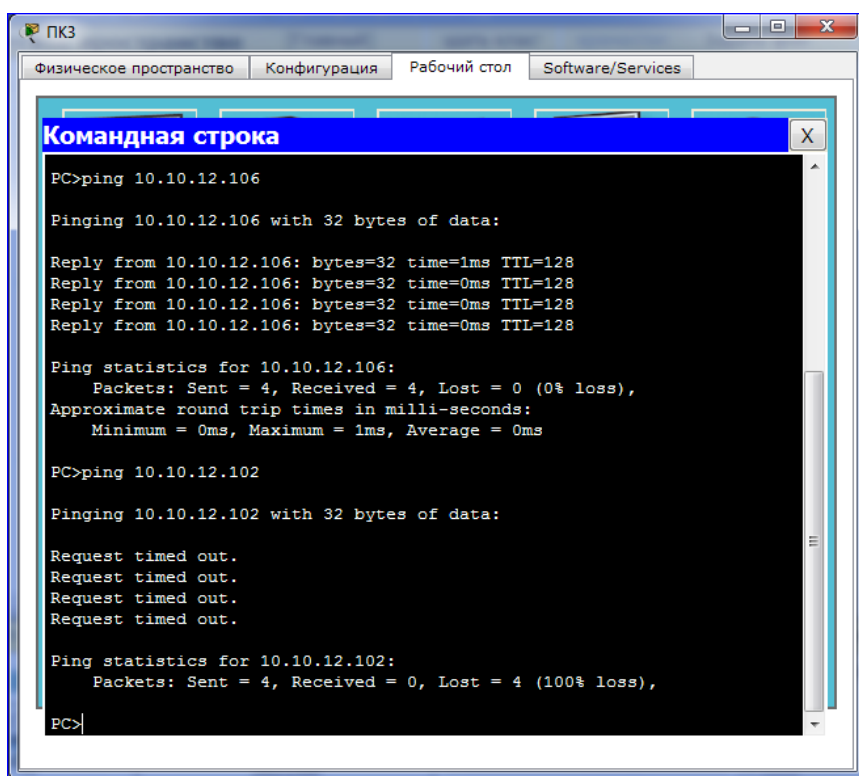


Рис.3.9 Проверка доступности компьютеров в одной VLAN и в разных.

12. Сформируем и пошлем широковещательный пакет например, в сети "Market".

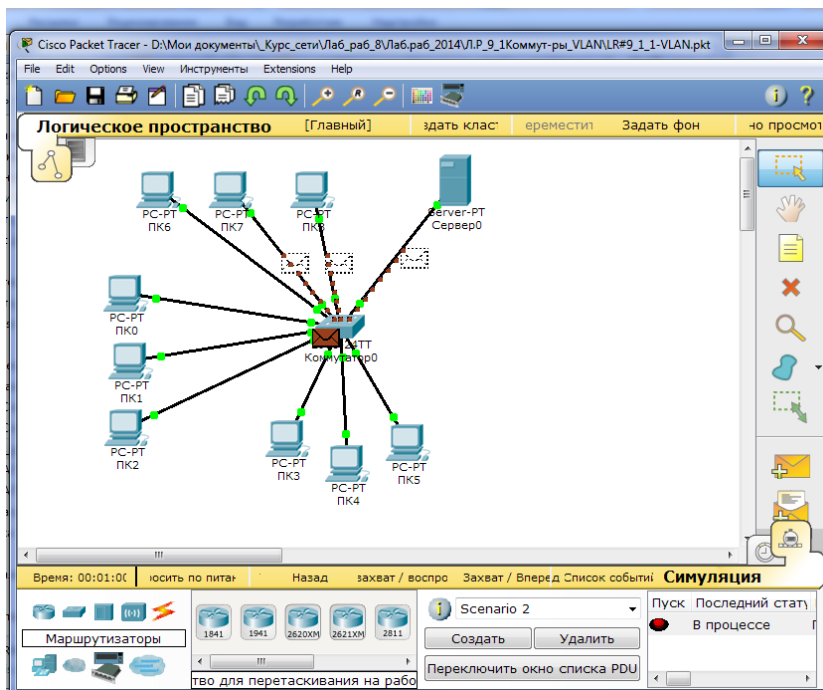


Рис. 3.10. Продвижение широковещательного трафика в пределах одной VLAN.

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

12. 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 октетов IP адреса назначают равным или визуально похожим на IDVLAN. Выполним данную рекомендацию:

- Адресное пространство подсети «**Бухгалтерия**» установим второй октет IP адреса равным  $IDVLAN = NN * 10 + 1$ , таким образом IP адреса для VLAN "бух", 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 октет: (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\_9-0-2\_FIO.pkt;

#### 4. VLAN на базе портов НЕСКОЛЬКИХ КОММУТАТОРОВ.

При построении VLAN's в сети с несколькими коммутаторами возникают определенные особенности. Рассмотрим на примере сеть с двумя коммутаторами. На ниже приведенном Рис.3. для примера два коммутатора SW1 и SW2 и восемь компьютеров включены в две VLAN: VLAN2 и VLAN10. Для того, чтобы хосты А, В, Е, F "увидели" друг друга. Они должны находиться в одном VLAN. То есть, необходимо каким-то образом указать коммутатору, что ещё на одном порту есть хосты в соответствующем VLAN'е. Для указанного примера достаточно добавить на коммутаторе sw1 порт 10 в VLAN 2, а на коммутаторе sw2 порт 9 в VLAN 2. Принадлежность к VLAN указывается настройкой портов (sw1 порт 10 и sw2 порт 9) в VLAN 2 в нетегированном режиме, т.е., с командой **switchport mode access** и далее с привязкой к VLAN **switchport access vlan 1**. После этого на коммутаторах в таблицах коммутации добавятся новые порты и соответствующие MAC-адреса хостов. Теперь четыре хоста на разных коммутаторах находятся в одном широковещательном сегменте.

В случае организации ещё одной VLAN 10 для хостов C, D, G, H приходится задействовать другие пару портов и дополнительно прокладывать линию связи, а это может быть ещё 100м кабеля. Для 10 VLAN's соответственно всё необходимо выполнить для 10-ти пар портов и проложить 10 линий связи. Таким образом данный метод организации VLAN является нерациональным и практически не используется.

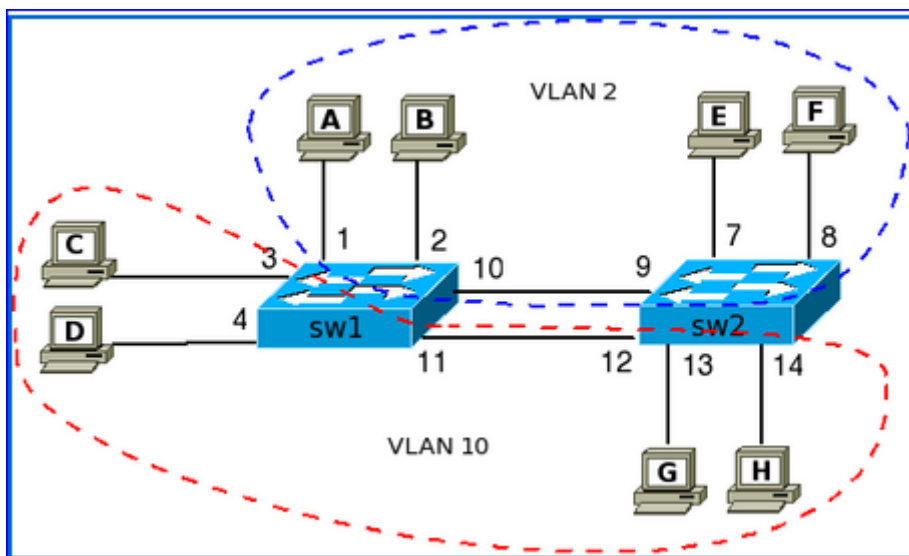


Рис 3.11. Построение виртуальных сетей на нескольких коммутаторах с группированием портов.

Для решения этой проблемы используются тегированные (помеченные) кадры и порты.

Тегированный порт позволяет коммутатору передать трафик нескольких VLAN'ов через один порт и сохранить при этом информацию о том, в пределах какого именно VLAN'a передается фрейм.

На коммутаторах sw1 и sw2 порты 21 и 22, соответственно, это тегированные порты.

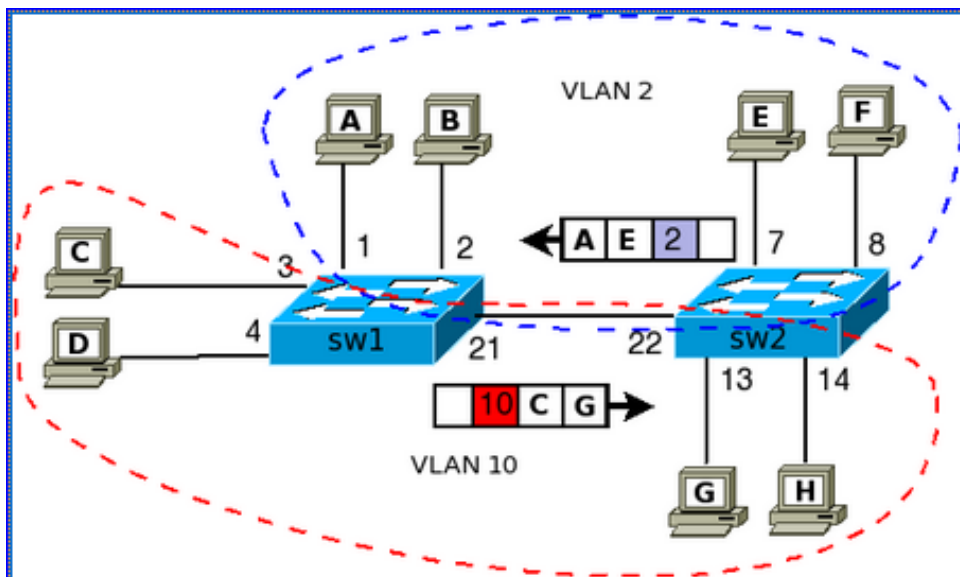


Рис 3.12. Построение виртуальных сетей на нескольких коммутаторах с использованием тегированных фреймов (кадров) и тегированных портов.

Для того, чтобы коммутаторы понимали какому VLAN принадлежит пришедший фрейм и использовали соответствующую таблицу коммутации для его обработки, выполняется тегирование фрейма. Например, если хост E передает фрейм хосту A, то коммутатор sw2 проверяет свою таблицу и видит, что хост A доступен через порт 22. Так как порт настроен как тегированный, то когда фрейм выходит с порта 22 в нём проставляется тег, который указывает какому VLAN'у принадлежит этот фрейм. В данном случае проставляется тег с VLAN'ом 2.

Коммутатор sw1 получает тегированный фрейм через тегированный порт 21. Для того чтобы определить на какой порт его передавать далее sw1 использует таблицу коммутации для VLAN 2 (так как этот VLAN был указан в теге). На коммутаторе sw1 порт 21 должен быть

настроен как тегированный для того чтобы коммутатор не отбрасывал тегированные фреймы, а считывал информацию тега. И соответственно чтобы он также пометал фрейм тегом, когда будет передаваться трафик коммутатору sw2.

Аналогичные действия выполняются, например, при передаче фрейма от хоста С хосту G.

Тегирование фрейма (кадра Ethernet в данном случае) производится путем добавления специального дополнительного поля в заголовок с пометкой о номере виртуальной сети. Дополнительное поле (tag) используется только тогда, когда кадр передается от коммутатора к коммутатору, а при передаче кадра конечному узлу оно обычно удаляется. При этом модифицируется протокол взаимодействия «коммутатор-коммутатор», а программное и аппаратное обеспечение конечных узлов остается неизменным.

С точки зрения удобства и гибкости настроек, VLAN на основе меток является лучшим решением, по сравнению с ранее описанными подходами.

Тегированный фрейм – помеченный кадр Ethernet, согласно стандарта IEEE 802.1Q имеет следующий формат:

<b>6</b>	<b>6</b>	<b>2</b>	<b>46-1500</b>	<b>4</b>
<b>DA</b>	<b>SA</b>	<b>Длина/Тип</b>	<b>Данные</b>	<b>FCS</b>

Рис 3.13. Исходный кадр Ethernet.

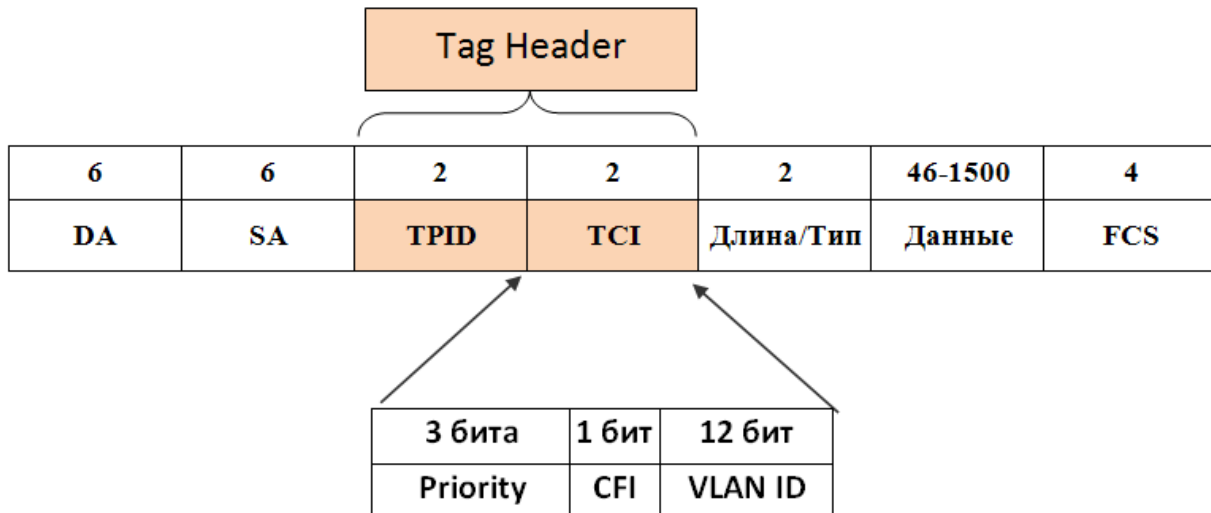


Рис 3.14. Тегированный (маркированный) кадр Ethernet стандарта IEEE 802.1Q.

Длина помеченного кадра Ethernet увеличивается на 4 байта и для кадра с максимальной длиной составит 1522 байта.

**TPID:** TPID –(Tag Protocol Identifier) поле идентификатора протокола тегов. В нем устанавливается значение 0x8100 для идентификации кадра в качестве кадра о принадлежности и с разметкой IEEE 802.1Q.

**TCI:** Tag Control Information - поле, инкапсулирующее в себе поля: *приоритета, канонического формата и идентификатора VLAN*:

- **Priority** — приоритет. Размер поля — 3 бита. Используется стандартом IEEE 802.1p для задания приоритета передаваемого трафика.
- **CFI: Canonical Format Indicator** — Индикатор канонического формата. Однобитовое поле. Если значение этого поля *равно 0*, то MAC-адрес имеет канонический формат и *соответствует кадру Ethernet*. Если значение этого поля *равно 1*, то MAC-адрес имеет неканонический формат (*Кадр Token Ring, FDDI*).
- **VLAN Identifier (VID)** — идентификатор VLAN'а. Размер поля — 12 бит. Указывает, какому VLAN'у принадлежит фрейм. Диапазон возможных значений VID от 0 до 4095. VID = 0 определяет, что данный кадр не несет информации о VLAN, а несет только

информацию о приоритете. VID = 4095 в оборудовании ZyXEL используется для внутренней коммутации (например, в DSLAM).

Существует аналогичный 802.1Q проприетарный протокол Cisco Systems — ISL, разработанный компанией до появления стандарта 802.1Q.

Введение стандарта 802.1Q позволило производителям оборудования преодолеть различия в фирменных реализациях VLAN и добиться совместимости при построении виртуальных локальных сетей. *Поддерживают технику VLAN как производители коммутаторов, так и сетевых адаптеров для серверов.*

Из выше сказанного, следует - порты коммутатора, поддерживающие VLAN'ы, (с некоторыми допущениями) можно разделить на два множества:

- **Тегированные порты** (или транковые порты, **trunk-порты** в терминологии Cisco).
- **Нетегированные порты** (или порты доступа, **access-порты** в терминологии Cisco);

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

Существуют два подхода к назначению порта в определённый VLAN:

- **Статическое назначение** — когда принадлежность порта VLAN'у задаётся администратором в процессе настройки;
- **Динамическое назначение** — когда принадлежность порта VLAN'у определяется в ходе работы коммутатора с помощью процедур, описанных в специальных стандартах, таких, например, как 802.1X.

В данной лабораторной работе рассмотрим статическое назначение.

В Cisco trunk'ом называется не только тегированный порт, но и агрегированный порт, в общем Port Trunking- это магистральный порт между двумя коммутаторами.

**Агрегирование каналов** (link aggregation) — технология, которая позволяет объединить несколько физических каналов в один логический. Такое объединение позволяет увеличивать пропускную способность и надежность канала. Агрегирование каналов может быть настроено между двумя коммутаторами, коммутатором и маршрутизатором, между коммутатором и хостом.

Для агрегирования каналов существуют другие названия:

- **Port Trunking** (в Cisco trunk'ом называется тегированный порт, поэтому с этим термином путаницы больше всего),
- **EtherChannel** (в Cisco так называется агрегирование каналов, это может относиться как к настройке статических агрегированных каналов, так и с использованием протоколов LACP или PAgP)
- И еще множество других: Ethernet trunk, NIC Teaming, Port Channel, Port Teaming

Совокупность физических каналов между двумя устройствами (рис. 3.) может быть заменена одним агрегированным логическим каналом (рис. ), получившим название транк (trunk).



Рис 3.15. Агрегированные линии (link aggregation) и порты Port Trunking.

Агрегирование каналов позволяет решить две задачи:

- повысить пропускную способность канала
- обеспечить резерв на случай выхода из строя одного из каналов

Большинство технологий по агрегированию позволяют объединять только параллельные каналы. То есть такие, которые начинаются на одном и том же устройстве и заканчиваются на другом.



Если рассматривать избыточные соединения между коммутаторами, то без использования специальных технологий для агрегирования каналов, передаваться данные будут только через один интерфейс, который не заблокирован STP. Такой вариант позволяет обеспечить резервирование каналов, но не дает возможности увеличить пропускную способность.

Коммутатор, при получении широковещательного фрейма через обычный интерфейс, отправляет его в агрегированный канал только через один интерфейс. А при получении широковещательного фрейма из агрегированного канала, не отправляет его назад.

Хотя агрегирование каналов позволяет увеличить пропускную способность канала, не стоит рассчитывать на идеальную балансировку нагрузки между интерфейсами в агрегированном канале. Технологии по балансировке нагрузки в агрегированных каналах, как правило, ориентированы на балансировку по таким критериям: MAC-адресам, IP-адресам, портам отправителя или получателя (по одному критерию или их комбинации).

То есть, реальная загруженность конкретного интерфейса никак не учитывается. Поэтому один интерфейс может быть загружен больше, чем другие. Более того, при неправильном выборе метода балансировки (или если недоступны другие методы) или в некоторых топологиях, может сложиться ситуация, когда реально все данные будут передаваться, например, через один интерфейс.

Некоторые проприетарные разработки позволяют агрегировать каналы, которые соединяют разные устройства. Таким образом, резервируется не только канал, но и само устройство. Такие технологии в общем, как правило, называются распределенным агрегированием каналов (у многих производителей есть своё название для этой технологии).

Будем рассматривать в основном агрегирование параллельных каналов.

Для агрегирования каналов в Cisco может быть использован один из трёх вариантов:

- **LACP** (Link Aggregation Control Protocol) стандартный протокол;
- **PAgP** (Port Aggregation Protocol) проприетарный протокол Cisco;
- Статическое агрегирование без использования протоколов.

Рассмотрим выполнение статическое агрегирования.

### Терминология и настройка.

При настройке агрегирования каналов на оборудовании Cisco используется несколько терминов:

- **EtherChannel** — технология агрегирования каналов. Термин, который использует Cisco для агрегирования каналов.
- **port-channel** — логический интерфейс, который объединяет физические интерфейсы.
- **channel-group** — команда, которая указывает какому логическому интерфейсу принадлежит физический интерфейс и какой режим используется для агрегирования.

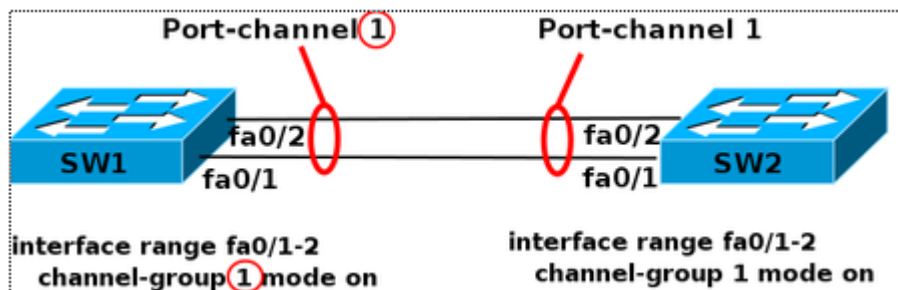


Рис 3.16. Термины и команды при настройке агрегированных линии и портов.

Эти термины используются при настройке, в командах просмотра, независимо от того, какой вариант агрегирования используется (какой протокол, какого уровня EtherChannel).

На схеме, число после команды channel-group указывает какой номер будет у логического интерфейса Port-channel. Номера логических интерфейсов с двух сторон агрегированного канала

не обязательно должны совпадать. Номера используются для того чтобы отличать разные группы портов в пределах одного коммутатора.

#### 4.1 Практическое выполнение: VLAN's, транкинговые порты, агрегация портов:

1. С помощью Packet Tracer создадим сеть, показанную на Рис 3.17

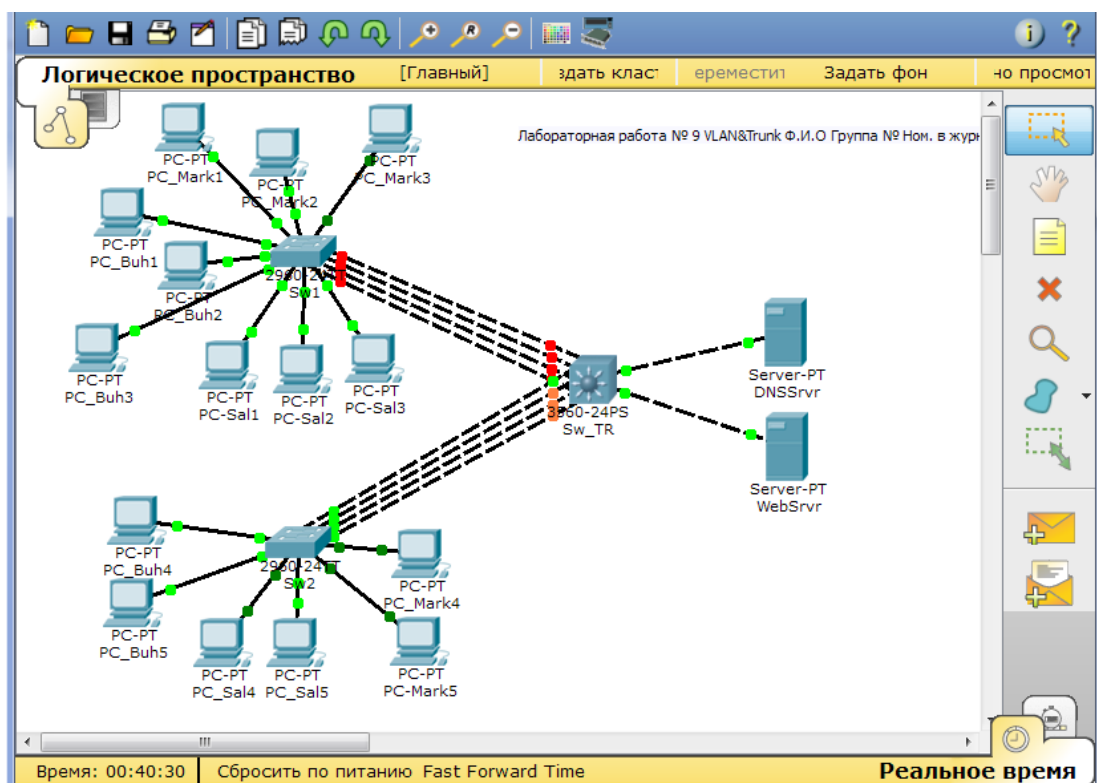


Рис. 3.17 Развернутая сеть с применением VLAN's, многоуровневого коммутатора Sw\_TR, агрегированных и транкиннг каналов.

При выполнении необходимо выполнить следующее:

- Для отчета сохранить ранее выполненную часть работы в отдельном файле, например LR\_9-1\_FIO.pkt;
  - Для дальнейшего выполнения работы, открываем сохраненный файл и вновь сохраняем его под именем LR\_9-2\_FIO.pkt;
  - Добавляем коммутаторы CISCO 2960-24PT и 3560-24PS, в качестве конечных устройств используем компьютеры PC-PT и Servser-PT;
  - На серверах Servser-PT, устанавливаем дополнительные модули «сетевой модуль Gigabit Ethernet Cisco **PT-HOST-NM-1CGE** однопортовый гигабитный медный Ethernet интерфейс. (*установка нового модуля производится при выключении питания!*)
  - Соединяем как показано на Рис 3.17, сохраняем файл; Для подключения серверов к SW-TR выбираем порты Gig0/1 и Gig0/2 на серверах Gig1.
  - Обозначить устройства (имена хостов, коммутаторов) аналогично Рис 3.17
  - Порты для параллельных связей Sw1-Sw-TR и Sw2-Sw\_TR выбирать из непрерывного диапазонов портов, например: порты Sw1 fa0/10-fa0/13 – Sw-TR fa0/1-4.
2. Для хостов PC-Buh4, PC-Buh5, PC-Sal4, PC-Sal5, PC-Mark4, PC-Mark5 назначим IP-адреса в соответствии с правилами раздел-3 п.11., например: PC-Buh4 10.121.12.104;
  3. Для серверов выберем, с учетом будущей VLAN\_5 **IDVLAN = NN\*10+5**, и правила **IP – адрес: 10.125.12.1 и 10.125.12.2**

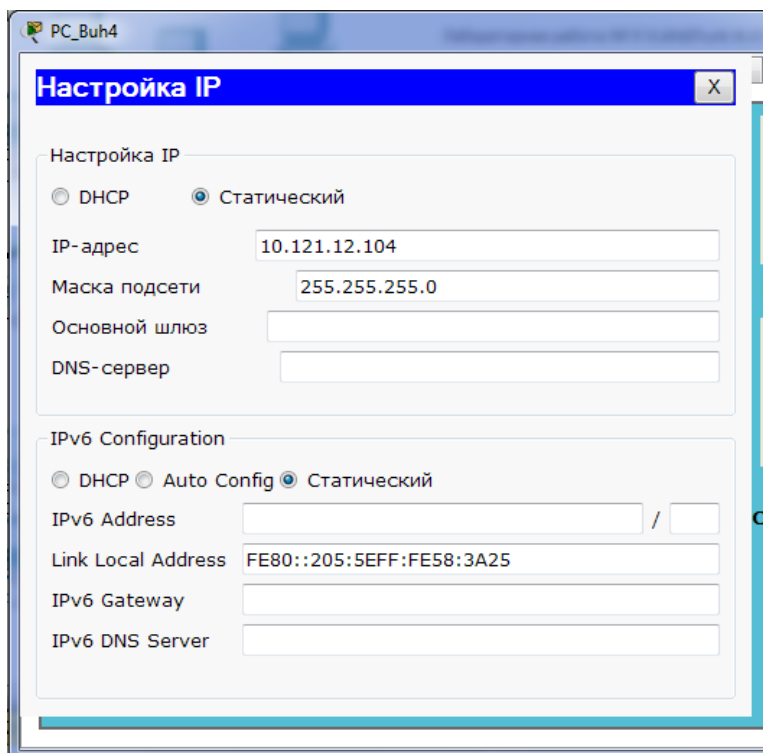


Рис. 3.18. Назначение IP адресов дополнительным компьютерам сети..

4. Сформируем таблицу конфигурации для коммутатора Sw2.

ТАБЛИЦА 3. 4 КОНФИГУРАЦИЯ ПОРТОВ КОММУТАТОРА SW2

№пп	Отдел	Компьютер	IP-адрес	№ порта коммутатора	IDVLAN
1	Бухгалтерия (Buh)	PC_Buh4	10.121.12.104	Fa 0/1	121
2		PC_Buh5	10.121.12.105	Fa 0/2	
3	Отдел продаж (Sales)	PC_Sal4	10.122.12.104	Fa 0/3	122
4		PC_Sal5	10.122.12.105	Fa 0/4	
5	Отдел маркетинга (Market)	PC_Mark4	10.123.12.104	Fa 0/5	123
6		PC_Mark5	10.123.12.105	Fa 0/6	

5. Для коммутатора Sw\_TR конфигурация будет следующей:

№пп	Отдел	Компьютер	IP-адрес	№ порта коммутатора	IDVLAN
1	Сервера	DNSSrvr	10.125.12.1	Gig 0/1	125
2		WebSrvr	10.125.12.2	Gig 0/2	

6. Аналогично создайте таблицу и для коммутатора Sw1. Таблицы представьте в отчете.

7. На коммутаторах SW2 и Sw-TR создадим Vlan's согласно выше представленным таблицам: Рис 3.13.

8. Прописываем порты Sw2 и Sw\_TR к созданным VLAN's, используя как и ранее команды **switchport mode access** и **switchport access vlan №**

*Sw2>enable*

*Sw2#conf t*

*Enter configuration commands, one per line. End with CNTL/Z.*

*Sw2(config)#no ip domain lookup*

*Sw2(config)#int range fa0/1-2*

```

Sw2(config-if-range)#switchport mode access
Sw2(config-if-range)#switchport access vlan 121
Sw2(config-if-range)#end
Sw2#

```

Аналогично конфигурируем порты Sw2 и для остальных VLAN's 122 и 123.

Для Sw3:

```

Sw_TR(config-if-range)#exit
Sw_TR(config)#vlan 125
Sw_TR(config-vlan)#name Srvr's
Sw_TR(config-vlan)#exit
Sw_TR(config)#int range Gig0/1-2
Sw_TR(config-if-range)#switchport mode access
Sw_TR(config-if-range)#switchport access vlan 125
Sw_TR(config-if-range)#end

```

9. Используя команды *Switch(config)#show vlan brief* или *sh vlan brief* из глобального режима посмотрим результаты конфигурации, зафиксируем в отчете.

```

Sw2 (config)#vlan 121,122,123
^
% Invalid input detected at '^' marker.

Sw2 (config)#vlan 121
Sw2 (config-vlan)#exit
Sw2 (config)#vlan 122
Sw2 (config-vlan)#exit
Sw2 (config)#vlan 123
Sw2 (config-vlan)#exit
Sw2 (config)#vlan 121 name Buh
^
% Invalid input detected at '^' marker.

Sw2 (config)#vlan 121
Sw2 (config-vlan)#name Buh
Sw2 (config-vlan)#exit
Sw2 (config)#vlan 122
Sw2 (config-vlan)#name Sales
Sw2 (config-vlan)#exit
Sw2 (config)#vlan 123
Sw2 (config-vlan)#name Market
Sw2 (config-vlan)#

```

Рис 3.13. Создание VLAN's в коммутаторе Sw2

10. Сконфигурируем параллельные порты Sw-TR, объединив их в логические порты с помощью функций агрегации:

```

Sw_TR>enable
Sw_TR#conf term
Sw_TR(config)#int range fa0/1-4
Sw_TR(config-if-range)#shutdown

```

```

Sw_TR(config-if-range)#channel-group 1 mode on
Sw_TR(config-if-range)#
Creating a port-channel interface Port-channel 1

%LINK-5-CHANGED: Interface Port-channel 1, changed state to up

Sw_TR(config-if-range)#exit
Sw_TR(config)#int range fa0/5-8
Sw_TR(config-if-range)#shutdown

```

```
Sw_TR(config-if-range)#channel-group 2 mode on
Sw_TR(config-if-range)#
Creating a port-channel interface Port-channel 2
```

11. Аналогично сконфигурируем порты на коммутаторах SW1 и SW2:

```
Sw1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Sw1(config)#int range fa0/10-13
Sw1(config-if-range)#channel-group 1 mode on
Sw1(config-if-range)#
%LINK-5-CHANGED: Interface Port-channel 1, changed state to up
```

12. Проверяем результат с помощью команды *sh etherchannel summary*

```
Sw2(config-if-range)#exit
Sw2(config)#exit
Sw2#
%SYS-5-CONFIG_I: Configured from console by console

Sw2#sh etherchannel summary
Flags:  D - down          P - in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
2      Po2 (SU)        -           Fa0/7 (D) Fa0/8 (D) Fa0/9 (D) Fa0/10 (D)
Sw2#
```

Рис. 3.20 Просмотр результата агрегации 4-х каналов на Sw2.

13. Сконфигурируем агрегируемые порты коммутатора Sw\_TR как тегированные. В терминологии CISCO такие порты также называются trunk, но в данном случае они несут дополнительную функцию: формируют и продвигают тегированные кадры между коммутаторами, принадлежащие разным VLAN's, направляя их на соответствующие access порты.

14. С помощью команды *vlan* добавим VLAN's 121-123 в базу данных коммутатора SW\_TR:

```
Sw_TR#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Sw_TR(config)#vlan 121
Sw_TR(config-vlan)#exit
Sw_TR(config)#vlan 122
Sw_TR(config-vlan)#name Sales
Sw_TR(config-vlan)#exit
Sw_TR(config)#vlan 123
Sw_TR(config-vlan)#name Market
Sw_TR(config-vlan)#exit
Sw_TR(config)#vlan 121
Sw_TR(config-vlan)#name Buh
Sw_TR(config-vlan)#exit
Sw_TR(config)#exit
Sw_TR#
```

15. Создадим статический транк сначала на коммутаторе Sw\_TR для двух агрегированных портов:

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



```
Sw_TR(config)#int Po1
```

```
Sw_TR(config-if)#switchport trunk encapsulation dot1q
```

Команда *switchport trunk encapsulation dot1q* позволяет коммутатору использовать формат тегированного кадра стандарта IEEE 802.1Q.

```
Sw_TR(config-if)#switchport mode trunk
```

Также необходимо указать перечень разрешенных VLAN для транкового порта

```
Sw_TR(config-if)#switchport trunk allowed vlan 121-123
```

```
Sw_TR(config-if)#exit
```

```
Sw_TR(config)#int range fa0/5-8
```

```
Sw_TR(config-if-range)#no shutdown
```

```
Sw_TR(config-if)#exit
```

```
Sw_TR(config)#int range fa0/1-4
```

```
Sw_TR(config-if-range)#no shutdown
```

Аналогично создадим trunk для второго агрегированного порта.

16. Проверяем наши настройки с помощью команды: `show interface trunk`

```
Sw_TR>enable
Sw_TR#show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Po1       on        802.1q         trunking    1
Po2       on        802.1q         trunking    1

Port      Vlans allowed on trunk
Po1       121-123
Po2       121-123

Port      Vlans allowed and active in management domain
Po1       121,122,123
Po2       121,122,123

Port      Vlans in spanning tree forwarding state and not pruned
Po1       121,122,123
Po2       121,122,123
Sw_TR#
```

Рис. 3.21 Результат настройки тегированных портов (trunk) на SW\_TR.

17. Сконфигурируем агрегированные порты на коммутаторах Sw1 и Sw2 как тегированные (транк) порты, применяя аналогичные команды

```
Sw2#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
Sw2(config)#int Po2
Sw2(config-if)#switchport mode trunk

Sw2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel 2,
down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel 2,
up

Sw2(config-if)#switchport trunk allowed vlan 121-123
Sw2(config-if)#
Sw2(config)#int range fa0/7-10
Sw2(config-if-range)#no shutdown
```

Не забывайте поднять физические порты командой *no shutdown*.

## 4.2 Настройка маршрутизации между VLAN

Все настройки по назначению портов в VLAN, сделанные ранее для Sw1, Sw2 и SW\_TR, сохраняются. Дальнейшие настройки подразумевают использование Sw\_TR как коммутатора 3 уровня. При такой схеме маршрутизатор не требуется. Коммутатор осуществляет маршрутизацию между сетями разных VLAN. На практике устанавливается маршрутизатор для перенаправления трафика предназначенного во внешние сети, например Интернет.

При настройке будем учитывать, что имеется четыре виртуальные локальные сети VLAN 121, VLAN 122, VLAN 123 и VLAN 125.

	VLAN/интерфейс 3го уровня	IP-адрес сети	IP- адрес интерфейса
1	121 (Buh)	10.121.12.0/24	10.121.12.1
2	122 (Sales)	10.122.12.0/24	10.122.12.1
3	123 (Market)	10.123.12.0/24	10.123.12.1
4	125 (Server's)	10.125.12.0/24	10.125.12.1

1. Включение маршрутизации на коммутаторе SW\_TR производится командой:  
***Sw\_TR(config)# ip routing.***
2. Далее создаются виртуальные интерфейсы для каждой VLAN:  
***Sw\_TR(config)#interface Vlan 121***
3. Созданному интерфейсу назначается IP-адрес в сети VLAN, где уже включены хосты.  
***Sw\_TR(config-if)#ip address 10.121.12.1 255.255.255.0***

Листинг дальнейших команд Sw\_TR представлен на Рисунке 3.22.

```
Sw_TR#conf term
Enter configuration commands, one per line. End with CNTL/Z.
Sw_TR(config)#ip routing
Sw_TR(config)#interface Vlan 121
Sw_TR(config-if)#
%LINK-5-CHANGED: Interface Vlan121, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan121, changed state to

Sw_TR(config-if)#ip address 10.121.12.1 255.255.255.0
Sw_TR(config-if)#exit
Sw_TR(config)#interface Vlan 122
Sw_TR(config-if)#
%LINK-5-CHANGED: Interface Vlan122, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan122, changed state to

Sw_TR(config-if)#ip address 10.122.12.1 255.255.255.0
Sw_TR(config-if)#exit
Sw_TR(config)#interface Vlan 123
Sw_TR(config-if)#
%LINK-5-CHANGED: Interface Vlan123, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan123, changed state to

Sw_TR(config-if)#ip address 10.123.12.1 255.255.255.0
Sw_TR(config-if)#exit
Sw_TR(config)#interface Vlan 125
Sw_TR(config-if)#
%LINK-5-CHANGED: Interface Vlan125, changed state to up
```

Рис 3.22 Создание виртуальных интерфейсов и назначение IP-адресов коммутатора Sw\_TR

4. Выполнение данной конфигурации коммутатора SW\_TR позволит осуществлять коммутацию кадров (frame's) Ethernet (канальный уровень OSI) и одновременно статическую маршрутизацию пакетов сетевого уровня – IP пакетов. Сетевое

устройство **SW\_TR** в данном случае является не только коммутатором, но и маршрутизатором – **шлюзом всей сети**.

5. Для обеспечения прохождения трафика между конечными устройствами разных подсетей необходимо на каждом компьютере установить IP адрес «Основной шлюз» («Рабочий стол-> Настройка IP») IP адрес виртуального интерфейса SW\_TR для данной VLAN сети, например в данном случае для VLAN -12 “Buh” -> **10.121.12.1**.

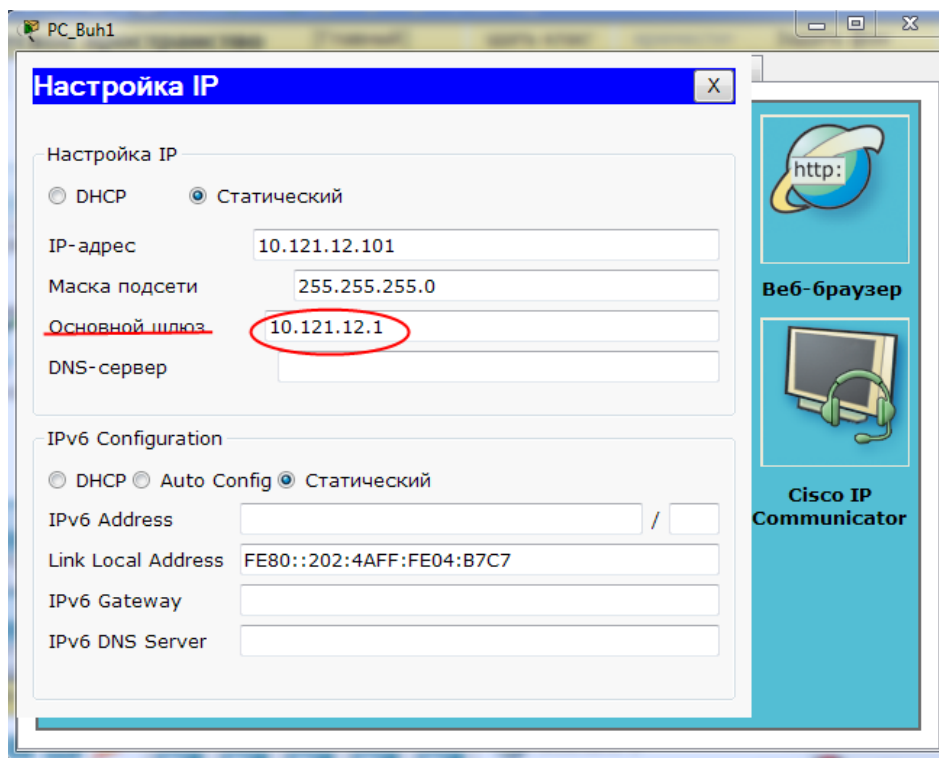


Рис 3.23.Дополнительная конфигурация компьютера PC-Buh1.

6. После дополнительной конфигурации всех компьютеров, в том числе и серверов, проверяем возможность прохождения сигналов с одной VLAN на другую, в частности с VLAN 121-123 на VLAN 125 (Server) с помощью команды ping. В отчете представить Screen Shot's.

### 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 trunk и 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.