**Практическая работа 9**

**Виртуальные локальные сети VLAN.**

VLAN (аббр. от англ. Virtual Local Area Network) — логическая («виртуальная») локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети.

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

Преимущества:

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

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

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

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

5 - Предотвращение широковещательных штормов и предотвращение петель.

**Задание 1. Настройка VLAN на одном коммутаторе Cisco.**

В данном задании рассматривается настройка VLAN на коммутаторе фирмы Сisco на его портах доступа. Создайте сеть, логическая топология которой представлена на рис. 1. Компьютеры соединены коммутатором Cisco 2960-24ТТ. В таблице 1 приведены адреса компьютеров.

Задача данной работы – сделать две независимые группы компьютеров: ПК0, ПК1 и ПК2 должны быть доступны только друг для друга, вторая независимая группа - компьютеры ПК3 и ПК4. Для этого создадим два отдельных VLAN (рис.1)

VLAN 3

VLAN 2

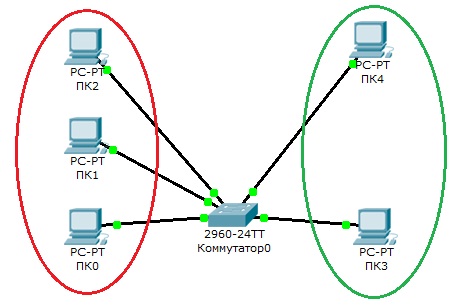


Рис. 1. Схема сети с одним коммутатором.

Таблица 1.

|  |  |  |
| --- | --- | --- |
| Компьютер | IP адрес | Порт коммутатора |
| ПК0 | 10.0.0.1/8 | 1 |
| ПК1 | 10.0.0.2/8 | 2 |
| ПК2 | 10.0.0.3/8 | 3 |
| ПК3 | 10.0.0.4/8 | 4 |
| ПК4 | 10.0.0.5/8 | 5 |

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

Для проверки конфигурации хоста ПК0 выполним команду ipconfig. Результат выполнения команды на рисунке 2. При желании можно выполнить аналогичную проверку на остальных хостах.

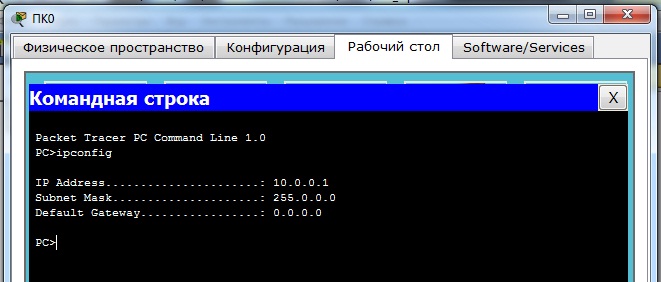


Рис. 2. Проверка конфигурации хоста

Используя команду PING проверим связь между всеми компьютерами. Сейчас они в одной сети и все доступны друг для друга

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

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

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

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

Switch>**en**

Switch#

Просмотрим информацию о существующих на коммутаторе VLAN-ах (рис. 3). Для этого выполним следующую команду:

Switch#**sh vl br**

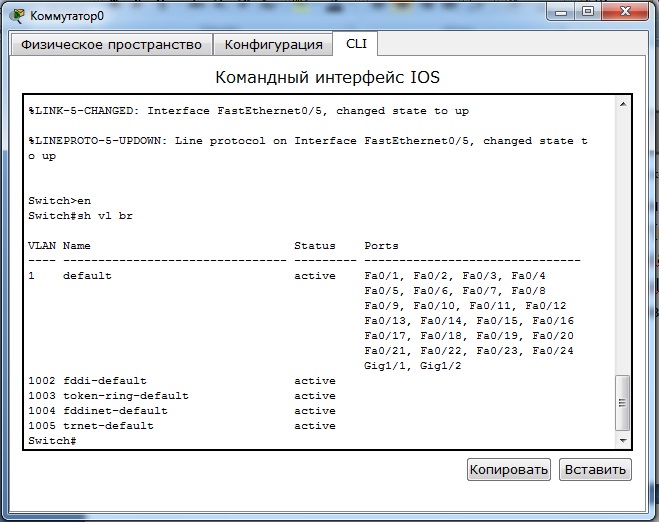


Рис. 3. Просмотр информации о VLAN на коммутаторе.

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

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

Switch#**conf t**

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

Switch(config)#

для перехода в режим конфигурации. Вводим команду VLAN 2. Данной командой вы создадите на коммутаторе VLAN с номером 2. Указатель ввода Switch(config)# изменится на Switch(config-vlan)# это свидетельствует о том, что вы конфигурируете уже не весь коммутатор в целом, а только отдельный VLAN, в данном случае VLAN номер 2. Если вы используете команду «vlan x», где x номер VLAN, когда VLAN x еще не создан на коммутаторе, то он будет автоматически создан и вы перейдете к его конфигурированию. Когда вы находитесь в режиме конфигурирования VLAN, возможно изменение параметров выбранной виртуальной сети, например можно изменить ее имя с помощью команды name.

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

Switch(config)#**vlan 2**

Switch(config-vlan)#**name subnet\_10**

Switch(config)#**interface range fastEthernet 0/1-3**

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

Switch(config-if-range)#**switchport access vlan 2**

Разберем данную конфигурацию. Как уже говорилось ранее командой VLAN 2, мы создаем на коммутаторе новый VLAN с номером 2. Команда **name subnet\_10** присваивает имя subnet\_10 виртуальной сети номер 2. Выполняя команду **interface range fastEthernet 0/1-3** мы переходим к конфигурированию интерфейсов fastEthernet0/1, fastEthernet0/2 и fastEthernet0/3 коммутатора. Ключевое слово **range** в данной команде, указывает на то, что мы будем конфигурировать не один единственный порт, а целый диапазон портов, в принципе ее можно не использовать, но тогда последние три строки придется заменить на:

Switch(config)#**interface fastEthernet 0/1**

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

Switch(config-if)#**switchport access vlan 2**

Switch(config)#**interface fastEthernet 0/2**

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

Switch(config-if)#**switchport access vlan 2**

Switch(config)#**interface fastEthernet 0/3**

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

Switch(config-if)#**switchport access vlan 2**

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

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

Выйдите из режима конфигурирования, дважды набрав команду **exit** и просмотрите результат конфигурирования (рис. 4), выполнив уже знакомую нам команду **sh vl br** еще раз:

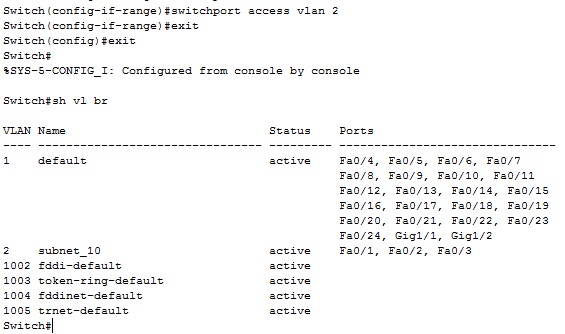


Рис. 4. Распределение портов на VLAN.

На коммутаторе появился еще один VLAN с номером 2 и именем subnet\_10, портами доступа которого являются fastEthernet0/1, fastEthernet0/2 и fastEthernet0/3.

Далее аналогичным образом создадим VLAN 3 с именем subnet\_192 и сделаем его портами доступа интерфейсы fastEthernet0/4 и fastEthernet0/5. Результат должен получиться следующим (рис. 5):

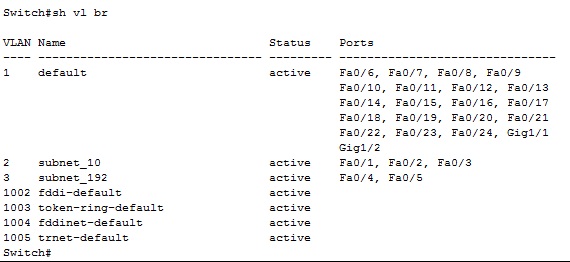


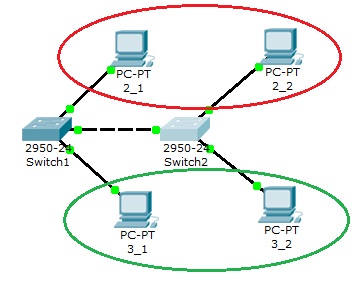
Рис. 5. Распределение портов на VLAN.

В принципе уже все готово и наша сеть настроена. Осталось лишь ее немного протестировать. Перейдите в консоль компьютера ПК0. Пропингуйте с него остальные компьютеры сети. Компьютеры ПК1 и ПК2 доступны, а компьютеры ПК3 и ПК4 не доступны. Все пять компьютеров теоретически должны находится в одной подсети 10.0.0.0/8 и видеть друг друга, на практике они находятся в разных виртуальных локальных сетях и поэтому не могут взаимодействовать между собой.

**Задание 2. Настройка VLAN на двух коммутаторах Cisco**

Создайте сеть, логическая топология которой представлена на рис. 6. Компьютеры соединены коммутатором Cisco 2950-24. В таблице 2 приведены адреса компьютеров.

VLAN 20



VLAN 30

Рис. 6. Схема сети.

Таблица 2.

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

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

Проверим связность получившейся сети. Для этого [пропингуем](http://www.netza.ru/2012/10/ping-tracert.html) с 2\_1 все остальные компьютеры. Поскольку пока в сети нет разделения на VLAN, то все компьютеры должны быть доступны.

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

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

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

Switch1#**conf t**

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

Switch(config)#

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

Switch1(config)#**vlan 20**

Switch1(config)#**interface fastEthernet 0/1**

Switch1(config-if-range)#**switchport mode access**

Switch1(config-if-range)#**switchport access vlan 20**

Switch1(config-if-range)#**exit**

Switch1(config)#**vlan 30**

Switch1(config)#**interface fastEthernet 0/2**

Switch1(config-if-range)#**switchport mode access**

Switch1(config-if-range)#**switchport access vlan 30**

Просмотрите информацию о существующих на коммутаторе VLAN-ах командой:

Switch1#**sh vl br**

У вас должен получится результат, показанный на рис. 7.

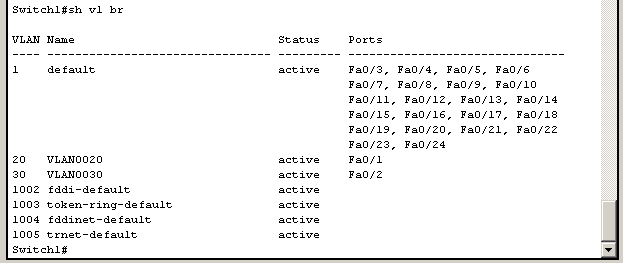


Рис. 7. Конфигурация Switch1.

Аналогичным образом сконфигурируйте Switch2 (рис. 8).

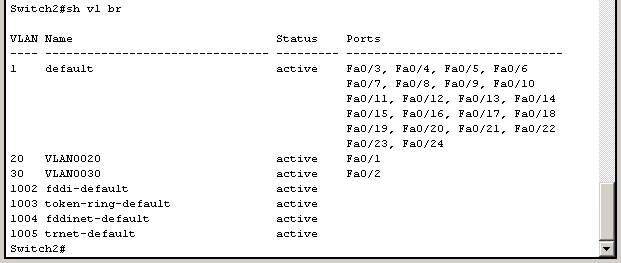


Рис. 8. Конфигурация Switch2.

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

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

Войдите в консоль коммутатора Switch1 и задайте транковый порт:

Switch1>**en**

Switch1#**conf t**

Switch1(config)#**interface fastEthernet 0/3**

Switch1(config)#**switchport mode trunk**

Switch1(config)#**no shutdown**

Switch1(config)#**exit**

Откройте конфигурацию коммутатора на интерфейсе FastEthernet0/3 и убедитесь, что порт транковый (рис. 9).

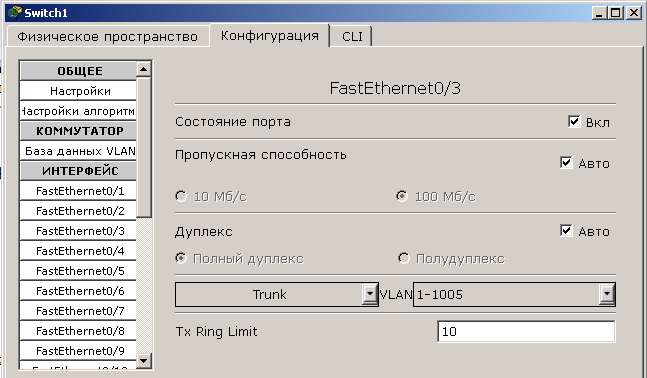


Рис. 9. Конфигурация интерфейса FastEthernet0/3.

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

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

Сохраните схему сети.

Теперь объединим две виртуальные сети с помощью маршрутизатора.

Добавьте в схему сети маршрутизатор, как показано на рис.8.9. Маршрутизатор соединен с интерфейсами **fastEthernet 0/4** коммутаторов.

Разобьем нашу сеть 10.0.0.0 на две подсети: 10.2.0.0 и 10.3.0.0. Для этого поменяйте IP адреса и маску подсети на 255.255.0.0, как указано в таблице 3.

Таблица 3.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Компьютер | IP адрес | Коммутатор | Порт коммутатора | Вилан |
| 2\_1 | 10.2.0.1/16 | Switch1 | 1 | VLAN 20 |
| 2\_2 | 10.2.0.3/16 | Switch2 | 1 | VLAN 20 |
| 3\_1 | 10.3.0.2/16 | Switch1 | 2 | VLAN 30 |
| 3\_2 | 10.3.0.4/16 | Switch2 | 2 | VLAN 30 |

Компьютеры должны пинговаться в пределах одного виллана и одной подсети.

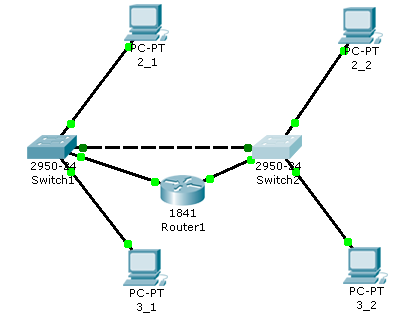


Рис. 10. Схема сети.

Обозначим на коммутаторах интерфейсы, подсоединенные к маршрутизатору в виртуальные сети.

Войдите в конфигурацию первого коммутатора Switch1 и задайте параметры четвертого порта:

Switch1(config)#**interface fastEthernet 0/4**

Switch1(config-if)#**switchport access vlan 20**

Проверьте настройки первого коммутатора Switch1 (рис. 11):

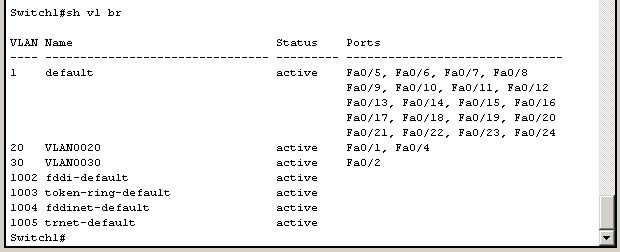


Рис. 11. Настройки коммутатора Switch1.

Войдите в конфигурацию второго коммутатора Switch2 и задайте параметры четвертого порта:

Switch2(config)#**interface fastEthernet 0/4**

Switch2(config-if)#**switchport access vlan 30**

Проверьте настройки второго коммутатора Switch2 (рис.12):

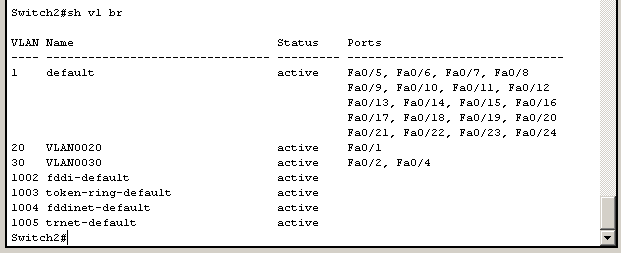


Рис.12. Настройки коммутатора Switch2.

Войдите в конфигурацию маршрутизатора и настройте IP адреса на маршрутизаторе:

Router1(config-if)#**interface fa0/0**

Router1(config-if)#**ip address 10.2.0.254 255.255.0.0**

Router1(config-if)#**no shutdown**

Router1(config-if)#**interface fa0/1**

Router1(config-if)#**ip address 10.3.0.254 255.255.0.0**

Router1(config-if)#**no shutdown**

С этого момента мы установили маршрутизацию между двумя подсетями. Осталось установить шлюзы на компьютерах (таблица 4).

Таблица 4.

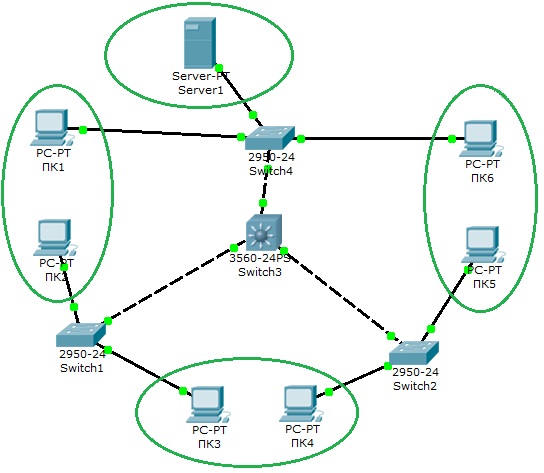
|  |  |
| --- | --- |
| Компьютер | Gataway |
| 2\_1 | 10.2.0.254 |
| 2\_2 | 10.2.0.254 |
| 3\_1 | 10.3.0.254 |
| 3\_2 | 10.3.0.254 |

Проверьте доступность компьютеров в сети. Теперь все компьютеры должны быть доступны и все адреса должны пинговаться.

**Задание 3. Настройка VLAN в корпоративной сети**

Создайте следующую схему сети (рис. 13):

VLAN 10



VLAN 11

VLAN 12

VLAN 13

Рис.13. Схема корпоративной сети.

Состав сети:

- три коммутатора второго уровня распределения 2950-24 (Switch1, Switch2, Switch4);

- центральный коммутатор третьего уровня 3560-24PS (Switch3), выполняющий роль роутера;

- сервер (Server1);

- три подсети по два узла в каждой

Задача:

Для любого вилана могут быть доступны только узлы этого же вилана и сервер Server1.

В таблице 5 и 6 приведены данные для установки параметров компьютеров и коммутаторов.

Таблица 5. Конфигурация компьютеров.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Компьютер | IP адрес | Коммутатор | Порт коммутатора | VLAN |
| ПК1 | 10.11.0.11/16 | Switch4 | 4 | VLAN 11 |
| ПК2 | 10.11.0.2/16 | Switch1 | 1 | VLAN 11 |
| ПК3 | 10.13.0.3/16 | Switch1 | 2 | VLAN 13 |
| ПК4 | 10.13.0.4/16 | Switch2 | 1 | VLAN 13 |
| ПК5 | 10.12.0.5/16 | Switch2 | 2 | VLAN 12 |
| ПК6 | 10.12.0.6/16 | Switch4 | 2 | VLAN 12 |
| Server1 | 10.10.0.7/16 | Switch4 | 1 | VLAN 10 |

Таблица 6. Связь коммутаторов по портам.

|  |  |
| --- | --- |
| Порт центрального коммутатора Switch3 | Порт коммутатора второго уровня распределения |
| 1 | Switch1 – 3 порт |
| 2 | Switch4 – 3 порт |
| 3 | Switch2 – 3 порт |

После настройки всех коммутаторов установите самостоятельно шлюзы на всех компьютерах и сервере.

Сконфигурируйте центральный коммутатор:

Этап 1.

Перейдите к конфигурации центрального коммутатора Switch3 и создайте на нем базу VLAN.

1. Создайте VLAN 10:

Switch3>**en**

Switch3#**conf t**

Switch3(config)#**vlan 10**

Switch3(config-vlan)#**exit**

2. Создайте VLAN 11, VLAN 12 и VLAN 13.

3. Настройте протокол VTP в режиме сервера:

Switch3(config)#**vtp domain HOME**

Switch3(config)#**vtp password HOME**

Switch3(config)#**vtp mode server**

4. Просмотрите информацию о конфигурации VTP:

Switch#**sh vtp status**

5. Настройте все интерфейсы на транк:

Switch3(config)#**int fa0/1**

Switch3(config-if)#**switchport mode trunk**

Switch3(config-if)#**exit**

и повторите эти настройки для второго и третьего интерфейсов.

Этап 2.

Перейдите к конфигурации коммутатора Switch4 и переведите его в режим client:

1. Создайте на коммутаторе VLAN 10 и задайте в нем порт 1 как access порт:

Switch4>**en**

Switch4#**conf t**

Switch4(config)#**vlan 10**

Switch4(config-vlan)#**exit**

Switch4(config)#**int fa0/1**

Switch4(config-if)#**switchport access vlan 10**

Switch4(config-if)#**switchport mode access**

Switch4(config-if)#**no shut**

2. Создайте на коммутаторе VLAN 11 и задайте в нем порт 4 как access порт.

3. Создайте на коммутаторе VLAN 12 и задайте в нем порт 2 как access порт.

4. Переведите коммутатор в режим clint:

Switch4(config)#**vtp domain HOME**

Switch4(config)#**vtp password HOME**

Switch4(config)#**vtp mode client**

**ВАЖНО!** При вводе имени домена и пароля соблюдайте нужный регистр.

Этап 4.

Перейдите к конфигурации коммутатора Switch1 и выподните следующие настройки:

.

1. Создайте на коммутаторе VLAN 11 и задайте в нем порт 1 как access порт.

2. Создайте на коммутаторе VLAN 13 и задайте в нем порт 2 как access порт.

3. Переведите коммутатор в режим client.

Этап 5.

Перейдите к конфигурации коммутатора Switch2.

1. Создайте на коммутаторе VLAN 12 и задайте в нем порт 2 как access порт.

2. Создайте на коммутаторе VLAN 13 и задайте в нем порт 1 как access порт.

3. Переведите коммутатор в режим client.

Этап 6.

Проверьте работоспособность сети на канальном уровне модели OSI.

После установки всех настроек таблица VLAN разойдется по коммутаторам с помощью протокола VTP.

В результате компьютеры, расположенные в одном виллане, будут доступны друг для друга, а другие компьютеры недоступны. Проверьте связь командой PING между следующими парами компьютеров:

- ПК1 – ПК2;

- ПК3 – ПК4;

- ПК5 – ПК6.

Если Вы все сделали правильно, то ping между парами пройдет, если нет – проверьте следующие установки:

- транковыми портами являются: на Switch3 все порты, на Switch1, Switch2 и Switch4 – третий порт;

- соединения интерфейсов на коммутаторах;

- названия и пароли доменов на каждом коммутаторе (команда sh vtp status);

- привязку интерфейсов к вилланам на коммутаторах (команда sh vl br).

Этап 7.

Настройка маршрутизации на центральном коммутаторе.

Создадим интерфейсы для каждого VLAN.

Настройка интерфейса для vlan 10 (шлюз по умолчанию):

Switch3(config)#**int vlan 10**

Switch3(config-if)#**ip address 10.10.0.1 255.255.0.0**

Switch3(config-if)#**no shut**

Switch3(config-if)#**exit**

Повторите эти настройки для каждого VLAN, задавая адрес IP: 10.[VLAN].0.1 и маску /16.

После этого зайдите в настройки каждого компьютера и установите нужный шлюз по умолчанию. Например для ПК1 – 10.11.0.1.

Включите маршрутизацию командой:

Switch3(config)#**ip routing**

Этап 8.

Проверьте работоспособность сети на сетевом уровне модели OSI.

После включения маршрутизации все компьютеры будут доступны с любого хоста.

Этап 9.

Выполним основную задачу работы: для любого вилана могут быть доступны только узлы этого же вилана и сервер Server1.

Для этого введем следующие ограничения на трафик сети:

1 - Разрешить пакеты от любого хоста к серверу.

2 - Разрешить пакеты от сервера до любого хоста.

3 – Трафик от одной подсети к этой же подсети разрешить.

4 – Правило по умолчанию: запретить всё остальное.

Ограничения на трафик сети задаются с помощью команды фильтрации **access-list**. Данная команда задает критерии фильтрации в списке опций разрешения и запрета, называемом списком доступа. Списки доступа имеют два правила: **permit** – разрешить и **deny** – запретить. Данные правила либо пропускают пакет дальше по сети, либо блокируют его доступ.

Более подробно списки доступа будут рассмотрены в лабораторной работе №14.

Открываем центральный коммутатор (Switch3) и меняем его конфигурацию с помощью команды фильтрации **access-list**:

Switch3(config)#**ip access-list extended 100**

(создается расширенный список доступа под номером 100)

Switch3(config-ext-nacl)#**permit ip any 10.10.0.0 0.0.0.255**

Switch3(config-ext-nacl)#**permit ip 10.10.0.0 0.0.0.255 any**

(разрешается доступ к сети 10.10.0.0/24)

Switch3(config-ext-nacl)#**permit ip 10.11.0.0 0.0.0.255 10.11.0.0 0.0.0.255**

Switch3(config-ext-nacl)#**permit ip 10.12.0.0 0.0.0.255 10.12.0.0 0.0.0.255**

Switch3(config-ext-nacl)#**permit ip 10.13.0.0 0.0.0.255 10.13.0.0 0.0.0.255**

(разрешается: доступ из сети 10.11.0.0/24 в эту же сеть;

доступ из сети 10.12.0.0/24 в эту же сеть;

доступ из сети 10.13.0.0/24 в эту же сеть).

Switch3(config-ext-nacl)#**exit**

Теперь этот access-list наложим на конкретный интерфейс и применим ко всем VLAN-ам на входящий трафик (опция **in –** на входящий трафик, **out –** на исходящий трафик):

Switch3(config)#**int vlan 10**

Switch3(config-if)#**ip access-group 100 in**

Этот шаг повторяем для каждого из VLAN-ов.

В результате получим:

для любого вилана могут быть доступны только узлы этого же вилана и сервер Server1.

**Самостоятельная работа № 9.1.**

На предприятии имеется два отдела, схема сетей которых представлена на рис. 14.

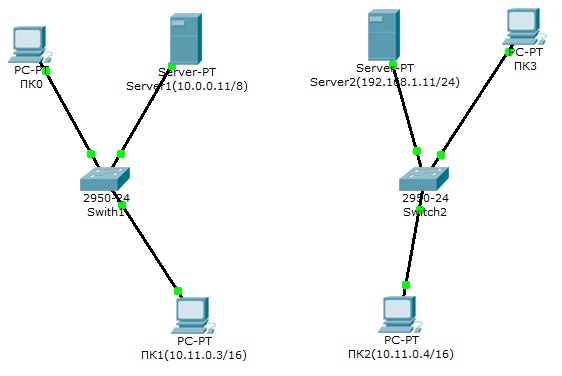


Рис. 14. Схема сетей отделов предприятия.

Отдел 1 – Switch1, отдел 2 – Switch2.

В каждой сети имеется сервер со службами DHCP, DNS и HTTP (на серверах Server1 и Server2 расположены интернет-сайты отделов).

Компьютеры ПК0 и ПК3 с DHCP серверов своих сетей получают параметры IP адреса и шлюз.

Компьютеры ПК1 и ПК2 находятся в отдельной сети в одном VLAN.

Задание:

Дополните схему сети маршрутизатором или коммутатором третьего уровня, чтобы обеспечить работу корпоративной сети в следующих режимах:

1 - компьютеры ПК0 и ПК3 должны открывать сайты каждого отдела;

2 – компьютеры ПК1 и ПК2 должны быть доступны только друг для друга.

**Контрольные вопросы.**

1. Для чего создаются виртуальные локальные сети? Каковы их достоинства?
2. Как связываются между собой VLAN и порты коммутатора?
3. Как обеспечивается общение между узлами разных виртуальных сетей?
4. Как обеспечивается управление виртуальными локальными сетями?
5. Можно ли построить VLAN на нескольких коммутаторах? Как это сделать?
6. Для чего служит идентификатор кадра (tag)? Где он размещается?
7. Что такое транк? Как он создается на коммутаторе и маршрутизаторе?
8. Какие команды используются для назначения VLAN на интерфейсы?
9. Какие команды используются для создания транковых соединений?
10. Какие команды используются для верификации VLAN?