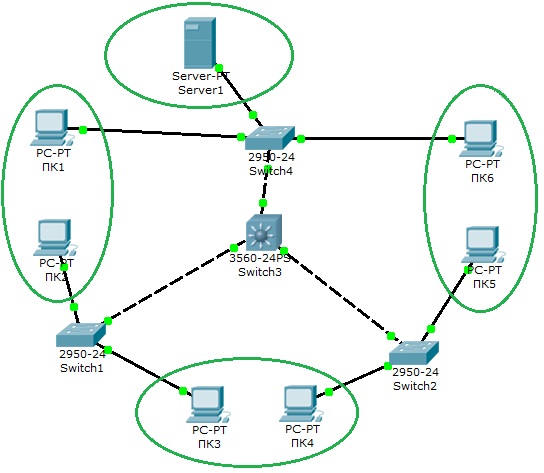
**Лабораторная работа. Настройка VLAN в корпоративной сети.**

Создайте следующую схему сети (рис.8.12):

VLAN 10



VLAN 11

VLAN 12

VLAN 13

Рис.8.12. 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 8.5 и 8.6 приведены данные для установки параметров компьютеров и коммутаторов.

Таблица 8.5. 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 8.6. 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 trunk encapsulation dot1q**

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.

Этап 3.

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 выполните 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 №3.**

Перенастроить сеть (Рис.8.12. Схема корпоративной сети) в соответствии со адресами своей сети

**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?