Лабораторная работа № 4

Часть 1. Связь между VLAN

Для минимизации широковещательных доменов реализуется разделение VLAN на уровне 2. Для обеспечения связи между VLAN наиболее часто используются следующие две технологии:

- **Интерфейс VLANIF**: это логические интерфейсы L3. После настройки интерфейса VLANIF и его IP-адреса устройство добавляет MAC-адрес и VID интерфейса VLANIF в таблицу MAC-адресов и устанавливает флаг передачи L3 для записи MAC-адреса. Когда MAC-адрес пункта назначения пакета совпадает с записью, пакет передается на 3 уровень для реализации L3 связи между сетями VLAN.

- **Подинтерфейс dot1q**: такие подинтерфейсы являются логическими интерфейсами L3. Подобно интерфейсу VLANIF, после настройки подинтерфейса dot1q и его IP-адреса устройство добавляет соответствующую запись MAC-адреса и устанавливает флаг передачи L3 для реализации связи между VLAN на уровне 3. Подинтерфейс dot1q применяется в сценариях, где к порту Ethernet уровня 3 подключается несколько VLAN.

Топология сети:

Компьютеры PC1 и PC2 принадлежат к разным VLAN. Для их взаимодействия необходимы интерфейсы VLANIF на S1 или подинтерфейсы dot1q на R1.

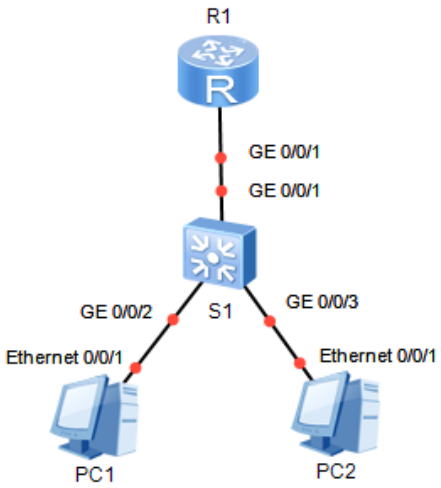

Рисунок 1.1. – Топология сети

План работы:

1. Настройка подинтерфейсов терминирования dot1q для реализации связи между VLAN.
2. Настройка интерфейсов VLANIF для реализации связи между VLAN.

Процедура конфигурирования:

Шаг 1. Настройте основные параметры устройств.

– Присвойте устройствам имена. Настройте IP-адреса и шлюзы PC1 и PC2 согласно таблице 1.1.

Таблица 1.1 – IP-адресация для PC.

Устройство	IP-адрес/маска	Шлюз
PC1	192.168.2.1/24	192.168.2.254
PC2	192.168.3.1/24	192.168.3.254

– На S1 назначьте GigabitEthernet0/0/2 и GigabitEthernet0/0/3 во VLAN 2 и VLAN 3 соответственно.

Шаг 2. Настройте подинтерфейсы терминирования dot1q для реализации связи между VLAN.

– Настройте магистральный порт на S1.

```
[S1]interface GigabitEthernet 0/0/1
[S1-GigabitEthernet0/0/1]port link-type trunk
[S1-GigabitEthernet0/0/1]port trunk allow-pass vlan 2 3
```

– Настройте подинтерфейс dot1q на маршрутизаторе R1.

```
[R1]interface GigabitEthernet 0/0/1.2
```

После создания подинтерфейса осуществляется переход в режим конфигурирования подинтерфейса. В этом примере цифра 2 указывает номер подинтерфейса. Рекомендуется, чтобы номер подинтерфейса совпадал с идентификатором VLAN.

```
[R1-GigabitEthernet0/0/1.2]dot1q termination vid 2
[R1-GigabitEthernet0/0/1.2]ip address 192.168.2.254 24
[R1-GigabitEthernet0/0/1.2]quit
[R1]interface GigabitEthernet 0/0/1.3
[R1-GigabitEthernet0/0/1.3]dot1q termination vid 3
[R1-GigabitEthernet0/0/1.3]ip address 192.168.3.254 24
[R1-GigabitEthernet0/0/1.3]quit
```

Команда **dot1q termination vid** *vlan-id* позволяет настраивать идентификатор VLAN для выполнения терминирования Dot1q на подинтерфейсе.

В этом примере, когда GigabitEthernet0/0/1 получает данные с тегами VLAN 2, он передает данные подинтерфейсу 2 для терминирования VLAN и последующей обработки. Данные, отправленные с подинтерфейса 2, также помечаются тегами VLAN 2.

```
[R1-GigabitEthernet0/0/1.2]arp broadcast enable
```

```
[R1-GigabitEthernet0/0/1.3]arp broadcast enable
```

Подинтерфейсы, выполняющие удаление тегов VLAN, не могут пересылать широковещательные пакеты и автоматически отбрасывают их при получении. Чтобы такие подинтерфейсы могли пересылать широковещательные пакеты, необходимо включить функцию широковещательной передачи ARP с помощью команды **arp broadcast enable**. На некоторых устройствах эта функция включена по умолчанию.

- Проверьте связь между VLAN.

Шаг 3. Удалите конфигурацию, созданную на предыдущем шаге. Настройте интерфейсы VLANIF для реализации связи между VLAN.

- Создайте интерфейс VLANIF на коммутаторе S1.

```
[S1]interface Vlanif 2
[S1-Vlanif2]ip address 192.168.2.254 24
[S1-Vlanif2]quit
[S1]interface Vlanif 3
[S1-Vlanif3]ip address 192.168.3.254 24
[S1-Vlanif3]quit
```

С помощью команды **interface vlanif** *vlan-id* можно создать интерфейс VLANIF и перейти в режим конфигурирования интерфейса VLANIF. Перед настройкой интерфейса VLANIF необходимо создать VLAN.

- Проверьте связь между VLAN.

Часть 2. Настройка ACL

Список контроля доступа (Access Control List, ACL) — это набор правил, разрешающих или запрещающих доступ. В каждом правиле определяется условие сопоставления пакетов. Это может быть адрес источника, адрес пункта назначения или номер порта.

ACL — это механизм фильтрации пакетов на основе правил. Пакеты, соответствующие списку ACL, обрабатываются на основе политики, определенной в ACL.

Топология сети:

В сети, показанной на рисунке 1.1, маршрутизатор R3 выполняет функции сервера, маршрутизатор R1 выполняет функции клиента, и они доступны для связи. Кроме того, на маршрутизаторе R1 созданы два логических интерфейса LoopBack 0 и LoopBack 1 для имитации двух пользователей-клиентов.

Один пользователь (LoopBack 1 на R1) должен удаленно управлять R3. Для гарантии того, что вход в R3 будет разрешен только пользователю, который соответствует политике безопасности, можно настроить Telnet на сервере, задать защиту паролем и сконфигурировать ACL.

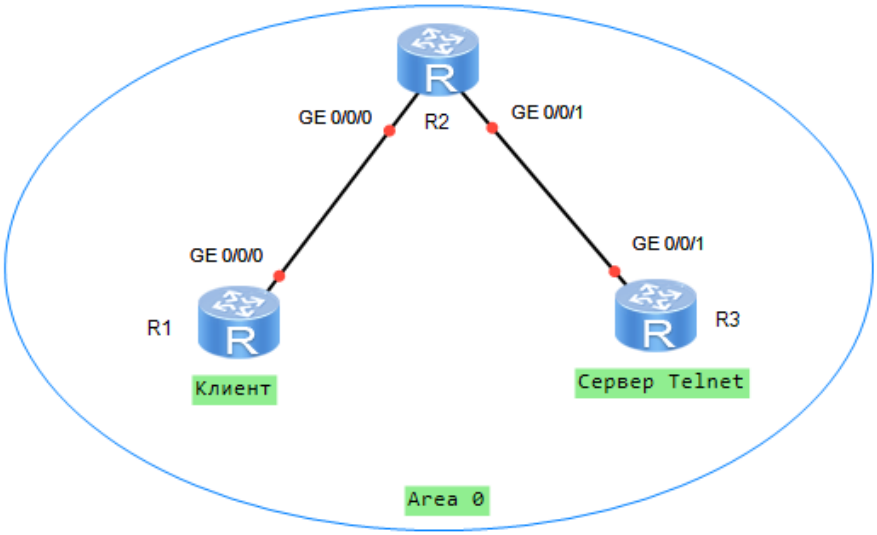

Рисунок 2.1 – Топология сети

План работы:

1. Настройка IP-адресов.
2. Настройка OSPF для обеспечения возможности сетевого подключения.
3. Создание ACL на основе необходимого трафика.
4. Настройка фильтрации трафика.

Процедура конфигурирования:

Шаг 1. Настройте IP-адреса.

– Настройте IP-адреса согласно таблице 2.1.

Таблица 2.1 – IP-адресация для маршрутизаторов

Устройство	Интерфейс	IP-адрес/маска
R1	GigabitEthernet0/0/0	10.1.2.1/24
	LoopBack0	10.1.1.1/24
	LoopBack1	10.1.4.1/24
R2	GigabitEthernet0/0/0	10.1.2.2/24
	GigabitEthernet0/0/1	10.1.3.2/24
R3	GigabitEthernet0/0/1	10.1.3.1/24

Шаг 2. Настройте OSPF для обеспечения возможности сетевого подключения.

– Настройте OSPF на маршрутизаторах R1, R2 и R3 и назначьте их в область 0, чтобы обеспечить возможность подключения.

– Выполните команду ping на маршрутизаторе R3, чтобы проверить возможность подключения к сети.

Шаг 3. Сконфигурируйте R3 в качестве сервера.

– Включите службу Telnet на R3, установите для уровня пользователя значение 3 и задайте для входа пароль — 1234567.

```
[R3]telnet server enable
```

– Команда telnet server enable позволяет включить службу Telnet.

```
[R3]user-interface vty 0 4
```

Команда **user-interface** позволяет перейти в режим интерфейса одного или нескольких пользователей. Пользовательский интерфейс терминала виртуального типа (Virtual Type Terminal, VTY) осуществляет управление и мониторинг входа пользователей в систему с помощью Telnet или SSH.

```
[R3-ui-vty0-4]user privilege level 3
[R3-ui-vty0-4]set authentication password cipher 1234567
```

Шаг 4. Настройте ACL на основе необходимого трафика.

Способ 1. Настройте ACL на интерфейсе VTY маршрутизатора R3, чтобы разрешить вход с R1 в R3 через Telnet, используя IP-адрес LoopBack 1.

```
[R3]acl 3000
[R3-acl-adv-3000]rule 5 permit tcp source 10.1.4.1 0.0.0.0
                 destination 10.1.3.1 0.0.0.0 destination-port eq 23
```

```
[R3-acl-adv-3000]rule 10 deny tcp source any
[R3-acl-adv-3000]quit
```

– Выполните фильтрацию трафика на интерфейсе VTY маршрутизатора R3.

```
[R3]user-interface vty 0 4
[R3-ui-vty0-4]acl 3000 inbound
```

– Выведите на экран конфигурацию ACL на R3.

```
[R3]display acl 3000

Advanced ACL 3000, 2 rules //Создан расширенный ACL. Он имеет номер
                             3000 и содержит два правила.
Acl's step is 5            //Правила ACL пронумерованы с шагом 5.
rule 5 permit tcp source 10.1.4.1 0 destination-port eq telnet
rule 10 deny tcp
```

Способ 2. Настройте ACL на физическом интерфейсе маршрутизатора R2, чтобы разрешить вход с R1 в R3 через Telnet, используя IP-адрес физического интерфейса.

– Настройте ACL на R2.

```
[R2]acl 3001
[R2-acl-adv-3001]rule 5 permit tcp source 10.1.4.1 0.0.0.0
                  destination 10.1.3.1 0.0.0.0 destination-port eq 23
[R2-acl-adv-3001]rule 10 deny tcp source any
[R2-acl-adv-3001]quit
```

– Выполните фильтрацию трафика на интерфейсе GE0/0/0 маршрутизатора R3.

```
[R2]interface GigabitEthernet0/0/0
[R2-GigabitEthernet0/0/0]traffic-filter inbound acl 3001
```

– Выведите на экран конфигурацию ACL на R2.

```
[R2]display acl 3001
Advanced ACL 3001, 2 rules
Acl's step is 5
rule 5 permit tcp source 10.1.4.1 0 destination 10.1.3.1 0 destination-
port eq telnet
rule 10 deny tcp
```

Шаг 5. Протестируйте доступ через Telnet и проверьте конфигурацию ACL.

– На маршрутизаторе R1 подключитесь через Telnet к серверу, используя указанный IP-адрес источника 10.1.1.1.

```
<R1>telnet -a 10.1.1.1 10.1.3.1
Press CTRL_] to quit telnet mode
Trying 10.1.3.1 ...
Error: Can't connect to the remote host
```

Команда **telnet** позволяет использовать протокол Telnet для входа на другое устройство.
-a source-ip-address: определяет IP-адрес источника. Пользователи могут связываться с сервером, используя указанный IP-адрес.

– На маршрутизаторе R1 подключитесь через Telnet к серверу, используя указанный IP-адрес источника 10.1.4.1.

```
<R1>telnet -a 10.1.4.1 10.1.3.1
Press CTRL_] to quit telnet mode
Trying 10.1.3.1 ...
Connected to 10.1.3.1 ...
Login authentication
Password:
```

Часть 3. Задание для самостоятельного выполнения.

Постройте топологию, изображенную на рисунке 3.1.

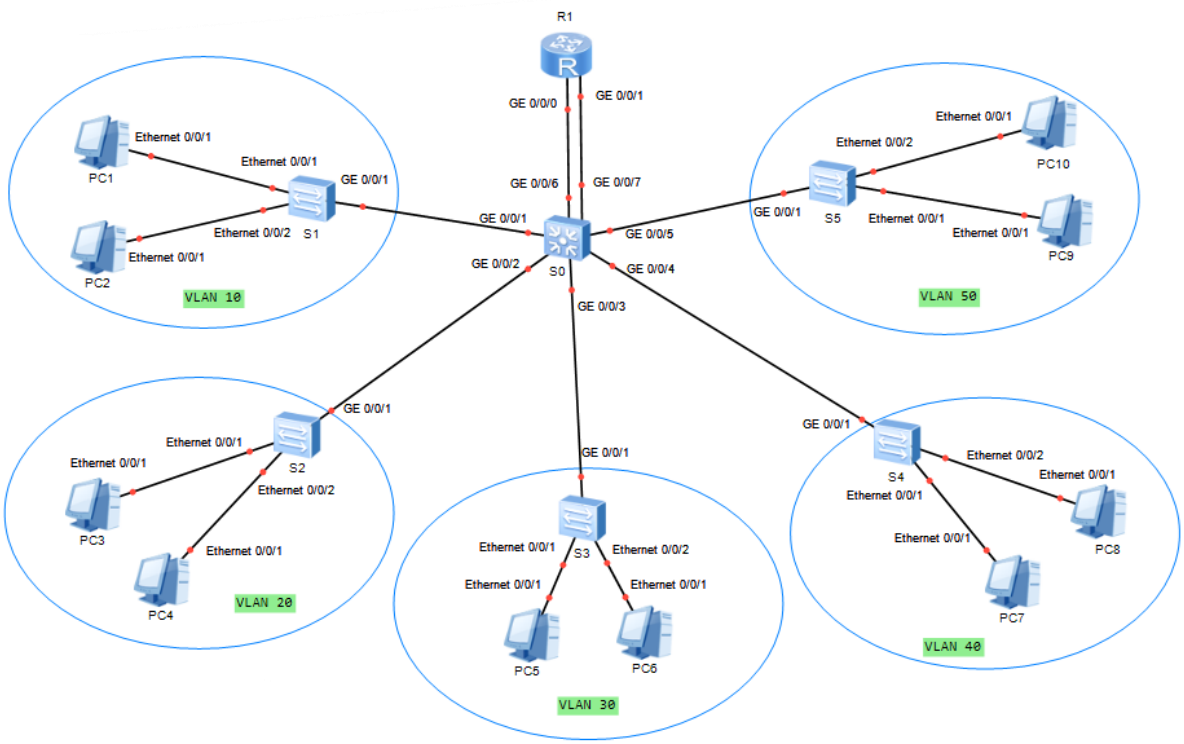

Рисунок 3.1 – Топология сети

План работы:

1. Настройка IP-адресации на компьютерах.
2. Настройка интерфейсов коммутаторов.
3. Настройка маршрутизации между VLAN.
4. Настройка ACL.

Процедура конфигурирования:

Шаг 1. Настройте основные параметры устройств.

Присвойте устройствам имена. Настройте IP-адреса и шлюзы PC1 – PC10 согласно таблице 3.1.

Таблица 3.1 – IP-адресация для PC.

Устройство	IP-адрес/маска	VLAN	Шлюз
PC1	192.168.10.1/24	10	192.168.10.254
PC2	192.168.10.2/24		
PC3	192.168.20.1/24	20	192.168.20.254
PC4	192.168.20.2/24		

PC5	192.168.30.1/24	30	192.168.30.254
PC6	192.168.30.2/24		
PC7	192.168.40.1/24	40	192.168.40.254
PC8	192.168.40.2/24		
PC9	192.168.50.1/24	50	192.168.50.254
PC10	192.168.50.2/24		

Шаг 2. Настройте VLAN на коммутаторах.

1. Настройте порты доступа на коммутаторах S1 – S5.

   Примечание: к оконечным устройствам чаще всего настраивается порт доступа (access port).

2. Настройте магистральные порты между коммутаторами S1 – S5 и коммутатором S0.

   Примечание: между коммутаторами в подавляющем большинстве случаев настраиваются магистральные порты (trunk port).

3. Проверьте доступность хостов, находящихся в одной подсети.
4. Проверьте доступность хостов, находящихся в разных VLAN.

Шаг 3. Настройте маршрутизацию между VLAN.

Сценарий 1. Маршрутизация с помощью многоуровневого коммутатора.

1. Настройте интерфейсы VLANIF на коммутаторе S0.
2. Проверьте доступность хостов, находящихся в разных VLAN.

Сценарий 2. Router-on-a-stick.

1. Отмените настройки, произведенные в сценарии 1.
2. Настройте агрегированный канал между R1 и S0 в режиме LACP.

   Примечание: при настройке агрегации на **R1** следует **<u>сначала</u>** перевести интерфейс Eth-Trunk из режима L2 в режим L3 командой **undo portswitch**, а затем производить необходимые настройки.

3. Настройте магистральный порт на S0.
4. Настройте подинтерфейсы на R1.
5. Проверьте доступность хостов, находящихся в разных VLAN.

Шаг 4. Запретите прохождение трафика между VLAN 10 и VLAN 50.

Шаг 5. Разрешите прохождение трафика между VLAN 20 и VLAN 40 только для хостов с четными IP-адресами.

Шаг 6. Запретите любым хостам с нечетными IP-адресами связь с VLAN 30 (кроме хостов, находящихся во VLAN 30).