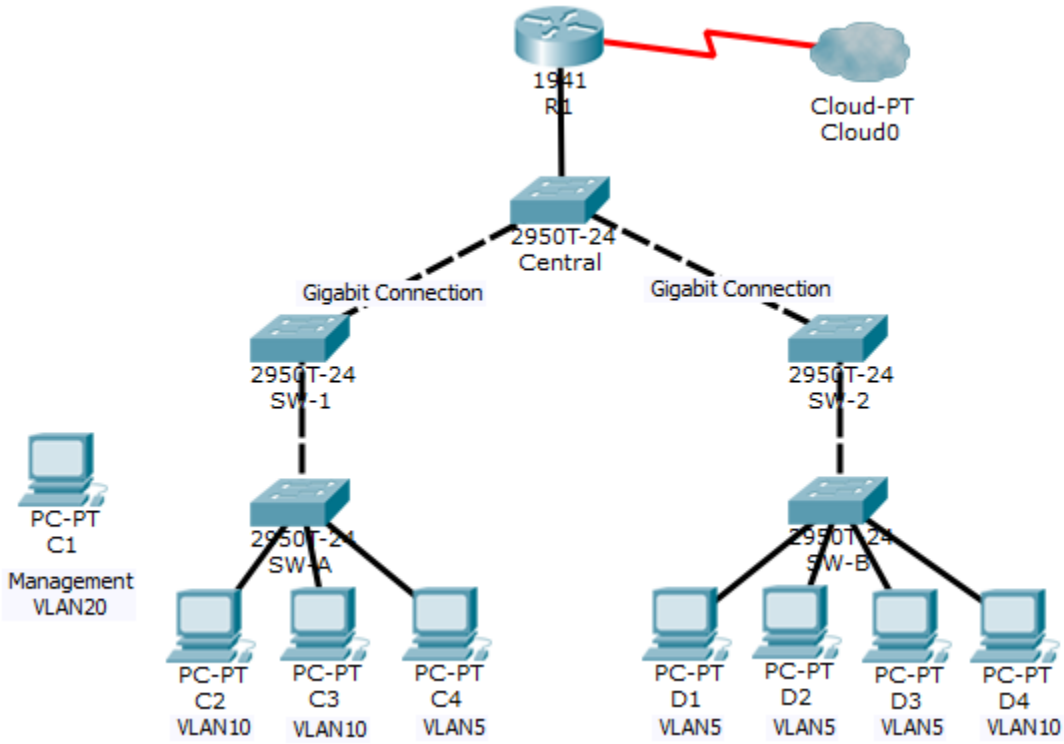
Packet Tracer. Обеспечение безопасности VLAN на 2-м уровне

Топология



Задачи

- Создание нового резервного канала между коммутаторами SW-1 и SW-2.
- Включение транкинга и конфигурирование защиты в новом магистральном канале между коммутаторами SW-1 и SW-2.
- Создание новой управляющей сети VLAN (VLAN 20) и подключение к ней управляющего ПК.
- Создание списка ACL для предотвращения доступа внешних пользователей к управляющей VLAN.

Исходные данные/сценарий

В настоящее время в сети компании настроено использование двух отдельных сетей VLAN: VLAN 5 и VLAN 10. Кроме того, для всех магистральных портов настроена нативная сеть VLAN 15. Сетевой администратор хочет добавить резервный канал между коммутаторами SW-1 и SW-2. Для канала должен быть включен транкинг и выполнены все требования безопасности.

Кроме того, сетевой администратор хочет подключить управляющий компьютер к коммутатору SW-A. Управляющий компьютер должен иметь возможность подключаться ко всем коммутаторам и маршрутизатору, но любые другие устройства не должны подключаться к управляющему компьютеру или коммутаторам. Администратор хочет создать новую сеть VLAN 20 для целей управления.

На всех устройствах были предварительно настроены следующие параметры.

- Пароль привилегированного доступа: **ciscoenpa55**
- Пароль консоли: **ciscoconpa55**
- Имя пользователя и пароль SSH: **SSHadmin/ciscosshpa55**

Часть 1: Проверка связи

Шаг 1: Проверьте связь между компьютерами C2 (VLAN 10) и C3 (VLAN 10).

Шаг 2: Проверьте связь между компьютерами C2 (VLAN 10) и D1 (VLAN 5).

Примечание. При использовании простого пакета PDU GUI отправьте эхо-запрос дважды, чтобы разрешить протокол ARP.

Часть 2: Создание резервного канала между коммутаторами SW-1 и SW-2

Шаг 1: Подключите коммутаторы SW-1 и SW-2.

С помощью кросс-кабеля подключите порт F0/23 на коммутаторе **SW-1** к порту F0/23 на коммутаторе **SW-2**.

Шаг 2: Включите транкинг, включая все механизмы обеспечения безопасности, на канале между коммутаторами SW-1 и SW-2.

Транкинг уже был настроен на всех ранее существовавших магистральных интерфейсах. Для нового канала необходимо настроить транкинг, включая все механизмы обеспечения безопасности. На обоих коммутаторах SW-1 и SW-2 настройте порт как магистральный (trunk), назначьте ему нативную сеть VLAN 15 и отключите автосогласование.

Часть 3: Настройка VLAN 20 в качестве управляющей сети VLAN

Сетевой администратор хочет обеспечить доступ ко всем коммутаторам и маршрутизаторам с помощью управляющего компьютера. В целях безопасности администратор планирует разместить все управляемые устройства в отдельной сети VLAN.

Шаг 1: Включите управляющую сеть VLAN (VLAN 20) на коммутаторе SW-A.

a. Включите VLAN 20 на коммутаторе **SW-A**.

b. Создайте интерфейс VLAN 20 и назначьте IP-адрес в сети 192.168.20.0/24.

Шаг 2: Включите одну и ту же управляющую сеть VLAN на всех остальных коммутаторах.

a. Создайте управляющую сеть VLAN на всех коммутаторах: **SW-B**, **SW-1**, **SW-2** и **Central**.

b. Создайте интерфейс VLAN 20 на всех коммутаторах и назначьте IP-адрес в сети 192.168.20.0/24.

Шаг 3: Подключите и настройте управляющий компьютер.

Подключите управляющий компьютер к порту F0/1 коммутатора SW-A и убедитесь, что ему назначен доступный IP-адрес в сети 192.168.20.0/24.

Шаг 4: На коммутаторе SW-A убедитесь, что управляющий компьютер является частью сети VLAN 20.

Интерфейс F0/1 должен являться частью сети VLAN 20.

Шаг 5: Проверьте связь управляющего компьютера со всеми коммутаторами.

Управляющий компьютер должен успешно отправлять эхо-запросы на коммутаторы **SW-A, SW-B, SW-B, SW-1, SW-2** и **Central**.

Часть 4: Настройка управляющего компьютера для доступа к маршрутизатору R1

Шаг 1: Включите новый субинтерфейс на маршрутизаторе R1.

a. Создайте субинтерфейс g0/0.3 и настройте для инкапсуляции (параметр encapsulation) значение dot1q 20 (чтобы учитывать VLAN 20).

b. Назначьте IP-адрес в сети 192.168.20.0/24.

Шаг 2: Проверьте связь между управляющим компьютером и маршрутизатором R1.

Не забудьте настроить шлюз по умолчанию на управляющем компьютере, чтобы обеспечить связь.

Шаг 3: Включите безопасность.

Управляющий компьютер должен иметь доступ к маршрутизатору, но никакие другие компьютеры не должны иметь доступа к управляющей сети VLAN.

a. Создайте список ACL, разрешающий только управляющему компьютеру доступ к маршрутизатору.

b. Примените список ACL к нужным интерфейсам.

Примечание. Список ACL можно создать несколькими способами, чтобы добиться необходимого уровня безопасности. Поэтому данная часть задания оценивается в зависимости от соответствующих требований к связи. Управляющий компьютер должен иметь доступ ко всем коммутаторам и маршрутизатору. Все остальные компьютеры не должны иметь возможности подключаться к каким-либо устройствам в VLAN.

Шаг 4: Проверьте безопасность.

a. Убедитесь, что только у управляющего компьютера есть доступ к маршрутизатору. Используйте SSH для доступа к маршрутизатору **R1** с именем пользователя **SSHadmin** и паролем **ciscosshpa55**.

```
PC> ssh -l SSHadmin 192.168.20.100
```

b. С управляющего компьютера отправьте эхо-запросы на коммутаторы **SW-A, SW-B** и маршрутизатор **R1**. Эхо-запросы выполнены успешно? Поясните ответ.

Эхо-запросы выполнены успешно, так как устройствам в сети VLAN20 не требуется прокладывать маршрут через маршрутизатор.

c. С компьютера **D1** отправьте эхо-запрос управляющему компьютеру. Эхо-запрос выполнен успешно? Поясните ответ.

Эхо-запрос был завершен неудачно, так как устройство не принадлежит сети VLAN 20, соответственно нет доступа к управляющему серверу из-за настроенных ACL-списков на маршрутизаторе

Шаг 5: Проверьте результаты.

Вы полностью выполнили задание. Нажмите **Check Results** (Проверить результаты) для просмотра отзыва и проверки завершенных обязательных компонентов.

Если на первый взгляд все компоненты правильные, но задание по-прежнему отображается как незавершенное, это может означать, что выполняются тесты связи для проверки работы списка ACL.

