Домашнее задание

Дисциплина	Защита компьютерных сетей и систем
Тема	Тема 21. Атаки на сетевое оборудование
Форма проверки	**Проверка преподавателем**
Имя преподавателя	Антон Носков
Время выполнения	60-120 минут
Цель задания	Научиться: ● создавать новый резервный канал между коммутаторами, ● создавать новую управляющую сеть VLAN и подключать к ней управляющего ПК, ● создавать список ACL для предотвращения доступа внешних пользователей к управляющей VLAN и предупреждения атак VLAN с переходом
Инструменты для выполнения ДЗ	Компьютер, симулятор сети передачи данных Cisco Packet Tracer 8.1.1, подключённый к интернету
Правила приёма работы	● Чтобы выполнить задание, используйте Cisco Packet Tracer. ● Файл с выполненным заданием сохраните под своей фамилией и разместите в ЛМС **(Ф. И. О.pka)**
Критерии оценки	**Задание оценивается в 10 баллов:** • **часть 1 — 1 балл,** • **часть 2 — 2 балла,** • **часть 3 — 3 балла,** • **часть 4 — 4 балла.** **Задание считается выполненным, если:** - решены все четыре части задания, - ссылка на файл с сохранённым заданием размещена в ЛМС. **Задание не выполнено, если:** **-** задание не решено или решено с существенными ошибками, - ссылка на файл с заданием не размещена в ЛМС
Дедлайн	Две недели после вебинара (точную дату см. в ЛМС)

Описание задания

Перед тем, как приступить к выполнению задания, установите симулятор сети передачи данных Cisco Packet Tracer 8.1.1.

Ссылки на ПО для разных ОС:

1. Windows 64 — Cisco Packet Tracer 8.1.1.
2. Ubuntu 64 — Cisco Packet Tracer 8.1.1.
3. macOS X — Cisco Packet tracer 8.1.1.

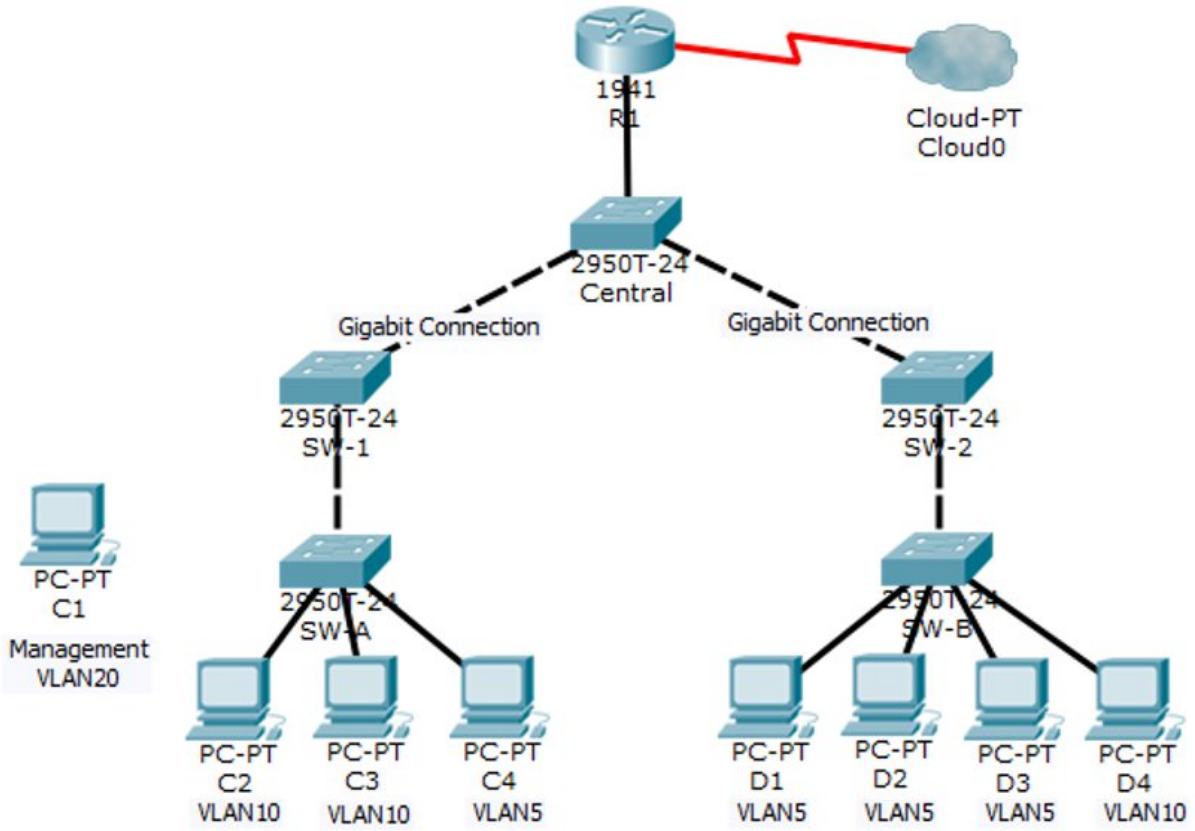
Инструкция по установке

Когда Cisco Packet Tracer выдаёт запрос авторизации, выберите Skills for all и авторизуйтесь через учётную запись Google. В некоторых сетях может потребоваться VPN при запуске Cisco Packet Tracer.

После установки Cisco Packet Tracer откройте файл **Layer 2 VLAN Security.pka** (размещён в ЛМС) и начинайте выполнять задание.

Исходные данные

Топология сети



Исходный сценарий

Сейчас в сети компании настроено использование двух отдельных сетей VLAN: VLAN 5 и VLAN 10. 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 включён транкинг и выполнены все требования безопасности.

Также 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 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 эта 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. Проверьте, успешно ли выполнены эхо-запросы. Поясните ответ.

_____

c. С компьютера D1 отправьте эхо-запрос управляющему компьютеру. Проверьте, успешно ли выполнены эхо-запросы. Поясните ответ.

_____

Примечание. Ответы на вопросы - обязательны!