Лабораторная работа. Реализация системы безопасности сети VLAN

Топология

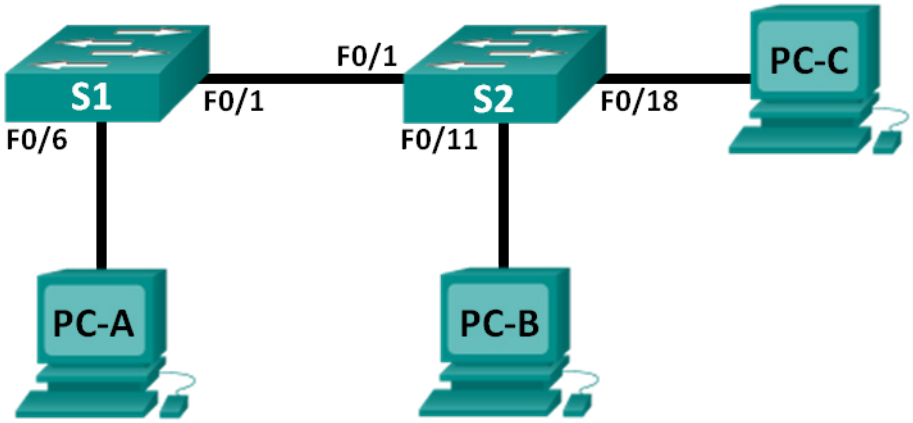

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
S1	VLAN 99	172.17.99.11	255.255.255.0	172.17.99.1
S2	VLAN 99	172.17.99.12	255.255.255.0	172.17.99.1
PC-A	Сетевой адаптер	172.17.99.3	255.255.255.0	172.17.99.1
PC-B	Сетевой адаптер	172.17.10.3	255.255.255.0	172.17.10.1
PC-C	Сетевой адаптер	172.17.99.4	255.255.255.0	172.17.99.1

Назначения VLAN

VLAN	Имя
10	Данные
99	Сеть Management&Native
999	Чёрный список

Задачи

Часть 1. Построение сети и настройка базовых параметров устройства

Часть 2. Внедрение средств обеспечения безопасности VLAN на коммутаторах

Исходные данные/Сценарий

Рекомендуется настраивать базовые параметры системы безопасности как на портах доступа, так и на транковых портах коммутатора. Это позволяет защитить сеть VLAN от угроз и возможного прослушивания сетевого трафика.

В этой лабораторной работе вам предстоит настроить на сетевых устройствах в топологии некоторые базовые параметры, проверить подключение, а затем применить на коммутаторах более надёжные меры безопасности. Вы изучите поведение коммутаторов Cisco при использовании различных команд **show**. Затем вам нужно будет применить меры безопасности.

Примечание. В лабораторной работе используются коммутаторы Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование других моделей коммутаторов и других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ.

Примечание. Убедитесь, что информация из коммутаторов удалена, и они не содержат конфигурации загрузки. Если вы не уверены в этом, обратитесь к преподавателю.

Необходимые ресурсы:

- 2 коммутатора (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);
- 3 компьютера (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через консольные порты;
- кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Построение сети и настройка базовых параметров устройства

В первой части лабораторной работы нужно настроить базовые параметры на коммутаторах и компьютерах. Имена и адреса устройств указаны в таблице адресации.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Выполните инициализацию и перезагрузку коммутаторов.

Шаг 3: Настройте IP-адреса на узлах PC-A, PC-B и PC-C.

Адреса узловых ПК можно посмотреть в таблице адресации.

Шаг 4: Настройте базовые параметры каждого коммутатора.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Назначьте **class** в качестве пароля привилегированного режима EXEC.

d. Назначьте **cisco** в качестве пароля паролей консоли и VTY и активируйте вход для консоли и VTY каналов.

e. Настройте logging synchronous для консоли и каналов vty.

Шаг 5: Настройте сети VLAN на каждом коммутаторе.

a. Создайте и назначьте имена сетям VLAN в соответствии с таблицей назначений VLAN.

b. Настройте IP-адрес, указанный в таблице адресации для сети VLAN 99 на обоих коммутаторах.

c. Настройте порт F0/6 на коммутаторе S1 в качестве порта доступа и назначьте его сети VLAN 99.

d. Настройте порт F0/11 на коммутаторе S2 в качестве порта доступа и назначьте его сети VLAN 10.

e. Настройте порт F0/18 на коммутаторе S2 в качестве порта доступа и назначьте его сети VLAN 99.

f. Выполните команду **show vlan brief**, чтобы проверить назначения VLAN и портов.

Какой сети VLAN будет принадлежать не назначенный порт, например F0/8 на коммутаторе S2?

Шаг 6: Настройте базовые параметры безопасности порта.

a. Настройте баннер MOTD (сообщение дня) для предупреждения пользователей о запрете несанкционированного доступа.

b. Зашифруйте все пароли.

c. Отключите все неиспользуемые физические порты.

d. Отключите основной текущий веб-сервис.

```
S1(config)# no ip http server
S2(config)# no ip http server
```

e. Сохраните текущую конфигурацию в загрузочную конфигурацию.

Шаг 7: Проверьте подключение между устройствами и сведения о VLAN.

a. Из командной строки на ПК-A отправьте эхо-запрос на административный адрес коммутатора S1. Успешно ли выполнен эхо-запрос? Почему?

b. От коммутатора S1 отправьте эхо-запрос на административный адрес коммутатора S2. Успешно ли выполнен эхо-запрос? Почему?

c. Из командной строки на PC-B отправьте эхо-запрос на административные адреса коммутаторов S1 и S2 и на IP-адреса PC-A и PC-C. Успешно ли выполнены эхо-запросы? Почему?

d. Из командной строки узла PC-C отправьте эхо-запрос на административные адреса коммутаторов S1 и S2. Успешно ли выполнены эхо-запросы? Почему?

Примечание. Для успешной передачи эхо-запросов может потребоваться отключение брандмауэра.

Часть 2: Реализация системы безопасности сети VLAN на коммутаторах

Шаг 1: Настройте транковые порты на коммутаторах S1 и S2.

a. Настройте порт F0/1 на коммутаторе S1 в качестве транкового порта.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
```

b. Настройте порт F0/1 на коммутаторе S2 в качестве транкового порта.

```
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
```

c. Проверьте транковую связь на коммутаторах S1 и S2. Выполните команду **show interface trunk** на обоих коммутаторах.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99,999
```

Шаг 2: Измените сеть native VLAN для транковых портов на коммутаторах S1 и S2.

Изменение сети native VLAN для транковых портов с VLAN 1 на другую сеть VLAN — это хороший способ обеспечения безопасности.

a. Укажите текущую сеть native VLAN для интерфейсов F0/1 коммутаторов S1 и S2.

b. Настройте сеть Management&Native VLAN 99 на транковом интерфейсе F0/1 коммутатора S1 в качестве сети native VLAN.

```
S1# config t
S1(config)# interface f0/1
S1(config-if)# switchport trunk native vlan 99
```

c. Подождите несколько секунд. Вы должны получить сообщения об ошибке в консольном сеансе на коммутаторе S1. Что означает сообщение %CDP-4-NATIVE_VLAN_MISMATCH:?

d. Настройте сеть VLAN 99 на транковом интерфейсе F0/1 коммутатора S2 в качестве сети native VLAN.

```
S2(config)# interface f0/1
S2(config-if)# switchport trunk native vlan 99
```

e. Убедитесь, что сетью native VLAN на обоих коммутаторах является VLAN 99. Ниже показаны выходные данные коммутатора S1.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port         Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,999
```

Шаг 3: Убедитесь, что трафик успешно проходит через транковый канал.

a. Из командной строки на ПК-A отправьте эхо-запрос на административный адрес коммутатора S1. Успешно ли выполнен эхо-запрос? Почему?

b. В консольном сеансе на коммутаторе S1 отправьте эхо-запрос на административный адрес коммутатора S2. Успешно ли выполнен эхо-запрос? Почему?

c. Из командной строки на PC-B отправьте эхо-запрос на административные адреса коммутаторов S1 и S2 и на IP-адреса PC-A и PC-C. Успешно ли выполнены эхо-запросы? Почему?

d. Из командной строки на PC-C отправьте эхо-запрос на административные адреса коммутаторов S1 и S2 и на IP-адрес узла PC-A. Успешно ли выполнены эхо-запросы? Почему?

Шаг 4: Запретите использование DTP на коммутаторах S1 и S2.

На коммутаторах Cisco используется собственный протокол, который известен как протокол динамического создания транкового канала (DTP). Некоторые порты автоматически согласовываются для транковой связи. Согласование рекомендуется отключать. Такое поведение по умолчанию можно увидеть, выполнив следующую команду:

```
S1# show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
<Output Omitted>
```

a. Отключите согласование на коммутаторе S1.

```
S1(config)# interface f0/1
S1(config-if)# switchport nonegotiate
```

b. Отключите согласование на коммутаторе S2.

```
S2(config)# interface f0/1
S2(config-if)# switchport nonegotiate
```

c. Убедитесь, что согласование отключено, с помощью команды **show interface f0/1 switchport** на коммутаторах S1 и S2.

```
S1# show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
<Output Omitted>
```

Шаг 5: Настройте функцию безопасности на портах доступа на коммутаторах S1 и S2.

Если устройство подключено к одному из этих портов, а интерфейс включён, транковая связь может быть успешной, даже если вы выключите на коммутаторах неиспользуемые оставшиеся порты. Кроме того, все порты по умолчанию находятся в сети VLAN 1. Рекомендуется перевести неиспользуемые порты в сеть VLAN «чёрной дыры». На данном этапе вам нужно отключить транковую связь на всех неиспользуемых портах. Также вам нужно назначить неиспользуемые порты сети VLAN 999. Для этой лабораторной работы на обоих коммутаторах будут настроены только порты со 2-го по 5-й.

a. Выполните команду **show interface f0/2 switchport** на коммутаторе S1. Обратите внимание на административный режим и состояние для согласования транковой связи.

```
S1# show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
<Output Omitted>
```

b. Отключите транковую связь на портах доступа коммутатора S1.

```
S1(config)# interface range f0/2 – 5
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
```

c. Отключите транковую связь на портах доступа коммутатора S2.

d. Убедитесь, что порт F0/2 на коммутаторе S1 настроен в качестве порта доступа.

```
S1# show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
```

```
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 999 (BlackHole)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<Output Omitted>
```

e. Убедитесь, что назначения портов VLAN настроены верно на обоих коммутаторах. Коммутатор S1 показан ниже в качестве примера.

```
S1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
10   Data                             active
99   Management&Native                active    Fa0/6
999  BlackHole                        active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
1002 fddi-default                       act/unsup
1003 token-ring-default                 act/unsup
1004 fddinet-default                    act/unsup
1005 trnet-default                      act/unsup
Restrict VLANs allowed on trunk ports.
```

По умолчанию все сети VLAN имеют доступ к транковым портам. Из соображений безопасности рекомендуется разрешать доступ к транковым каналам вашей сети только для нужных сетей VLAN.

f. Разрешите доступ к транковому порту F0/1 на коммутаторе S1 только для сетей VLAN 10 и 99.

```
S1(config)# interface f0/1
S1(config-if)# switchport trunk allowed vlan 10,99
```

g. Разрешите доступ к транковому порту F0/1 на коммутаторе S2 только для сетей VLAN 10 и 99.

h. Проверьте разрешённые сети VLAN. Выполните команду **show interface trunk** в привилегированном режиме на коммутаторах S1 и S2.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,99

Port        Vlans allowed and active in management domain
Fa0/1       10,99

Port        Vlans in spanning tree forwarding state and not pruned
```

```
Fa0/1       10,99
```

Какой получен результат?

Вопросы на закрепление

Есть ли проблемы в системе безопасности коммутатора Cisco с конфигурацией по умолчанию? Какие именно?