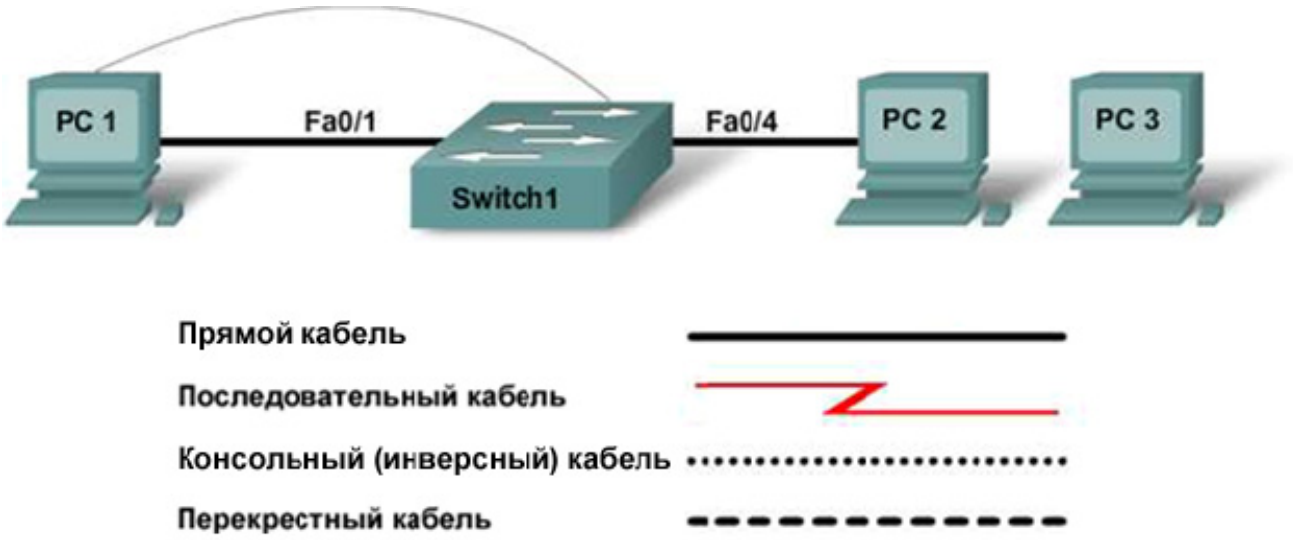
Лабораторная работа 3.1.4. Применение базовых мер безопасности для коммутатора



Наименование устройства	IP-адрес	Маска подсети	Шлюз по умолчанию	Секретный пароль привилегированного доступа	Пароль доступа к каналам vty и консоли
PC 1	192.168.1.3	255.255.255.0	192.168.1.1		
PC 2	192.168.1.4	255.255.255.0	192.168.1.1		
PC 3	192.168.1.5	255.255.255.0	192.168.1.1		
Switch1	192.168.1.2	255.255.255.0	192.168.1.1	class	cisco

Задачи

- Задать в настройках конфигурации пароли для защиты доступа к командной строке.
- Задать в настройках конфигурации коммутатора необходимость удаления информации о состоянии сервера в целях безопасности.
- Настройка безопасности порта.
- Отключить неиспользуемые порты.
- Выполнить тестирование конфигурации путем подключения неопределенных узлов к безопасным портам.

Исходные данные/подготовка

В данной лабораторной работе требуется организовать сеть, аналогичную той, что изображена на диаграмме топологии.

Необходимо использовать следующие ресурсы:

- коммутатор Cisco 2960 или аналог;
- три компьютера с ОС Windows, хотя бы один из которых должен иметь программу эмуляции терминала;
- один или большее количество консольных кабелей с разъемами RJ45 и DB9;
- два прямых кабеля Ethernet (для подсоединения ПК 1 и ПК 2 к коммутатору);
- доступ к командной строке ПК;
- доступ к сетевой конфигурации TCP/IP ПК.

ПРИМЕЧАНИЕ. Убедитесь в том, что начальная конфигурация коммутатора удалена. Инструкции по удалению начальной конфигурации коммутаторов и маршрутизаторов см. в руководстве по проведению лабораторной работы на веб-сайте академии Cisco в разделе Tools (Инструменты).

Шаг 1. Подсоединение ПК 1 к коммутатору

а. Подсоедините ПК 1 к порту коммутатора Fa0/1. Выполните настройку ПК 1, задав IP-адрес, маску подсети и шлюз по умолчанию согласно таблице (см. выше).

б. С ПК 1 запустите программу эмуляции терминала и установите сеанс связи с коммутатором.

Шаг 2. Подсоединение ПК 2 к коммутатору

а. Подсоедините ПК 2 к интерфейсу Fa0/4 коммутатора.

б. Выполните настройку ПК 2, задав IP-адрес, маску подсети и шлюз по умолчанию согласно таблице (см. выше).

Шаг 3. Настройка ПК 3 без подключения

Для целей данной лабораторной работы требуется третий узел.

а. В качестве IP-адреса ПК 3 укажите 192.168.1.5. Маска подсети - 255.255.255.0, шлюз по умолчанию - 192.168.1.1.

б. Подключать этот компьютер к коммутатору на данном этапе не следует. Он будет использоваться позднее для тестирования безопасности.

Шаг 4. Настройка начальной конфигурации коммутатора

а. В качестве имени узла коммутатора задайте **Switch1**.

```
Switch>enable
Switch#config terminal
Switch(config)#hostname Switch1
```

б. В качестве пароля привилегированного режима EXEC укажите **cisco**.

```
Switch1(config)#enable password cisco
```

в. В качестве пароля с шифрованием привилегированного режима EXEC укажите **class**.

```
Switch1(config)#enable secret class
```

г. Укажите необходимость использования пароля в строках виртуального терминала и консоли, а также обязательного запроса пароля при входе в систему.

```
Switch1(config)#line console 0
Switch1(config-line)#password cisco
Switch1(config-line)#login
Switch1(config-line)#line vty 0 15
Switch1(config-line)#password cisco
Switch1(config-line)#login
Switch1(config-line)#end
```

д. Завершите сеанс консоли и войдите в систему снова.

Какой пароль запросила система при входе в привилегированный режим EXEC?

_____

Почему?

_____

Шаг 5. Настройка интерфейса управления коммутатора в сети VLAN 1

а. Войдите в режим конфигурации интерфейса для VLAN 1.

```
Switch1(config)#interface vlan 1
```

б. Задайте IP-адрес, маску подсети и шлюз по умолчанию для интерфейса управления.

```
Switch1(config-if)#ip address 192.168.1.2 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config-if)#exit
Switch1(config)#ip default-gateway 192.168.1.1
Switch1(config)#end
```

Почему интерфейс VLAN1 требует IP-адрес для этой локальной сети?

_____

Для чего предназначен шлюз по умолчанию?

_____

Шаг 6. Проверка настроек управления локальными сетями

а. Убедитесь, что IP-адрес интерфейса управления коммутатора VLAN 1 и IP-адреса ПК 1 и ПК 2 расположены в одной сети. Введите команду **show running-config**, чтобы проверить настройку IP-адреса на коммутаторе.

б. Проверьте настройки интерфейса в VLAN 1.

```
Switch1#show interface vlan 1
```

Какова полоса пропускания этого интерфейса?

_____

Каковы состояния VLAN?

VLAN 1 _____, а линейный протокол _____.

Шаг 7. Отключение функции http-сервера на коммутаторе

Отключите функцию http-сервера на коммутаторе.

```
Switch1(config)#no ip http server
```

Шаг 8. Проверка подключений

а. Для проверки правильной настройки конфигурации узлов и коммутатора выполните с узлов тестирование доступности IP-адреса коммутатора с помощью эхо-запроса.

Успешно ли выполнен эхо-запрос? _____

Если эхо-запрос выполнить не удалось, проверьте подсоединения и конфигурацию еще раз. Убедитесь в том, что все кабели подключены правильно и надежно. Проверьте конфигурацию узла и коммутатора.

б. Сохраните конфигурацию.

Шаг 9. Запись MAC-адресов узлов

Определите и запишите адреса 2-го уровня сетевых интерфейсных плат. В командной строке на каждом компьютере введите **ipconfig /all**.

ПК1 _____

ПК2 _____

ПК3 _____

Шаг 10. Определение MAC-адресов, полученных коммутатором

Выясните, какие MAC-адреса определил коммутатор с помощью команды **show mac-address-table**, введенной в приглашение привилегированного режима EXEC.

```
Switch1#show mac-address-table
```

Сколько динамических адресов присутствует? _____

Сколько всего динамических адресов присутствует? _____

Соответствуют ли MAC-адреса MAC-адресам узла? _____

Шаг 11. Просмотр параметров команды show mac-address-table

Просмотрите параметры, доступные для команды **show mac-address-table**.

```
Switch1(config)#show mac-address-table ?
```

Какие параметры доступны? _____

_____

Шаг 12. Назначение статического MAC-адреса

Задайте статический MAC-адрес на интерфейсе Fa0/4. Используйте адрес, записанный для ПК 2 на шаге 9. MAC-адрес 00e0.2917.1884 используется только в этом примере.

```
Switch1(config)#mac-address-table static 00e0.2917.1884 vlan 1
interface fastethernet 0/4
```

Шаг 13. Проверка результатов

а. Выполните проверку записей в таблице MAC-адресов.

```
Switch1#show mac-address-table
```

Сколько динамических MAC-адресов присутствует сейчас в таблице? _____

Сколько статических MAC-адресов присутствует сейчас в таблице? _____

б. Удалите статический адрес из таблицы MAC-адресов.

```
Switch1(config)#no mac-address-table static 00e0.2917.1884 vlan 1
interface fastethernet 0/4
```

Шаг 14. Перечисление параметров безопасности порта

а. Определите параметры безопасности для интерфейса FastEthernet 0/4.

```
Switch1(config)#interface fastethernet 0/4
Switch1(config-if)#switchport port-security ?
```

Какие параметры доступны? _____

б. Чтобы разрешить порту FastEthernet 0/4 коммутатора принимать только одно устройство, настройте конфигурацию безопасности порта.

```
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport port-security
Switch1(config-if)#switchport port-security mac-address sticky
```

в. Выйдите из режима конфигурации и проверьте настройки безопасности порта.

```
Switch1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Fa0/4        1             0                0            Shutdown
---------------------------------------------------------------------------
```

Что произойдет, если вместо ПК 2 к интерфейсу Fa0/4 попытается подключиться другой узел?

_____

Шаг 15. Ограничение числа узлов для каждого порта

а. На интерфейсе FastEthernet 0/4 установите значение максимального числа MAC-адресов порта в значение 1.

```
Switch1(config-if)#switchport port-security maximum 1.
```

б. Отсоедините ПК, подсоединенный к FastEthernet 0/4. Подсоедините ПК 3 к FastEthernet 0/4. ПК 3 присвоили IP-адрес 192.168.1.5, но он еще не подключен к коммутатору. Чтобы вызвать трафик, возможно, понадобится выполнить тестирование доступности адреса 192.168.1.2 коммутатора.

Зафиксируйте свои наблюдения. _____

_____

Шаг 16. Настройка порта на отключение при нарушении безопасности

а. В случае нарушения безопасности интерфейс отключится. Чтобы порт отключался при нарушении безопасности, введите следующую команду:

```
Switch1(config-if)#switchport port-security violation shutdown
```

Какие еще параметры безопасности порта доступны? _____

_____

б. При необходимости протестируйте доступность адреса 192.168.1.2 коммутатора с ПК 3 192.168.1.5. Этот ПК теперь подключен к интерфейсу FastEthernet 0/4. Это обеспечивает движение трафика от ПК к коммутатору.

в. Зафиксируйте свои наблюдения.

_____

_____

г. Проверьте настройки безопасности порта.

```
Switch1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Fa0/4        1             1                0            Shutdown
---------------------------------------------------------------------------
```

Шаг 17. Отображение информации о конфигурации порта 0/4

Для просмотра информации, касающейся только порта FastEthernet 0/4, введите команду **show interface fastethernet 0/4** в приглашение режима привилегированного доступа EXEC.

```
Switch1#show interface fastethernet 0/4
```

В каком состоянии находится этот интерфейс?

FastEthernet0/4 _____, а линейный протокол _____.

Шаг 18. Повторное включение порта

а. Если произошло нарушение безопасности и порт отключился, воспользуйтесь командой **shutdown/no shutdown** для повторного включения порта.

б. Попробуйте повторно включить порт несколько раз, переключаясь между исходным узлом порта 0/4 и каким-либо новым. Подключите исходный узел, введите команду **no shutdown** на интерфейсе и выполните тестирование связи с помощью команды ping.

Тестирование связи с помощью команды ping следует повторить несколько раз; можно также использовать команду **ping 192.168.1.2 –n 200**. Эта команда устанавливает число пакетов, равное 200, а не 4. Затем поменяйте узлы и повторите попытку.

Шаг 19. Отключение неиспользуемых портов

Отключите любые порты коммутатора, которые не используются.

```
Switch1(config)#interface range Fa0/2 – 3
Switch1(config-if-range)#shutdown
Switch1(config-if-range)#exit
Switch1(config)#interface range Fa0/5 – 24
Switch1(config-if-range)#shutdown

Switch1(config)#interface range gigabitethernet0/1 - 2
Switch1(config-if-range)#shutdown
```

Шаг 20. Вопросы для обсуждения

а. Зачем следует включать безопасность порта на коммутаторе? _____

_____

б. Зачем нужно отключать неиспользуемые порты коммутатора? _____

_____

