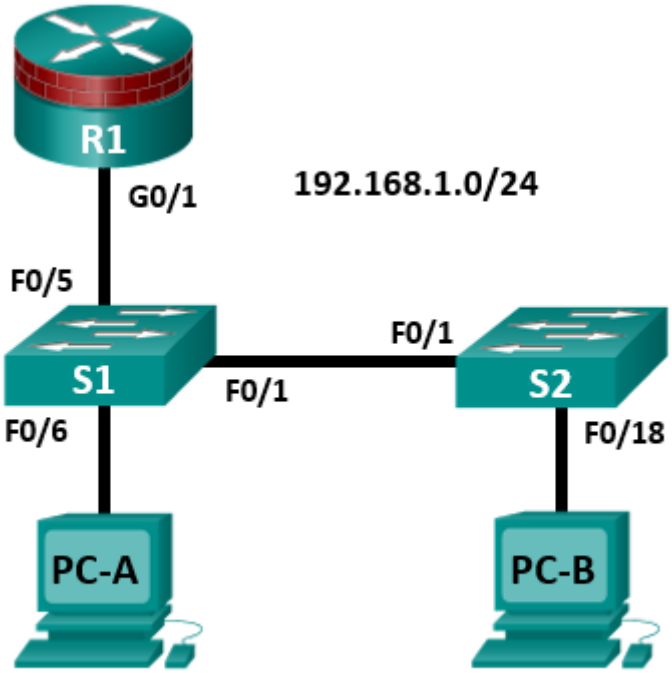
CCNA Security

Лабораторная работа. Защита коммутаторов 2-го уровня

Топология



Примечание. В устройствах ISR G1 используются интерфейсы FastEthernet вместо GigabitEthernet.

Таблица IP-адресов

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию	Порт коммутатора
R1	G0/1	192.168.1.1	255.255.255.0	Н/П	S1 F0/5
S1	VLAN 1	192.168.1.2	255.255.255.0	Н/П	Н/П
S2	VLAN 1	192.168.1.3	255.255.255.0	Н/П	Н/П
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1	S1 F0/6
PC-B	NIC	192.168.1.11	255.255.255.0	192.168.1.1	S2 F0/18

Задачи

Часть 1. Настройка базовых параметров коммутатора

- Создайте топологию.
- Настройте имя хоста, IP-адрес и пароли для доступа.

Часть 2. Настройка IP DHCP Snooping

- Настройте DHCP на маршрутизаторе R1.
- Настройте связь между сетями VLAN на маршрутизаторе R1.
- Настройте интерфейс F0/5 коммутатора S1 как магистральный канал.
- Проверьте работу DHCP на компьютерах PC-A и PC-B.
- Включите DHCP Snooping.
- Проверьте DHCP Snooping.

Исходные данные/сценарий

Инфраструктура на уровне 2 состоит из множества взаимно подключенных коммутаторов Ethernet. Большинство пользовательских устройств, таких как компьютеры, принтеры, IP-телефоны и другие хосты, подключаются к сети через коммутаторы уровня 2. В результате, коммутаторы могут представлять угрозу сетевой безопасности. По аналогии с маршрутизаторами коммутаторы также являются объектом атак внутренних злоумышленников. Программное обеспечение Cisco IOS для коммутаторов предоставляет множество опций по обеспечению безопасности, предназначенных для различных функций и протоколов коммутаторов.

В данной лабораторной работе вы настроите доступ по SSH и безопасность на уровне 2 на коммутаторах S1 и S2. Вы также настроите функцию DHCP Snooping для предотвращения атак истощение DHCP (DHCP Starvation) и поддельный DHCP-сервер (DHCP Spoofing).

Примечание. В данной лабораторной работе используются команды и выходные данные маршрутизатора Cisco 1941 с ПО Cisco IOS версии 15.4(3)M2 (с лицензией Security Technology Package). Команды коммутатора и выходные данные соответствуют коммутаторам Cisco WS-C2960-24TT-L с ОС Cisco IOS Release 15.0(2)SE4 (образ C2960-LANBASEK9-M). Допускается использование других маршрутизаторов, коммутаторов и версий Cisco IOS. См. сводную таблицу по интерфейсам маршрутизаторов в конце этой лабораторной работы для определения идентификаторов интерфейсов с учетом оборудования в лаборатории. Доступные пользователю команды и выходные данные могут различаться в зависимости от используемых версий маршрутизатора, коммутатора и Cisco IOS.

Примечание. Убедитесь, что маршрутизаторы и коммутаторы сброшены и не имеют конфигурацию запуска.

Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с образом Cisco IOS Release 15.4(3)M2 и лицензией Security Technology Package)
- 2 коммутатора (Cisco 2960 с образом IOS с криптографией для поддержки SSH – Release 15.0(2)SE7 или аналогичная)
- 2 ПК (Windows 7 или 8, с установленным SSH-клиентом)
- Кабели Ethernet, как показано на топологической схеме
- Консольные кабели для настройки сетевых устройств Cisco

Часть 1: Настройка базовых параметров коммутатора

В части 1 вы создадите топологию сети и настроите базовые параметры, такие как имена хостов, IP-адреса и пароли для доступа к устройствам.

Шаг 1: Подключите сетевые кабели, как показано на топологической схеме.

Присоедините устройства, как показано на топологической схеме, и установите необходимые кабельные соединения.

Шаг 2: Настройте основные параметры для маршрутизатора и каждого коммутатора.

Все задачи необходимо выполнить на маршрутизаторе R1 и коммутаторах S1 и S2. В качестве примера здесь показана процедура для коммутатора S1.

a. Задайте имена хостов, как показано на топологической схеме.

b. Настройте IP-адреса интерфейсов, как показано в таблице IP-адресов. Следующая конфигурация отображает управляющий интерфейс VLAN 1 на коммутаторе S1.


```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shutdown
```

c. Чтобы предотвратить попытки маршрутизатора или коммутатора неправильно интерпретировать введенные команды, отключите функцию DNS-поиска. В качестве примера здесь приведен коммутатор S1.

```
S1(config)# no ip domain-lookup
```

d. Доступ к коммутатору по HTTP включен по умолчанию. Запретите доступ по HTTP, отключив серверы HTTP и HTTPS.

```
S1(config)# no ip http server
S1(config)# no ip http secure-server
```

Примечание. На коммутаторе должен быть установлен образ IOS с криптографией для поддержки команды **ip http secure-server**. Доступ к маршрутизатору по HTTP отключен по умолчанию.

e. Настройте пароль привилегированного доступа.

```
S1(config)# enable algorithm-type scrypt secret cisco12345
```

f. Установите пароль для консоли.

```
S1(config)# line console 0
S1(config-line)# password ciscoconpass
S1(config-line)# exec-timeout 5 0
S1(config-line)# login
S1(config-line)# logging synchronous
```

Шаг 3: Настройте параметры IP для хостов.

Настройте статический IP-адрес, маску подсети и шлюз по умолчанию для компьютеров PC-A и PC-B, как показано в таблице IP-адресов.

Шаг 4: Проверьте базовую связь по сети.

a. Отправьте эхо-запросы с компьютеров PC-A и PC-B на интерфейс F0/1 маршрутизатора R1 по IP-адресу **192.168.1.1.**

Если запросы завершаются с ошибкой, измените значения основных параметров устройства перед тем, как продолжить работу.

b. Отправьте эхо-запрос с компьютера PC-A на компьютер PC-B.

Если запрос завершается с ошибкой, измените значения основных параметров устройства перед тем, как продолжить работу.

Шаг 5: Сохраните основные конфигурации для маршрутизатора и обоих коммутаторов.

Сохраните текущую конфигурацию в конфигурацию запуска в привилегированном режиме.

```
S1# copy running-config startup-config
```

Часть 2: Настройка DHCP Snooping

DHCP Snooping – это функция системы Cisco Catalyst, позволяющая определить порты, которые могут отвечать на запросы DHCP. Она позволяет только авторизированным серверам DHCP отвечать на запросы DHCP и распределять клиентам информацию о сети.

Задача 1: Настройка DHCP.

Шаг 1: Настройте DHCP на маршрутизаторе R1 для VLAN 1.

```
R1(config)# ip dhcp pool CCNAS
R1(dhcp-config)# network 192.168.1.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.1.1
```



```
R1(config)# ip dhcp excluded-address 192.168.1.1 192.168.1.4
```

Шаг 2: Настройте DHCP на маршрутизаторе R1 для VLAN 20.

```
R1(config)# ip dhcp pool 20Users
R1(dhcp-config)# network 192.168.20.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.20.1
R1(config)# ip dhcp excluded-address 192.168.20.1 192.168.20.4
```

Задача 2: Настройка связи между сетями VLAN.

Шаг 1: Настройте субинтерфейсы на маршрутизаторе R1.

```
R1(config)# interface g0/1
R1(config-if)# shutdown
R1(config-if)# no ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# int g0/1.1
R1(config-if)# encapsulation dot1q 1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# int g0/1.20
R1(config-if)# encapsulation dot1q 20
R1(config-if)# ip address 192.168.20.1 255.255.255.0
```

Шаг 2: Настройте интерфейс F0/5 коммутатора S1 в качестве магистрального порта.

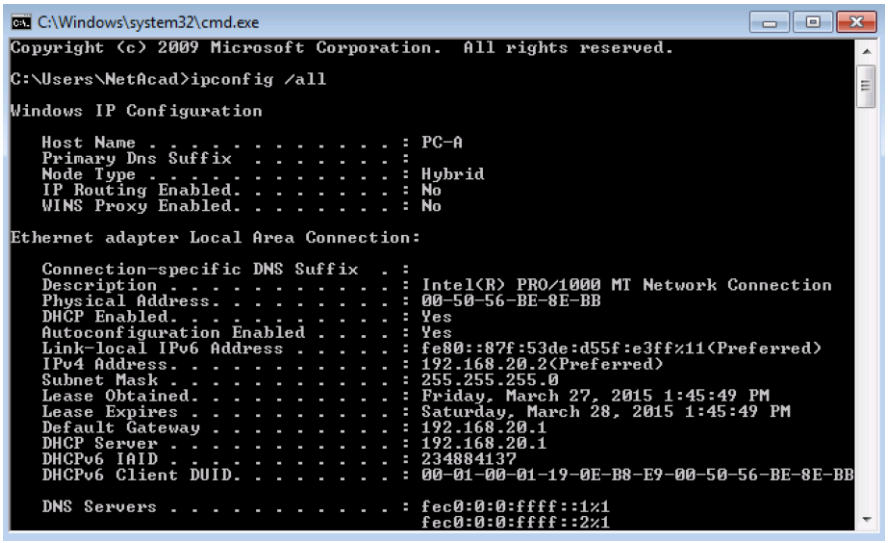
```
S1(config)# int f0/5
S1(config-if)# switchport mode trunk
```

Шаг 3: Настройте компьютеры PC-A и PC-B на получение IP-адреса с помощью DHCP.

Измените сетевые настройки на компьютерах PC-A и PC-B, чтобы они автоматически получали IP-адрес.

Шаг 4: Проверьте функционирование DHCP.

Используйте команду ipconfig в командной строке компьютеров PC-A и PC-B.



Задача 3: Настройка DHCP Snooping.

Шаг 1: Включите глобально функцию DHCP Snooping.

```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping information option
```

Шаг 2: Включите DHCP Snooping для VLAN 1 и 20.

```
S1(config)# ip dhcp snooping vlan 1,20
```

Шаг 3: Ограничьте число DHCP-запросов на интерфейсе.

```
S1(config)# interface f0/6
S1(config-if)# ip dhcp snooping limit rate 10
S1(config-if)# exit
```

Шаг 4: Определите доверенные интерфейсы. Ответы DHCP разрешены только через доверенные порты.

```
S1(config)# interface f0/5
S1(config-if)# description connects to DHCP server
S1(config-if)# ip dhcp snooping trust
```

Шаг 5: Проверьте конфигурацию DHCP Snooping.

```
S1# show ip dhcp snooping

DHCP snooping is configured on following VLANs:
1,20
DHCP snooping is operational on following VLANs:
1,20
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 0022.568a.3a80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
FastEthernet0/5            yes        yes             unlimited
FastEthernet0/6                  no            no              10
```

Шаг 6: Настройте поддельный DHCP на маршрутизаторе R2 для VLAN 20.

```
R2(config)# ip dhcp pool 20Users
R2(dhcp-config)# network 192.168.20.0 255.255.255.0
R2(dhcp-config)# default-router 192.168.20.1
R2(config)# ip dhcp excluded-address 192.168.20.1 192.168.20.4
```

Шаг 7: Проверьте как будет DHCP snooping реагировать на запросы адресной информации с PC-B.

Используйте вначале команду ipconfig /release, а затем ipconfig /renew в командной строке компьютера PC-B.


```
S1#
*Mar  1 03:34:08.570: %DHCP_SNOOPING-5-DHCP_SNOOPING_NONZERO_GIADDR: DHCP_SNOOPING drop message
with non-zero giaddr or option82 value on untrusted port, message type: DHCPDISCOVER, MAC sa:
5254.0091.f2a2
```

Сводная таблица по интерфейсам маршрутизаторов

Сводная таблица по интерфейсам маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet 1**	**Интерфейс Ethernet 2**	**Последовательный интерфейс 1**	**Последовательный интерфейс 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Примечание. Чтобы узнать конфигурацию маршрутизатора, определите его тип по интерфейсам, а также по количеству имеющихся интерфейсов. Эффективно перечислить все комбинации настроек для маршрутизатора каждого класса невозможно. В данной таблице приведены идентификаторы возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов в устройстве. В эту таблицу не включены какие-либо иные типы интерфейсов, даже если в определенном маршрутизаторе они могут присутствовать. В качестве примера можно привести интерфейс ISDN BRI. В строке в скобках приведены официальные аббревиатуры, которые могут использоваться в командах Cisco IOS для представления интерфейсов.

