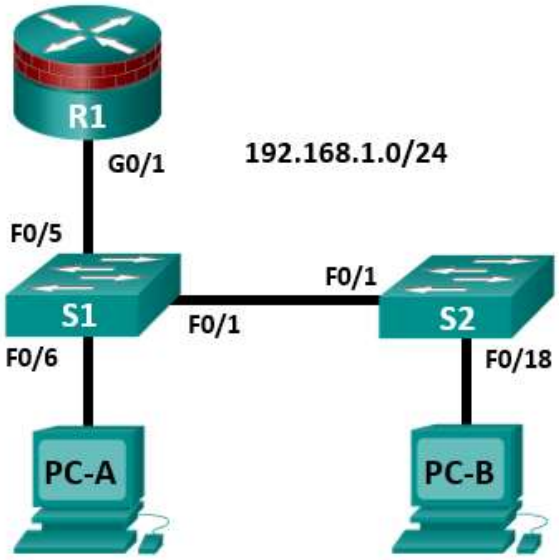
CCNA Security

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 доступа к коммутаторам по SSH

- На коммутаторе настройте доступ по SSH, версия 2.
- Настройте SSH-клиент для доступа к коммутатору.
- Проверьте конфигурацию.

Часть 3. Настройка защищенных магистральных каналов и портов доступа

- Настройте режим магистральных портов.
- Измените нативную VLAN для магистральных портов.
- Проверьте конфигурацию магистральных каналов.
- Включите функцию контроля шторма трафика для широковещательных рассылок.
- Настройте порты доступа.
- Включите PortFast и BPDU Guard.
- Проверьте BPDU Guard.
- Включите Root Guard.
- Включите Loop Guard.
- Настройте и проверьте безопасность портов.
- Отключите неиспользуемые порты.
- Переместите порты из VLAN 1 по умолчанию в другую VLAN.
- Настройте на порте функцию PVLAN Edge.

Часть 4. 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 различные меры защиты коммутаторов, включая функции безопасности портов доступа и Spanning Tree Protocol (STP), такие как BPDU Guard и Root Guard.

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 доступа к коммутаторам по SSH

В части 2 вы настроите на коммутаторах S1 и S2 поддержку подключений по SSH и установите клиентское программное обеспечение SSH на компьютеры.

Примечание. Для настройки SSH требуется образ IOS коммутатора, поддерживающий криптографию. Если используется другая версия образа, вы не сможете указать SSH в качестве входного протокола для линий vty, и команды **crypto** будут недоступны.

Задача 1: Настройка SSH-сервера на маршрутизаторах S1 и S2 с помощью CLI.

В этой задаче с помощью CLI настройте безопасное управление коммутатором посредством SSH вместо Telnet. Secure Shell (SSH) – это сетевой протокол, предназначенный для установления защищенного соединения с эмуляцией терминала с коммутатором или иным сетевым устройством. SSH шифрует все сведения, которые поступают по сетевому каналу, и обеспечивает аутентификацию удаленного компьютера. SSH быстро заменяет Telnet в качестве инструмента удаленного входа в систему для специалистов по сетям. В рабочих сетях крайне рекомендуется использовать SSH вместо Telnet.

Примечание. Для поддержки SSH коммутатор должен быть настроен на использование локальной аутентификации или AAA.

Шаг 1: Настройте доменное имя.

Войдите в режим глобальной настройки и задайте доменное имя.

```
S1# conf t
S1(config)# ip domain-name ccnasecurity.com
```

Шаг 2: Настройте привилегированного пользователя для входа через SSH-клиент.

Используйте команду **username**, чтобы создать ID пользователя с наиболее высоким уровнем привилегий и секретным паролем.

```
S1(config)# username admin privilege 15 algorithm-type scrypt secret cisco12345
```


Шаг 3: Сгенерируйте пару ключей шифрования RSA для маршрутизатора.

Коммутатор использует пару ключей RSA для аутентификации и шифрования передаваемых SSH-данных.

Задайте количество битов модуля для RSA-ключей, равное **1024**. Значение по умолчанию – 512, диапазон – от 360 до 2048.

```
S1(config)# crypto key generate rsa general-keys modulus 1024
 The name for the keys will be: S1.ccnasecurity.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#
00:15:36: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Шаг 4: Включите SSH версии 2.

```
S1(config)# ip ssh version 2
```

Шаг 5: Проверьте конфигурацию SSH.

a. Используйте команду **show ip ssh** для просмотра текущих настроек.

```
S1# show ip ssh
```

b. Заполните следующую информацию на основе выходных данных для команды **show ip ssh.**

Активная версия SSH: _____

Время ожидания аутентификации: _____

Повторные попытки аутентификации: _____

Шаг 6: Настройте время ожидания SSH и параметры аутентификации.

Значения времени ожидания и параметров аутентификации SSH по умолчанию можно изменить на более ограничительные с помощью следующих команд.

```
S1(config)# ip ssh time-out 90
S1(config)# ip ssh authentication-retries 2
```

Шаг 7: Настройте входящие линии vty.

a. Настройте доступ по vty на линиях 0–4. Установите уровень привилегий 15. Это позволит пользователю с самым высоким уровнем привилегий (**15**) при доступе к линиям vty автоматически переходить в привилегированный режим. Остальные пользователи по умолчанию будут переходить в пользовательский режим. Установите для учетных записей локальных пользователей обязательный вход в систему и проверку, а также прием только SSH-подключений.

```
S1(config)# line vty 0 4
S1(config-line)# privilege level 15
S1(config-line)# exec-timeout 5 0
S1(config-line)# login local
S1(config-line)# transport input ssh
S1(config-line)# exit
```

b. Отключите вход в систему на линиях vty 5–15 коммутатора путем запрета транспортного входа.

```
S1(config)# line vty 5 15
S1(config-line)# transport input none
```


Шаг 8: Сохраните текущую конфигурацию в конфигурацию запуска.

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

Задача 2: Настройка клиента SSH.

PuTTy и Tera Term – это программы эмуляции терминала, которые могут поддерживать клиентские подключения по SSHv2. В данной лабораторной работе используется PuTTY.

Шаг 1: (Необязательно) Скачайте и установите SSH-клиент на компьютеры PC-A и PC-B.

Если SSH-клиент еще не установлен, скачайте PuTTY по следующей ссылке:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

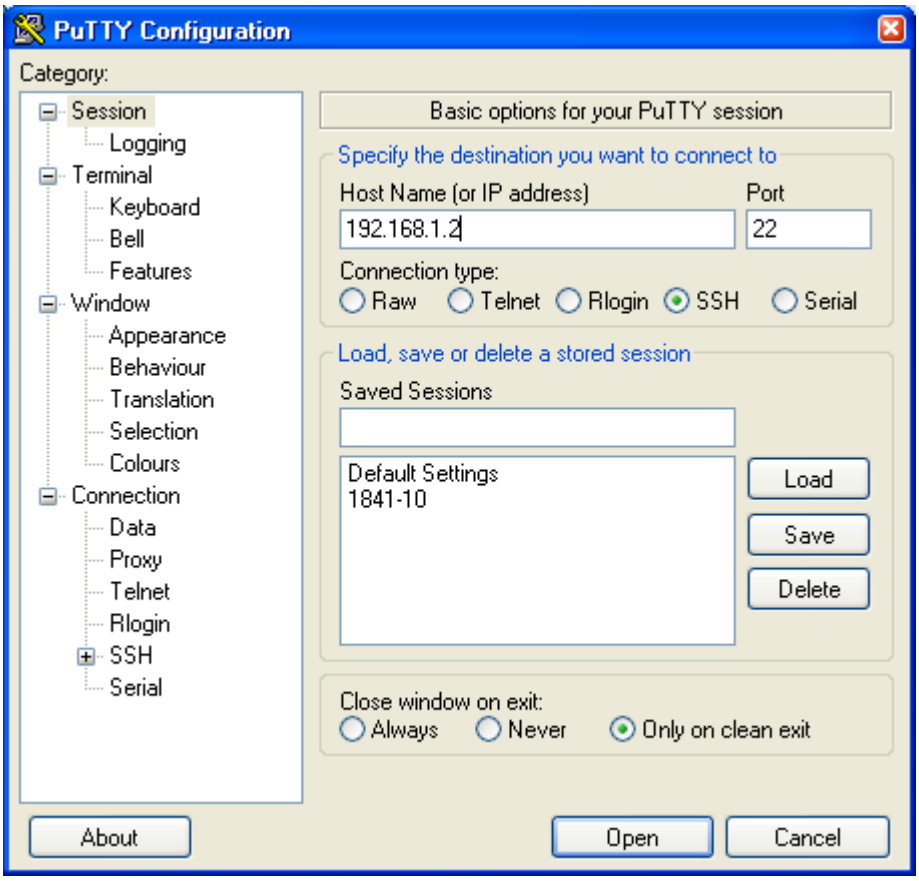
Примечание. Данная процедура предназначена для PuTTY и относится к компьютеру PC-A.

Шаг 2: Проверьте связь по SSH между компьютером PC-A и коммутатором S1.

a. Запустите PuTTY, дважды щелкнув значок **putty.exe** (при получении запроса нажмите **Run**).

b. В поле **Host Name (or IP address)** введите IP-адрес коммутатора S1 **192.168.1.2.**

c. Убедитесь, что выбран переключатель **SSH.** PuTTY по умолчанию использует SSH версии 2.

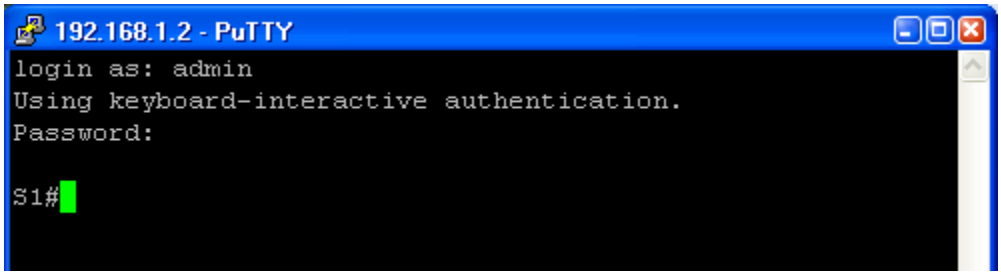


d. Нажмите **Open**.

Примечание. При первом подключении пользователю выдается запрос PuTTY Security Alert, сообщающий, что ключ хоста сервера не сохранен в реестре.

e. В окне PuTTY Security Alert нажмите **Yes,** чтобы сохранить в кеше ключ хоста сервера.

f. В окне PuTTY введите имя пользователя **admin** и пароль **cisco12345.**



g. В привилегированном режиме для коммутатора S1 введите команду **show users**.

```
S1# show users
```

Какие пользователи сейчас подключены к коммутатору S1?

_____

_____

h. Закройте окно сеанса PuTTY SSH с помощью команды **exit** или **quit.**

Попытайтесь открыть сеанс Telnet с коммутатором S1 через PC-A. Вам удалось это сделать? Поясните ответ.

_____

_____

Шаг 3: Сохраните конфигурацию.

Сохраните текущую конфигурацию в конфигурацию запуска в привилегированном режиме.

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

Часть 3: Настройка защищенных магистральных каналов и портов доступа

В части 3 вы настроите магистральные порты, измените нативную VLAN для магистральных портов и проверите конфигурацию магистральных каналов.

Защита магистральных портов позволит остановить атаки перехода в сетях VLAN. Лучшим способом предотвращения базовой атаки перехода в сетях VLAN является явное отключение транкинга на всех портах, кроме тех, которым транкинг необходим. На нужных магистральных портах отключите согласования DTP (автоматический транкинг) и включите транкинг вручную. Если на интерфейсе транкинг не требуется, настройте порт как порт доступа. Это отключает транкинг на интерфейсе.

Примечание. Задачи необходимо выполнить на коммутаторах S1 и S2, как указано.

Задача 1: Защита магистральных портов.

Шаг 1: Настройте S1 в качестве корневого коммутатора.

Для данной лабораторной работы коммутатор S2 на данный момент выполняет роль корневого моста. Вы настроите коммутатор S1 в качестве корневого моста. Для этого следует изменить уровень приоритета ID моста.

a. Войдите в режим глобальной настройки с консоли коммутатора S1.

b. Приоритет по умолчанию для коммутаторов S1 и S2 – 32769 (32768 + 1 с System ID Extension). Установите для коммутатора S1 приоритет **0**, чтобы он стал корневым коммутатором.

```
S1(config)# spanning-tree vlan 1 priority 0
S1(config)# exit
```

Примечание. Чтобы сделать коммутатор S1 корневым для VLAN 1, также можно использовать команду **spanning-tree vlan 1 root primary**.

c. Введите команду **show spanning-tree** и убедитесь, что коммутатор S1 является корневым мостом, определите используемые порты и их состояние.

```
S1# show spanning-tree

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    1
              Address     001d.4635.0c80
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    1      (priority 0 sys-id-ext 1)
              Address     001d.4635.0c80
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Fa0/6            Desg FWD 19        128.6    P2p
```

d. Какой приоритет имеет коммутатор S1?

_____

Какие порты используются и каково их состояние?

_____

_____

Шаг 2: Настройте магистральные порты на коммутаторах S1 и S2.

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

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

Примечание. Если в лабораторной работе используется коммутатор 3560, пользователь должен сначала ввести команду **switchport trunk encapsulation dot1q.**

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

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


c. Убедитесь, что порт F0/1 на коммутаторе S1 работает в магистральном (транкинговом) режиме, с помощью команды **show interfaces trunk**.

```
S1# show interfaces 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

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

Шаг 3: Измените нативную VLAN для магистральных портов на коммутаторах S1 и S2.

a. Благодаря изменению нативной VLAN для магистральных портов на неиспользуемую VLAN можно предотвращать атаки перехода по сетям VLAN.

Учитывая выходные данные команды **show interfaces trunk** на предыдущем шаге, какая VLAN является нативной для магистрального интерфейса F0/1 коммутатора S1?

_____

b. Установите в качестве нативной VLAN магистрального интерфейса F0/1 коммутатора S1 неиспользуемую сеть VLAN 99.

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

c. Следующее сообщение должно появиться через короткое время:

```
02:16:28: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (99),
with S2 FastEthernet0/1 (1).
```

Что означает данное сообщение?

_____

_____

_____

_____

d. Установите в качестве нативной VLAN на магистральном интерфейсе F0/1 коммутатора S2 сеть VLAN 99.

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


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

Благодаря установке значения **nonegotiate** для магистрального порта также можно нейтрализовывать атаки перехода по сетям VLAN, так как выключается операция генерации кадров DTP.

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

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

Шаг 5: Проверьте конфигурацию транкинга на порте F0/1.

```
S1# show interfaces f0/1 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

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1

S1# show interfaces 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
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (Inactive)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
```



```
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Шаг 6: Проверьте конфигурацию с помощью команды show run.

С помощью команды **show run** отобразите текущую конфигурацию, начиная с первой строки, где встречается «0/1».

```
S1# show run | begin 0/1
interface FastEthernet0/1
 switchport trunk native vlan 99
 switchport mode trunk
 switchport nonegotiate

<output omitted>
```

Задача 2: Защита портов доступа.

В ходе атак на сеть злоумышленники стремятся замаскировать свою систему или мошеннический коммутатор, который они добавили в топологическую схему, и представить их в виде корневого моста путем изменения параметров STP корневого моста. Если порт, настроенный с функцией PortFast, получает пакет BPDU, STP может заблокировать порт с помощью функции BPDU Guard.

Шаг 1: Отключите транкинг на портах доступа коммутатора S1.

a. На коммутаторе S1 настройте для Fa0/5 (порт, к которому подключен маршрутизатор R1) только режим доступа.

```
S1(config)# interface f0/5
S1(config-if)# switchport mode access
```

b. На коммутаторе S1 настройте для Fa0/6 (порт, к которому подключен PC-A) только режим доступа.

```
S1(config)# interface f0/6
S1(config-if)# switchport mode access
```

Шаг 2: Отключите транкинг на портах доступа коммутатора S2.

На коммутаторе S2 настройте для Fa0/18 (порт, к которому подключен PC-B) только режим доступа.

```
S2(config)# interface f0/18
S2(config-if)# switchport mode access
```

Задача 3: Защита от атак на STP.

В топологической схеме есть всего лишь два коммутатора и нет резервных трактов, однако протокол STP по-прежнему активен. На данном шаге необходимо включить функции безопасности коммутатора, которые позволят помешать злоумышленникам манипулировать коммутаторами с помощью специальных методов для STP.

Шаг 1: Включите PortFast на портах доступа коммутаторов S1 и S2.

Функция PortFast настроена на портах доступа, подключенных к компьютеру или серверу, что позволяет им намного быстрее становиться активными.

a. Включите PortFast на порте доступа Fa0/5 коммутатора S1.

```
S1(config)# interface f0/5
S1(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs,
concentrators, switches, bridges, etc... to this interface when portfast is enabled, can cause
temporary bridging loops. Use with CAUTION

%Portfast has been configured on FastEthernet0/5 but will only
 have effect when the interface is in a non-trunking mode.
```

b. Включите PortFast на порте доступа Fa0/6 коммутатора S1.

```
S1(config)# interface f0/6
S1(config-if)# spanning-tree portfast
```

c. Включите PortFast на порте доступа Fa0/18 коммутатора S2.

```
S2(config)# interface f0/18
S2(config-if)# spanning-tree portfast
```

Шаг 2: Включите функцию BPDU Guard на портах доступа коммутаторов S1 и S2.

BPDU Guard – это функция, позволяющая предотвращать появление мошеннических коммутаторов и спуфинг на портах доступа.

a. Включите BPDU Guard на порте F0/6 коммутатора.

```
S1(config)# interface f0/6
S1(config-if)# spanning-tree bpduguard enable

S2(config)# interface f0/18
S2(config-if)# spanning-tree bpduguard enable
```

Примечание. Функции PortFast и BPDU Guard также можно включить глобально с помощью команд **spanning-tree portfast default** и **spanning-tree portfast bpduguard** в режиме глобальной настройки.

Примечание. BPDU Guard можно включить на всех портах доступа, на которых включена функция PortFast. Эти порты не должны никогда получать пакеты BPDU. BPDU Guard лучше всего развернуть на пользовательских портах, чтобы предотвращать добавление злоумышленниками мошеннических коммутаторов в сеть. Если в порте включена функция BPDU Guard и на него поступает пакет BPDU, порт отключается, и его необходимо будет снова включить вручную. На порте также можно настроить параметр **err-disable timeout,** чтобы порт мог автоматически восстанавливаться по окончании заданного периода времени.

b. Убедитесь, что функция BPDU Guard включена, с помощью команды **show spanning-tree interface f0/6 detail** на коммутаторе S1.

```
S1# show spanning-tree interface f0/6 detail

Port 6 (FastEthernet0/6) of VLAN0001 is designated forwarding
   Port path cost 19, Port priority 128, Port Identifier 128.6.
   Designated root has priority 1, address 001d.4635.0c80
   Designated bridge has priority 1, address 001d.4635.0c80
   Designated port id is 128.6, designated path cost 0
   Timers: message age 0, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   The port is in the portfast mode
   Link type is point-to-point by default
   Bpdu guard is enabled
   BPDU: sent 3349, received 0
```


Шаг 3: Включите Root Guard.

BPDU Guard – это еще одна функция, позволяющая предотвращать появление мошеннических коммутаторов и спуфинг. BPDU Guard можно включить на всех портах коммутатора, которые не являются корневыми. Обычно эта функция включена на портах, подключенных к граничным коммутаторам, которые никогда не должны получать пакеты BPDU более высокого уровня. Каждый коммутатор должен иметь только один корневой порт, который является наилучшим путем к корневому коммутатору.

a. Следующая команда позволяет настроить функцию Root Guard на интерфейсе Gi0/1 коммутатора S2. Обычно это делается в случае, когда к этому порту подключен другой коммутатор. Root Guard лучше всего устанавливать на портах, к которым подключены коммутаторы, которые не должны быть корневыми мостами. В топологической схеме лабораторной работы порт F0/1 на коммутаторе S1 является наиболее логичным претендентом для функции Root Guard. Однако в качестве примера показан порт Gi0/1 коммутатора S2, потому что для соединения между коммутаторами чаще всего используются порты Gigabit.

```
S2(config)# interface g0/1
S2(config-if)# spanning-tree guard root
```

b. С помощью команды **show run | begin Gig** убедитесь, что функция Root Guard настроена.

```
S2# show run | begin Gig
interface GigabitEthernet0/1
 spanning-tree guard root
```

Примечание. Порт Gi0/1 коммутатора S2 в данный момент неактивен, соответственно, он не участвует в STP. В противном случае, вы могли бы использовать команду **show spanning-tree interface Gi0/1 detail.**

Примечание. Выражение в команде **show run | begin** чувствительно к регистру.

c. Если на порт, где включена функция BPDU Guard, поступает пакет BPDU более высокого уровня, он переходит в состояние root-inconsistent. С помощью команды **show spanning-tree inconsistentports** определите наличие портов, которые в настоящее время получают пакеты BPDU более высокого уровня, которые поступать не должны.

```
S2# show spanning-tree inconsistentports

Name                 Interface              Inconsistency
-------------------- ---------------------- ------------------
Number of inconsistent ports (segments) in the system : 0
```

Примечание. Функция Root Guard позволяет подключенному коммутатору участвовать в STP до тех пор, пока устройство не попытается стать корневым. Если Root Guard блокирует порт, его последующее восстановление произойдет автоматически. Порт возвращается в состояние пересылки после прекращения поступления сообщений BPDU более высокого уровня.

Шаг 4: Включите Loop Guard.

Функция STP Loop Guard обеспечивает дополнительную защиту от закольцовывания при передаче на уровне 2 (петель STP). Петля STP появляется, когда порт в состоянии блокировки STP в топологии с резервированием ошибочно переходит в состояние пересылки. Обычно это происходит из-за того, что один из портов топологии с физическим резервированием (необязательно порт с блокировкой STP) больше не получает пакеты STP BPDU. Если все порты находятся в состоянии пересылки (forwarding), то это приводит к появлению петель (закольцовывания). Если порт, на котором включена функция Loop Guard, перестает получать пакеты BPDU из назначенного порта в сегменте, он переходит в состояние loop inconsistent вместо перехода в состояние forwarding. Как правило, состояние loop inconsistent является блокирующим, поэтому никакой трафик не пересылается. Если порт снова обнаруживает пакеты BPDU, он автоматически восстанавливается и переходит в состояние блокировки (blocking).

a. Функцию Loop Guard следует применять к неназначенным портам. Таким образом, на некорневых коммутаторах может быть настроена глобальная команда.

```
S2(config)# spanning-tree loopguard default
```


b. Проверьте конфигурацию Loopguard.

```
S2# show spanning-tree summary
Switch is in pvst mode

Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is enabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                    0         0        0          3          3
---------------------- -------- --------- -------- ---------- ----------
```

Задача 4: Настройка безопасности портов и отключение неиспользуемых портов.

Коммутаторы могут подвергаться атакам на таблицу CAM, также называемую таблицей MAC-адресов, атакам с переполнением, атакам со спуфингом MAC-адресов, а также попыткам неавторизованного подключения к портам коммутатора. В этой задаче необходимо настроить функцию безопасности портов (port security) для ограничения количества MAC-адресов, которые могут быть изучены на портах коммутатора, и отключения порта в случае превышения этого количества.

Шаг 1: Запишите MAC-адрес интерфейса Fa0/0 маршрутизатора R1.

В CLI на маршрутизаторе R1 используйте команду **show interface** и запишите MAC-адрес интерфейса.

```
R1# show interfaces g0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e1 (bia fc99.4775.c3e1)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
<Output Omitted>
```

Какой MAC-адрес имеет интерфейс G0/1 маршрутизатора R1?

_____

_____

Шаг 2: Настройте базовый уровень безопасности портов.

Данную процедуру следует выполнить на всех используемых портах доступа. В качестве примера здесь приведен порт Fa0/5 коммутатора S1.

a. В CLI коммутатора S1 войдите в режим интерфейсной настройки порта, подключенного к маршрутизатору (Fast Ethernet 0/5).

```
S1(config)# interface f0/5
```

b. Выключите порт коммутатора.

```
S1(config-if)# shutdown
```

c. Включите функцию безопасности портов (port security) на порте.

```
S1(config-if)# switchport port-security
```

Примечание. Порт коммутатора должен быть настроен как порт доступа для включения безопасности портов.

Примечание. Если ввести только команду **switchport port-security**, будет установлено максимальное количество MAC-адресов, равное **1,** и действие при нарушении – **shutdown**. Для изменения поведения по умолчанию можно использовать команды **switchport port-security maximum** и **switchport port-security violation**.

d. Настройте статическую запись для MAC-адреса интерфейса Fa0/1/ маршрутизатора R1, записанного на шаге 1.

```
S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx
```

Примечание. *xxxx.xxxx.xxxx* – фактический MAC-адрес интерфейса G0/1 маршрутизатора.

Примечание. Вы также можете использовать команду **switchport port-security mac-address sticky**, чтобы добавить все безопасные MAC-адреса, которые динамически сохранены на порте (в пределах их максимального количества) в текущую конфигурацию коммутатора.

e. Включите порт коммутатора.

```
S1(config-if)# no shutdown
```

Шаг 3: Проверьте безопасность портов на интерфейсе Fa0/5 коммутатора S1.

a. На коммутаторе S1 введите команду **show port-security** и убедитесь, что безопасность портов настроена на его интерфейсе F0/5.

```
S1# show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Каково число нарушений безопасности? _____

Каково состояние порта F0/5?

_____

_____

Какое значение имеют Last Source Address и VLAN?

_____

_____

b. В CLI маршрутизатора R1 отправьте эхо-запрос на PC-A, чтобы проверить связь. Это также позволит убедиться, что MAC-адрес интерфейса Fa0/1 маршрутизатора R1 сохранен (изучен) на коммутаторе.

```
R1# ping 192.168.1.10
```

c. Теперь нарушьте правило безопасности: измените MAC-адрес интерфейса маршрутизатора. Войдите в режим интерфейсной настройки для Fast Ethernet 0/1. Настройте MAC-адрес интерфейса, используя значение **aaaa.bbbb.cccc.**

```
R1(config)# interface G0/1
R1(config-if)# mac-address aaaa.bbbb.cccc
R1(config-if)# end
```

Примечание. Для получения аналогичных результатов вы также можете изменить MAC-адрес ПК, подключенного к порту F0/6 коммутатора S1.

d. В CLI маршрутизатора R1 отправьте эхо-запрос на компьютер PC-A. Запрос выполнен успешно? Поясните ответ.

_____

_____

e. На консоли коммутатора S1 посмотрите сообщения, когда порт F0/5 обнаруживает недопустимый MAC-адрес.

```
*Jan 14 01:34:39.750: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/5, putting Fa0/5
in err-disable state
*Jan 14 01:34:39.750: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused
by MAC address aaaa.bbbb.cccc on port FastEthernet0/5.
*Jan 14 01:34:40.756: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed
state to down
*Jan 14 01:34:41.755: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to down
```

f. На коммутаторе введите команду **show port-security** и убедитесь, что безопасность портов была нарушена.

```
S1# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)         (Count)
---------------------------------------------------------------------
      Fa0/5            1           1                 1         Shutdown
---------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192

S1# show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : aaaa.bbbb.cccc:1
Security Violation Count   : 1
```



```
S1# show port-security address
Secure Mac Address Table
------------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                    (mins)
----    -----------       ----                          -----   -------------
   1    fc99.4775.c3e1    SecureConfigured              Fa0/5        -
------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 8192
```

g. Удалите жестко закодированный MAC-адрес из маршрутизатора и снова включите интерфейс Fast Ethernet 0/1.

```
R1(config)# interface g0/1
R1(config-if)# no mac-address aaaa.bbbb.cccc
```

Примечание. Это действие восстановит исходный MAC-адрес интерфейса FastEthernet.

На маршрутизаторе R1 попробуйте снова отправить эхо-запрос на компьютер PC-A по адресу 192.168.1.10. Эхо-запрос выполнен успешно? Почему?

_____

_____

Шаг 4: Сбросьте состояние error disabled порта Fa0/5 коммутатора S1.

a. На консоли коммутатора S1 сбросьте ошибку и снова включите порт с помощью команд, приведенных в следующем примере. Это изменит состояние порта с Secure-shutdown на Secure-up.

```
S1(config)# interface f0/5
S1(config-if)# shutdown
S1(config-if)# no shutdown
```

Примечание. Это предполагает, что устройство/интерфейс с недопустимым MAC-адресом было удалено или на нем была восстановлена исходная конфигурация устройства или интерфейсов.

b. Снова отправьте эхо-запрос на компьютер PC-A с маршрутизатора R1. На этот раз запрос должен быть выполнен успешно.

```
R1# ping 192.168.1.10
```

Шаг 5: Удалите базовую безопасность портов на порте Fa0/5 коммутатора S1.

На консоли коммутатора S1 удалите безопасность портов на Fa0/5. Эту процедуру также можно использовать для повторного включения порта, но команды **port security** должны быть перенастроены.

```
S1(config)# interface f0/5
S1(config-if)# no switchport port-security
S1(config-if)# no switchport port-security mac-address fc99.4775.c3e1
```

Вы также можете использовать следующие команды для сброса настроек интерфейса в значения по умолчанию:

```
S1(config)# default interface f0/5
S1(config)# interface f0/5
```

Примечание. Для команды **default interface** также необходимо перенастроить порт как порт доступа, чтобы снова включить команды безопасности.

Шаг 6: (Необязательно) Настройте безопасность портов для VoIP.

В данном примере показаны типовые настройки безопасности для голосового порта. Разрешены три MAC-адреса, и они должны быть сохранены (изучены) динамически. Один MAC-адрес предназначен для IP телефона, второй – для коммутатора и третий – для ПК, подключенного к IP-телефону. В случае нарушения данной политики порт будет выключен. Время устаревания для изученных MAC-адресов установлено равным двум часам.

В следующем примере показан порт F0/18 коммутатора S2.

```
S2(config)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport port-security
S2(config-if)# switchport port-security maximum 3
S2(config-if)# switchport port-security violation shutdown
S2(config-if)# switchport port-security aging time 120
```

Шаг 7: Отключите неиспользуемые порты на коммутаторах S1 и S2.

В качестве дополнительной меры безопасности выключите порты, которые не используются на коммутаторе.

a. На коммутаторе S1 используются порты F0/1, F0/5 и F0/6. Остальные порты Fast Ethernet и два порта Gigabit Ethernet будут отключены.

```
S1(config)# interface range f0/2 - 4
S1(config-if-range)# shutdown
S1(config-if-range)# interface range f0/7 - 24
S1(config-if-range)# shutdown
S1(config-if-range)# interface range g0/1 - 2
S1(config-if-range)# shutdown
```

b. На коммутаторе S2 используются порты Fa0/1 и Fa0/18. Остальные порты Fast Ethernet и Gigabit Ethernet будут отключены.

```
S2(config)# interface range f0/2 – 17 , f0/19 – 24 , g0/1 - 2
S2(config-if-range)# shutdown
```

Шаг 8: Переместите активные порты в сеть VLAN, отличную от сети VLAN 1 по умолчанию.

В качестве дополнительной меры безопасности вы можете переместить все активные пользовательские порты и порты маршрутизатора в сеть VLAN, отличную от VLAN 1 по умолчанию, в обоих коммутаторах.

a. Настройте новую VLAN для пользователей в обоих коммутаторах с помощью следующих команд:

```
S1(config)# vlan 20
S1(config-vlan)# name Users

S2(config)# vlan 20
S2(config-vlan)# name Users
```

b. Добавьте текущие активные порты доступа (не магистральные) в новую VLAN.

```
S1(config)# interface f0/6
S1(config-if-range)# switchport access vlan 20

S2(config)# interface f0/18
S2(config-if)# switchport access vlan 20
```


Примечание. Это позволит заблокировать связь между пользовательскими хостами и IP-адресами управляющей сети VLAN коммутатора, которой в данный момент является VLAN 1. Коммутатор все еще доступен и может быть настроен с помощью консольного подключения.

Примечание. Для организации доступа к коммутатору по SSH необходимо назначить отдельный порт в качестве управляющего и добавить его во VLAN 1, в которую включена специальная управляющая рабочая станция. Более продуманным решением является создание новой сети VLAN для управления коммутаторами (или использование существующей нативной сети для магистральных каналов VLAN 99) и настроить отдельную подсеть для управляющей и пользовательских сетей VLAN. В части 4 необходимо включить транкинг с субинтерфейсами на маршрутизаторе R1 для обеспечения связи между управляющей VLAN и пользовательскими сетями VLAN.

Шаг 9: Настройте порт с функцией PVLAN Edge.

Для некоторых приложений требуется отсутствие передачи трафика между портами одного коммутатора на уровне 2, чтобы один сосед не видел трафик, генерируемый другим соседом. Использование функции Private VLAN (PVLAN) Edge, также называемой защищенными портами, в подобной среде гарантирует отсутствие обмена одноадресным, широковещательным или групповым трафиком между этими портами коммутатора. Функция PVLAN Edge может быть реализована только на портах одного коммутатора и имеет локальное значение.

Например, чтобы предотвратить обмен трафиком между компьютером PC-A на коммутаторе S1 (порт Fa0/6) и хостом на другом порте в S1 (к примеру, Fa0/7, который был до этого отключен), можно использовать команду **switchport protected** для активации функции PVLAN Edge на этих двух портах. Используйте команду в режиме интерфейсной настройки **no switchport protected** для отключения защищенного порта.

a. В режиме интерфейсной настройки настройте функцию PVLAN Edge с помощью следующих команд:

```
S1(config)# interface f0/6
S1(config-if)# switchport protected
S1(config-if)# interface f0/7
S1(config-if)# switchport protected
S1(config-if)# no shut
S1(config-if)# end
```

b. Убедитесь, что функция PVLAN Edge (защищенный порт) включена на порте Fa0/6.

```
S1# show interfaces fa0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 20 (Users)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
```



```
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: true
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

c. Деактивируйте защищенный порт на интерфейсах Fa0/6 и Fa0/7, используя следующие команды:

```
S1(config)# interface range f0/6 - 7
S1(config-if-range)# no switchport protected
```

Часть 4: 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
```

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
R1(config-if)# int g0/1.99
R1(config-if)# encapsulation dot1q 99
R1(config-if)# ip address 192.168.99.1 255.255.255.0
```


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

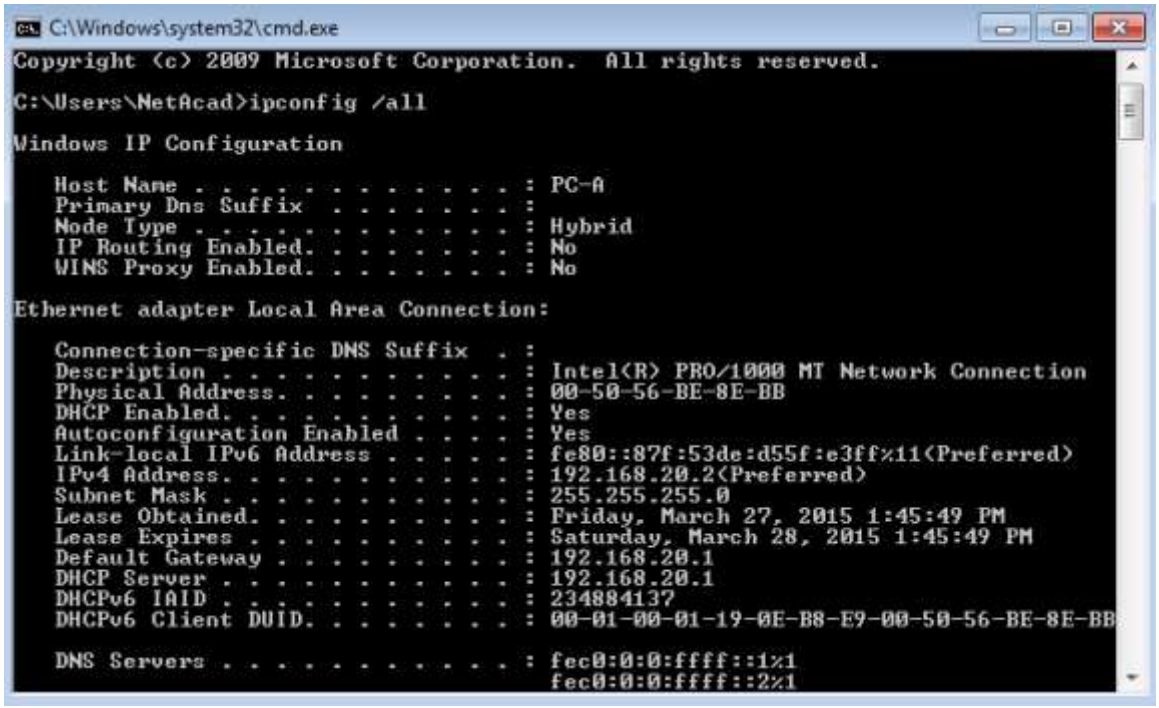
```
S1(config)# int f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
```

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
```


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.

