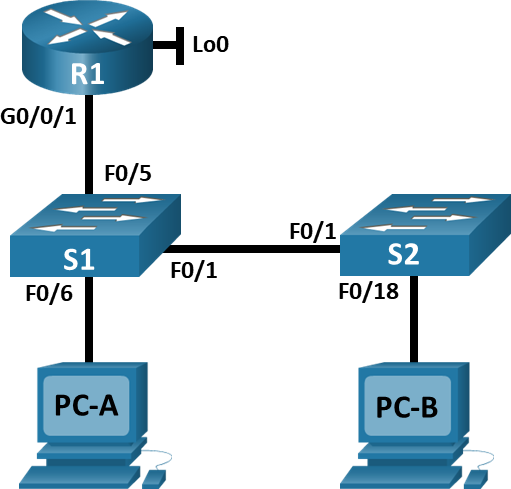
Лабораторная работа № 7: Конфигурация безопасности коммутатора

**Выполнил студент: Ло Ван Хунг (X=15)**

**Группа: ИНБО-04-20**

**Топология**



**Таблица адресации**

|  |  |  |  |
| --- | --- | --- | --- |
| **Устройство** | **interface/vlan** | **IP-адрес** | **Маска подсети** |
| R1\_Lo | G0/0/1 | 192.168.25.1 | 255.255.255.0 |
| Loopback 0 | 10.10.1.1 | 255.255.255.0 |
| S1 | VLAN 16 | 192.168.25.201 | 255.255.255.0 |
| S2 | VLAN 16 | 192.168.25.202 | 255.255.255.0 |
| PC A | NIC | DHCP | 255.255.255.0 |
| PC B | NIC | DHCP | 255.255.255.0 |

**Цели**

### Часть 1. Настройка основного сетевого устройства

* Создайте сеть.
* Настройте маршрутизатор R1\_ФАМИЛИЯ.
* Настройка и проверка основных параметров коммутатора

### Часть 2. Настройка сетей VLAN

* Сконфигруриуйте VLAN X+10.
* Сконфигруриуйте SVI для VLAN X+10.
* Настройте VLAN 333 с именем Native на S1 и S2.
* Настройте VLAN 999 с именем ParkingLot на S1 и S2.

### Часть 3: Настройки безопасности коммутатора.

* Реализация магистральных соединений 802.1Q.
* Настройка портов доступа
* Безопасность неиспользуемых портов коммутатора
* Документирование и реализация функций безопасности порта.
* Реализовать безопасность DHCP snooping .
* Реализация PortFast и BPDU Guard
* Проверка сквозной связанности.

**Необходимые ресурсы**

* 1 Маршрутизатор (Cisco 4221 с универсальным образом Cisco IOS XE версии 16.9.3 или аналогичным)
* 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
* 2 ПК (ОС Windows с программой эмуляции терминалов, такой как Tera Term)
* Консольные кабели для настройки устройств Cisco IOS через консольные порты.
* Кабели Ethernet, расположенные в соответствии с топологией

**Инструкции**

# Часть 1. Настройка основного сетевого устройства

## Шаг 1. Создайте сеть.

1. Создайте сеть согласно топологии.
2. Инициализация устройств

Изображение выглядит как диаграмма

Автоматически созданное описание

## Шаг 2. Настройте маршрутизатор R1\_ФАМИЛИЯ.

1. Загрузите следующий конфигурационный скрипт на R1\_Dinh.

enable

configure terminal hostname R1\_Lo

no ip domain lookup

ip dhcp excluded-address 192.168.25.1 192.168.25.9

ip dhcp excluded-address 192.168.25.201 192.168.25.202

!

ip dhcp pool Students

network 192.168.25.0 255.255.255.0

default-router 192.168.25.1 domain-name CCNA2.Lab-7

!

interface Loopback0

ip address 10.10.1.1 255.255.255.0

!

interface GigabitEthernet0/0/1 description Link to S1

ip dhcp relay information trust-all

interface GigabitEthernet0/0/1

ip address 192.168.25.1 255.255.255.0

no shutdown

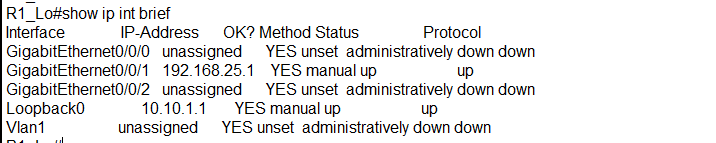
!

line con 0

logging synchronous exec-timeout 0 0

1. Проверьте конфигурацию сетевых интерфейсов на R1\_ФАМИЛИЯ.

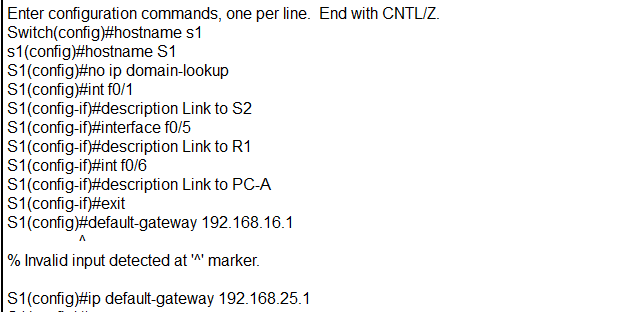
R1\_Lo#show ip interface brief



1. Убедитесь, что IP-адресация и интерфейсы находятся в состоянии up / up (при необходимости устраните неполадки).

## Шаг 3. Настройка и проверка основных параметров коммутатора

1. Настройте имя хоста для коммутаторов S1 и S2.
2. Запретите нежелательный поиск в DNS.
3. Настройте описания интерфейса для портов, которые используются в S1 и S2.
4. Установите для шлюза по умолчанию для VLAN управления значение 192.168.X+10.1 на обоих коммутаторах.



Изображение выглядит как текст

Автоматически созданное описание

# Часть 2. Настройка сетей VLAN на коммутаторах.

## Шаг 1. Сконфигруриуйте VLAN X+10.

Добавьте VLAN X+10 на S1 и S2 и назовите VLAN - **Management.**

****

****

## Шаг 2. Сконфигруриуйте SVI для VLAN X+10.

Настройте IP-адрес в соответствии с таблицей адресации для SVI для VLAN X+10 на S1 и S2. Включите интерфейсы SVI и предоставьте описание для интерфейса.

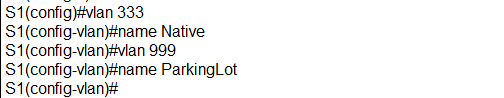
Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание

**Шаг 3. Настройте VLAN 333 с именем Native на S1 и S2. Шаг 4. Настройте VLAN 999 с именем ParkingLot на S1 и S2.**

****

**Изображение выглядит как текст

Автоматически созданное описание**

**Часть 3. Настройки безопасности коммутатора.**

## Шаг 1. Релизация магистральных соединений 802.1Q.

1. Настройте все магистральные порты Fa0/1 на обоих коммутаторах для использования VLAN 333 в качестве native VLAN.

**Изображение выглядит как текст

Автоматически созданное описание**

Изображение выглядит как текст

Автоматически созданное описание

1. Убедитесь, что режим транкинга успешно настроен на всех коммутаторах с помощью команды

**show interface trunk** на обоих коммутаторах.

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание

1. Отключить согласование DTP F0/1 на S1 и S2.



Изображение выглядит как текст

Автоматически созданное описание

1. Проверьте с помощью команды **show interfaces**. Пример:

## Шаг 2. Настройка портов доступа

1. На S1 настройте F0/5 и F0/6 в качестве портов доступа и свяжите их с VLAN X+10.

Изображение выглядит как текст

Автоматически созданное описание

1. На S2 настройте порт доступа Fa0/18 и свяжите его с VLAN X+10.

Изображение выглядит как текст

Автоматически созданное описание

## Шаг 3. Безопасность неиспользуемых портов коммутатора

1. На S1 и S2 переместите неиспользуемые порты из VLAN 1 в VLAN 999 и отключите неиспользуемые порты.

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание

1. Убедитесь, что неиспользуемые порты отключены и связаны с VLAN 999, введя команду **show interfaces status**.

Изображение выглядит как стол

Автоматически созданное описание

Изображение выглядит как стол

Автоматически созданное описание

## Шаг 4. Документирование и реализация функций безопасности порта.

Интерфейсы F0/6 на S1 и F0/18 на S2 настроены как порты доступа. На этом шаге вы также настроите безопасность портов на этих двух портах доступа.

1. На S1 введите команду **show port-security interface f0/6** для отображения настроек по умолчанию безопасности порта для интерфейса F0/6. Запишите свои ответы ниже.

Изображение выглядит как текст

Автоматически созданное описание

|  |  |
| --- | --- |
| **Конфигурация безопасности порта по умолчанию** | |
| **Функция** | **Настройка по умолчанию** |
| Защита портов | Disabled |
| Максимальное количество записей MAC-адресов | 1 |
| Режим проверки на нарушение безопасности (Violation Mode) | Shutdown |
| Aging Time | 0 mins |
| Aging Type | Absolute |
| Secure Static Address Aging | Disabled |
| Sticky MAC Address | 0 |

1. На S1 включите защиту порта на F0/6 со следующими настройками:
   * Максимальное количество записей MAC-адресов: **3**
   * Режим безопасности: **restrict**
   * Aging time: **60 мин.**
   * Aging type: **неактивный**

**Изображение выглядит как текст

Автоматически созданное описание**

1. Проверьте настройки защиты порта (**port-security**) на S1 для интерфейса F0/6. Далее просмотрите выходные данные команды **show port-security address**.

Изображение выглядит как текст, письмо

Автоматически созданное описание

1. Включите безопасность порта для F0/18 на S2. Настройте каждый активный порт доступа таким образом, чтобы он автоматически добавлял адреса МАС, изученные на этом порту, в текущую конфигурацию.

Изображение выглядит как текст

Автоматически созданное описание

1. Настройте следующие параметры безопасности порта на S2 F0/18:
   * Максимальное количество записей MAC-адресов: **2**
   * Тип безопасности: **Protect**
   * Aging time: **60 мин.**

**Изображение выглядит как текст

Автоматически созданное описание**

1. Проверьте настройки защиты порта (**port-security**) на S2 для интерфейса F0/18. Далее просмотрите выходные данные команды **show port-security address**.

Изображение выглядит как текст

Автоматически созданное описание

## Шаг 5. Реализовать безопасность DHCP snooping.

1. На S2 включите DHCP snooping и настройте DHCP snooping во VLAN X+10.
2. Настройте магистральные порты на S2 как доверенные порты.
3. Ограничьте ненадежный порт Fa0/18 на S2 пятью DHCP-пакетами в секунду.

Изображение выглядит как текст

Автоматически созданное описание

1. Проверьте DHCP Snooping на S2 с помощью команды **show ip dhcp snooping**.

Изображение выглядит как текст

Автоматически созданное описание

1. В командной строке на PC-B освободите, а затем обновите IP-адрес.

C:\> **ipconfig /release**

C:\> **ipconfig /renew**

**Изображение выглядит как текст

Автоматически созданное описание**

1. Проверьте привязку отслеживания DHCP с помощью команды **show ip dhcp snooping binding**.

Изображение выглядит как стол

Автоматически созданное описание

## Шаг 6. Реализация PortFast и BPDU Guard

1. Настройте PortFast на всех портах доступа, которые используются на обоих коммутаторах.

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание

1. Включите защиту BPDU на портах доступа VLAN X+10 для S1 и S2, подключенных к PC-A и PC-B.





1. Убедитесь, что защита BPDU и PortFast включены на соответствующих портах с помощью команды **show spanning-tree interface f0/6 detail**.

Изображение выглядит как текст

Автоматически созданное описание

## Шаг 7. Проверьте наличие сквозного подключения.

Отправьте эхо-запрос между всеми устройствами в таблице IP-адресации.

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание

# Вопросы для защиты теоретической части (глава 11)

1. **Для чего необходимо обеспечить безопасность портов коммутатора? Что произойдет, если к порту с включенной безопасностью подключают более одного устройства и почему?**

Обеспечение безопасности портов коммутатора необходимо для предотвращения несанкционированного доступа к сети, защиты от атак и утечек конфиденциальной информации. Безопасность портов коммутатора обычно достигается с помощью функций, таких как Port Security, DHCP Snooping, IP Source Guard, и других.

Port Security - это технология безопасности, которая позволяет управлять доступом к сети на уровне порта коммутатора. Она позволяет ограничить количество устройств, подключенных к порту коммутатора, и контролировать доступ к порту на основе MAC-адреса устройства. Если к порту, на котором включена безопасность, подключают более одного устройства, то возможны следующие последствия:

* Нарушение политики безопасности сети: если к порту подключают несанкционированные устройства, они могут получить доступ к сети, нарушив политику безопасности и создав уязвимость в сети.
* Ограничение доступа к сети: если к порту коммутатора подключены более одного устройства, то коммутатор может заблокировать порт для предотвращения нарушения политики безопасности.
* Снижение производительности сети: если к порту коммутатора подключено большое количество устройств, то это может привести к снижению производительности сети из-за перегрузки порта.

1. **Какое минимальное и максимальное количество MAC-адресов может быть разрешено на одном порту коммутатора? Опишите все существующие способы изучения MAC-адресов на коммутаторе.**

Минимальное количество MAC-адресов, которое может быть разрешено на одном порту коммутатора, зависит от настроек безопасности порта. Если на порту включена функция безопасности Port Security и установлено ограничение на один MAC-адрес, то только одно устройство с определенным MAC-адресом будет разрешено подключаться к порту. Если на порту не установлено ограничение, то на порту может быть любое количество устройств с различными MAC-адресами.

Максимальное количество MAC-адресов, которое может быть разрешено на одном порту коммутатора, также зависит от настроек коммутатора и сетевых условий. Некоторые коммутаторы могут поддерживать до 8, 16, 32 или более MAC-адресов на порту. Однако, если на порту подключено слишком много устройств, это может привести к перегрузке порта и снижению производительности сети.

Существуют различные способы изучения MAC-адресов на коммутаторе:

* Команда show mac address-table - эта команда показывает таблицу MAC-адресов, которую коммутатор использует для определения, на какой порт отправлять пакеты для каждого MAC-адреса.
* Команда show interface - эта команда показывает информацию о каждом порте коммутатора, включая количество принятых и переданных кадров, количество ошибок и текущий MAC-адрес.
* Команда show mac-address - эта команда показывает все MAC-адреса, которые были зарегистрированы на коммутаторе.
* Команда show arp - эта команда показывает таблицу ARP (Address Resolution Protocol), которая связывает IP-адреса с соответствующими MAC-адресами.

1. **Опишите существующие типы устаревания безопасности порта. Каким образом можно активировать отключенный по ошибке порт коммутатора?**

Существует несколько типов устаревания безопасности порта на коммутаторе:

* Aging - это тип устаревания, при котором записи о MAC-адресах удаляются, когда они становятся неактивными в течение заданного периода времени. Обычно этот период настраивается вручную и может быть от нескольких секунд до нескольких дней.
* Absolute - это тип устаревания, при котором записи о MAC-адресах удаляются, когда проходит заданный период времени с момента их добавления в таблицу. Этот период также настраивается вручную и может быть от нескольких минут до нескольких дней.

Чтобы активировать отключенный по ошибке порт коммутатора, нужно выполнить следующие действия:

* Убедитесь, что порт физически подключен к устройству.
* Проверьте конфигурацию порта, чтобы убедиться, что порт не находится в режиме "отключен".
* Если порт находится в режиме "отключен", включите его с помощью команды "no shutdown".
* Проверьте статус порта с помощью команды "show interfaces [interface]".

1. **Дайте характеристику режимам нарушения безопасности порта. В чем заключается опасность включенного протокола согласования DTP?**

Существуют три режима нарушения безопасности порта на коммутаторе:

* Shutdown - порт отключается, когда происходит нарушение безопасности, и его нужно вручную восстанавливать.
* Protect - пакеты, нарушающие безопасность, отбрасываются, но порт продолжает работать.
* Restrict - пакеты, нарушающие безопасность, записываются в журнал, но порт продолжает работать.

Включенный протокол согласования DTP (Dynamic Trunking Protocol) может представлять опасность в некоторых ситуациях. DTP является протоколом управления каналом между двумя коммутаторами, который может автоматически настраивать порты для работы в режиме транка (trunk). Если злоумышленник подключает свой собственный коммутатор к порту с включенным DTP, то он может автоматически получить доступ к VLAN-ам, которые должны быть защищены, или настроить свой собственный порт в режиме транка и получить доступ к трафику из других VLAN-ов. Поэтому важно отключать DTP на портах, которые не должны работать в режиме транка, и использовать статические настройки транка, если требуется работа в этом режиме.

1. **Опишите суть технологии DHCP Snooping. Для чего может понадобиться динамическая проверка ARP?**

DHCP Snooping - это технология безопасности на коммутаторе, которая позволяет контролировать процесс выдачи IP-адресов клиентам DHCP на сети. Она основана на фильтрации и проверке DHCP-трафика на портах коммутатора. DHCP Snooping автоматически создает список доверенных портов, которые могут обеспечить правильную выдачу IP-адресов, и запрещает выдачу IP-адресов на недоверенных портах.

В рамках DHCP Snooping на коммутаторе включается следующее:

* Определение доверенных портов (uplink-порты, порты к серверам DHCP, и т.д.)
* Отслеживание и сохранение информации о том, какие IP-адреса были выданы клиентам DHCP на доверенных портах
* Блокировка DHCP-трафика на недоверенных портах, чтобы предотвратить выдачу нежелательных IP-адресов
* Динамическая проверка ARP (Dynamic ARP Inspection - DAI) - это еще одна технология безопасности на коммутаторе, которая используется для защиты от атак типа ARP Spoofing. Она основана на проверке корректности ARP-запросов и ARP-ответов на портах коммутатора. Если обнаруживается подозрительный ARP-трафик, коммутатор блокирует его и отправляет уведомление администратору.

Динамическая проверка ARP может быть полезна для защиты от атак типа ARP Spoofing, которые могут использоваться злоумышленниками для перехвата трафика на сети или для проведения Man-in-the-Middle атак.

1. **Перечислите рекомендации по настройке портов с помощью динамической проверки ARP. Почему необходимо включать функции BPDU Guard И PortFast?**

Рекомендации по настройке портов с помощью динамической проверки ARP:

* Включить функцию DAI на всех портах коммутатора, кроме доверенных портов, которые соединены с доверенными устройствами.
* Настроить список доверенных IP-адресов на портах, связанных с доверенными устройствами. Это позволит DAI проверять только ARP-трафик, связанный с этими устройствами.
* Установить ограничение на количество ARP-запросов, отправляемых на порт за определенный интервал времени. Это позволит предотвратить возможные атаки типа ARP Flood.
* Включить функцию DHCP Snooping на коммутаторе. Это поможет предотвратить атаки типа DHCP Spoofing и защитить клиентов от получения нежелательных IP-адресов.

Почему необходимо включать функции BPDU Guard и PortFast:

* BPDU Guard - это функция безопасности, которая предотвращает возможность появления петель на сети. Если коммутатор получает BPDU-пакет на недоверенном порту, то порт блокируется, чтобы предотвратить возможность появления петель на сети.
* PortFast - это функция, которая позволяет ускорить процесс обнаружения и переключения порта в режим пропуска пакетов (forwarding mode) при подключении устройства к порту коммутатора. Это помогает уменьшить время, необходимое для подключения клиента к сети.
* Включение функций BPDU Guard и PortFast является хорошей практикой настройки безопасности на портах коммутатора, чтобы обеспечить безопасность и быстродействие сети.

1. **Какие шаги необходимо предпринять для устранения угрозы VLAN Hopping?**

VLAN Hopping - это атака на сеть, которая может позволить злоумышленнику получить несанкционированный доступ к сетевым ресурсам, находящимся в других VLAN. Чтобы устранить угрозу VLAN Hopping, можно выполнить следующие шаги:

* Отключить неиспользуемые порты: если на коммутаторе есть неиспользуемые порты, их следует отключить. Это поможет предотвратить возможность внедрения злоумышленника на неиспользуемый порт.
* Настроить порты как недоверенные: настройте порты, которые соединяются с устройствами на других конечных точках сети, как недоверенные. Это ограничит возможность VLAN Hopping.
* Ограничить доступ к VLAN: ограничьте доступ к VLAN с помощью функции "VLAN Access Control Lists" (VACL) или "Private VLAN". Это поможет предотвратить возможность злоумышленникам переходить с одной VLAN на другую.
* Отключить функцию Dynamic Trunking Protocol (DTP): DTP может использоваться злоумышленниками для перехвата трафика на различных VLAN. Отключите DTP, чтобы предотвратить возможность VLAN Hopping.
* Включить функцию "Port Security": включите функцию Port Security на портах коммутатора, чтобы ограничить возможность злоумышленников подключаться к портам, которые соединены с другими VLAN.
* Включить "BPDU Guard": включите функцию BPDU Guard на портах, которые не используются для соединения других коммутаторов. Это поможет предотвратить возможность злоумышленников подключаться к портам, которые не предназначены для соединения с другими коммутаторами.
* Ограничить VLAN на транк-портах: ограничьте VLAN на транк-портах, чтобы предотвратить возможность перехода между VLAN на разных коммутаторах.

1. **Что рекомендуется сделать при использовании сети native VLAN? Какие два типа портов коммутаторов используются на коммутаторах Cisco в составе средств защиты от атак DHCP- спуфинга?**

При использовании сети native VLAN, рекомендуется выполнить следующие шаги:

* Изменить номер VLAN по умолчанию: номер VLAN по умолчанию (VLAN 1) часто используется для настройки сети native VLAN. Рекомендуется изменить номер VLAN по умолчанию на другое значение.
* Назначить другой VLAN в качестве native: вместо VLAN 1 рекомендуется назначить другой VLAN в качестве native VLAN.
* Использовать VLAN-базированные аутентификацию: для повышения безопасности рекомендуется использовать VLAN-базированные аутентификацию, которая позволяет ограничить доступ к VLAN.

Для защиты от атак DHCP-спуфинга на коммутаторах Cisco используются следующие типы портов:

* Trusted (доверенные) порты: эти порты используются для соединения с DHCP-сервером или другими доверенными устройствами. На таких портах разрешены только ответы DHCP-сервера.
* Untrusted (недоверенные) порты: эти порты используются для соединения с устройствами конечных пользователей. На таких портах запрещены DHCP-ответы и разрешены только DHCP-запросы.

1. **Почему устройства уровня 2 считаются самым слабым звеном в инфраструктуре безопасности компании? Где хранятся динамически определяемые MAC-адреса, когда включена функция sticky learning?**

Устройства уровня 2 (коммутаторы) считаются самым слабым звеном в инфраструктуре безопасности компании по нескольким причинам:

* Они работают на физическом уровне сети, где нет механизмов аутентификации и шифрования.
* Коммутаторы не имеют встроенных механизмов защиты от атак на сетевой уровень, таких как атаки на протоколы, например, ARP Spoofing и DHCP Spoofing.
* Коммутаторы могут стать жертвой атак, направленных на сброс конфигурации порта или перенаправление трафика.

При включенной функции sticky learning, динамически определяемые MAC-адреса хранятся в памяти коммутатора. При использовании функции sticky learning, коммутатор автоматически запоминает MAC-адреса, связанные с портом, и отбрасывает все пакеты, содержащие другие MAC-адреса, приходящие на этот порт. Таким образом, функция sticky learning помогает предотвратить атаки на сетевой уровень, связанные с подменой MAC-адресов.