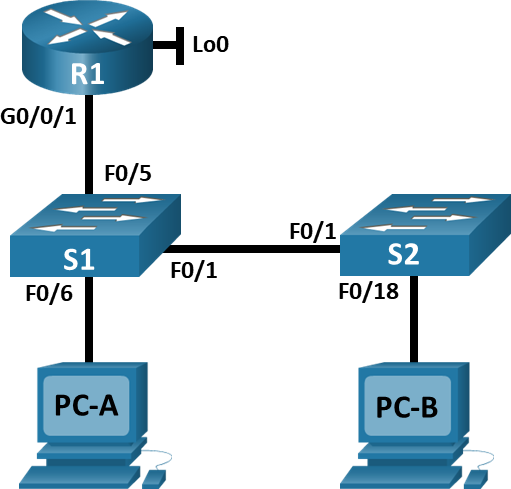


Конфигурация безопасности коммутатора

**Топология**



**Таблица адресации**

|  |  |  |  |
| --- | --- | --- | --- |
| **Устройство** | **interface/vlan** | **IP-адрес** | **Маска подсети** |
| R1\_ФАМИЛИЯ | G0/0/1 | 192.168.X+10.1 | 255.255.255.0 |
| Loopback 0 | 10.10.1.1 | 255.255.255.0 |
| S1 | VLAN X+10 | 192.168.X+10.201 | 255.255.255.0 |
| S2 | VLAN X+10 | 192.168.X+10.202 | 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

## Шаг 2. Настройте маршрутизатор R1\_ФАМИЛИЯ.

1. Загрузите следующий конфигурационный скрипт на R1\_ФАМИЛИЯ.

enable

configure terminal hostname R1\_ФАМИЛИЯ no ip domain lookup

ip dhcp excluded-address 192.168.X+10.1 192.168.X+10.9

ip dhcp excluded-address 192.168.X+10.201 192.168.X+10.202

!

ip dhcp pool Students

network 192.168.X+10.0 255.255.255.0

default-router 192.168.X+10.1 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 trusted

ip address 192.168.X+10.1 255.255.255.0

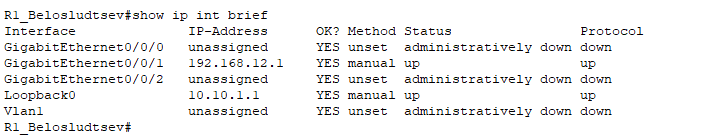
no shutdown

!

line con 0

logging synchronous exec-timeout 0 0

1. Проверьте конфигурацию сетевых интерфейсов на R1\_ФАМИЛИЯ.

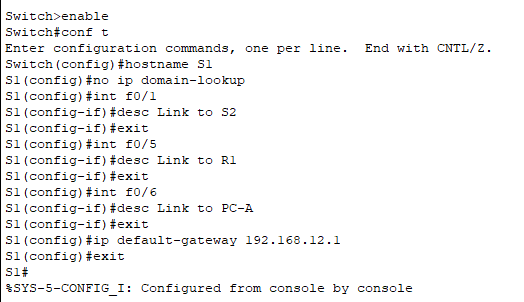


1. Убедитесь, что IP-адресация и интерфейсы находятся в состоянии up / up (при необходимости устраните неполадки).

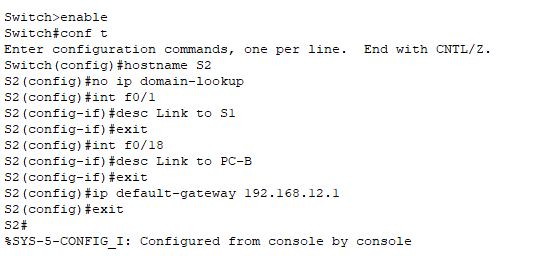
## Шаг 3. Настройка и проверка основных параметров коммутатора

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.

**Настройка коммутатора S1:**



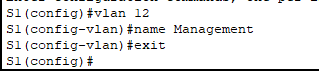
**Настройка коммутатора S2:**

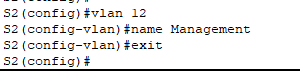


# Часть 2. Настройка сетей VLAN на коммутаторах.

## Шаг 1. Сконфигруриуйте VLAN X+10.

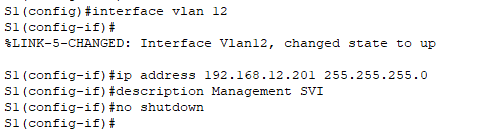
Добавьте VLAN X+10 на S1 и S2 и назовите VLAN - **Management.**

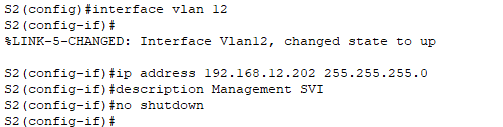
****

****

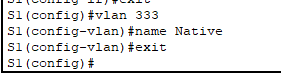
## Шаг 2. Сконфигруриуйте SVI для VLAN X+10.

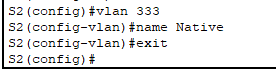
Настройте IP-адрес в соответствии с таблицей адресации для SVI для VLAN X+10 на S1 и S2. Включите интерфейсы SVI и предоставьте описание для интерфейса.



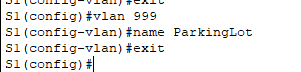


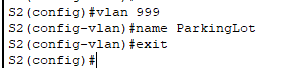
**Шаг 3. Настройте VLAN 333 с именем Native на S1 и S2.**

****

****

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

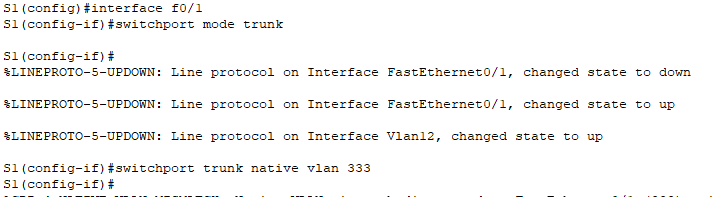
****

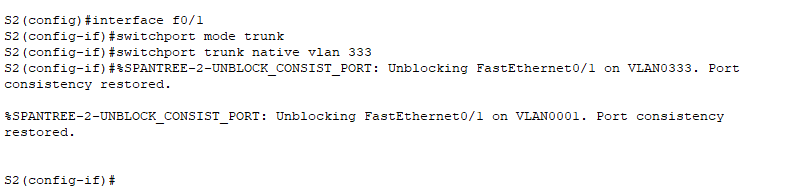
****

# Часть 3. Настройки безопасности коммутатора.

## Шаг 1. Релизация магистральных соединений 802.1Q.

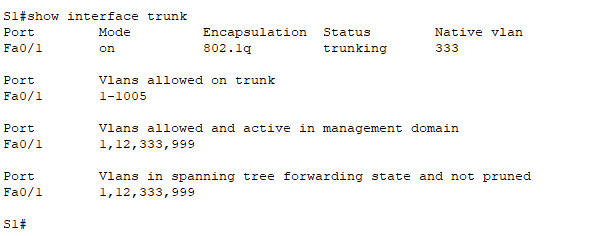
1. Настройте все магистральные порты Fa0/1 на обоих коммутаторах для использования VLAN 333 в качестве native VLAN.

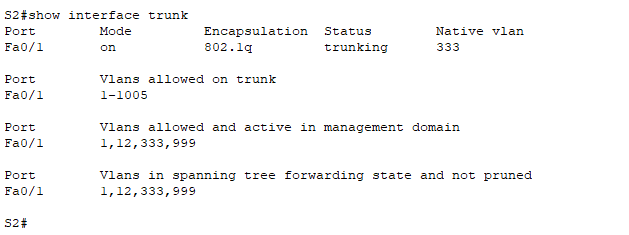




1. Убедитесь, что режим транкинга успешно настроен на всех коммутаторах с помощью команды

**show interface trunk** на обоих коммутаторах.





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





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

### S1# show interfaces f0/1 switchport | include Negotiation

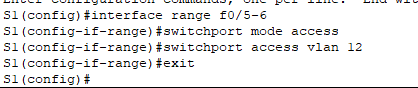
Negotiation of Trunking: Off



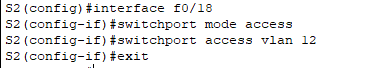


## Шаг 2. Настройка портов доступа

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

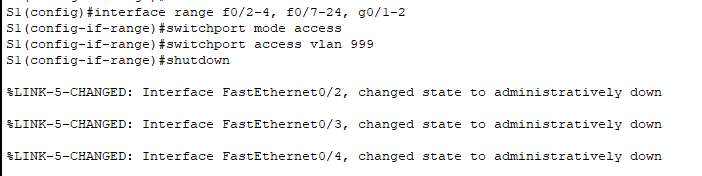


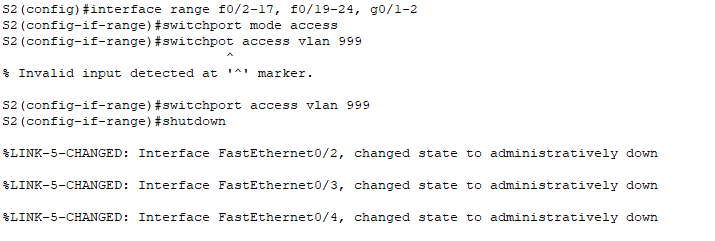
1. На S2 настройте порт доступа Fa0/18 и свяжите его с VLAN X+10.



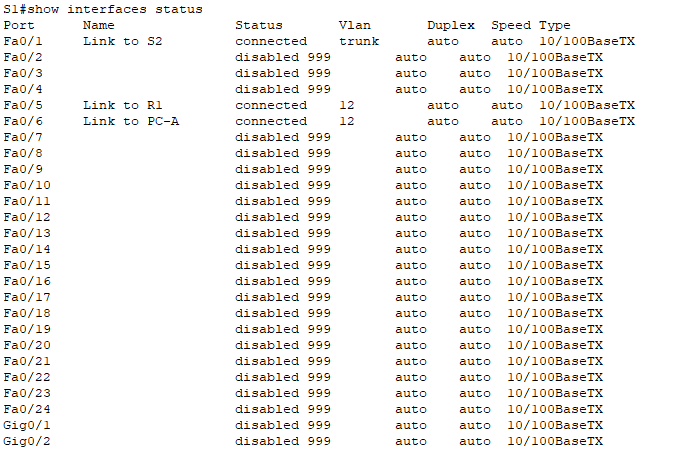
## Шаг 3. Безопасность неиспользуемых портов коммутатора

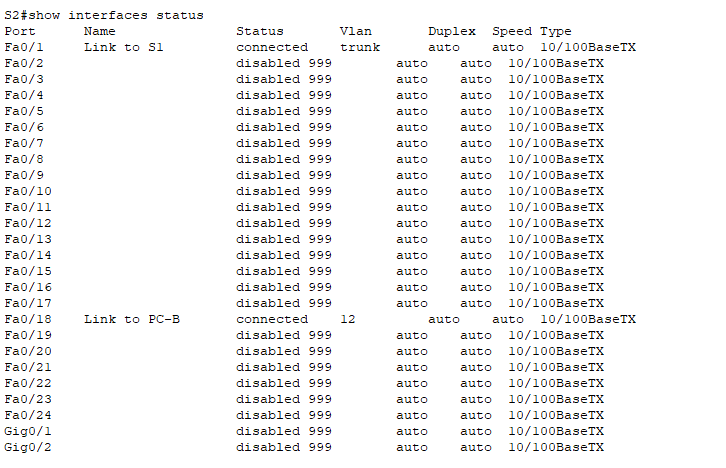
1. На S1 и S2 переместите неиспользуемые порты из VLAN 1 в VLAN 999 и отключите неиспользуемые порты.





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





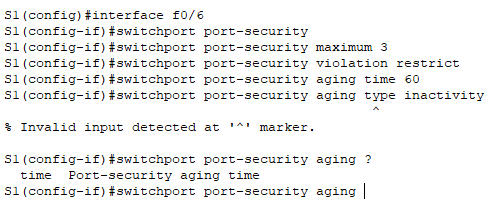
## Шаг 4. Документирование и реализация функций безопасности порта.

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.

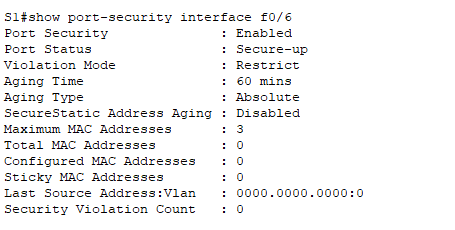
1. На S1 введите команду **show port-security interface f0/6** для отображения настроек по умолчанию безопасности порта для интерфейса F0/6. Запишите свои ответы ниже.

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

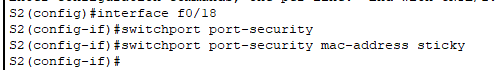
1. На S1 включите защиту порта на F0/6 со следующими настройками:
   * Максимальное количество записей MAC-адресов: **3**
   * Режим безопасности: **restrict**
   * Aging time: **60 мин.**
   * Aging type: **неактивный**



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



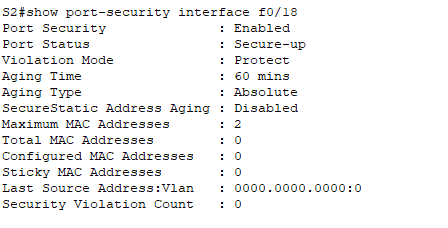
1. Включите безопасность порта для F0/18 на S2. Настройте каждый активный порт доступа таким образом, чтобы он автоматически добавлял адреса МАС, изученные на этом порту, в текущую конфигурацию.



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

****

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

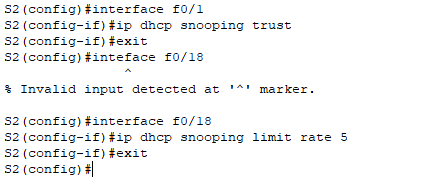


## Шаг 5. Реализовать безопасность DHCP snooping.

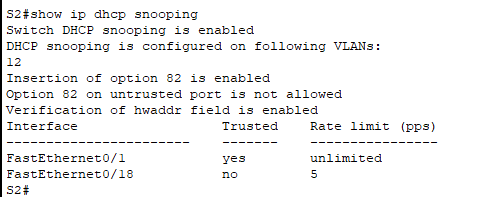
1. На S2 включите DHCP snooping и настройте DHCP snooping во VLAN X+10.



1. Настройте магистральные порты на S2 как доверенные порты.
2. Ограничьте ненадежный порт Fa0/18 на S2 пятью DHCP-пакетами в секунду.



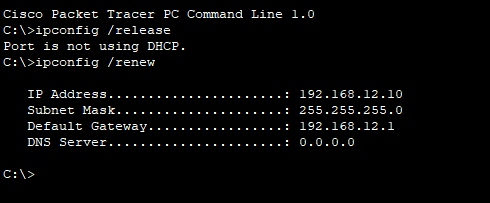
1. Проверьте DHCP Snooping на S2 с помощью команды **show ip dhcp snooping**.



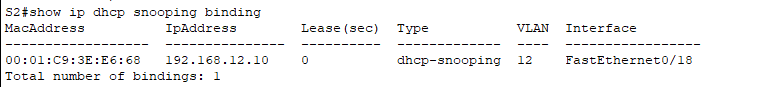
1. В командной строке на PC-B освободите, а затем обновите IP-адрес.

C:\Users\Student> **ipconfig /release**

C:\Users\Student> **ipconfig /renew**

****

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



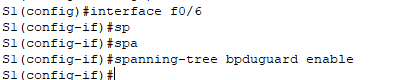
## Шаг 6. Реализация PortFast и BPDU Guard

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



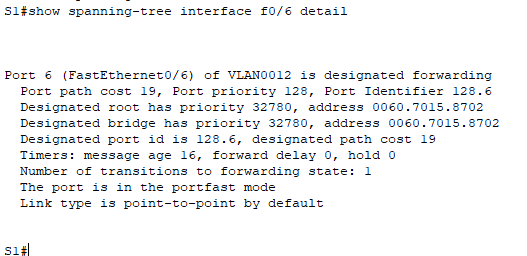


1. Включите защиту BPDU на портах доступа VLAN X+10 для S1 и S2, подключенных к PC-A и PC-B.





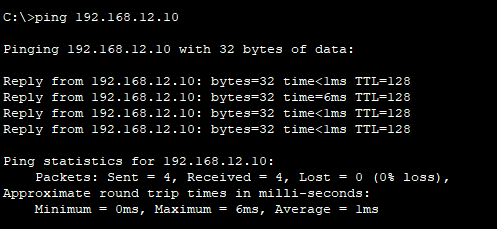
1. Убедитесь, что защита BPDU и PortFast включены на соответствующих портах с помощью команды **show spanning-tree interface f0/6 detail**.



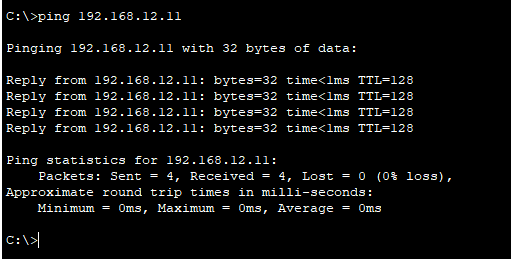
## Шаг 7. Проверьте наличие сквозного ⁪подключения.

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

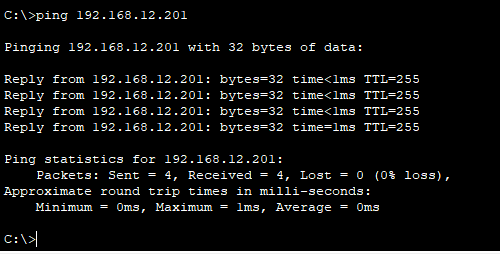
**PC-A -> PC-B:**



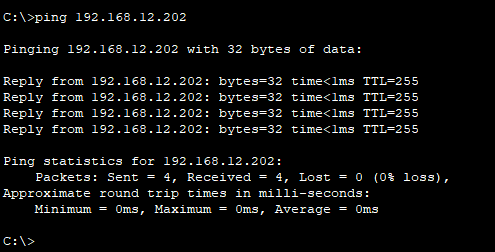
**PC-B -> PC-A:**



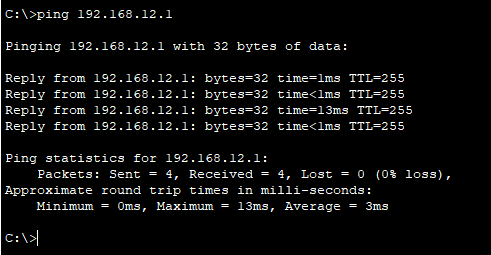
**PC-A -> S1:**



**PC-A -> S2:**



**PC-B -> R1:**



# 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?

Для того, чтобы предотвратить атаки 2-го уровня, которые являются одними из самых простых для развертывания хакерами, но эти угрозы также можно смягчить с помощью некоторых распространенных решений 2-го уровня.

Если активный с включенной безопасностью и к этому порту подключено более одного устройства, порт перейдет в состояние error-disabled.

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

Максимальное количество защищенных MAC-адресов, которые можно настроить, зависит от коммутатора и IOS. Может быть 8192

Коммутатор может быть настроен на изучение MAC-адресов на защищенном порту одним из трех способов:

1. Ручная конфигурация. Администратор вручную настраивает статический MAC-адрес(а)

2. Динамическое изучение. Текущий MAC-адрес источника для устройства, подключенного к порту, автоматически защищается, но не добавляется в конфигурацию запуска. Если коммутатор перезагружен, порт должен будет повторно узнать MAC-адрес устройства.

3. Динамическое изучение – Sticky. Администратор может включить коммутатор для динамического изучения MAC-адреса и «привязать» его к работающей. Сохранение текущей конфигурации передаст динамически изученный MAC-адрес в NVRAM.

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

Устаревание безопасности порта может использоваться для установки времени устаревания статических и динамических защищенных адресов на порту:

* Абсолютный. Защищенные адреса порта удаляются по истечении указанного времени устаревания.
* По таймеру неактивности. Безопасные адреса на порту удаляются, только если они неактивны в течение указанного времени.

Чтобы повторно включить порт, сначала используйте команду shutdown, затем используйте команду no shutdown, чтобы сделать порт работоспособным, как показано в примере.

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

**shutdown (default)** Порт немедленно переходит в состояние отключения по ошибке, выключает светодиод порта и отправляет сообщение системного журнала. Для этого режима предусмотрено увеличение значения счётчика нарушений. Когда безопасный порт находится в состоянии отключения по ошибке, администратор должен повторно включить его, введя команды shutdown и no shutdown.

**restrict (ограничение)** Порт отбрасывает пакеты с неизвестными адресами источника, пока вы не удалите достаточное количество безопасных MAC-адресов, чтобы опуститься ниже максимального значения или пока не увеличится максимальное значение. Этот режим вызывает увеличение счетчика нарушений безопасности и генерирует сообщение системного журнала (syslog).

**protect (защита)** Это наименее безопасный из режимов нарушения безопасности. Порт отбрасывает пакеты с неизвестными адресами источника, пока вы не удалите достаточное количество безопасных MACадресов, чтобы опуститься ниже максимального значения или пока не увеличится максимальное значение. Нет сообщений в системном журнале (syslog).

Суть уязвимости заключается в том, что протокол DTP включен по умолчанию на всех современных коммутаторах Cisco. При этом каждый порт коммутатора настроен в режиме Dynamic Auto. То есть порт будет ожидать инициации транка со стороны соседа.

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

DHCP Snooping - это технология безопасности уровня 2, предназначенная для защиты от атак с использованием протокола.

Динамическая проверка ARP (DAI) требует отслеживания DHCP и помогает предотвратить атаки ARP

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

1. Включить отслеживание DHCP на глобальном уровне.

2. Включите отслеживание DHCP на выбранных VLAN.

3. Включить DAI на выбранных VLAN.

4. Настройте доверенные интерфейсы для отслеживания DHCP и проверки ARP.

Чтобы нейтрализовать атаки манипуляций с протоколом STP, используем средства защиты PortFast и Bridge Protocol Data Unit (BPDU) Guard

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

**Шаг 1.** Отключите согласование DTP (автоматические магистральные каналы) на немагистральных портах с помощью команды интерфейсной настройки switchport mode access.

**Шаг 2.** Отключите неиспользуемые порты и назначьте их неиспользуемой VLAN.

**Шаг 3.** Вручную включите магистральный канал на магистральном порту с помощью команды интерфейсной настройки switchport mode trunk.

**Шаг 4.** Установите для native VLAN, VLAN, отличную от VLAN 1, с помощью команды switchport trunk native vlan vlan\_number.

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?

Установить для native VLAN, VLAN, отличную от VLAN 1.

Два типа портов коммутаторов Cisco, используемых для защиты от DHCP-спуфинга:

1) Порты доверенные (trusted ports) - принимают DHCP-ответы.

2) Порты недоверенные (untrusted ports) - DHCP-ответы с них отбрасываются.

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, так как:

- Они работают на канальном уровне и лишены средств контроля на сетевом уровне.

- Зачастую имеют минимальные встроенные средства безопасности.

- Подвержены большому количеству потенциальных атак (VLAN Hopping, MAC Spoofing и др.).

Сохранение текущей конфигурации передаст динамически изученный MAC-адрес в NVRAM