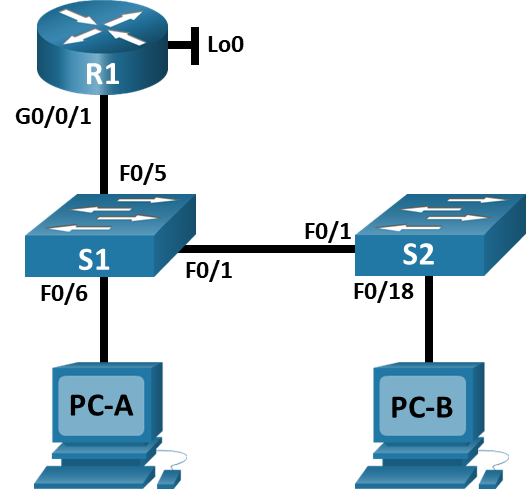


**Конфигурация безопасности коммутатора**

# Топология



# Таблица адресации

|  |  |  |  |
| --- | --- | --- | --- |
| **Устройство** | **interface/vlan** | **IP-адрес** | **Маска подсети** |
| R1\_ФАМИЛИЯ  *R1* | G0/0/1 | 192.168.34.1 | 255.255.255.0 |
| Loopback 0 | 10.10.1.1 | 255.255.255.0 |
| S1 | VLAN 34 | 192.168.34.201 | 255.255.255.0 |
| S2 | VLAN 34 | 192.168.34.202 | 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

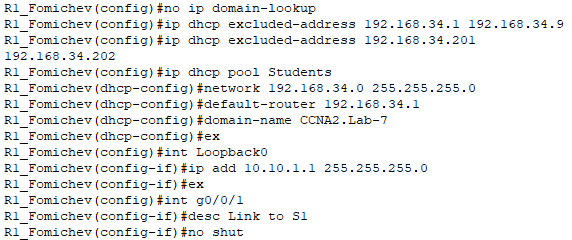
**Часть 1. Настройка основного сетевого устройства**

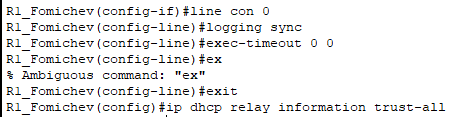
**Шаг 1. Создайте сеть.**

1. Создайте сеть согласно топологии.
2. Инициализация устройств

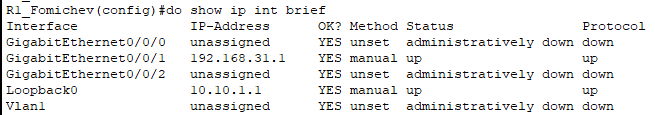
**Шаг 2. Настройте маршрутизатор R1\_ФАМИЛИЯ.**

1. Загрузите следующий конфигурационный скрипт на R1\_ФАМИЛИЯ.





1. Проверьте конфигурацию сетевых интерфейсов на R1\_ФАМИЛИЯ.

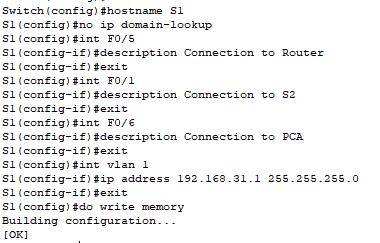


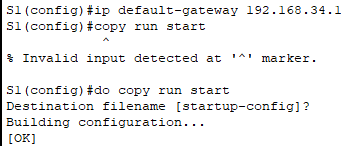
1. Убедитесь, что IP-адресация и интерфейсы находятся в состоянии up / up (при необходимости устраните неполадки).

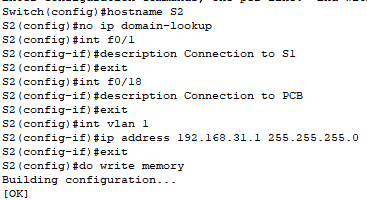
*Закройте окно настройки.*

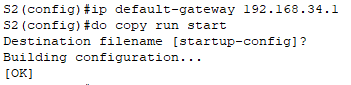
**Шаг 3. Настройка и проверка основных параметров коммутатора**

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.









**Часть 2. Настройка сетей VLAN на коммутаторах.**

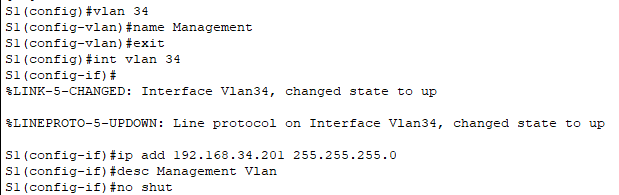
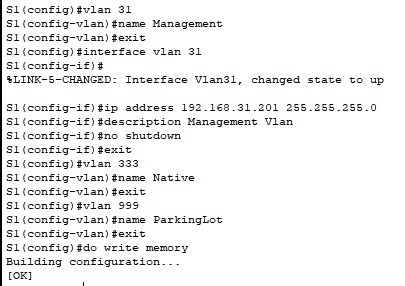
**Шаг 1. Сконфигруриуйте VLAN X+10.**

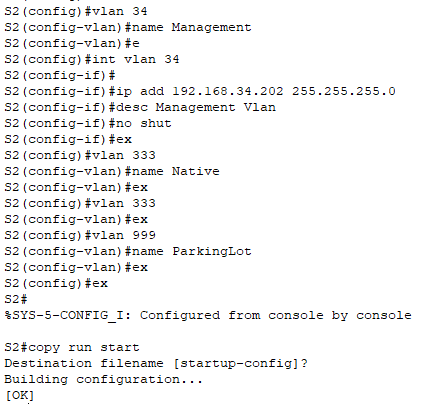
Добавьте VLAN X+10 на S1 и S2 и назовите VLAN - **Management.**

**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.**

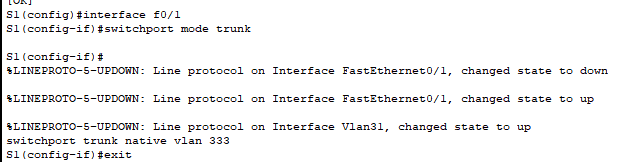
****

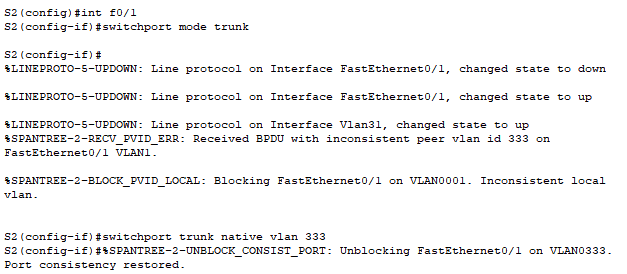


**Часть 3. Настройки безопасности коммутатора.**

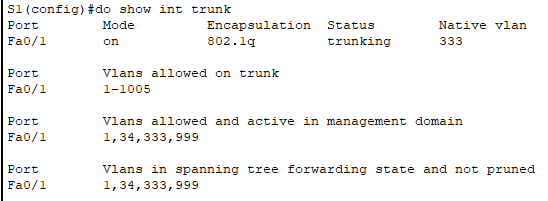
**Шаг 1. Релизация магистральных соединений 802.1Q.**

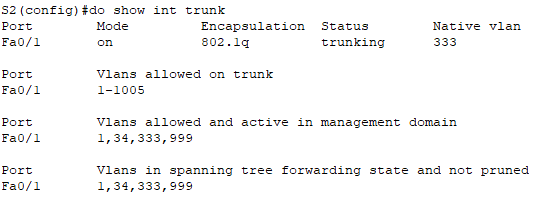
1. Настройте все магистральные порты Fa0/1 на обоих коммутаторах для использования VLAN 333 в качестве native VLAN.



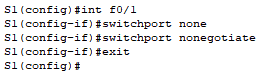


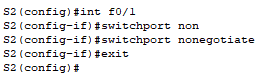
1. Убедитесь, что режим транкинга успешно настроен на всех коммутаторах с помощью команды **show interface trunk** на обоих коммутаторах.





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





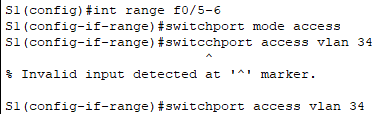
1. Проверьте с помощью команды **show interfaces**. Пример:



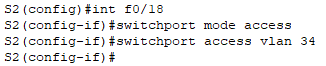


**Шаг 2. Настройка портов доступа**

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

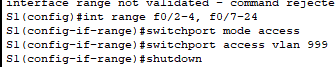


1. На S2 настройте порт доступа Fa0/18 и свяжите его с VLAN X+10.



**Шаг 3. Безопасность неиспользуемых портов коммутатора**

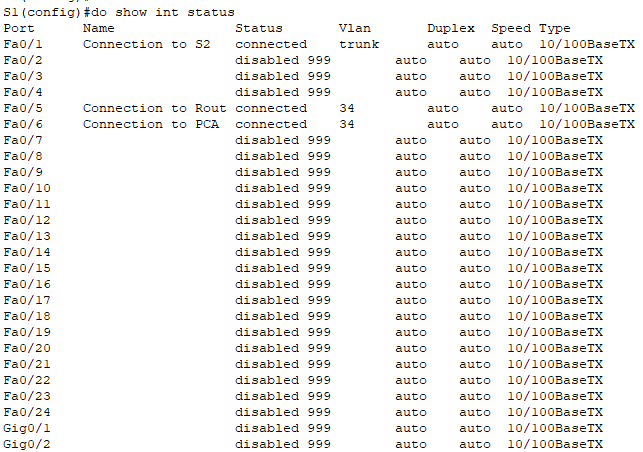
1. На S1 и S2 переместите неиспользуемые порты из VLAN 1 в VLAN 999 и отключите неиспользуемые порты.

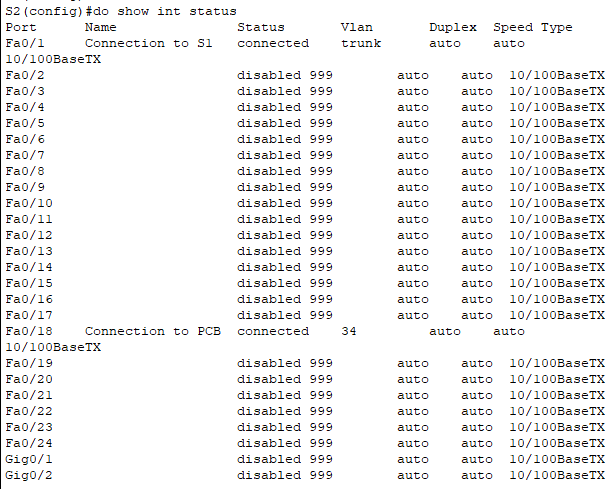






1. Убедитесь, что неиспользуемые порты отключены и связаны с VLAN 999, введя команду **show interfaces status**.

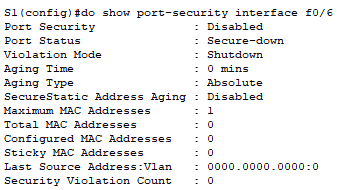




**Шаг 4. Документирование и реализация функций безопасности порта.**

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.

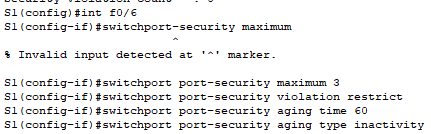


1. На S1 включите защиту порта на F0/6 со следующими настройками:

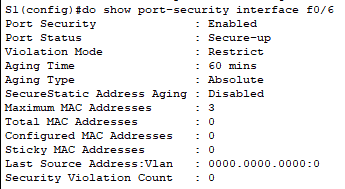
o Максимальное количество записей MAC-адресов: **3**

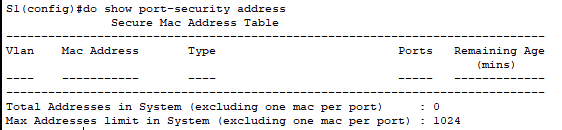
o Режим безопасности: **restrict**

* + Aging time: **60 мин.**



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

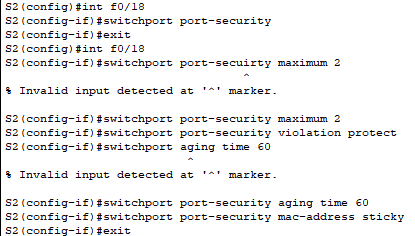




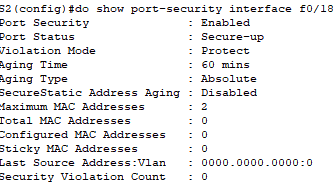
1. Включите безопасность порта для F0/18 на S2. Настройте каждый активный порт доступа таким образом, чтобы он автоматически добавлял адреса МАС, изученные на этом порту, в текущую конфигурацию.

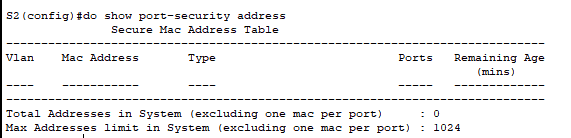


1. Настройте следующие параметры безопасности порта на S2 F0/18:
   * Максимальное количество записей MAC-адресов: **2**
   * Тип безопасности: **Protect**
   * Aging time: **60 мин.**



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.



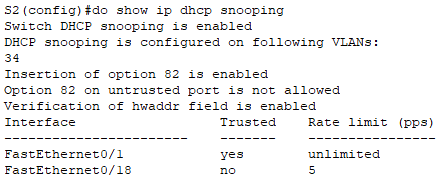
1. Настройте магистральные порты на S2 как доверенные порты.



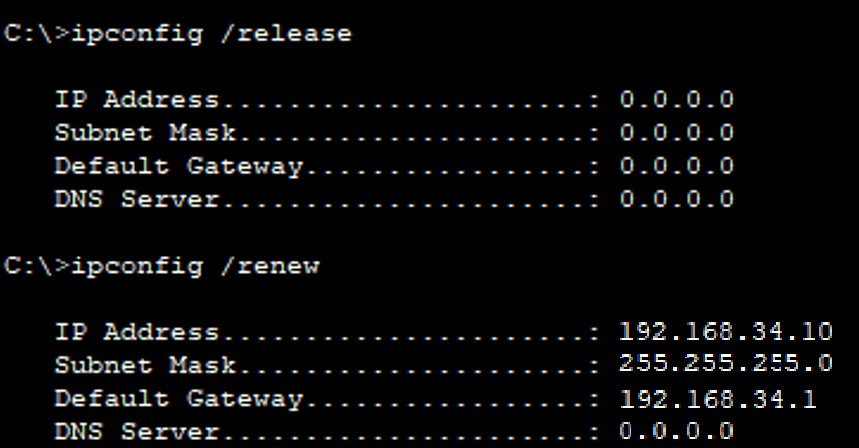
1. Ограничьте ненадежный порт Fa0/18 на S2 пятью DHCP-пакетами в секунду.



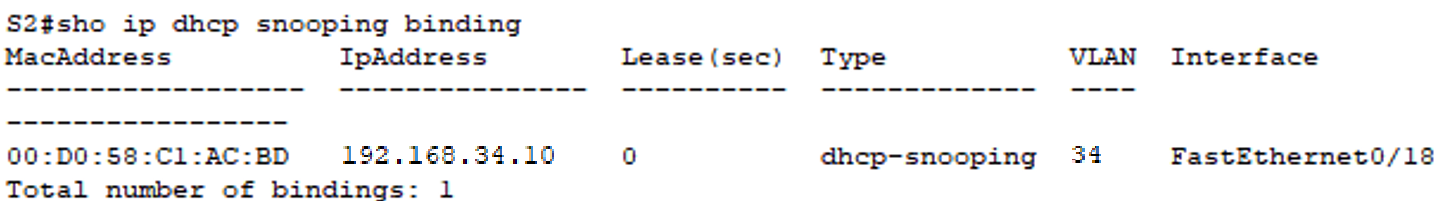
1. Проверьте DHCP Snooping на S2 с помощью команды **show ip dhcp snooping**.



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

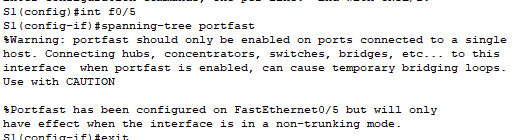


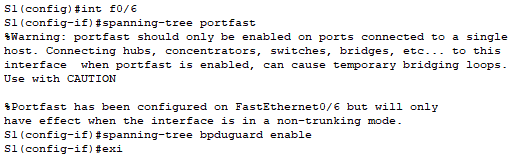
1. Проверьте привязку отслеживания DHCP с помощью команды **show ip dhcp snooping binding**.

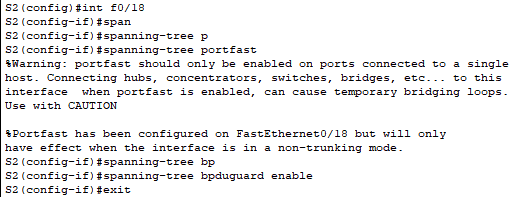


**Шаг 6. Реализация PortFast и BPDU Guard**

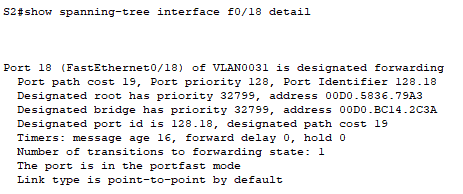
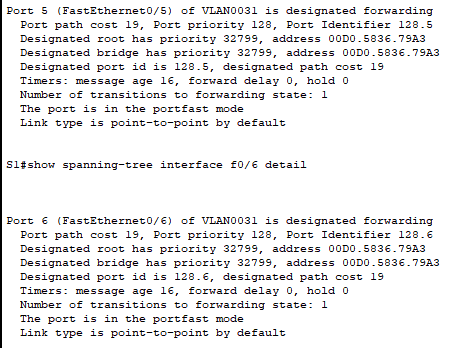
1. Настройте PortFast на всех портах доступа, которые используются на обоих коммутаторах.
2. Включите защиту BPDU на портах доступа VLAN X+10 для S1 и S2, подключенных к PC-A и PC-B.





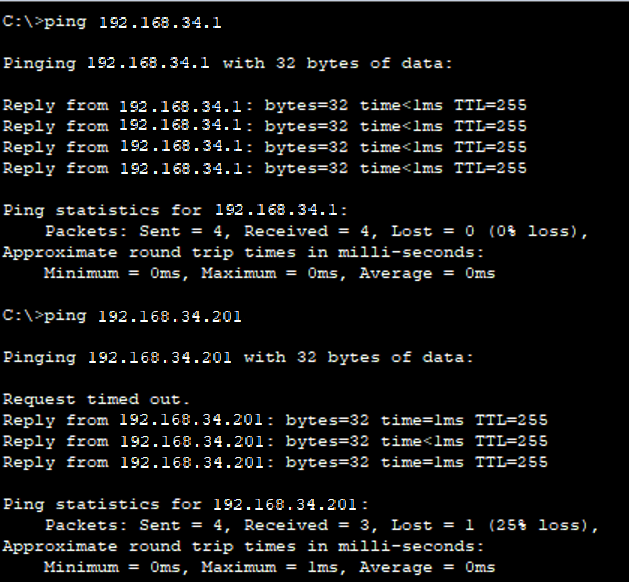


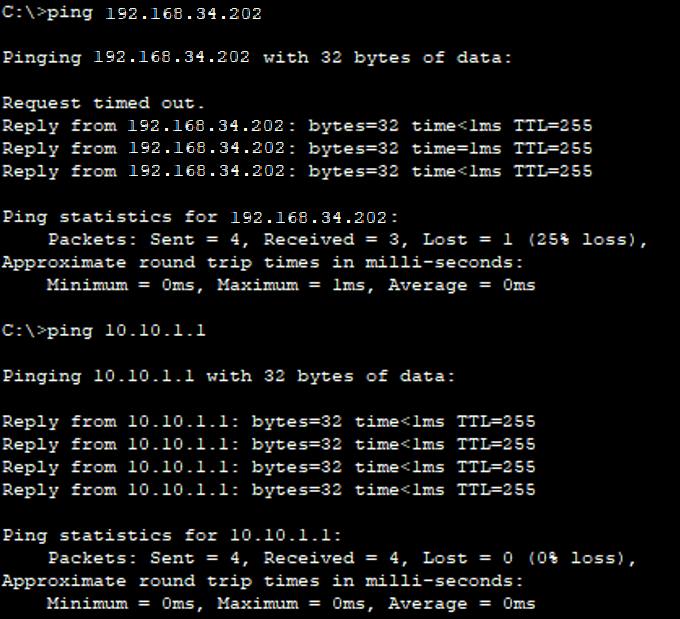
1. Убедитесь, что защита BPDU и PortFast включены на соответствующих портах с помощью команды **show spanning-tree interface f0/6 detail**.



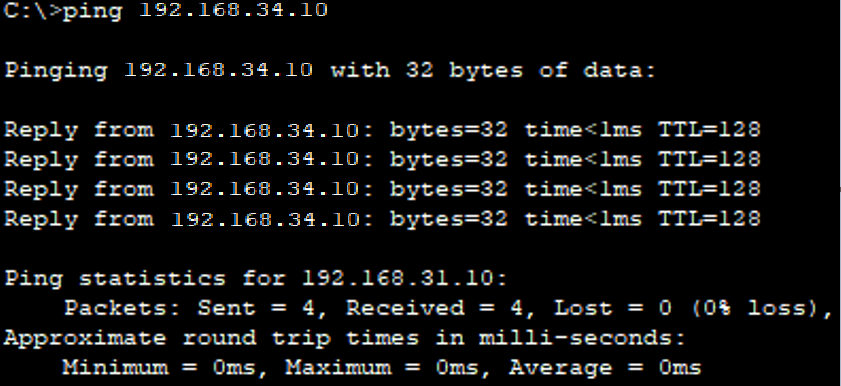
**Шаг 7. Проверьте наличие сквозного подключения.**

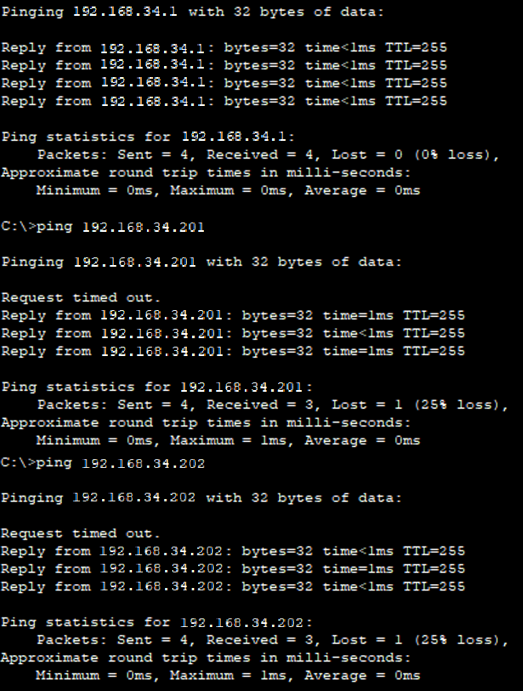
Отправьте эхо-запрос между всеми устройствами в таблице IP-адресации.



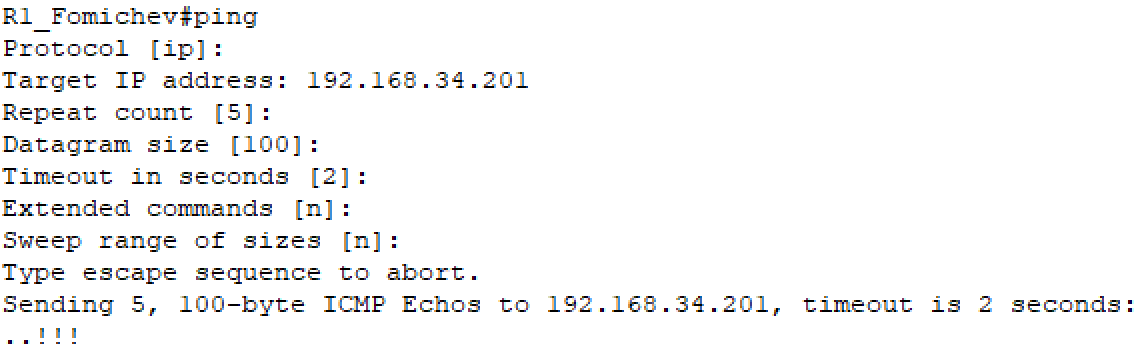


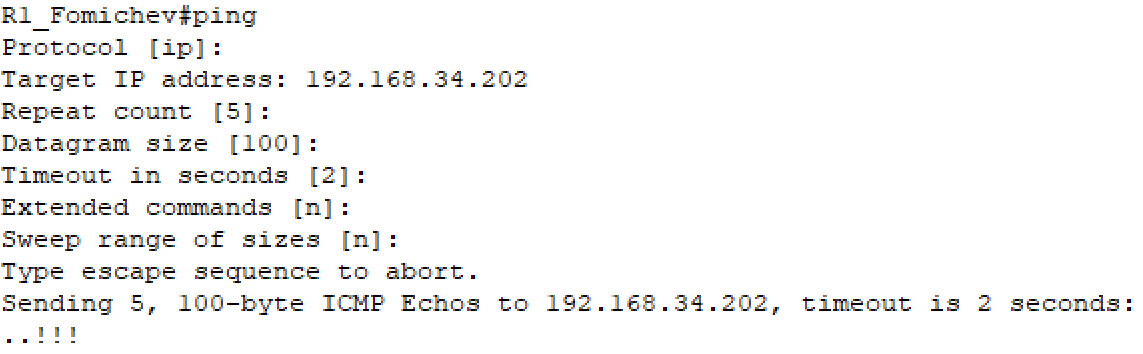
Отправка ping с PC-B



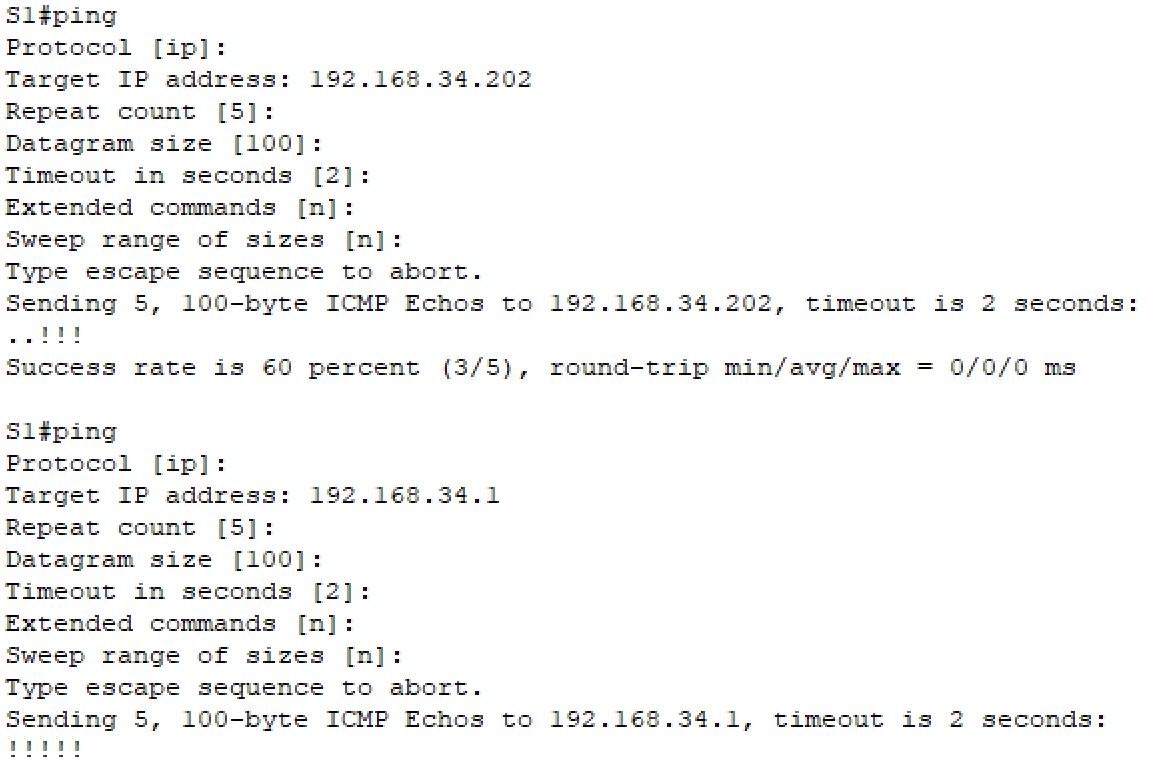


Отправка ping с PC-A





Отправка ping с R1\_Fomichev



Отправка ping с S1

**Вопросы для защиты теоретической части (глава 11)**

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

Ответ: Обеспечение безопасности портов коммутатора необходимо для предотвращения несанкционированного доступа к сети и защиты от атак, таких как атаки мак-флуда или атаки переполнения камеры MAC-адресов. Если к порту с включенной безопасностью подключают более одного устройства, то возникает риск возникновения мак-флуда или атаки переполнения камеры MAC-адресов, что может привести к отказу в обслуживании (DoS) или возможности злоумышленнику проникнуть в сеть.

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

Ответ: Минимальное количество MAC-адресов, разрешенных на одном порту коммутатора, - один. Максимальное количество зависит от настроек коммутатора, но обычно оно ограничено одним MAC-адресом. Существующие способы изучения MAC-адресов на коммутаторе включают в себя статическое изучение MAC-адресов, динамическое изучение с помощью протокола MAC-адресного изучения (MAC-адреса), а также изучение с использованием механизма статического изучения (sticky learning).

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

Ответ: Существующие типы устаревания безопасности порта включают в себя статическое устаревание, динамическое устаревание и устаревание по неприкосновенности. Чтобы активировать отключенный по ошибке порт коммутатора, вы можете использовать команду no shutdown в режиме конфигурации интерфейса.

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

Ответ: Режимы нарушения безопасности порта включают в себя отклонение, отключение и защиту. Отклонение позволяет записывать нарушения в системный журнал без принятия каких-либо мер. Отключение отключает порт, если нарушение безопасности обнаружено. Защита автоматически закрывает порт и предотвращает дальнейшие нарушения. Опасность включенного протокола согласования DTP заключается в том, что злоумышленник может использовать этот протокол для внедрения в сеть с целью выполнения атак вроде атаки мак-флуда или атаки переполнения камеры MAC-адресов.

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

Ответ: DHCP Snooping - это технология, которая используется для защиты сети от атак DHCP-отравления или от других атак, связанных с DHCP. Он контролирует передачу DHCP-сообщений на недоверенных портах и регистрирует информацию о DHCP-клиентах. Динамическая проверка ARP может потребоваться для защиты сети от атак перехвата ARP или от других атак, связанных с ARP, путем мониторинга ARP-таблиц и предотвращения подмены MAC-адресов.

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

Ответ: Рекомендации по настройке портов с использованием динамической проверки ARP включают в себя настройку доверенных портов для устройств, которые отправляют ARP-запросы, и настройку недоверенных портов для всех остальных портов. Включение функций BPDU Guard и PortFast необходимо для обеспечения безопасности сети и предотвращения возможных атак, таких как атаки на мак-адреса и атаки на маршрутизаторы.

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

Ответ: Для устранения угрозы VLAN Hopping необходимо настроить протоколы безопасности VLAN, такие как Private VLANs, а также настроить механизмы защиты от атак, такие как DHCP Snooping и Dynamic ARP Inspection.

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

Ответ: При использовании сети native VLAN рекомендуется настроить разрешение безопасности порта для всех портов, находящихся в сети native VLAN. Два типа портов коммутаторов Cisco, используемых в качестве средств защиты от атак DHCP-спуфинга, включают в себя доверенные порты и недоверенные порты.

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

Ответ: Устройства уровня 2 считаются самым слабым звеном в инфраструктуре безопасности компании, потому что они имеют ограниченные механизмы защиты и могут быть подвержены различным атакам, таким как атаки мак-адресов и атаки переполнения камеры MAC-адресов. Динамически определяемые MAC-адреса, когда включена функция sticky learning, хранятся во временном кэше коммутатора.