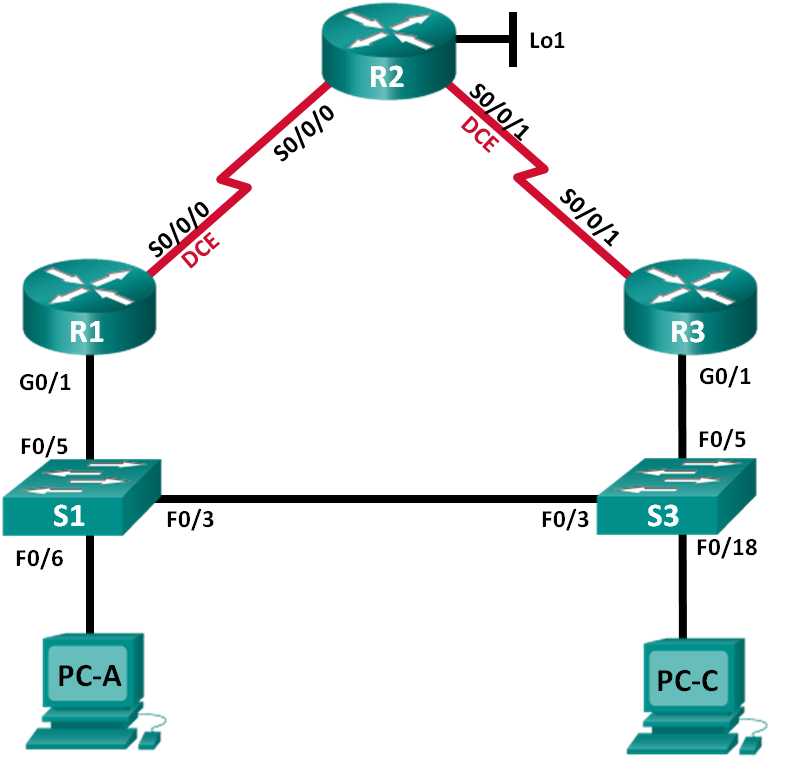


**Настройка HSRP**

# Топология



**8**

# Таблица адресации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска подсети** | **Шлюз по умолчанию** |
| R1 | G0/1 | 192.168.1.1 | 255.255.255.0 | — |
| S0/0/0 (DCE) | 10.1.1.1 | 255.255.255.252 | — |
| R2\_ФАМИЛИЯ | S0/0/0 | 10.1.1.2 | 255.255.255.252 | — |
| S0/0/1 (DCE) | 10.2.2.2 | 255.255.255.252 | — |
| Lo1 | 209.165.221.225 | 255.255.255.224 | — |
| R3 | G0/1 | 192.168.1.3 | 255.255.255.0 | — |
| S0/0/1 | 10.2.2.1 | 255.255.255.252 | — |
| S1 | VLAN 1 | 192.168.1.11 | 255.255.255.0 | 192.168.1.1 |
| S3 | VLAN 1 | 192.168.1.13 | 255.255.255.0 | 192.168.1.3 |
| PC-A | NIC | 192.168.1.31 | 255.255.255.0 | 192.168.1.1 |
| PC-C | NIC | 192.168.1.33 | 255.255.255.0 | 192.168.1.3 |

# Задачи

**Часть 1. Построение сети и проверка соединения**

**Часть 2. Настройка обеспечения избыточности на первом хопе с помощью HSRP**

# Необходимые ресурсы

* 3 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3

(универсальный образ) или аналогичная модель)

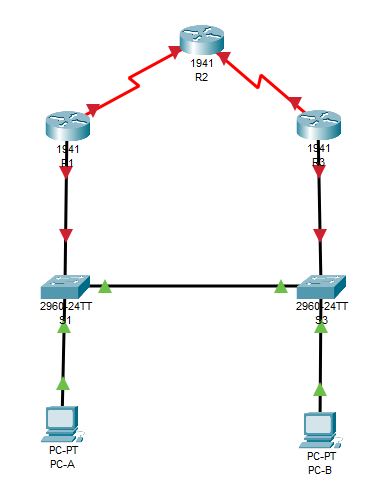
* 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
* 2 компьютера (ОС Windows с программой эмуляции терминала, например, Tera Term)
* Консольные кабели для настройки устройств Cisco IOS через консольные порты
* Кабели Ethernet и последовательные кабели согласно топологии

# Часть 1: Построение сети и проверка связи

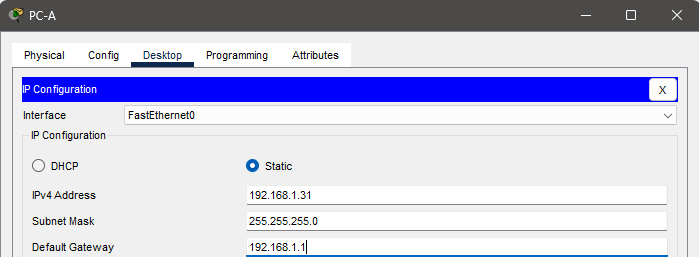
В первой части вам предстоит настроить топологию сети и выполнить базовую настройку, например IP-адреса интерфейсов, статическую маршрутизацию, доступ к устройствам и пароли.

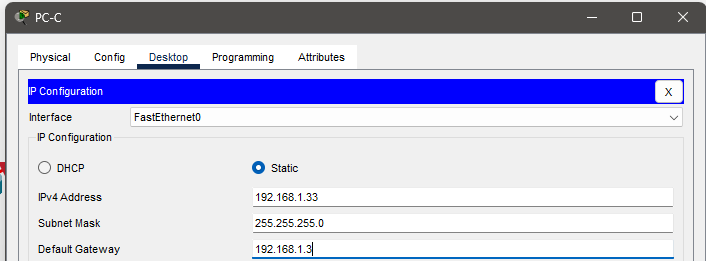
**Шаг 1: Создайте сеть согласно топологии.**

Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.



**Шаг 2: Настройте узлы ПК.**



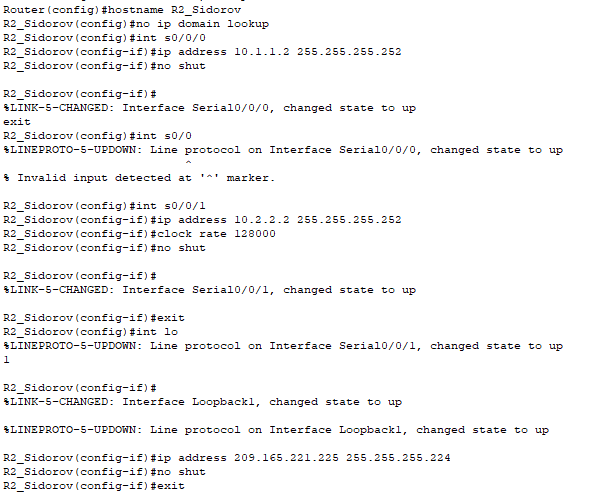


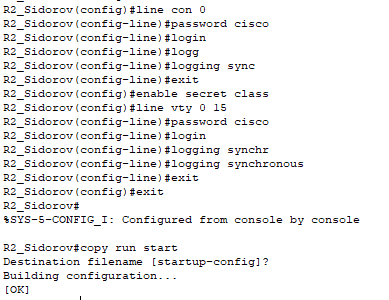
**Шаг 3: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.**

**Шаг 4: Произведите базовую настройку маршрутизаторов.**

1. Отключите поиск DNS.
2. Присвойте имена устройствам в соответствии с топологией.
3. Настройте IP-адреса для маршрутизаторов, указанных в таблице адресации.
4. Установите тактовую частоту на **128000** для всех последовательных интерфейсов маршрутизатора DCE.
5. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.
6. Назначьте **cisco** в качестве пароля консоли и VTY и включите запрос пароля при подключении.
7. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.
8. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

**R2\_Sidorov, по аналогии R1 и R3 в соответствии с таблицей адресации**

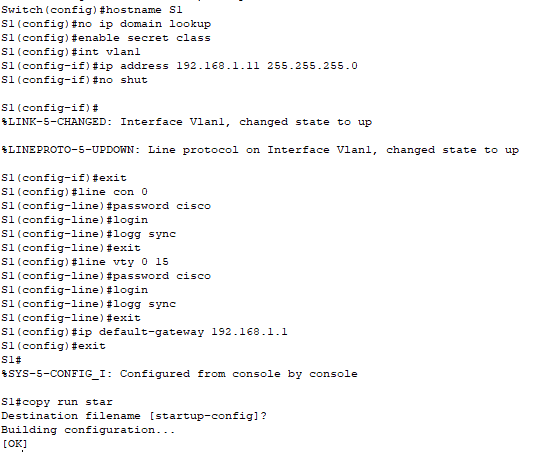




**Шаг 5: Настройте базовые параметры каждого коммутатора.**

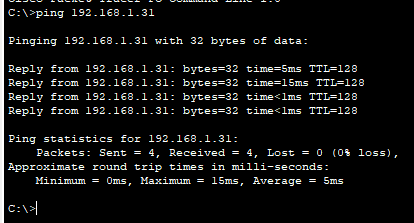
1. Отключите поиск DNS.
2. Присвойте имена устройствам в соответствии с топологией.
3. Назначьте **class** в качестве зашифрованного пароля доступа к привилегированному режиму.
4. Настройте IP-адреса для коммутаторов, указанных в таблице адресации.
5. На каждом коммутаторе настройте шлюз по умолчанию.
6. Назначьте **cisco** в качестве пароля консоли и VTY и включите запрос пароля при подключении.
7. Настройте **logging synchronous**, чтобы сообщения от консоли не могли прерывать ввод команд.
8. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

**S1, по аналогии для S3 в соответствии с таблицей адресации**



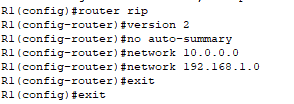
**Шаг 6: Проверьте подключение между PC-A и PC-C.**

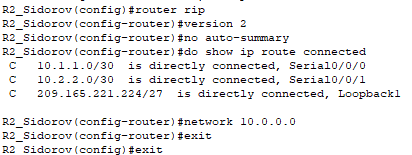
Отправьте ping-запрос с компьютера PC-A на компьютер PC-C. Удалось ли получить ответ?

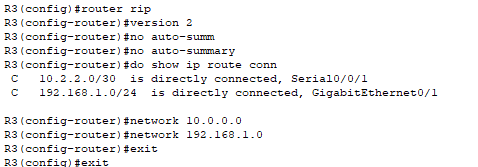


**Шаг 7: Настройте маршрутизацию.**

1. Настройте RIP версии 2 на всех маршрутизаторах. Добавьте в процесс RIP все сети, кроме 209.165.X+200.224/27.



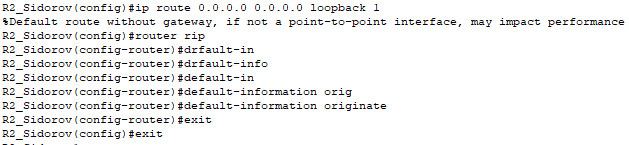




1. Настройте маршрут по умолчанию на маршрутизаторе R2\_ФАМИЛИЯ с использованием Lo1 в качестве интерфейса выхода в сеть 209.165.X+200.224/27.
2. На маршрутизаторе R2\_ФАМИЛИЯ используйте следующие команды для перераспределения маршрута по умолчанию в процесс RIP.

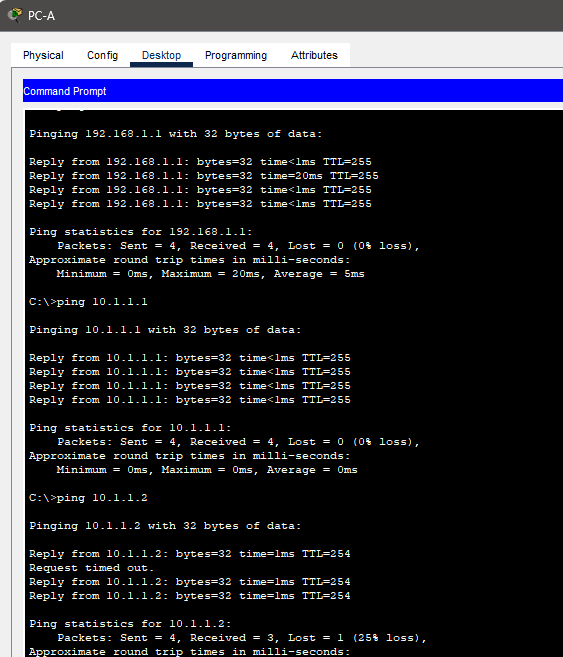
R2\_ФАМИЛИЯ(config)# **router rip**

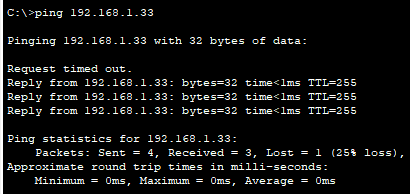
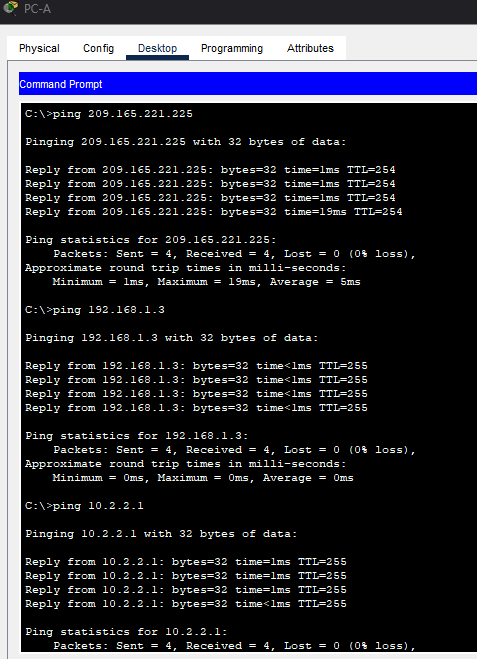
R2\_ФАМИЛИЯ(config-router)# **default-information originate**



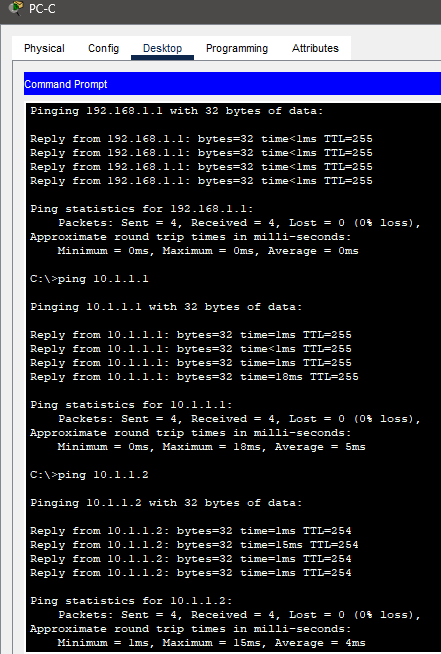
**Шаг 8: Проверьте подключение.**

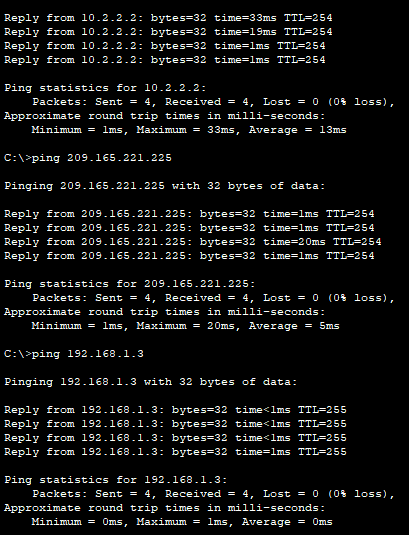
1. Необходимо получить ответ на ping-запросы с компьютера PC-A от каждого интерфейса на маршрутизаторах R1, R2\_ФАМИЛИЯ и R3, а также от компьютера PC-C. Удалось ли получить все ответы?

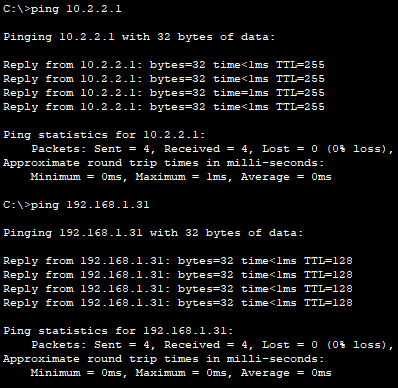




1. Необходимо получить ответ на ping-запросы с компьютера PC-C от каждого интерфейса на маршрутизаторах R1, R2\_ФАМИЛИЯ и R3, а также от компьютера PC-A. Удалось ли получить все ответы?







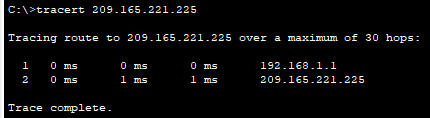
# Часть 2: Настройка обеспечения избыточности на первом хопе с помощью HSRP

Даже если топология спроектирована с учетом избыточности (два маршрутизатора и два коммутатора в одной сети LAN), оба компьютера, PC-A и PC-C, необходимо настраивать с одним адресом шлюза. PC-A использует R1, а PC-C — R3. В случае сбоя на одном из этих маршрутизаторов или интерфейсов маршрутизаторов компьютер может потерять подключение к сети Интернет.

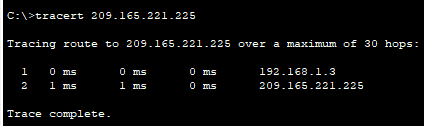
В части 2 вам предстоит изучить поведение сети до и после настройки протокола HSRP. Для этого вам понадобится определить путь, по которому проходят пакеты, чтобы достичь loopback-адрес на R2\_ФАМИЛИЯ.

**Шаг 1: Определите путь интернет-трафика для PC-A и PC-C.**

В командной строке на PC-A введите команду **tracert** для loopback-адреса 209.165.X+200.225 на маршрутизаторе R2\_ФАМИЛИЯ.

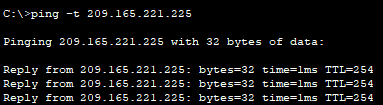


В командной строке на PC-С введите команду **tracert** для loopback-адреса 209.165.X+200.225 на маршрутизаторе R2\_ФАМИЛИЯ.

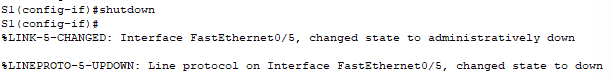


**Шаг 2: Запустите сеанс эхо-тестирования на PC-A и разорвите соединение между S1 и R1.**

1. В командной строке на PC-A введите команду **ping –t** для адреса **209.165.X+200.225** на маршрутизаторе R2\_ФАМИЛИЯ. Убедитесь, что окно командной строки открыто.

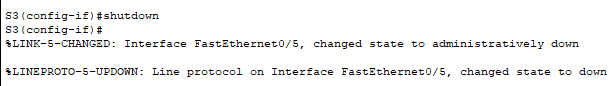


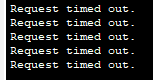
1. В процессе эхо-тестирования отсоедините кабель Ethernet от интерфейса F0/5 на S1. Отключение интерфейса F0/5 на S1 приведет к тому же результату.



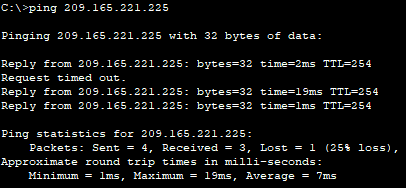


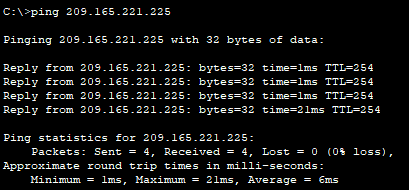
1. Какими были бы результате при повторении шагов 2a и 2b на компьютере PC-C и коммутаторе S3?





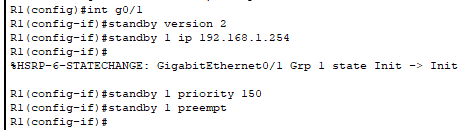
1. Повторно подсоедините кабели Ethernet к интерфейсу F0/5 или включите интерфейс F0/5 на S1 и S3, соответственно. Повторно отправьте эхо-запросы на 209.165.X+200.225 с компьютеров PC-A и PC-C, чтобы убедиться в том, что подключение восстановлено.



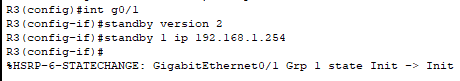


**Шаг 3: Настройте HSRP на R1 и R3.**

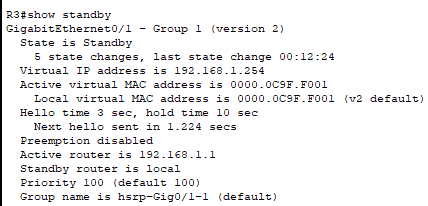
В этом шаге вам предстоит настроить HSRP и изменить адрес шлюза по умолчанию на компьютерах PC-A, PC-C, S1 и коммутаторе S2 на виртуальный IP-адрес для HSRP. R1 назначается активным маршрутизатором с помощью команды приоритета HSRP. a. Настройте протокол HSRP на маршрутизаторе R1.

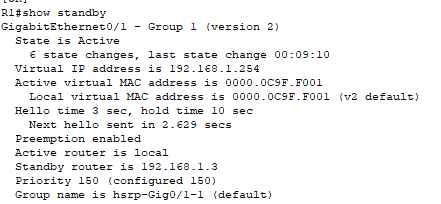


1. Настройте протокол HSRP на маршрутизаторе R3.

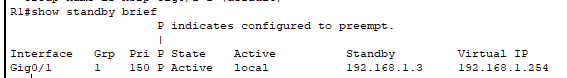


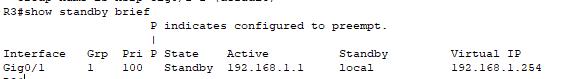
1. Проверьте HSRP, выполнив команду **show standby** на R1 и R3.





1. Используйте команду **show standby brief** на R1 и R3, чтобы просмотреть сводку состояния HSRP. Выходные данные приведены ниже.

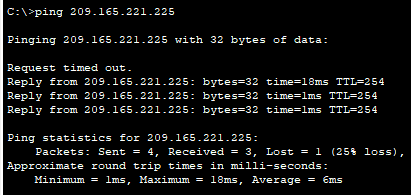


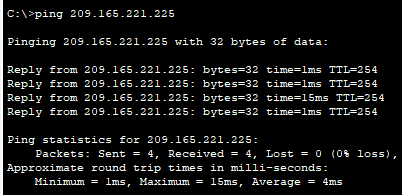


1. Измените адрес шлюза по умолчанию для PC-A, PC-C, S1 и S3. Какой адрес следует использовать?

**192.168.1.254**

1. Проверьте новые настройки. Отправьте эхо-запрос с PC-A и с PC-C на loopback-адрес маршрутизатора R2\_ФАМИЛИЯ. Успешно ли выполнены эхо-запросы?

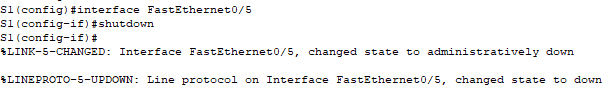


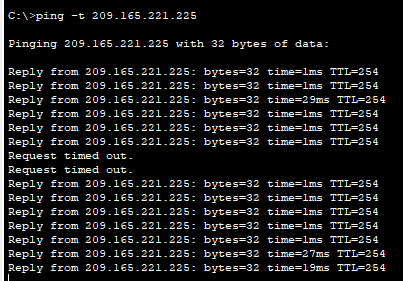


**Шаг 4: Запустите сеанс эхо-тестирования на PC-A и разорвите соединение**

**с коммутатором, подключенным к активному маршрутизатору HSRP (R1).**

1. В командной строке на PC-A введите команду **ping –t** для адреса 209.165.X+200.225 на маршрутизаторе R2. Убедитесь, что окно командной строки открыто.
2. Во время отправки эхо-запроса отсоедините кабель Ethernet от интерфейса F0/5 на коммутаторе S1 или выключите интерфейс F0/5.

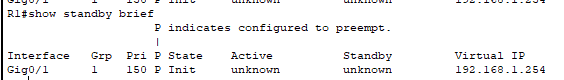


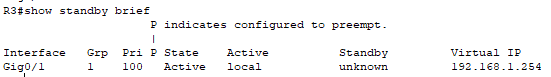


**Шаг 5: Проверьте настройки HSRP на маршрутизаторах R1 и R3.**

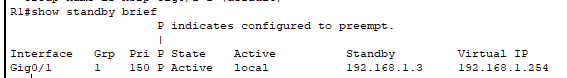
1. Выполните команду **show standby brief** на маршрутизаторах R1 и R3.

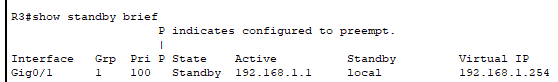
**До включения**





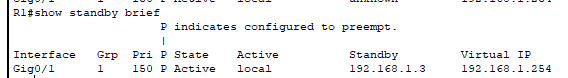
**После включения**

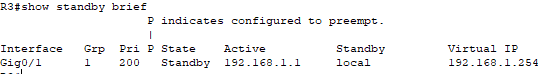




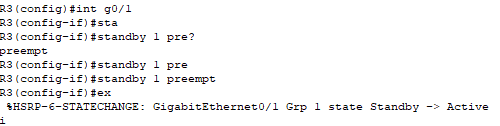
**Шаг 6: Изменение приоритетов HSRP.**

1. Измените приоритет HSRP на 200 на маршрутизаторе R3. Какой маршрутизатор является активным?

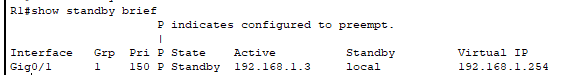


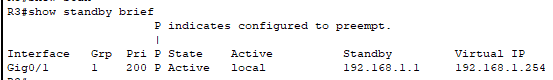


1. Выполните команду, чтобы сделать активным маршрутизатор R3 без изменения приоритета. Какую команду вы использовали?



1. Используйте команду **show**, чтобы убедиться, что R3 является активным маршрутизатором.





## Вопросы для защиты теоретической части (главы 9, 10, 16)

**Для чего необходимо резервирование маршрутизаторов? Опишите преимущества протокола HSRP.**

Резервирование маршрутизаторов необходимо для обеспечения непрерывной работы сети в случае отказа одного из маршрутизаторов. Протокол HSRP (Hot Standby Router Protocol) предоставляет механизм резервирования, позволяющий создать виртуальный маршрутизатор, который будет служить как резервный для активного маршрутизатора. Преимущества HSRP включают в себя увеличение надежности сети, улучшение доступности ресурсов, а также возможность балансировки нагрузки.

**Какие роли исёполняют активный, резервный и виртуальный маршрутизатор? Каким образом происходит процесс выбора активного маршрутизатора?**

Активный маршрутизатор: основной маршрутизатор, обрабатывающий трафик в сети.

Резервный маршрутизатор: запасной маршрутизатор, готовый заменить активный в случае его отказа.

Виртуальный маршрутизатор: абстрактная сущность, создаваемая протоколом HSRP для представления группы активного и резервного маршрутизаторов.

Процесс выбора активного маршрутизатора основан на приоритете, который назначается каждому маршрутизатору. Маршрутизатор с наивысшим приоритетом становится активным. В случае равенства приоритетов используется MAC-адрес маршрутизатора для выбора активного.

**Что происходит в случае сбоя активного маршрутизатора? Что произойдет, если в сети появится маршрутизатор с более высоким приоритетом?**

При сбое активного маршрутизатора резервный маршрутизатор автоматически принимает роль активного, чтобы обеспечить непрерывность работы сети. Если в сети появится маршрутизатор с более высоким приоритетом, он станет активным, а бывший активный маршрутизатор примет роль резервного.

Что необходимо сделать для возобновления процесса выбора активного маршрутизатора? Опишите состояния протокола HSRP.

Для возобновления процесса выбора активного маршрутизатора необходимо изменить условия приоритета (например, изменить приоритет текущего активного маршрутизатора или добавить новый маршрутизатор с более высоким приоритетом). Состояния протокола HSRP включают в себя:

Initial (Инициализация)

Learn (Обучение)

Listen (Слушание)

Speak (Речь)

Standby (Резервный)

Active (Активный)

**В каком случае сработает приоритетное вытеснение маршрутизатора? Опишите принцип работы сетевой атаки DDoS.**

Приоритетное вытеснение маршрутизатора сработает, если в сеть войдет маршрутизатор с более высоким приоритетом, чем у текущего активного маршрутизатора, заставив его стать резервным. Сетевая атака DDoS (Distributed Denial of Service) предполагает насыщение целевой системы или сети трафиком из большого количества источников, что приводит к перегрузке и отказу в обслуживании.

**Дайте характеристику компонентам AAA. Как будет вести себя коммутатор в результате успешной атаки на таблицу CAM?**

Компоненты AAA (Authentication, Authorization, Accounting) обеспечивают механизмы аутентификации, авторизации и учета пользователей в сети. Коммутатор в результате успешной атаки на таблицу CAM (Content Addressable Memory) может потерять информацию о соответствии MAC-адресов и портов, что приведет к некорректному пересылке пакетов и возможному отказу в обслуживании.

**Опишите принцип работы атаки с двойным тегированием. В чем заключается опасность ARP атак?**

Атака с двойным тегированием (Double Tagging) заключается в манипуляции с VLAN тегами в сети, что может позволить злоумышленнику получить доступ к данным в других VLAN. Опасность ARP атак (Address Resolution Protocol) заключается в возможности перехвата и подмены ARP-запросов и ответов, что может привести к перенаправлению трафика на злоумышленный узел.

**В чем заключается потенциальная опасность использование протокола CDP? Как поступит маршрутизатор, если на нем не настроен маршрут по умолчанию и пакет должен быть перенаправлен в сеть назначения, которая не указана в его таблице маршрутизации?**

Потенциальная опасность использования протокола CDP (Cisco Discovery Protocol) заключается в возможности получения злоумышленником информации о топологии сети и используемых устройствах. Если на маршрутизаторе не настроен маршрут по умолчанию и пакет должен быть перенаправлен в сеть назначения, которая не указана в его таблице маршрутизации, маршрутизатор отклонит пакет и отправит сообщение об ошибке.

**Какие данные могут быть получены с помощью протокола CDP? Каким образом можно провести атаку STP протокола?**

С помощью протокола CDP можно получить информацию о соседних устройствах, используемых интерфейсах и их параметрах, таких как платформа и версия программного обеспечения. Атаку на протокол STP (Spanning Tree Protocol) можно провести, например, с помощью подмены BPDU-пакетов (Bridge Protocol Data Units), что может привести к созданию петли в сети и нарушению ее работы.

**В чем заключается опасность DHCP-спуфинга? Опишите метод сетевой атаки VLAN Hopping.**

Опасность DHCP-спуфинга заключается в возможности злоумышленника подменить легитимный DHCP-сервер в сети, предоставив клиентам некорректную конфигурацию сети, например, указав в качестве шлюза злонамеренный маршрутизатор. Метод сетевой атаки VLAN Hopping основан на эксплуатации недостатков конфигурации коммутаторов, позволяющих злоумышленнику получить доступ к данным в других VLAN путем отправки трафика, содержащего двойные VLAN теги.