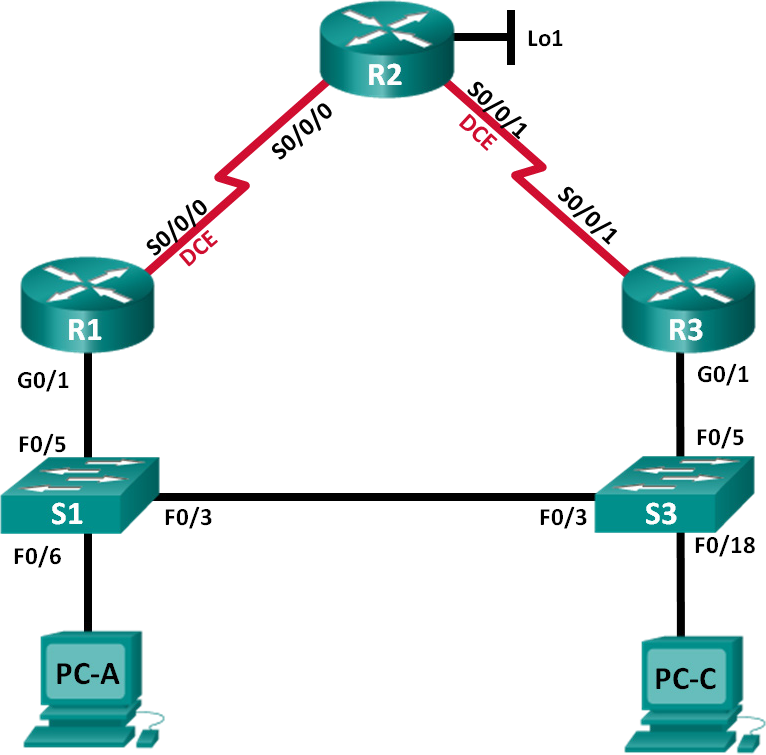


Настройка HSRP

**Топология**



**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.X+200.225 | 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**

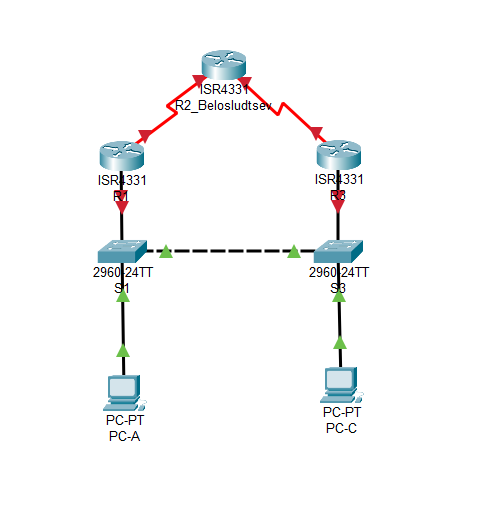
* 3 маршрутизатора (Cisco 1941 с операционной системой Cisco IOS версии 15.2(4)M3 (универсальный образ) или аналогичная модель)
* 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
* 2 компьютера (ОС Windows с программой эмуляции терминала, например, 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.

## PC-A:

## 

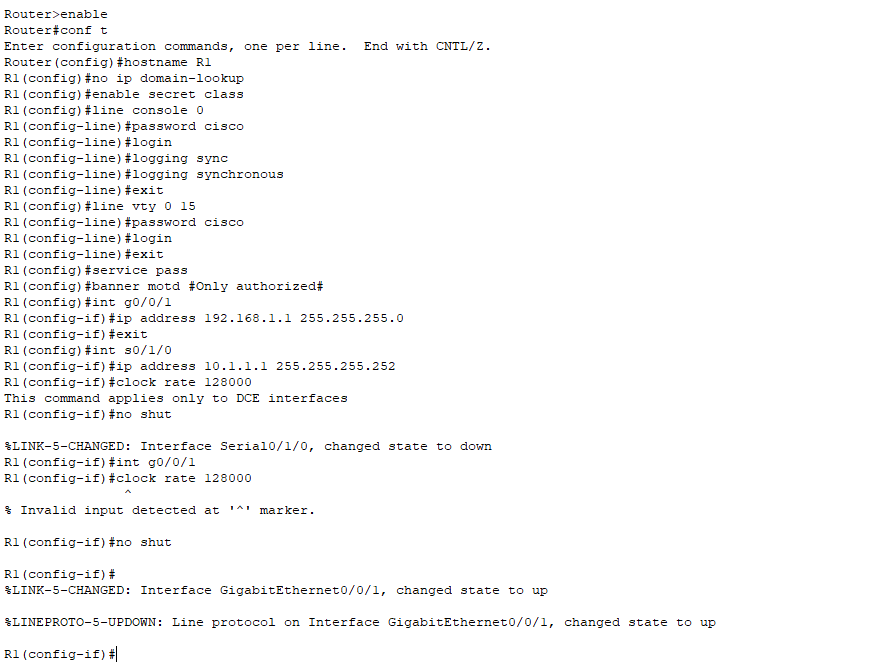
## PC-:

## 

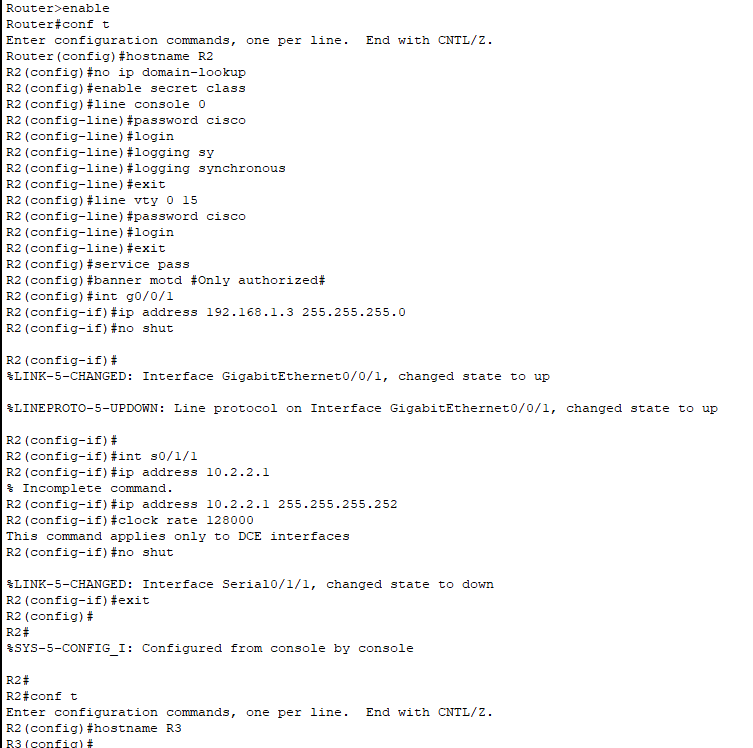
**Шаг 3: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов. Шаг 4: Произведите базовую настройку маршрутизаторов.**

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.

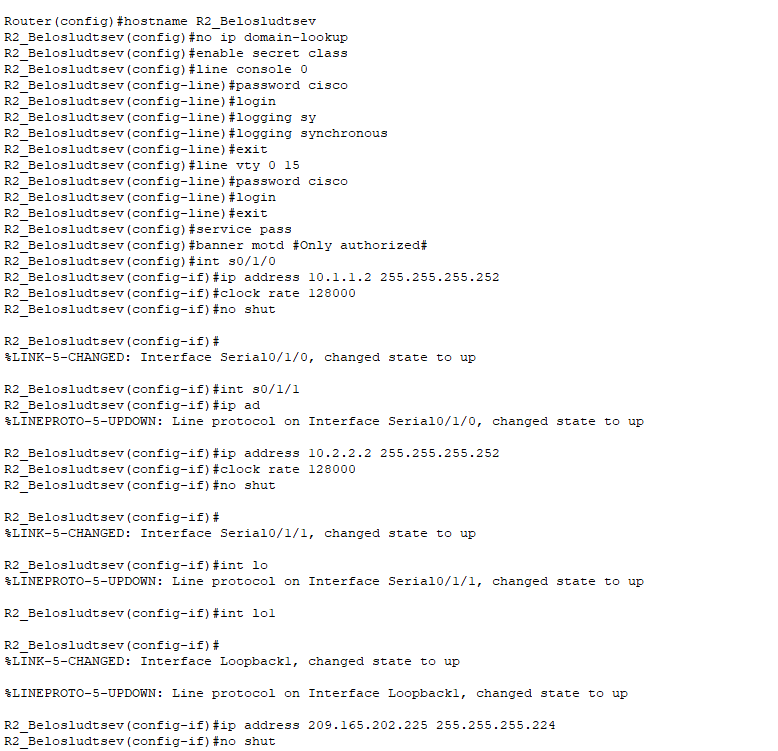
Настройка R1:



Настройка R3:



Настройка R2:



## 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.

Настройка S1:



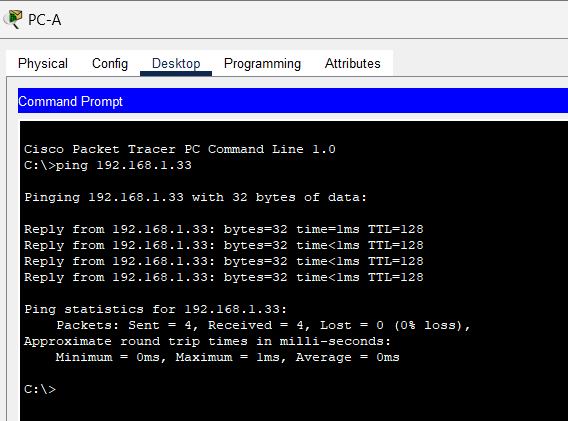
Настройка S3:



## 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?

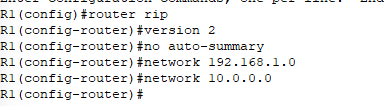
Если команды ping завершились неудачно и связь установить не удалось, исправьте ошибки в основных настройках устройства.



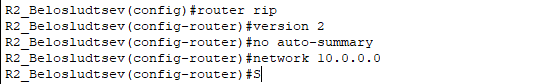
## Шаг 7: Настройте маршрутизацию.

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

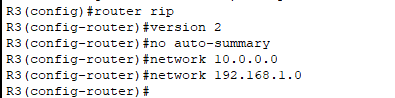
Настройка R1:



Настройка R2:



Настройка R3:



1. Настройте маршрут по умолчанию на маршрутизаторе R2\_ФАМИЛИЯ с использованием Lo1 в качестве интерфейса выхода в сеть 209.165.X+200.224/27.



1. На маршрутизаторе R2\_ФАМИЛИЯ используйте следующие команды для перераспределения маршрута по умолчанию в процесс RIP.

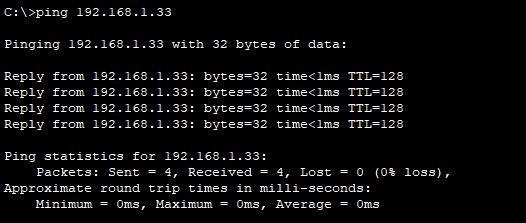
R2\_ФАМИЛИЯ(config)# **router rip**

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

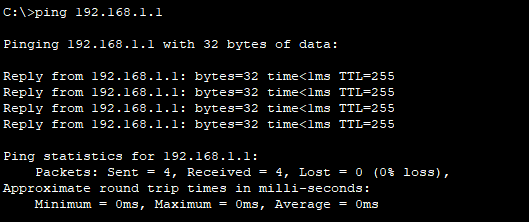


## Шаг 8: Проверьте подключение.

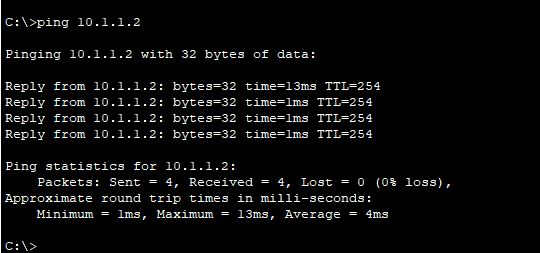
1. Необходимо получить ответ на ping-запросы с компьютера PC-A от каждого интерфейса на маршрутизаторах R1, R2\_ФАМИЛИЯ и R3, а также от компьютера PC-C. Удалось ли получить все ответы?

PC-A -> PC-C:  


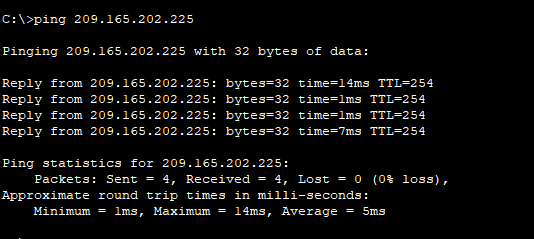
PC-A -> R1:



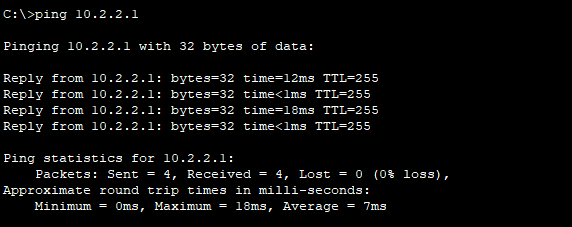
PC-A -> R2:



PC-A -> R2 (Lo1):

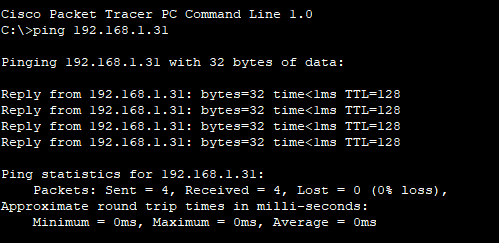


PC-A -> R3:

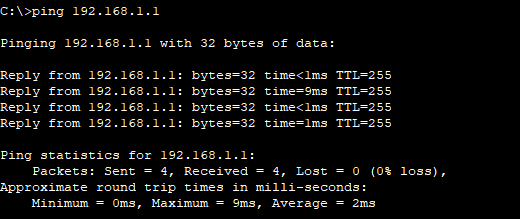


Если команды ping завершились неудачно и связь установить не удалось, исправьте ошибки в основных настройках устройства.

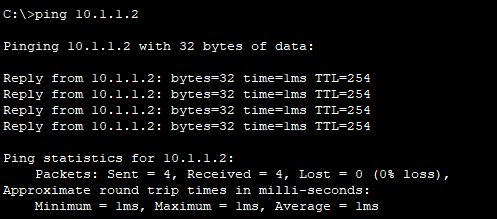
1. Необходимо получить ответ на ping-запросы с компьютера PC-C от каждого интерфейса на маршрутизаторах R1, R2\_ФАМИЛИЯ и R3, а также от компьютера PC-A. Удалось ли получить все ответы?

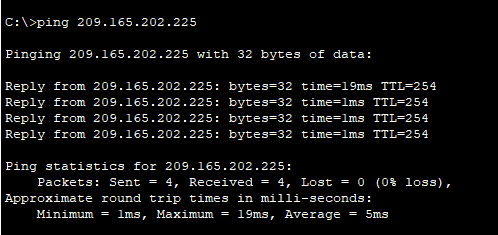
PC-C -> PC-A:  


PC-C -> R1:

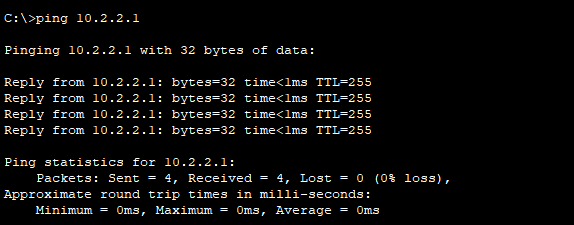


PC-C -> R2:

PC-C -> R2 (Lo1):



PC-C -> R3:



Если команды ping завершились неудачно и связь установить не удалось, исправьте ошибки в основных настройках устройства.

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

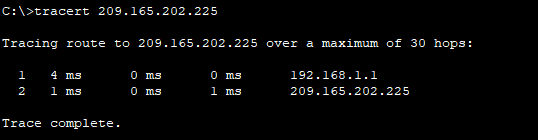
Даже если топология спроектирована с учетом избыточности (два маршрутизатора и два коммутатора в одной сети LAN), оба компьютера, PC-A и PC-C, необходимо настраивать с одним адресом шлюза. PC-A использует R1, а PC-C — R3. В случае сбоя на одном из этих маршрутизаторов или интерфейсов маршрутизаторов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

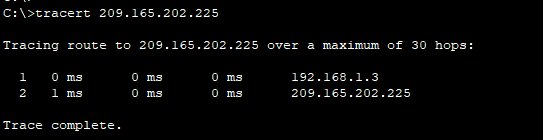
1. В командной строке на PC-A введите команду **tracert** для loopback-адреса 209.165.X+200.225 на маршрутизаторе R2\_ФАМИЛИЯ.

Какой путь прошли пакеты от PC-A до 209.165.X+200.225?



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

Какой путь прошли пакеты от PC-C до 209.165.X+200.225?



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

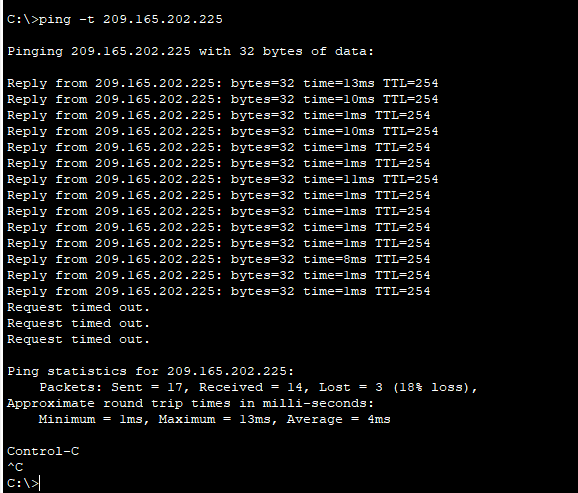
1. В командной строке на PC-A введите команду **ping –t** для адреса **209.165.X+200.225**

на маршрутизаторе R2\_ФАМИЛИЯ. Убедитесь, что окно командной строки открыто.

**Примечание**. Чтобы прервать отправку эхо-запросов, нажмите комбинацию клавиш **Ctrl**+**C** или закройте окно командной строки.

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.

Что произошло с трафиком эхо-запросов?



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

То же самое

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.

1. Настройте протокол HSRP на маршрутизаторе R1.

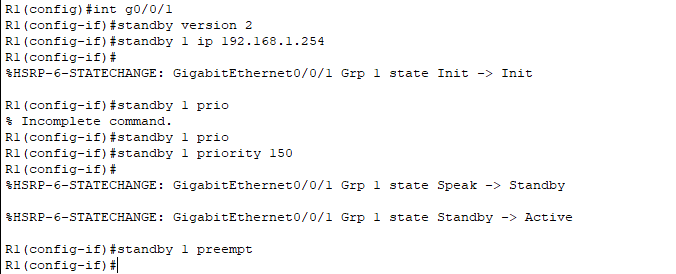
R1(config)# **interface g0/1**

R1(config-if)# **standby version 2**

R1(config-if)# **standby 1 ip 192.168.1.254**

R1(config-if)# **standby 1 priority 150**

R1(config-if)# **standby 1 preempt**

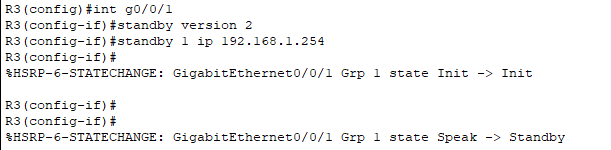
****

1. Настройте протокол HSRP на маршрутизаторе R3.

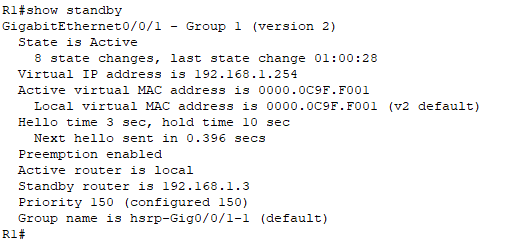
R3(config)# **interface g0/1**

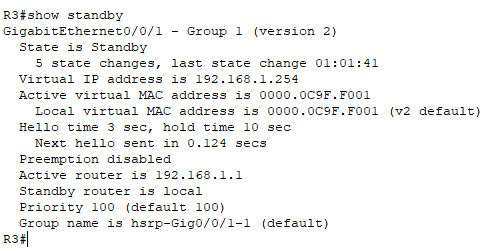
R3(config-if)# **standby version 2**

R3(config-if)# **standby 1 ip 192.168.1.254**

****

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

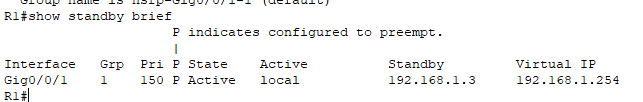


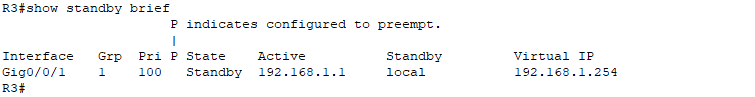


Используя указанные выходные данные, ответьте на следующие вопросы: Какой маршрутизатор является активным?

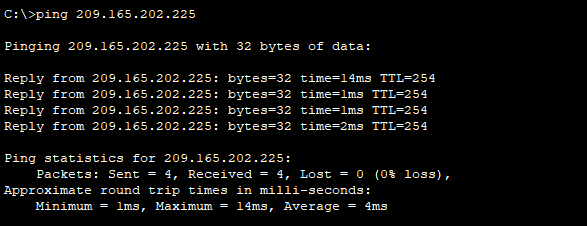
Какой MAC-адрес используется для виртуального IP-адреса? Какой IP-адрес и приоритет используются для резервного маршрутизатора?

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

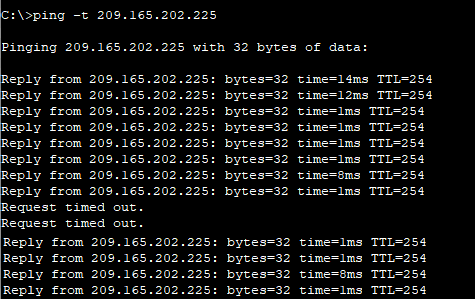


## Шаг 4: Запустите сеанс эхо-тестирования на PC-A и разорвите соединение

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

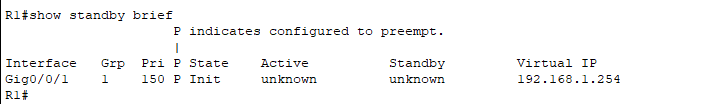
1. В командной строке на PC-A введите команду **ping –t** для адреса 209.165.X+200.225 на маршрутизаторе R2. Убедитесь, что окно командной строки открыто.
2. Во время отправки эхо-запроса отсоедините кабель Ethernet от интерфейса F0/5 на коммутаторе S1 или выключите интерфейс F0/5.

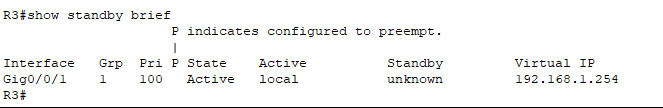
Что произошло с трафиком эхо-запросов?



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

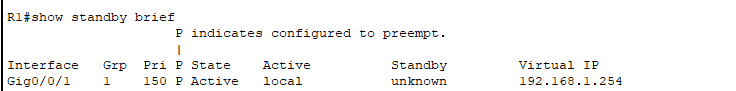
1. Выполните команду **show standby brief** на маршрутизаторах R1 и R3.

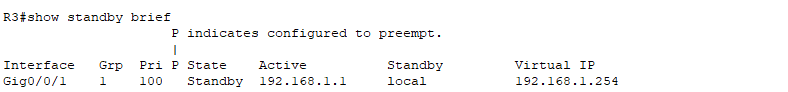




Какой маршрутизатор является активным?

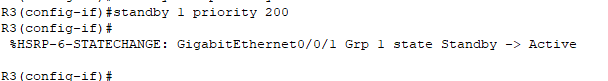
Повторно подключите кабель, соединяющий коммутатор и маршрутизатор, иливключите интерфейс F0/5. Какой маршрутизатор теперь является активным? Поясните ответ.

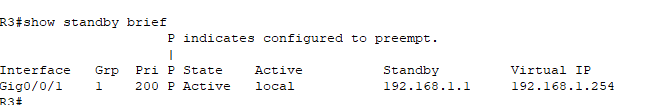




## Шаг 6: Изменение приоритетов HSRP.

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

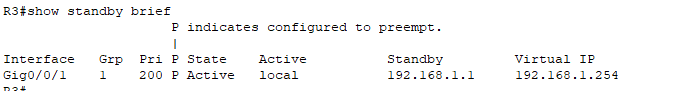




1. Выполните команду, чтобы сделать активным маршрутизатор R3 без изменения приоритета. Какую команду вы использовали?



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



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

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

Резервирование - Способ избежать потери доступа к внешней сети в случае сбоя маршрутизатора по умолчанию.

Протокол HSRP обеспечивает высокую доступность сети благодаря предоставлению функций обеспечения избыточности для маршрутизации на первом хопе для IPv4-узлов в сетях, настроенных с использованием IPv4-адреса шлюза по умолчанию.

2. Какие роли исполняют активный, резервный и виртуальный маршрутизатор? Каким образом происходит процесс выбора активного маршрутизатора?

Активным называется устройство, используемое для маршрутизации пакетов; резервным — устройство, которое задействуется в случае сбоя активного устройства или при выполнении предварительно заданных условий. Задача резервного маршрутизатора HSRP заключается в мониторинге рабочего состояния группы HSRP и быстром переходе к выполнению функций пересылки пакетов в случае сбоя активного маршрутизатора.

Роль активных и резервных маршрутизаторов определяется во время процесса выбора HSRP. По умолчанию в качестве активного выбирается маршрутизатор с максимальным в численном отношении адресом IPv4. Однако всегда лучше контролировать, как сеть будет работать в нормальных условиях, чем оставлять это на волю случая.

• Для определения активного маршрутизатора можно использовать приоритет HSRP.

• Маршрутизатор с наивысшим приоритетом HSRP станет активным маршрутизатором.

• По умолчанию приоритет HSRP равен 100.

• Если приоритеты равны, то в качестве активного выбирается маршрутизатор с максимальным в численном отношении адресом IPv4. • Чтобы настроить маршрутизатор в качестве активного, используйте команду интерфейса standby priority. Приоритеты HSRP имеют диапазон от 0 до 255.

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

В случае сбоя роль активного выполняет резервный

По умолчанию, после того как маршрутизатор становится активным, он остается таковым, даже если в сети появляется другой маршрутизатор с более высоким приоритетом HSRP.

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

Чтобы принудительно провести новый процесс выборов HSRP, когда маршрутизатор с более высоким приоритетом подключается в оперативный режим, необходимо включить механизм приоритетного вытеснения с помощью команды интерфейса standby preempt.

Initial – изменение конфигурации или вперве доступен

Learn – не определил вирт адрес, ждет сообщение от активного

Listen – известен адрес, но ни является ни активным ни резервным

Speak – отправляет периодические приветствия и участвует в выборе активного и/или резервного

Standby - кандидат на роль следующего активного маршрутизатора и периодически отправляет сообщения приветствия.

5. В каком случае сработает приоритетное вытеснение маршрутизатора? Опишите принцип работы сетевой атаке DDoS.

Приоритетное вытеснение позволяет маршрутизатору стать активным, только если у него более высокий приоритет. Если у маршрутизатора такой же приоритет, но больший адрес IPv4, он не будет вытеснять действующий активный маршрутизатор

Распределенный отказ в обслуживании (DDoS) – это скоординированная атака со многих устройств, называемых зомби, с целью ослабления или прекращения публичного доступа к веб-сайту и ресурсам организации.

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

Сервисы обеспечения сетевой безопасности AAA (аутентификация, авторизация и учет) предоставляют базовую архитектуру для настройки средств управления доступом на сетевом устройстве. ААА позволяет контролировать, какие пользователи имеют право доступа к сети (аутентификация), какие действия они могут выполнять, находясь в сети (авторизация), а также позволяет следить за их действиями во время доступа к сети (учет).

Злоумышленники изменяют MAC-адрес своего хоста в соответствии с другим известным MAC-адресом целевого хоста. Коммутатор перезаписывает текущую запись в таблице CAM и назначает MAC-адрес новому порту. Затем он пересылает кадры, предназначенные для целевого хоста, на атакующий хост

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

Атака с двойным тегированием — это один из типов атаки VLAN hopping, целью которой является получение несанкционированного доступа к виртуальной локальной сети.

Злоумышленник отправляет на доступный ему порт пакет данных, содержащий две метки VLAN: одна из них принадлежит доступному для него сегменту, а другая указывает на закрытую целевую сеть.

Первый маршрутизатор, на который поступает пакет, проверяет и удаляет тег VLAN злоумышленника. Данные передаются на второй свитч как легитимный пакет для атакуемой VLAN.

Хосты передают ARP-запрос в широковещательном режиме другим хостам в сегменте, чтобы определить MAC- адрес хоста с конкретным IP-адресом. Все хосты в подсети получают и обрабатывают этот ARP-запрос. Хост с IP-адресом, соответствующим ARP-запросу, отправляет ARP-ответ

Проблема заключается в том, что злоумышленник может отправить коммутатору сообщение gratuitous ARP, содержащее поддельный MAC-адрес, и коммутатор соответствующим образом обновит свою таблицу MAC- адресов. В типичной атаке субъект угрозы может отправлять незапрошенные ответы ARP другим узлам в подсети с MAC-адресом субъекта угрозы и IP-адресом шлюза по умолчанию

8. 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?

Информация протокола CDP отправляется через порты с поддержкой CDP в периодических незашифрованных широковещательных рассылках. Данные протокола CDP включают IP-адрес устройства, версию ОС IOS, а также сведения о платформе, возможностях и VLAN с нетегированным трафиком.

Если на маршрутизаторе не настроен маршрут по умолчанию (default route), и пакет должен быть перенаправлен в сеть назначения, которая не указана в его таблице маршрутизации, маршрутизатор обычно примет решение в зависимости от своей конфигурации:

Отправка ICMP сообщения об ошибке: Маршрутизатор может отправить обратно исходному узлу ICMP сообщение о недостижимости сети (Destination Unreachable), если такая функция включена в его настройках.

Пропуск пакета: Маршрутизатор может просто пропустить пакет без какого-либо ответа, что приведет к тому, что отправитель пакета может попытаться отправить его снова или принять другие меры для доставки.

Поиск альтернативных маршрутов: Некоторые маршрутизаторы могут пытаться использовать протокол маршрутизации для поиска альтернативных маршрутов к сети назначения. Если такие маршруты существуют, маршрутизатор может попытаться перенаправить пакет через один из них.

Отбрасывание пакета: В некоторых случаях маршрутизатор может просто отбросить пакет, если нет возможности определить путь доставки и нет настроенных механизмов для обработки таких ситуаций.

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

Данные протокола CDP включают IP-адрес устройства, версию ОС IOS, а также сведения о платформе, возможностях и VLAN с нетегированным трафиком.

Сетевые злоумышленники могут манипулировать протоколом связующего дерева (STP) для проведения атаки путем подмены корневого моста и изменения топологии сети. Злоумышленники могут сделать так, чтобы их хосты выглядели как корневые мосты, и в результате перехватить весь трафик ближайшего коммутируемого домена. Эта STP-атака нейтрализуется за счет реализации BPDU Guard на всех портах доступа.

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

Атака типа «DHCP-спуфинг» состоит в том, что к сети подключается мошеннический DHCP-сервер и предоставляет ложные параметры настройки IP легитимным клиентам. Подставной сервер может предоставлять различные неправильные сведения

VLAN hopping позволяет видеть трафик из одной VLAN в другой VLAN без помощи маршрутизатора. В базовой атаке VLAN hopping, атакующий настраивает узел так, чтобы он действовал как коммутатор, чтобы использовать функцию автоматического согласования магистрального порта включенную по умолчанию на большинстве портов коммутатора. Злоумышленник настраивает хост на подделку сигналов 802.1Q и проприетарной сигнализации DTP-протокола Cisco для магистрального канала между коммутаторами. В случае успеха коммутатор устанавливает магистральную связь с хостом. Теперь злоумышленник может получить доступ ко всем VLAN на коммутаторе. Хакер может отправлять и получать трафик в любой VLAN, эффективно переключаясь между VLAN.