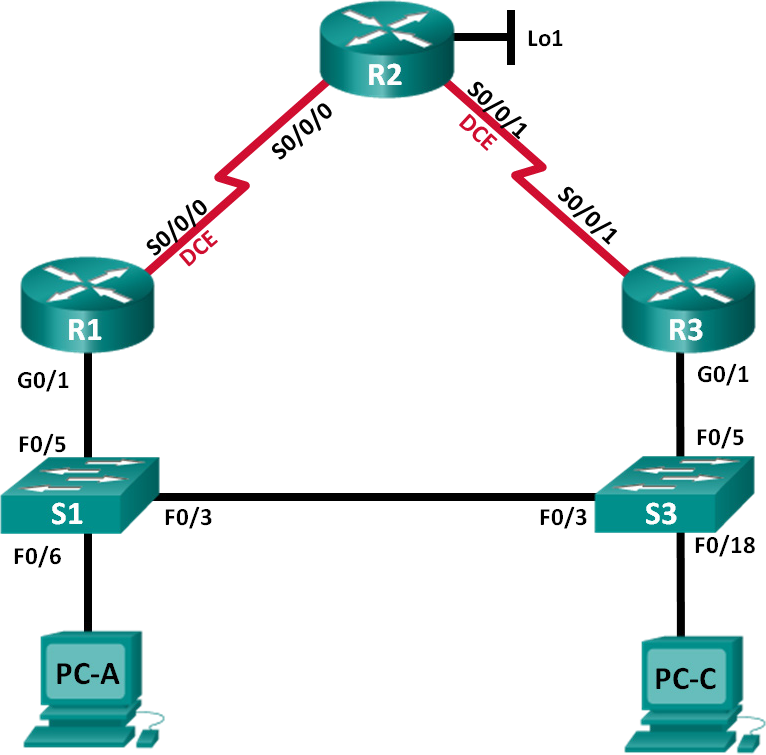
Лабораторная работа № 12: Настройка HSRP

**Выполнил студент: Ло Ван Хунг**

**Бариант: 15 (X)**

**Группа: ИНБО-04-20**

**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\_Dinh | S0/0/0 | 10.1.1.2 | 255.255.255.252 | — |
| S0/0/1 (DCE) | 10.2.2.2 | 255.255.255.252 | — |
| Lo1 | **209.165.215.225** | 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**

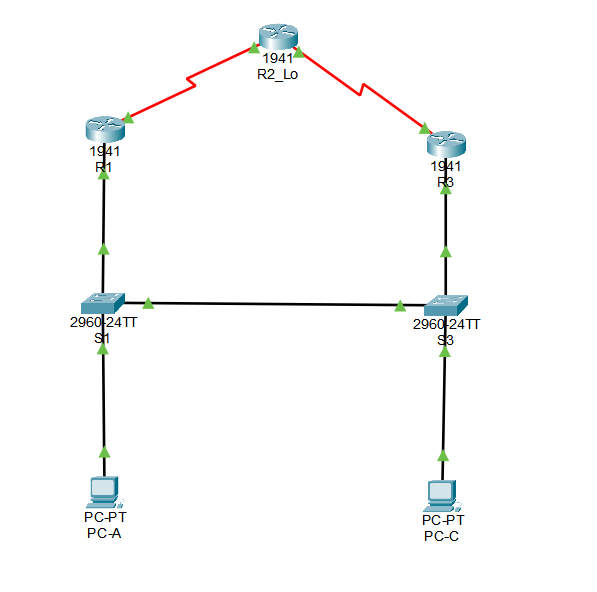
**Часть 2. Настройка обеспечения избыточности на первом хопе с помощью HSRP**

**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.

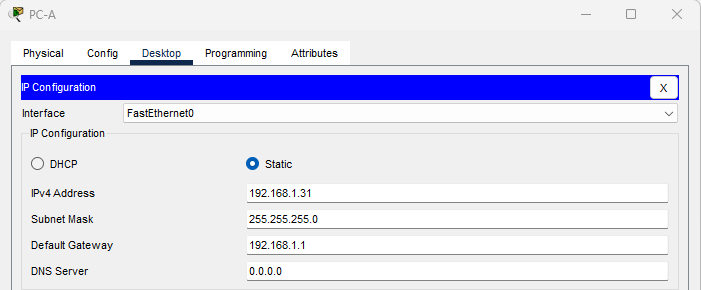


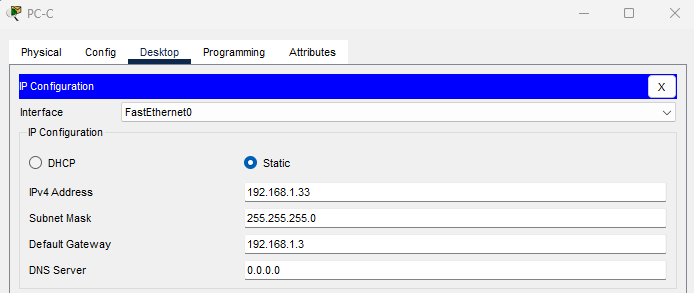
### Шаг 1: Создайте сеть согласно топологии.

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

### Шаг 2: Настройте узлы ПК.

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

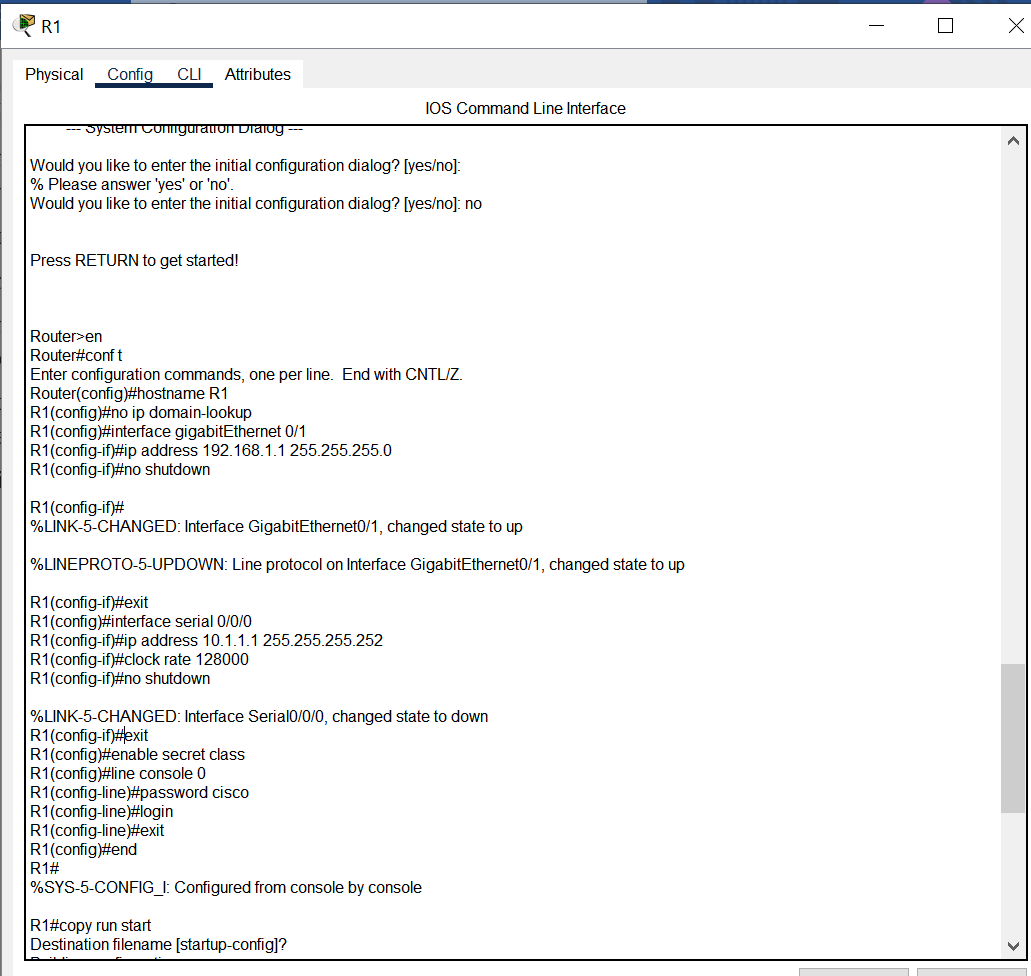
****

****

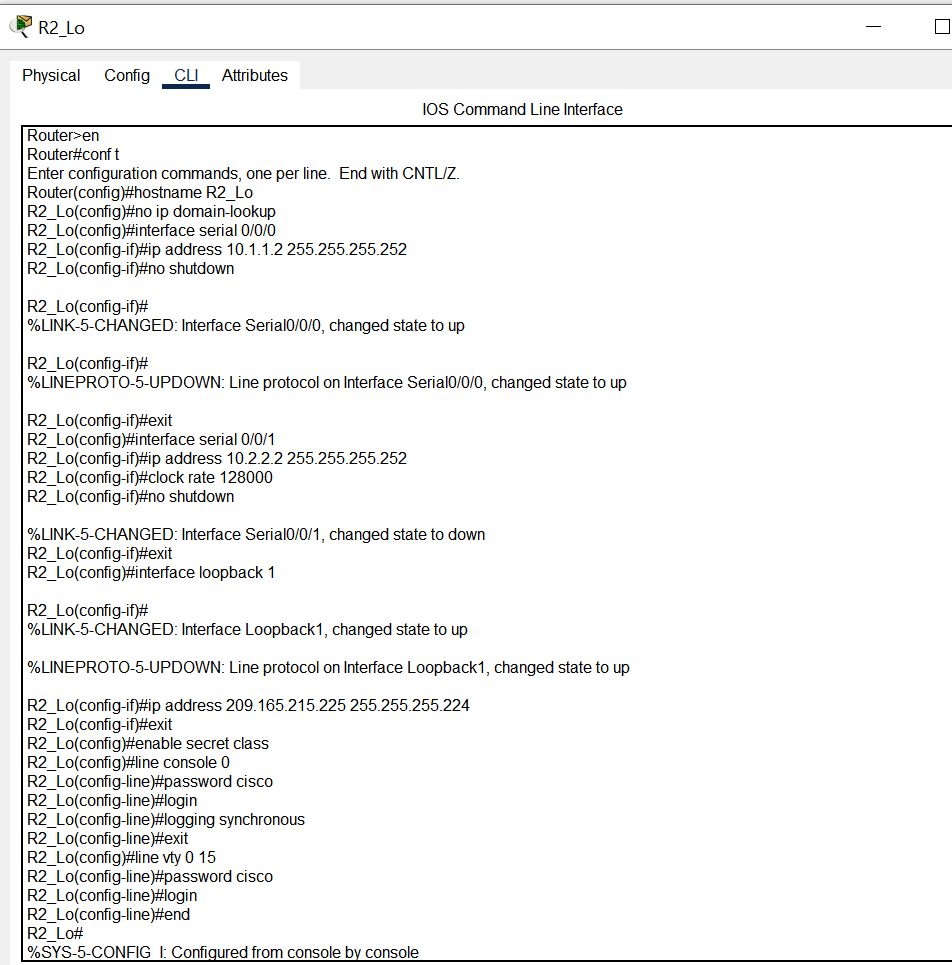
**Шаг 4: Произведите базовую настройку маршрутизаторов.**

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.

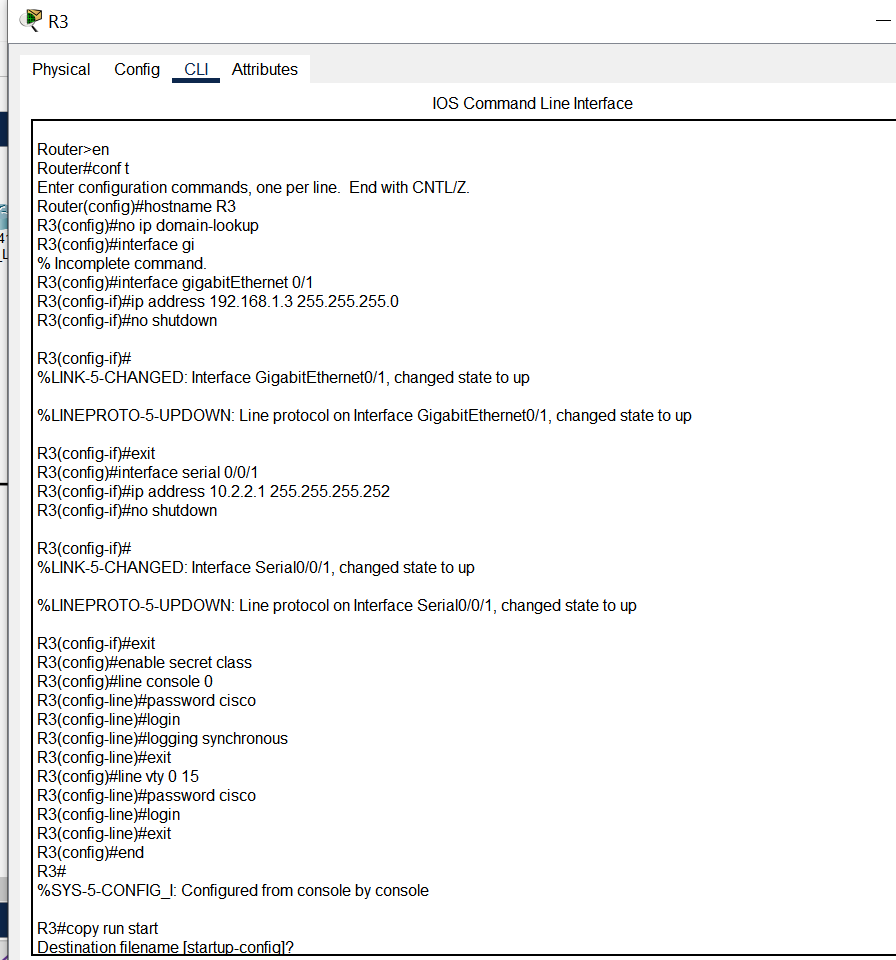
**R1:**



**R2\_Lo:**



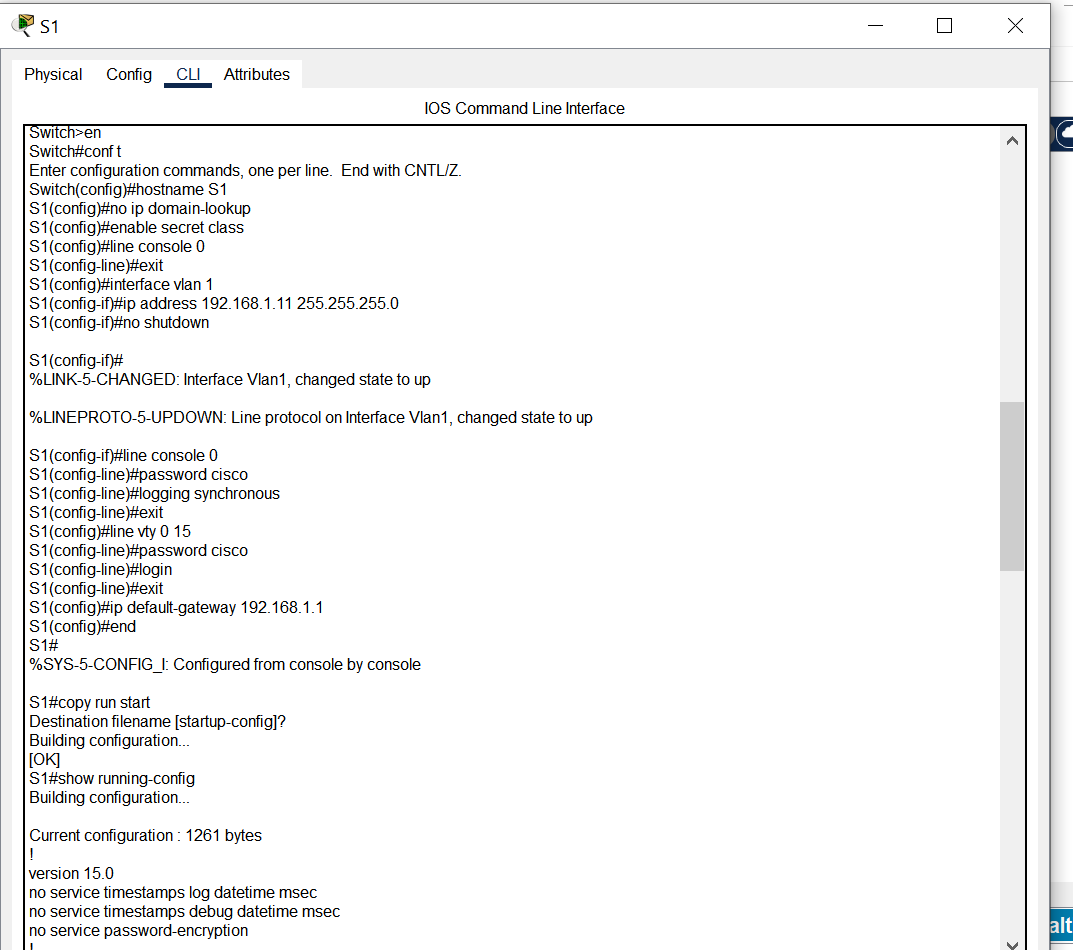
**R3:**



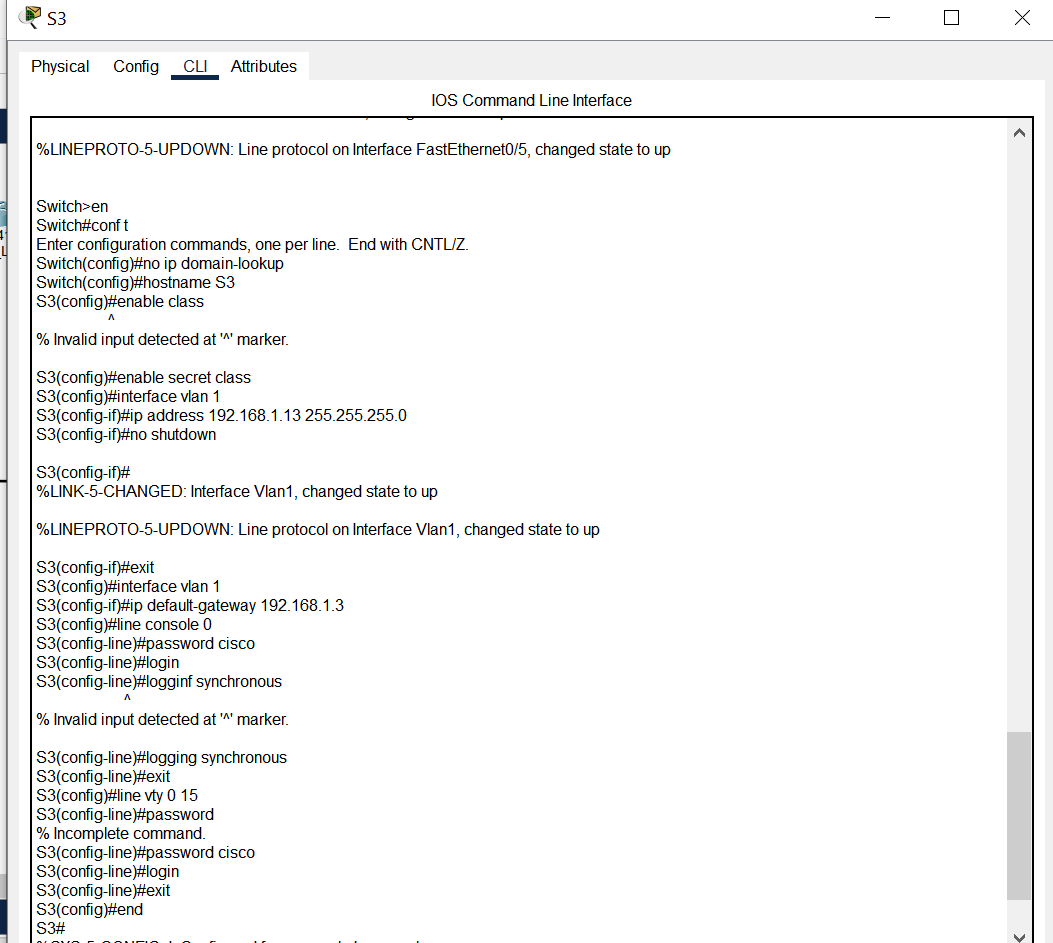
### Шаг 5: Настройте базовые параметры каждого коммутатора.

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:**

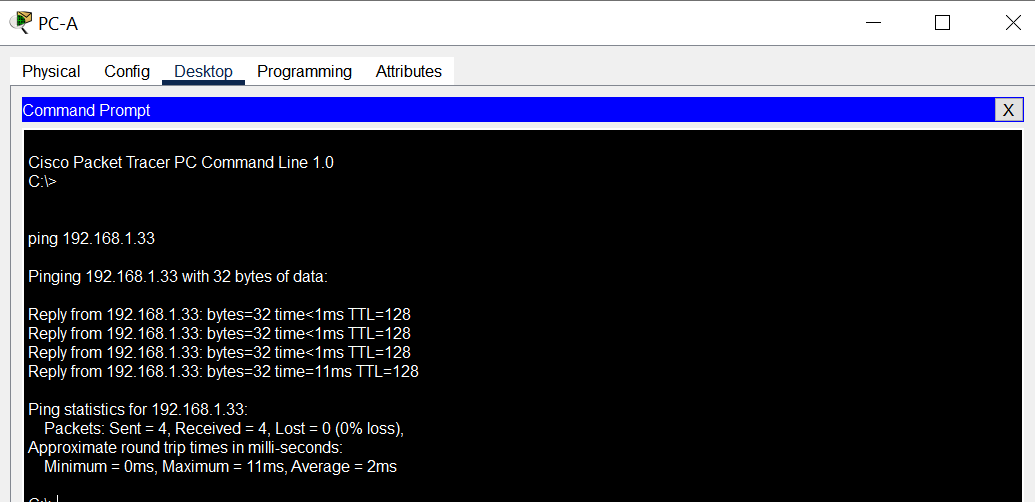


**S3:**



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

Отправьте ping-запрос с компьютера PC-A на компьютер PC-C. Удалось липолучить ответ? **Да**



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

### Шаг 7: Настройте маршрутизацию.

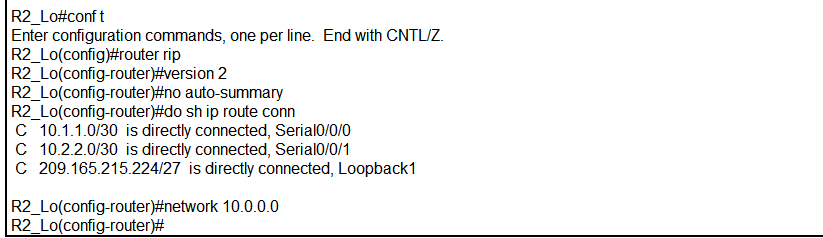
1. Настройте RIP версии 2 на всех маршрутизаторах. Добавьте в процесс RIP все сети, кроме 209.165.X+200.224/27.

**R1:**

Изображение выглядит как логотип

Автоматически созданное описание

**R2:**

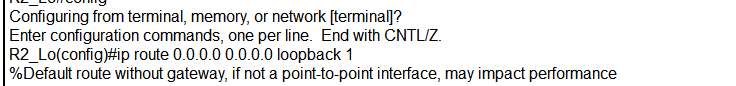


**R3:**

Изображение выглядит как текст

Автоматически созданное описание

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.

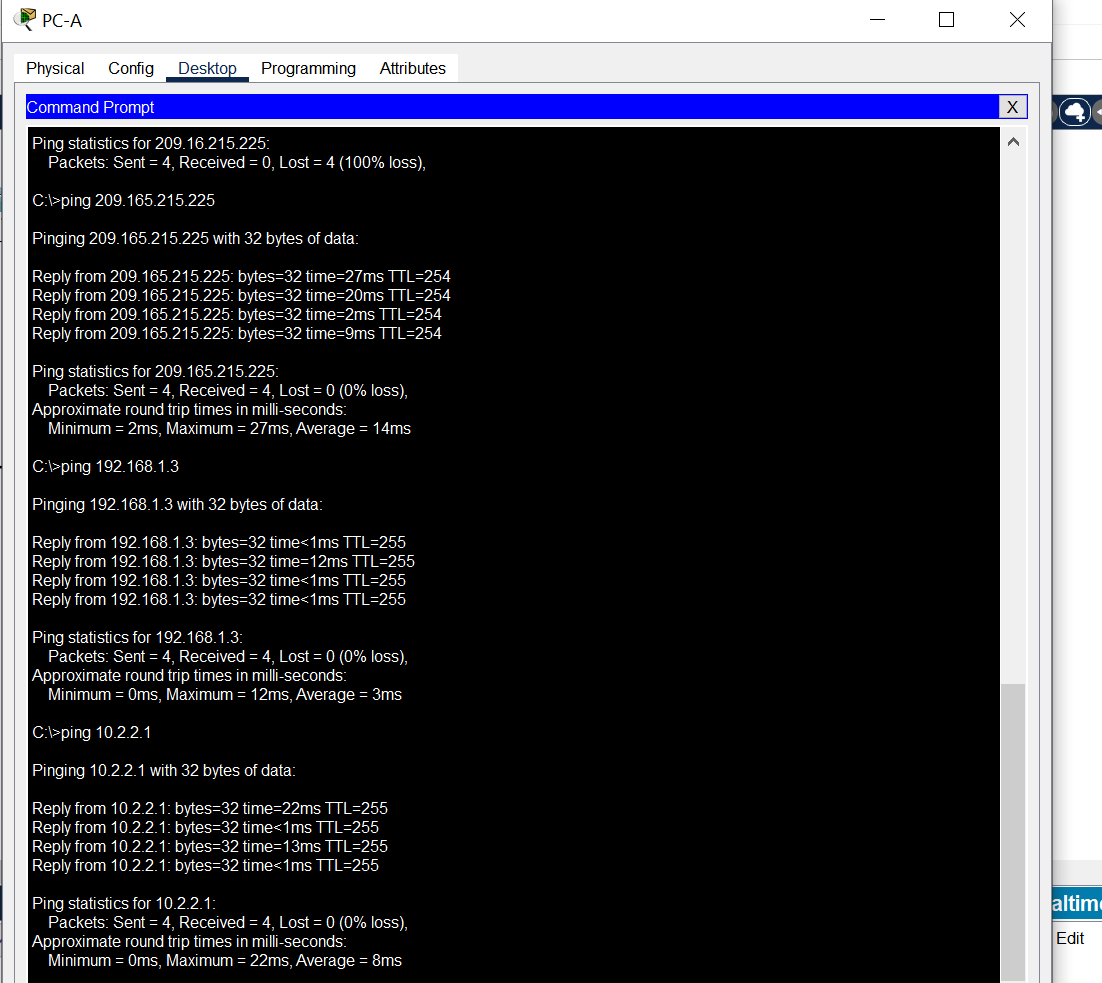
R2\_ФАМИЛИЯ(config)# **router rip**

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

****

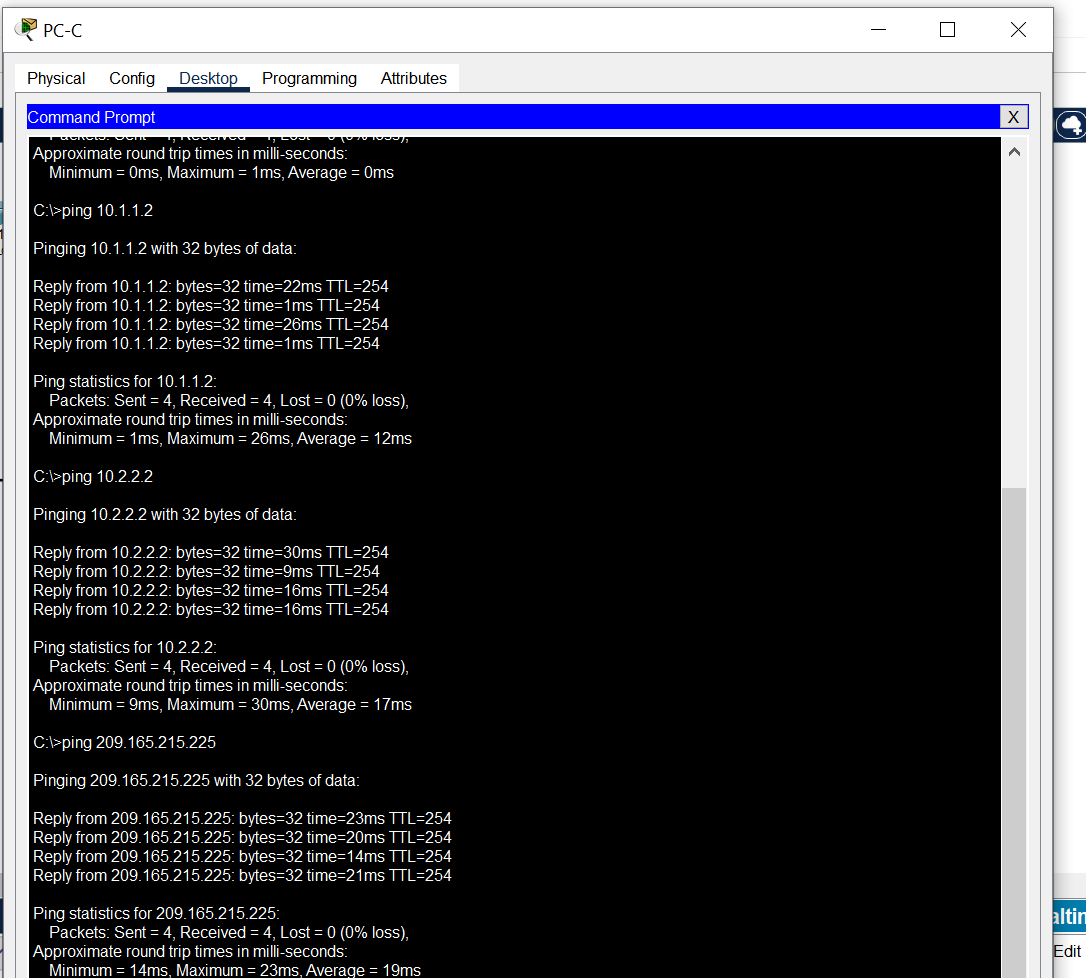
### Шаг 8: Проверьте подключение.

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? **Да**



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? **Да**

****

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.

Изображение выглядит как текст

Автоматически созданное описание

Какой путь прошли пакеты от PC-A до 209.165.X+200.225? PC-A -> R1 -> R2

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

Изображение выглядит как текст

Автоматически созданное описание

Какой путь прошли пакеты от PC-C до 209.165.X+200.225? **PC-C -> R3 -> R2**

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

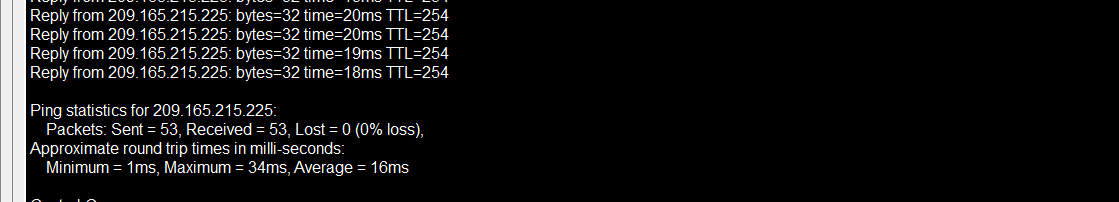
1. В командной строке на PC-A введите команду **ping –t** для адреса **209.165.X+200.225**

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

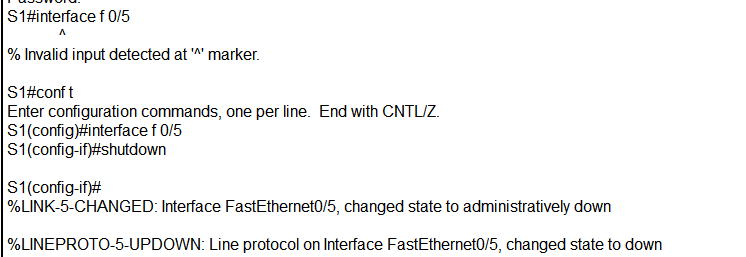
Изображение выглядит как текст

Автоматически созданное описание

**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.

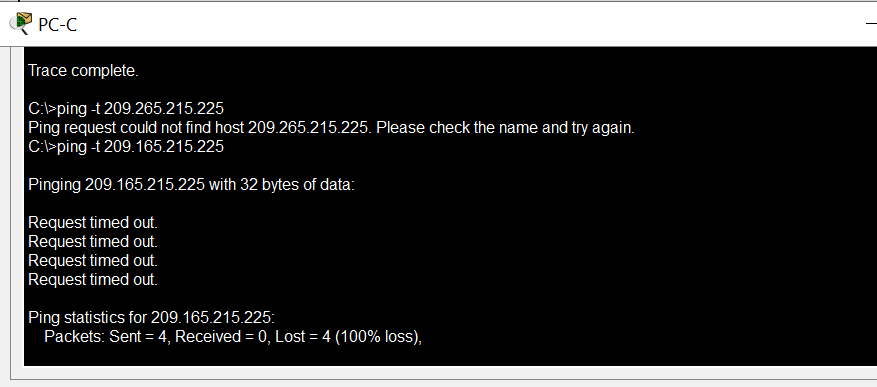


Что произошло с трафиком эхо-запросов?

Изображение выглядит как текст

Автоматически созданное описание

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.

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание

### 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.

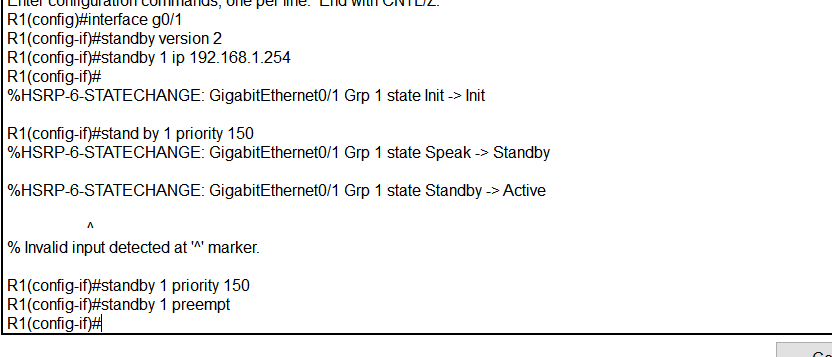
R1(config)# **interface g0/1**

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**

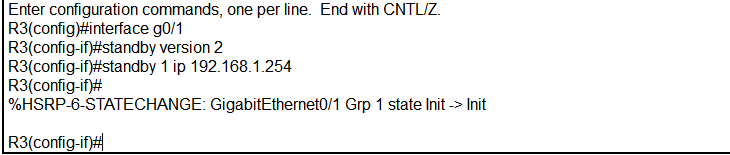
****

1. Настройте протокол HSRP на маршрутизаторе R3.

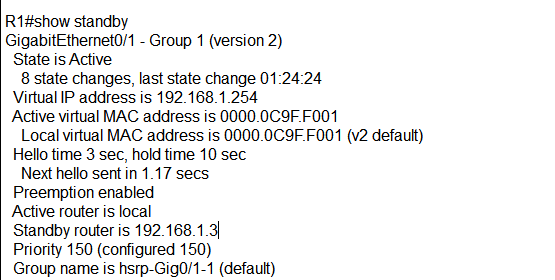
R3(config)# **interface g0/1**

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.



Изображение выглядит как текст

Автоматически созданное описание

Используя указанные выходные данные, ответьте на следующие вопросы: Какой маршрутизатор является активным? **GigabitEthernet0/1**

Какой MAC-адрес используется для виртуального IP-адреса? **0000.0C9F.F001** Какой IP-адрес и приоритет используются для резервного маршрутизатора? **192.168.1.254**

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

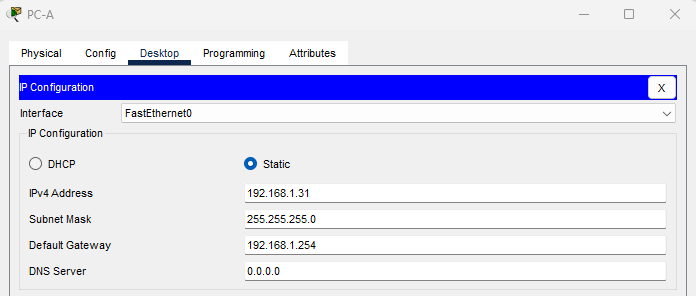
Изображение выглядит как текст, письмо

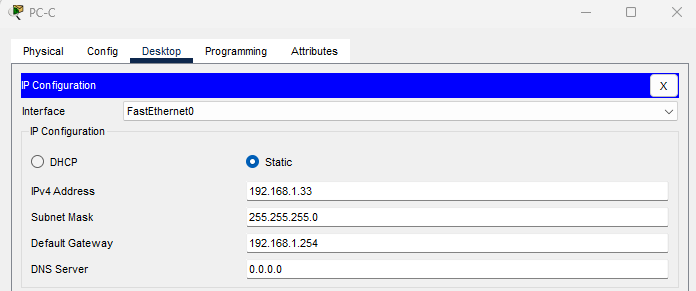
Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание

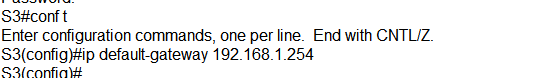
1. Измените адрес шлюза по умолчанию для PC-A, PC-C, S1 и S3. Какой адрес следует использовать?



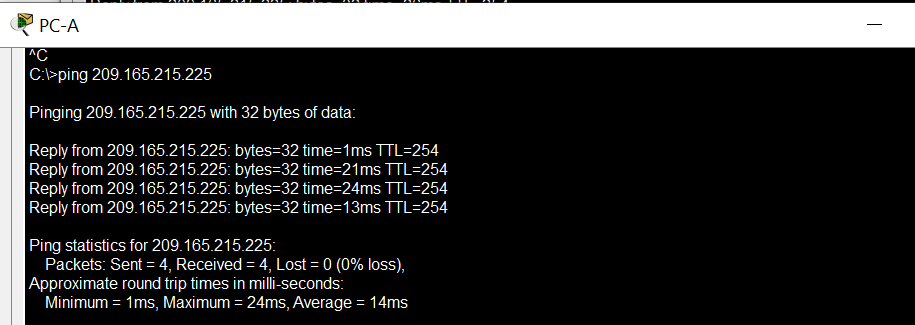


Изображение выглядит как текст

Автоматически созданное описание



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? **Да, можно**



Изображение выглядит как текст

Автоматически созданное описание

### 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.

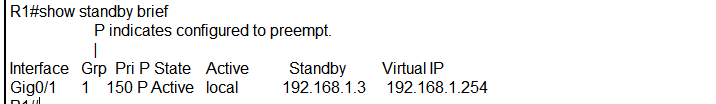
Изображение выглядит как текст

Автоматически созданное описание

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.

****

Изображение выглядит как текст

Автоматически созданное описание

Какой маршрутизатор является активным? **G0/1**

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

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

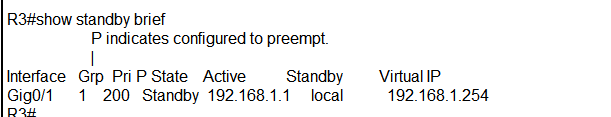
Автоматически созданное описание

### Шаг 6: Изменение приоритетов HSRP.

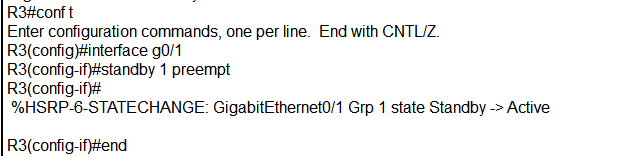
1. Измените приоритет HSRP на 200 на маршрутизаторе R3. Какой маршрутизатор является активным?

Изображение выглядит как текст

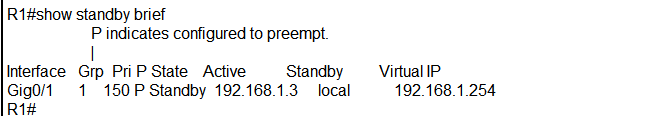
Автоматически созданное описание



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.



Изображение выглядит как текст

Автоматически созданное описание

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

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

Резервирование маршрутизаторов является важным элементом обеспечения высокой доступности сети. В случае отказа активного маршрутизатора, резервный маршрутизатор может быстро взять на себя его функции и обеспечить непрерывность работы сети.

Протокол HSRP (Hot Standby Router Protocol) является одним из протоколов резервирования маршрутизаторов. Его преимущества:

* Высокая скорость переключения между активным и резервным маршрутизаторами.
* Поддержка дополнительных опций, таких как приоритет и отслеживание интерфейсов.
* Работа с протоколами маршрутизации, включая RIP, OSPF и EIGRP.
* Простота настройки и поддержки.
* Поддержка IPv4 и IPv6.

В HSRP используется виртуальный IP-адрес, который представляет группу маршрутизаторов HSRP. Один маршрутизатор в группе является активным, а другой - резервным. Активный маршрутизатор пересылает пакеты, а резервный маршрутизатор следит за ним и готов к работе на случай сбоя активного маршрутизатора.

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

В схеме резервирования маршрутизаторов с применением протокола HSRP выделяются три роли:

* Активный маршрутизатор (Active) — маршрутизатор, который в текущий момент времени осуществляет пересылку трафика на сеть назначения.
* Резервный маршрутизатор (Standby) — маршрутизатор, который ожидает, когда активный маршрутизатор перестанет функционировать, чтобы занять его место и стать активным.
* Виртуальный маршрутизатор (Virtual) — представляет собой виртуальный IP-адрес, который используется как шлюз по умолчанию для устройств, подключенных к локальной сети.

Выбор активного маршрутизатора происходит на основе значения приоритета (Priority), который может быть задан вручную или автоматически рассчитываться на основе качества канала связи (например, меньшее значение задержки). Маршрутизатор с наибольшим значением приоритета становится активным, а маршрутизаторы с меньшим приоритетом — резервными. Если приоритеты маршрутизаторов равны, то выбирается маршрутизатор с наивысшим IP-адресом.

При отказе активного маршрутизатора, резервный маршрутизатор поднимает виртуальный IP-адрес и начинает пересылку трафика, таким образом, обеспечивается непрерывность работы сети.

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

В случае сбоя активного маршрутизатора резервный маршрутизатор автоматически становится активным и начинает обрабатывать сетевой трафик. При этом виртуальный IP-адрес переходит на резервный маршрутизатор. Если в сети появится маршрутизатор с более высоким приоритетом, то он станет активным, а текущий активный маршрутизатор будет переведен в состояние резервного. При этом виртуальный IP-адрес также переходит на новый активный маршрутизатор. В общем случае, выбор активного маршрутизатора происходит на основе приоритета, но также может учитываться доступность интерфейсов, качество соединения и другие факторы, зависящие от конкретной реализации протокола.

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

Для возобновления процесса выбора активного маршрутизатора необходимо выполнить перезагрузку или перевыбор активного маршрутизатора вручную.

Протокол HSRP имеет четыре состояния:

* Initial - начальное состояние. Маршрутизатор не имеет информации о других маршрутизаторах, работающих с протоколом HSRP.
* Learn - маршрутизатор узнает о существовании других маршрутизаторов, работающих с HSRP, и узнает, какой маршрутизатор имеет более высокий приоритет.
* Listen - маршрутизатор прослушивает сообщения от других маршрутизаторов, работающих с HSRP, и может получать обновления конфигурации от более приоритетного маршрутизатора.
* Speak - маршрутизатор отправляет сообщения HSRP на групповой адрес и принимает сообщения от других маршрутизаторов, работающих с HSRP, для проверки своего статуса.
  1. **В каком случае сработает приоритетное вытеснение маршрутизатора? Опишите принцип работы сетевой атаке DDoS.**

Приоритетное вытеснение маршрутизатора возможно в случае, если в сети появится новый маршрутизатор с более высоким приоритетом, чем текущий активный маршрутизатор HSRP. В этом случае новый маршрутизатор станет активным, а старый маршрутизатор будет вытеснен в роли резервного.

DDoS (Distributed Denial of Service) является типом сетевой атаки, при которой множество устройств, обычно компьютеров или других подключенных к сети устройств, работают вместе, чтобы уменьшить или полностью прервать доступ к сервису или ресурсу. Эти устройства называются ботами, зомби-компьютерами или устройствами-участниками. Целью DDoS атаки является перегрузка сетевого соединения, сервера или другого устройства, путем отправки большого количества запросов на обработку данных, что может привести к временному или постоянному отказу в обслуживании и прерыванию работы сети или приложения. Для проведения такой атаки может использоваться как статический список IP-адресов, так и динамические списки, формируемые в режиме реального времени на основе протоколов, подобных протоколу HSRP.

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

Компоненты AAA - это аутентификация, авторизация и учет (Accounting), которые используются для обеспечения безопасности в сетях.

* Аутентификация - это процесс проверки подлинности пользователей или устройств в сети. Например, при подключении пользователя к сети, ему может быть предложен ввод имени пользователя и пароля для проверки его подлинности.
* Авторизация - это процесс предоставления пользователям прав на выполнение определенных операций в сети. Например, администратор сети может предоставить права доступа к определенным сетевым ресурсам только определенным пользователям.
* Учет (Accounting) - это процесс отслеживания использования сетевых ресурсов пользователями. Например, администратор сети может отслеживать время, когда пользователь подключился к сети и использовал определенные ресурсы.

При успешной атаке на таблицу CAM (Content-Addressable Memory) коммутатор может начать вести себя неправильно, так как таблица CAM используется для хранения информации о MAC-адресах устройств, подключенных к коммутатору. Если таблица CAM была подвергнута атаке, то коммутатор может перестать правильно пересылать данные и может допускать ошибки в своей работе.

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

Атака с двойным тегированием (Double Tagging Attack) является методом обхода механизмов безопасности на коммутаторах, основанных на протоколе 802.1Q. Атакующий отправляет пакет с двумя тегами VLAN, первый тег оригинальный, а второй созданный атакующим. Коммутатор, который работает в режиме транк, может принять такой пакет и использовать второй тег в качестве исходного VLAN, что позволяет атакующему получить доступ к трафику, который находится в другом VLAN.

ARP (Address Resolution Protocol) атака – это метод атаки на сетевые устройства, основанный на подмене ARP-запросов и ответов. Атакующий может отправить ложный ARP-ответ, представляющий себя в качестве владельца IP-адреса, который фактически находится на другом устройстве. Это может привести к перехвату трафика, перехвату данных или отказу в обслуживании. Злоумышленник может использовать ARP-атаку, чтобы перехватить данные, передаваемые через коммутатор, и даже внести изменения в сетевой трафик, направленный на конкретный узел.

* 1. **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?**

Протокол CDP (Cisco Discovery Protocol) используется для обмена информацией между соседними устройствами Cisco в сети. Его потенциальная опасность заключается в том, что он может быть использован злоумышленниками для сбора информации об устройствах в сети, такой как тип и версия устройства, используемые интерфейсы и т.д., что может быть использовано для проведения атак на сетевые устройства.

Если на маршрутизаторе не настроен маршрут по умолчанию и пакет должен быть перенаправлен в сеть назначения, которая не указана в его таблице маршрутизации, то маршрутизатор будет использовать протокол маршрутизации для поиска маршрута к сети назначения. Если в сети настроены только статические маршруты, то необходимо добавить маршрут для данной сети в таблицу маршрутизации маршрутизатора. Если используется динамическая маршрутизация, то маршрутизатор будет искать маршрут с помощью протокола маршрутизации, такого как OSPF или EIGRP. Если маршрут не будет найден, то пакет будет отброшен.

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

Протокол CDP (Cisco Discovery Protocol) позволяет обнаруживать на сети устройства Cisco и получать информацию о них. С помощью CDP можно получить следующие данные об устройствах: имя устройства, тип и модель устройства, версия операционной системы, список соседних устройств и их интерфейсов, время работы устройства.

Атака на протокол STP (Spanning Tree Protocol) может быть проведена путем отправки фальшивых BPDU (Bridge Protocol Data Unit) на сеть. Эти пакеты могут содержать неправильную информацию о топологии сети и привести к перестроению дерева Spanning Tree, что может привести к сбоям в работе сети. Атака на STP может быть предотвращена настройкой безопасности на коммутаторах, например, отключением ненужных портов или использованием BPDU Guard для блокировки портов, которые принимают неправильные BPDU.

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

DHCP-спуфинг - это тип атаки на сети, который позволяет злоумышленнику получать несанкционированный доступ к сети, выдавая клиентам DHCP некорректные сетевые настройки. При успешной атаке злоумышленник может перехватить сетевой трафик, перенаправить его на свой компьютер и проводить прочие кибератаки.

VLAN Hopping - это сетевая атака, в которой злоумышленник пытается получить несанкционированный доступ к сети VLAN через другую VLAN. Для проведения атаки злоумышленник может использовать несколько методов, например, Double Tagging и Switch Spoofing. В случае Double Tagging, злоумышленник отправляет тегированные фреймы, которые содержат два VLAN тега, на несколько портов коммутатора. Коммутатор, получивший такой фрейм, может ошибочно присвоить ему принадлежность к другой VLAN и передать его на эту VLAN. Switch Spoofing в свою очередь заключается в том, что злоумышленник подделывает MAC-адреса и отправляет фреймы, притворяясь под устройство, которое имеет доступ к нужной VLAN. В результате успешной атаки VLAN Hopping, злоумышленник получает доступ к данным, которые находятся в другой VLAN.