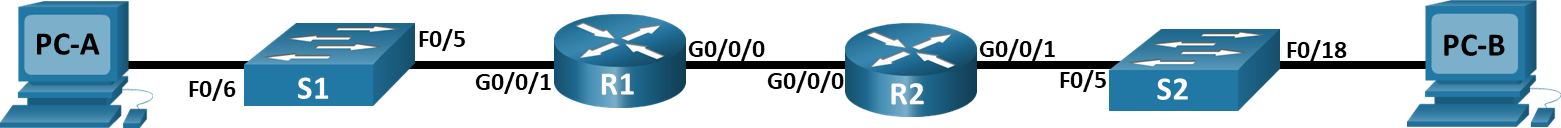


Реализация DHCPv4

**Топология**



**Таблица адресации**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска подсети** | **Шлюз по умолчанию** |
| R1\_Sidorov | G0/0/0 | 10.0.0.1 | 255.255.255.252 | — |
| G0/0/1 | — | — |
| G0/0/1.100 | 192.168.1.1 | 255.255.255.192 |
| G0/0/1.221 | 192.168.1.65 | 255.255.255.224 |
| G0/0/1.1000 | — | — |
| R2 | G0/0/0 | 10.0.0.2 | 255.255.255.252 | — |
| G0/0/1 | 192.168.1.97 | 255.255.255.240 | *—* |
| S1 | VLAN 215 | 192.168.1.66 | 255.255.255.224 | 192.168.1.65 |
| S2 | VLAN 1 | 192.168.1.98 | 255.255.255.240 | 192.168.1.97 |
| PC-A | NIC | DHCP | DHCP | DHCP |
| PC-B | NIC | DHCP | DHCP | DHCP |

**Таблица VLAN**

|  |  |  |
| --- | --- | --- |
| **VLAN** | **Имя** | **Назначенный интерфейс** |
| 1 | Нет | S2: F0/18 |
| 100 | Clients | S1: F0/6 |
| 221 | Management | S1: VLAN 221 |
| 999 | Parking\_Lot | S1: F0/1-4, F0/7-24, G0/1-2 |
| 1000 | Native | — |

**Задачи**

**Часть 1. Создание сети и настройка основных параметров устройства**

**Часть 2. Настройка и проверка двух серверов DHCPv4 на R1\_ФАМИЛИЯ Часть 3. Настройка и проверка DHCP-ретрансляции на R2**

**Необходимые ресурсы**

* 2 маршрутизатора (Cisco 4221 с универсальным образом Cisco IOS XE версии 16.9.4 или аналогичным)
* 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.2(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. Создание сети и настройка основных параметров устройства**

В первой части лабораторной работы вам предстоит создать топологию сети и настроить базовые параметры для узлов ПК и коммутаторов.

# Шаг 1. Создание схемы адресации

Подсеть сети 192.168.1.0/24 в соответствии со следующими требованиями:

1. Одна подсеть «Подсеть A», поддерживающая 58 хостов (клиентская VLAN на R1\_ФАМИЛИЯ). Подсеть A

Запишите первый IP-адрес в таблице адресации для R1\_ФАМИЛИЯ G0/0/1.100.

1. Одна подсеть «Подсеть B», поддерживающая 28 хостов (управляющая VLAN на R1\_ФАМИЛИЯ). Подсеть B:

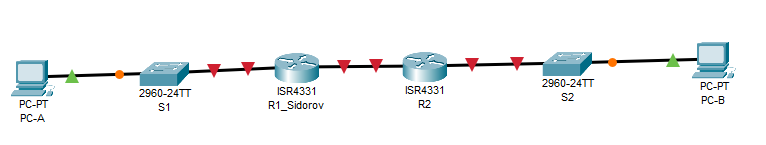
Запишите первый IP-адрес в таблице адресации для R1\_ФАМИЛИЯ G0/0/1.X+200. Запишите второй IP-адрес в таблице адресов для S1 VLAN X+200 и введите соответствующий шлюз по умолчанию.

1. Одна подсеть «Подсеть C», поддерживающая 12 узлов (клиентская сеть на R2). Подсеть C:

Запишите первый IP-адрес в таблице адресации для R2 G0/0/1. Запишите второй IP-адрес в таблице адресов для S2 VLAN 1 и введите соответствующий шлюз по умолчанию.

# Шаг 2. Создайте сеть согласно топологии.

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

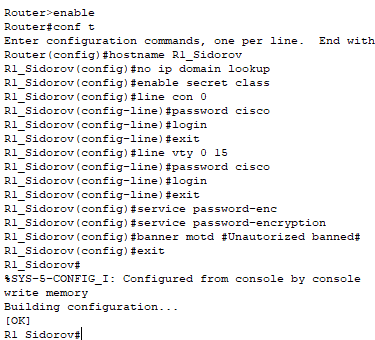


# Шаг 3. Произведите базовую настройку маршрутизаторов.

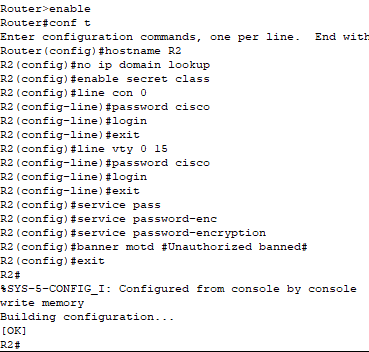
1. Назначьте маршрутизатору имя устройства.
2. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
3. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
4. Назначьте **cisco** в качестве пароля консоли и включите вход в систему по паролю.
5. Назначьте **cisco** в качестве пароля VTY и включите вход в систему по паролю.
6. Зашифруйте открытые пароли.
7. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.
8. Сохраните текущую конфигурацию в файл загрузочной конфигурации.
9. Установите часы на маршрутизаторе на сегодняшнее время и дату.

**Примечание.** Вопросительный знак (**?**) позволяет открыть справку с правильной последовательностью параметров, необходимых для выполнения этой команды.

**Настройка первого маршрутизатора:**

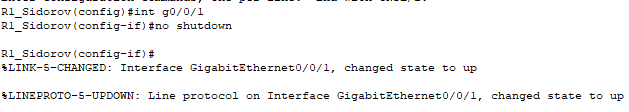


**Настройка второго маршрутизатора:**



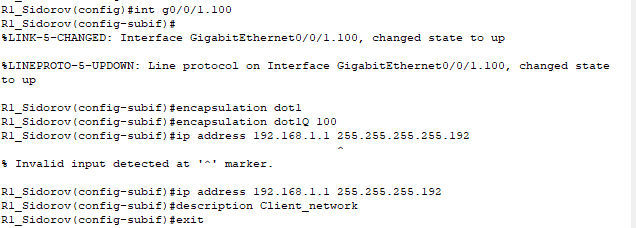
# Шаг 4. Настройка маршрутизации между сетями VLAN на маршрутизаторе R1\_ФАМИЛИЯ

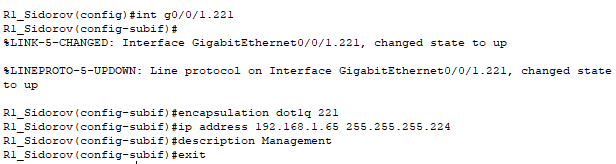
1. Активируйте интерфейс G0/0/1 на маршрутизаторе.

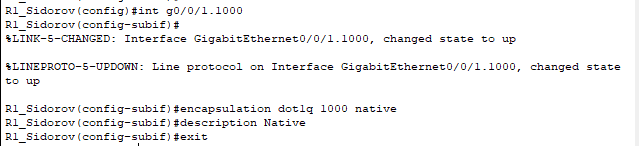


1. Настройте подинтерфейсы для каждой VLAN в соответствии с требованиями таблицы IP- адресации. Все субинтерфейсы используют инкапсуляцию 802.1Q и назначаются первый

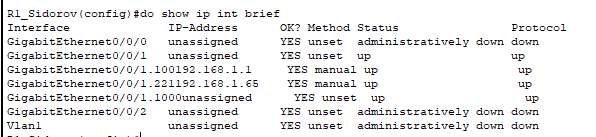
полезный адрес из вычисленного пула IP-адресов. Убедитесь, что подинтерфейсу для native VLAN не назначен IP-адрес. Включите описание для каждого подинтерфейса.





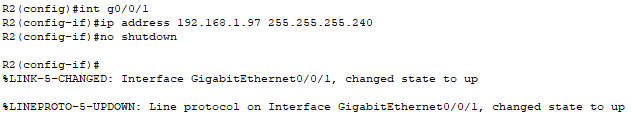


1. Убедитесь, что вспомогательные интерфейсы работают.

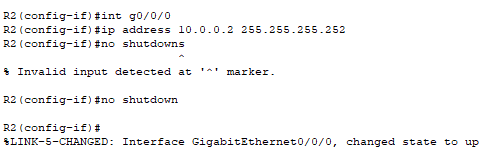


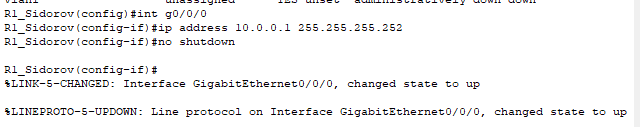
# Шаг 5. Настройте G0/1 на R2, затем G0/0/0 и статическую маршрутизацию для обоих маршрутизаторов

1. Настройте G0/0/1 на R2 с первым IP-адресом подсети C, рассчитанным ранее.



1. Настройте интерфейс G0/0/0 для каждого маршрутизатора на основе приведенной выше таблицы IP-адресации.



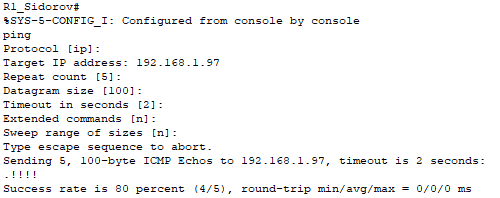


1. Настройте маршрут по умолчанию на каждом маршрутизаторе, указываемом на IP-адрес G0/0/0 на другом маршрутизаторе.





1. Убедитесь, что статическая маршрутизация работает с помощью отправки эхо-запроса до адреса G0/0/1 R2 от R1\_ФАМИЛИЯ.



1. Сохраните текущую конфигурацию в файл загрузочной конфигурации.



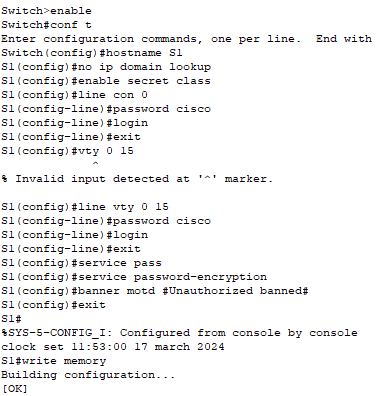


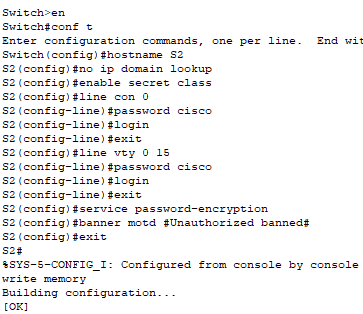
# Шаг 6. Настройте базовые параметры каждого коммутатора.

1. Присвойте коммутатору имя устройства.
2. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
3. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
4. Назначьте **cisco** в качестве пароля консоли и включите вход в систему по паролю.
5. Назначьте **cisco** в качестве пароля VTY и включите вход в систему по паролю.
6. Зашифруйте открытые пароли.
7. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.
8. Сохраните текущую конфигурацию в файл загрузочной конфигурации.
9. Установите часы на маршрутизаторе на сегодняшнее время и дату.

**Примечание.** Вопросительный знак (**?**) позволяет открыть справку с правильной последовательностью параметров, необходимых для выполнения этой команды.

1. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

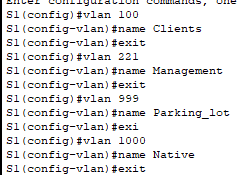




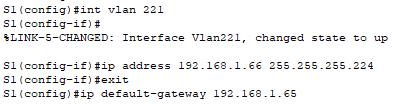
# Шаг 7. Создайте сети VLAN на коммутаторе S1.

Примечание. S2 настроен только с базовыми настройками.

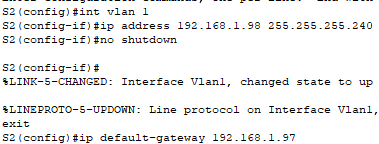
1. Создайте необходимые VLAN на коммутаторе 1 и присвойте им имена из приведенной выше таблицы.



1. Настройте и активируйте интерфейс управления на S1 (VLAN X+200), используя второй IP-адрес из подсети, рассчитанный ранее. Кроме того установите шлюз по умолчанию на S1.

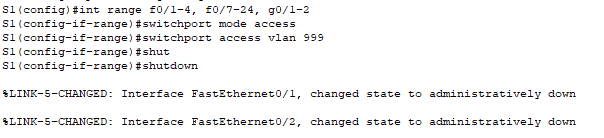


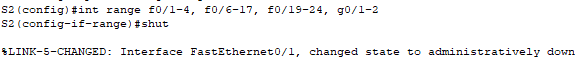
1. Настройте и активируйте интерфейс управления на S2 (VLAN 1), используя второй IP-адрес из подсети, рассчитанный ранее. Кроме того, установите шлюз по умолчанию на S2



1. Назначьте все неиспользуемые порты S1 VLAN Parking\_Lot, настройте их для статического режима доступа и административно деактивируйте их. На S2 административно деактивируйте все

неиспользуемые порты.

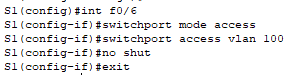




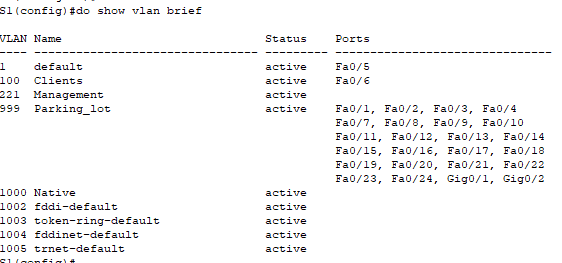
**Примечание.** Команда interface range полезна для выполнения этой задачи с минимальным количеством команд.

# Шаг 8. Назначьте сети VLAN соответствующим интерфейсам коммутатора.

1. Назначьте используемые порты соответствующей VLAN (указанной в таблице VLAN выше) и настройте их для режима статического доступа.



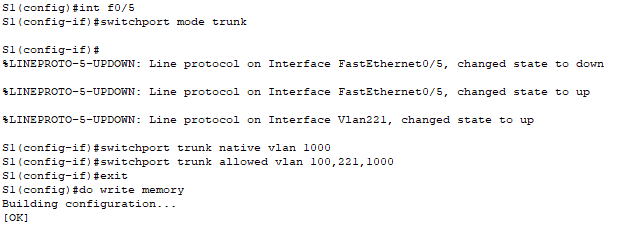
1. Убедитесь, что VLAN назначены на правильные интерфейсы.



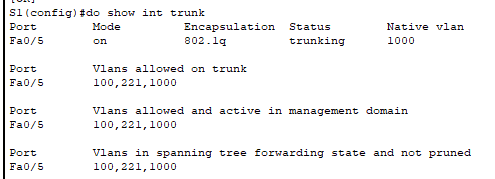
1. Почему интерфейс F0/5 указан в VLAN 1? Потому что данный интерфейс не был назначен ни одному из созданных VLAN => он указан VLAN 1

# Шаг 9. Вручную настройте интерфейс S1 F0/5 в качестве транка 802.1Q.

1. Измените режим порта коммутатора, чтобы принудительно создать магистральный канал.
2. В рамках конфигурации транкового канала установите для native VLAN значение 1000.
3. В качестве другой части конфигурации магистрали укажите, что VLAN 100, X+200 и 1000 могут проходить по транковому каналу.
4. Сохраните текущую конфигурацию в файл загрузочной конфигурации.



1. Проверьте состояние транкового канала.



Какой IP-адрес был бы у ПК, если бы он был подключен к сети с помощью DHCP? Один из указанных в подсети A

**Часть 2. Настройка и проверка двух серверов DHCPv4 на R1\_ФАМИЛИЯ**

В части 2 необходимо настроить и проверить сервер DHCPv4 на R1\_ФАМИЛИЯ. Сервер DHCPv4 будет обслуживать две подсети, подсеть A и подсеть C.

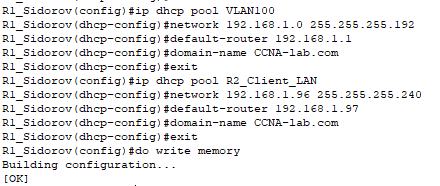
# Шаг 1. Настройте R1\_ФАМИЛИЯ с пулами DHCPv4 для двух поддерживаемых подсетей.

**Ниже приведен только пул DHCP для подсети A**

1. Исключите первые пять используемых адресов из каждого пула адресов.



1. Создайте пул DHCP (используйте уникальное имя для каждого пула).
2. Укажите сеть, поддерживающую этот DHCP-сервер.
3. В качестве имени домена укажите CCNA-lab.com.
4. Настройте соответствующий шлюз по умолчанию для каждого пула DHCP.
5. Настройте время аренды на 2 дня 12 часов и 30 минут. (lease 2 12 30)
6. Затем настройте второй пул DHCPv4, используя имя пула R2\_Client\_LAN и вычислите сеть, шлюз по умолчанию, и используйте то же имя домена и время аренды, что и предыдущий пул DHCP.

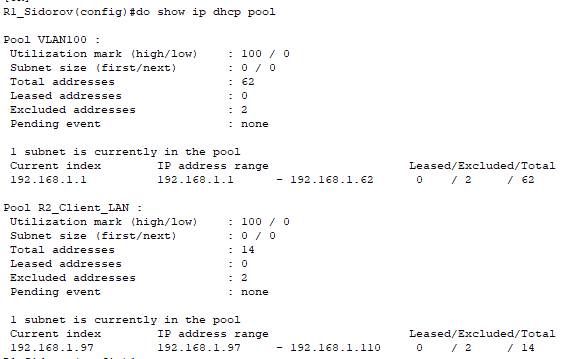


# Шаг 2. Сохраните конфигурацию.

Сохраните текущую конфигурацию в файл загрузочной конфигурации.

# Шаг 3. Проверка конфигурации сервера DHCPv4

1. Чтобы просмотреть сведения о пуле, выполните команду **show ip dhcp pool** .



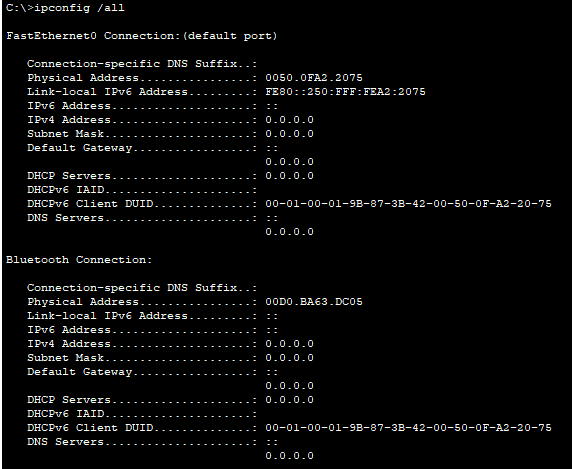
1. Выполните команду **show ip dhcp bindings** для проверки установленных назначений адресов DHCP.



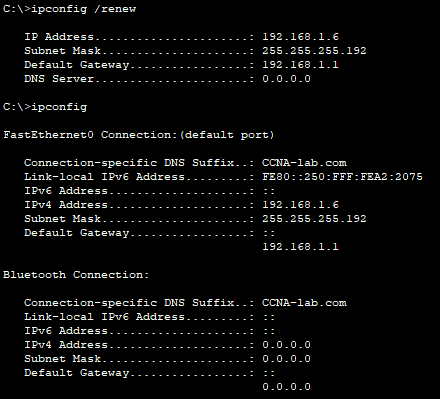
1. Выполните команду **show ip dhcp server statistics** для проверки сообщений DHCP.

# Шаг 4. Попытка получить IP-адрес от DHCP на PC-A

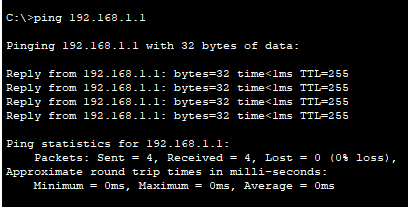
1. Из командной строки компьютера PC-A выполните команду **ipconfig /all**.



1. После завершения процесса обновления выполните команду **ipconfig** для просмотра новой информации об IP-адресе.



1. Проверьте подключение с помощью эхо-запроса на IP-адрес интерфейса R1\_ФАМИЛИЯ G0/0/1.

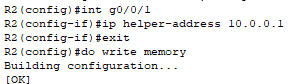


**Часть 3. Настройка и проверка DHCP-ретрансляции на R2**

В части 3 настраивается R2 для ретрансляции DHCP-запросов из локальной сети на интерфейсе G0/0/1 на DHCP-сервер (R1\_ФАМИЛИЯ).

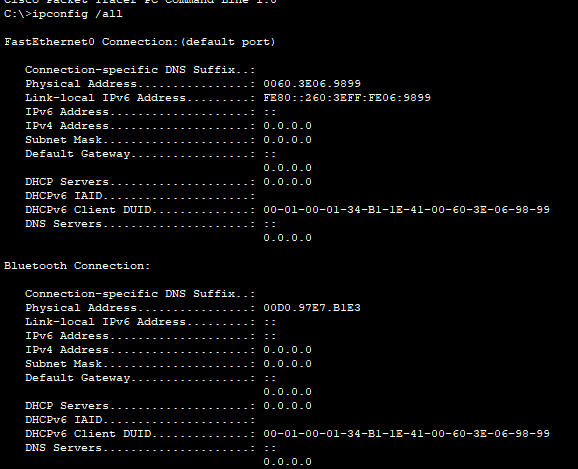
# Шаг 1. Настройка R2 в качестве агента DHCP-ретрансляции для локальной сети на G0/0/1

1. Настройте команду **ip helper-address** на G0/0/1, указав IP-адрес G0/0/0 R1\_ФАМИЛИЯ.
2. Сохраните конфигурацию.

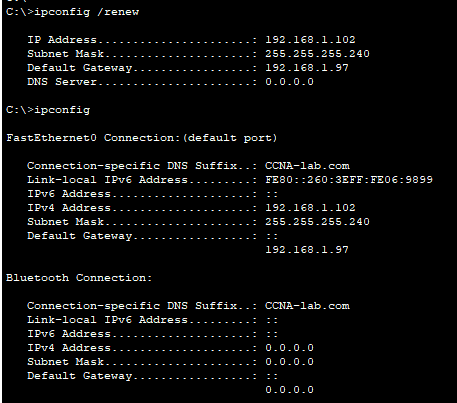


# Шаг 2. Попытка получить IP-адрес от DHCP на PC-B

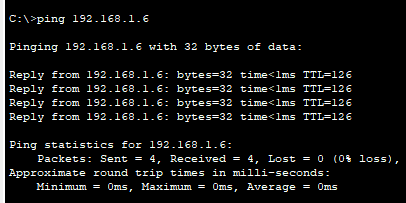
1. Из командной строки компьютера PC-B выполните команду **ipconfig /all**.



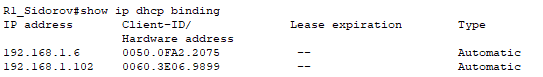
1. После завершения процесса обновления выполните команду **ipconfig** для просмотра новой информации об IP-адресе.



1. Проверьте подключение с помощью эхо-запроса на IP-адрес интерфейса R1\_ФАМИЛИЯ G0/0/1.



1. Выполните **show ip dhcp binding** для R1\_ФАМИЛИЯ для проверки назначений адресов в DHCP.



**Вопросы для защиты теоретической части (главы 7, 8)**

1. **Опишите назначение протокола DHCP. Назовите основные преимущества протокола DHCP**

Протокол динамической конфигурации узла v4 (DHCPv4) динамически назначает адреса IPv4 и другую информацию о конфигурации сети. Поскольку стационарные ПК обычно составляют основную часть сетевых узлов, протокол DHCPv4 является крайне полезным инструментом, позволяющим сетевым администраторам значительно экономить время.

1. **Опишите принцип работы протокола DHCP. Какой тип рассылки используется в сообщении DHCP Discover и почему?**

DHCPv4 работает по модели «клиент-сервер». Когда клиент подключается к серверу DHCPv4, сервер присваивает или сдает ему в аренду IPv4-адрес. . Поскольку клиент не может знать, к какой подсети он относится, сообщение DHCPDISCOVER представляет собой широковещательную рассылку IPv4 (IPv4-адрес назначения 255.255.255.255)

1. **Укажите основные шаги для получения IP-адреса при использовании протокола DHCPv4. Какие основные действия необходимо предпринять для настройки сервера DHCPv4?**

1. Обнаружение DHCP (DHCPDISCOVER)

2. Предложение DHCP (DHCPOFFER)

3. Запрос DHCP (DHCPREQUEST)

4. Подтверждение DHCP (DHCPACK)

Шаг 1. Исключение IPv4-адресов. Можно исключить один адрес или диапазон адресов, задав адреса нижнего и верхнего пределов диапазона. В число исключенных адресов должны входить адреса, присвоенные маршрутизаторам, серверам, принтерам и другим устройствам, которые были или будут настроены вручную. Можно также ввести команду несколько раз. Команда ip dhcp excluded-address low-address [top-address]

Шаг 2. Определите имя пула DHCPv4. Команда ip dhcp pool pool-name (имя пула) создает пул с заданным именем и переводит маршрутизатор в режим конфигурации протокола DHCPv4

Шаг 3. Создайте пул DHCPv4. Пул адресов и основной шлюз маршрутизатора должны быть настроены. Используйте команду network для определения диапазона доступных адресов. Используйте команду default-router, чтобы задать основной шлюз маршрутизатора

1. **Какой тип рассылки используется в сообщении DHCP Request и почему? Какие шаги используются для продления аренды IP-адреса при использовании протокола DHCPv4?**

Применение широковещательной рассылки обусловлено тем, что на момент отправки DHCP Request клиент ещё не имеет присвоенного IP-адреса, и ему неизвестен адрес DHCP-сервера. Поэтому клиент отправляет свой запрос широковещательно на весь локальный сегмент сети, чтобы обеспечить получение ответа от доступного DHCP-сервера.

1. Запрос DHCP (DHCPREQUEST). Перед окончанием аренды клиент отправляет сообщение DHCPREQUEST непосредственно DHCPv4-серверу, который первоначально предложил IPv4-адрес. Если сообщение DHCPACK не получено за определенный период времени, клиент отправляет другое сообщение DHCPREQUEST широковещательной рассылкой, чтобы другой DHCPv4- сервер мог продлить срок аренды.

2. Подтверждение DHCP (DHCPACK). При получении сообщения DHCPREQUEST сервер подтверждает информацию об аренде ответным сообщением DHCPACK.

1. **Для чего необходимо использовать DHCPv4-ретрансляцию? Перечислите варианты назначения GUA для IPv6.**

DHCPv4-ретрансляция используется в сетях, где клиенты DHCP находятся в другом сегменте сети, отличном от сегмента, на котором находится DHCP-сервер. Варианты назначения глобальных уникальных адресов (GUA) для IPv6 включают: статическое назначение, автоматическое назначение с использованием DHCPv6 и назначение с помощью Stateless Address Autoconfiguration (SLAAC).

1. **Охарактеризуйте работу метода SLAAC. Какие флаги используются в сообщении RA и что они означают?**

SLAAC - это служба без определения состояния, которая означает, что нет сервера, который поддерживает информацию о сетевых адресах, чтобы знать, какие IPv6-адреса используются и какие из них доступны. SLAAC отправляет периодические ICMPv6 RA-сообщения (то есть каждые 200 секунд), предоставляя адресацию и другую информацию о конфигурации для узлов для автонастройки их IPv6 адреса на основе информации в RA.

Сообщение ICMPv6 RA содержит следующие три флага:

Флаг A. Флаг автонастройки адреса означает использование автоматической настройки адресов без состояния (SLAAC) для создания GUA IPv6

Значение флага O, равное 1, используется для информирования клиента о том, что на DHCPv6-сервере без отслеживания состояния доступна дополнительная информация о конфигурации.

Флаг M. Флаг конфигурации управляемого адреса означает использование сервера DHCPv6 с сохранением состояния для получения GUA IPv6.

1. **Охарактеризуйте работу метода DHCPv6 без сохранения состояния. Опишите методы, используемые для генерации идентификатора интерфейса при использовании SLAAC.**

Если RA указывает метод DHCPv6 без учета состояния, узел использует информацию из сообщения RA для адресации и связывается с сервером DHCPv6 для получения дополнительной информации

1. **Охарактеризуйте работу метода DHCPv6 с сохранением состояния. Опишите основные шаги работы DHCPv6.**

DHCPv6 с сохранением состояния (stateful DHCPv6) используется для назначения IP-адресов и других настроек. Основные шаги работы DHCPv6 включают в себя передачу сообщения DHCPv6 Solicit, получение DHCPv6 Advertisement от сервера и назначение IP-адреса.

1. **Как клиент IPv6 может убедиться в уникальности своего IPv6-адреса, полученного с помощью метода SLAAC? Какие основные действия необходимо предпринять для настройки сервера DHCPv6?**

Когда клиент IPv6 использует метод SLAAC (Stateless Address Autoconfiguration) для получения своего IPv6-адреса, он формирует свой адрес на основе префикса, который объявлен в сети, и своего MAC-адреса. Уникальность адреса обеспечивается за счет уникальности MAC-адреса клиента. Однако, чтобы убедиться в уникальности своего адреса, клиент может выполнить следующие действия:

Произвести проверку на конфликт адресов: Клиент может отправить сообщение Neighbor Solicitation (NS) с целью проверить, используется ли его IPv6-адрес уже другим устройством в сети. Если клиент не получит ответ на такое сообщение, это означает, что его адрес уникален в сети.

Проверить локальные таблицы ассоциации адресов: Клиент может проверить свои локальные таблицы ассоциации адресов (ARP для IPv4, NDP для IPv6) на наличие конфликтов. Если клиент обнаружит, что его IPv6-адрес уже ассоциирован с другим устройством, он должен запросить новый адрес.

Для настройки сервера DHCPv6 (Dynamic Host Configuration Protocol version 6) основные действия включают в себя следующее:

Настройка интерфейса для работы с DHCPv6: Настройте интерфейс на сервере DHCPv6, чтобы он был способен слушать DHCPv6 запросы. Например:

Router(config)# interface gigabitethernet0/0

Router(config-if)# ipv6 dhcp server <пул\_адресов>

Создание DHCPv6 пула: Создайте пул DHCPv6, в котором будет указан диапазон IPv6-адресов, которые сервер DHCPv6 будет выдавать клиентам. Например:

Router(config)# ipv6 dhcp pool <имя\_пула>

Router(config-dhcp)# address prefix <префикс\_сети> <длина\_префикса>

Router(config-dhcp)# dns-server <IPv6\_DNS\_сервер>

Настройка параметров DHCPv6: Укажите другие параметры DHCPv6, такие как DNS-серверы, адрес шлюза и дополнительные параметры, если необходимо.

Активация DHCPv6 на интерфейсе: Активируйте DHCPv6 на интерфейсе, чтобы сервер DHCPv6 начал обрабатывать DHCPv6 запросы от клиентов. Например:

Router(config-if)# ipv6 nd other-config-flag