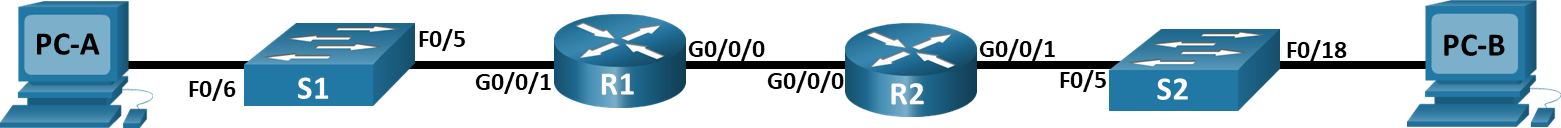
Лабораторная работа № 6: Реализация DHCPv4

**Выполнил студент: Ло Ван Хунг (X = 15)**

**Группа: ИНБО-04-20**

**Топология**



**Таблица адресации**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Устройство** | **Интерфейс** | **IP-адрес** | **Маска подсети** | **Шлюз по умолчанию** |
| R1\_Lo | 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 |
| G0/0/1.215 | 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 |
| 215 | Management | S1: VLAN 215 |
| 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\_Dinh). Подсеть A: **192.168.1.0/26**

Запишите первый IP-адрес в таблице адресации для R1\_DinhG0/0/1.100.

1. Одна подсеть «Подсеть B», поддерживающая 28 хостов (управляющая VLAN на R1\_ФАМИЛИЯ). Подсеть B: **192.168.1.64/27**

Запишите первый IP-адрес в таблице адресации для R1\_Dinh G0/0/1.206. Запишите второй IP-адрес в таблице адресов для S1 VLAN 206 и введите соответствующий шлюз по умолчанию.

1. Одна подсеть «Подсеть C», поддерживающая 12 узлов (клиентская сеть на R2). Подсеть C: **192.168.1.96/28**

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.

Изображение выглядит как диаграмма

Автоматически созданное описание

# Шаг 3. Произведите базовую настройку маршрутизаторов.

1. Назначьте маршрутизатору имя устройства.

router(config)# **hostname R1\_Lo**

1. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

R1\_Lo(config)# **no ip domain-lookup**

1. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.

R1\_Lo(config)# **enable secret class**

1. Назначьте **cisco** в качестве пароля консоли и включите вход в систему по паролю.

R1\_Lo(config)# **line console 0**

R1\_Lo(config-line)# **password cisco**

R1\_Lo(config-line)# **login**

1. Назначьте **cisco** в качестве пароля VTY и включите вход в систему по паролю.

R1\_Lo(config)# **line vty 0 15**

R1\_Lo(config-line)# **password cisco**

R1\_Lo(config-line)# **login**

1. Зашифруйте открытые пароли.

R1\_Lo(config)# **service password-encryption**

1. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.

R1\_Lo(config)# **banner motd $ Hi, I’m R1\_Dinh! $**

1. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

R1\_Lo# **copy running-config startup-config**

1. Установите часы на маршрутизаторе на сегодняшнее время и дату.

R1\_Lo# **clock set 21:00:00 21 APRIL 2023**

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

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание

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

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

R1\_Lo(config)# **interface g0/0/1**

R1\_Lo(config-if)# **no shutdown**

R1\_Lo(config-if)# **exit**

Изображение выглядит как текст

Автоматически созданное описание

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.

R1\_Lo(config)# **interface g0/0/1.100**

R1\_Lo(config-subif)# **description Client Network**

R1\_Lo(config-subif)# **encapsulation dot1q 100**

R1\_Lo(config-subif)# **ip address 192.168.1.1 255.255.255.192**

R1\_Lo(config-subif)# **interface g0/0/1.215**

R1\_Lo(config-subif)# **encapsulation dot1q 215**

R1\_Lo(config-subif)# **description Management Network**

R1\_Lo(config-subif)# **ip address 192.168.1.65 255.255.255.224**

R1\_Lo(config-subif)# **interface g0/0/1.1000**

R1\_Lo(config-subif)# **encapsulation dot1q 1000 native**

R1\_Lo(config-subif)# **description Native VLAN**

**Изображение выглядит как текст

Автоматически созданное описание**

Изображение выглядит как текст

Автоматически созданное описание

1. Убедитесь, что вспомогательные интерфейсы работают.

R1\_Lo# **show ip interface brief**

Изображение выглядит как текст

Автоматически созданное описание

# 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.

R2(config)# **interface g0/0/1**

R2(config-if)# **ip address 192.168.1.97 255.255.255.240**

R2(config-if)# **no shutdown**

R2(config-if)# **exit**

Изображение выглядит как текст

Автоматически созданное описание

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

R1\_Lo(config)# **interface g0/0/0**

R1\_Lo(config-if)# **ip address 10.0.0.1 255.255.255.252**

R1\_Lo(config-if)# **no shutdown**

Изображение выглядит как текст

Автоматически созданное описание

R2(config)# **interface g0/0/0**

R2(config-if)# **ip address 10.0.0.2 255.255.255.252**

R2(config-if)# **no shutdown**

Изображение выглядит как текст

Автоматически созданное описание

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

R1\_Lo(config)# **ip route 0.0.0.0 0.0.0.0 10.0.0.2**

R2(config)# **ip route 0.0.0.0 0.0.0.0 10.0.0.1**

1. Убедитесь, что статическая маршрутизация работает с помощью отправки эхозапроса до адреса G0/0/1 R2 от R1\_ФАМИЛИЯ.  
   R1\_Lo# **ping 192.168.1.97**

Изображение выглядит как текст

Автоматически созданное описание

1. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

R1\_Lo# **copy running-config startup-config**

# Шаг 6. Настройте базовые параметры каждого коммутатора.

1. Присвойте коммутатору имя устройства.

switch(config)# **hostname S1**

1. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

S1(config)# **no ip domain-lookup**

1. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.

S1(config)# **enable secret class**

1. Назначьте **cisco** в качестве пароля консоли и включите вход в систему по паролю.

S1(config)# **line console 0**

S1(config-line)# **password cisco**

S1(config-line)# **login**

1. Назначьте **cisco** в качестве пароля VTY и включите вход в систему по паролю.

S1(config)# **line vty 0 4**

S1(config-line)# **password cisco**

S1(config-line)# **login**

1. Зашифруйте открытые пароли.

S1(config)# **service password-encryption**

1. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.

S1(config)# **banner motd $ Unauthorized access í prohibited $**

1. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

S1# **copy running-config startup-config**

1. Установите часы на маршрутизаторе на сегодняшнее время и дату.

S1# **clock set 23:36:00 21 April 2023**

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

1. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

S1# **copy running-config startup-config**

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание

# 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.

S1(config)# **vlan 100**

S1(config-vlan)# **name Clients**

S1(config-vlan)# **vlan 215**

S1(config-vlan)# **name Management**

S1(config-vlan)# **vlan 999**

S1(config-vlan)# **name Parking\_Lot**

S1(config-vlan)# **vlan 1000**

S1(config-vlan)# **name Native**

S1(config-vlan)# **exit**

Изображение выглядит как текст

Автоматически созданное описание

1. Настройте и активируйте интерфейс управления на S1 (VLAN 206), используя второй IP-адрес из подсети, рассчитанный ранее. Кроме того установите шлюз по умолчанию на S1.

S1(config)# **interface vlan 215**

S1(config-if)# **ip address 192.168.1.66 255.255.255.224**

S1(config-if)# **no shutdown**

S1(config-if)# **exit**

S1(config)# **ip default-gateway 192.168.1.65**

Изображение выглядит как текст

Автоматически созданное описание

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

S2(config)# **interface vlan 1**

S2(config-if)# **ip address 192.168.1.98 255.255.255.240**

S2(config-if)# **no shutdown**

S2(config-if)# **exit**

S2(config)# **ip default-gateway 192.168.1.97**

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.

S1(config)# **interface range f0/1 – 4, f0/7 – 24, g0/1 – 2**

S1(config-if-range)# **switchport mode access**

S1(config-if-range)# **switchport access vlan 999**

S1(config-if-range)# **shutdown**

S1(config-if-range)# **exit**

Изображение выглядит как текст, письмо

Автоматически созданное описание

S2(config)# **interface range f0/1 – 4, f0/6 – 17, f0/19 – 24, g0/1 – 2**

S2(config-if-range)# **switchport mode access**

S2(config-if-range)# **shutdown**

S2(config-if-range)# **exit**

Изображение выглядит как текст, письмо

Автоматически созданное описание

**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.

S1(config)# **interface f0/6**

S1(config-if)# **switchport mode access**

S1(config-if)# **switchport access vlan 100**

1. Убедитесь, что VLAN назначены на правильные интерфейсы.

S1# **show vlan brief**

Изображение выглядит как текст

Автоматически созданное описание

1. Почему интерфейс F0/5 указан в VLAN 1?

**Порт 5 находится в сети VLAN по умолчанию и не настроен транк 802.1Q.**

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

1. Измените режим порта коммутатора, чтобы принудительно создать магистральный канал.

S1(config)# **interface f0/5**

S1(config-if)# **switchport mode trunk**

1. В рамках конфигурации транкового канала установите для native VLAN значение 1000.

S1(config-if-range)# **switchport trunk native vlan 1000**

1. В качестве другой части конфигурации магистрали укажите, что VLAN 100, 206 и 1000 могут проходить по транковому каналу.

S1(config-if-range)# **switchport trunk allowed vlan 100,206,1000**

1. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

S1(config)# **exit**

S1# **copy running-config startup-config**

1. Проверьте состояние транкового канала.

S1# **show interfaces trunk**

Изображение выглядит как текст

Автоматически созданное описание

Какой IP-адрес был бы у ПК, если бы он был подключен к сети с помощью DHCP?

**Они будут самостоятельно настраивать автоматический частный IP-адрес (APIPA) в диапазоне 169.254.x.x.**

**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.

R1\_Lo(config)# **ip** **dhcp excluded-address 192.168.1.1 192.168.1.5**

1. Создайте пул DHCP (используйте уникальное имя для каждого пула).

R1\_Lo(config)# **ip** **dhcp pool R1\_Client\_LAN**

1. Укажите сеть, поддерживающую этот DHCP-сервер.

R1\_Lo(dhcp–config)# **network 192.168.1.0 255.255.255.192**

1. В качестве имени домена укажите CCNA-lab.com.

R1\_Lo(dhcp–config)# **domain-name ccna-lab.com**

1. Настройте соответствующий шлюз по умолчанию для каждого пула DHCP.

R1\_Lo(dhcp–config)# **default-router 192.168.1.1**

1. Настройте время аренды на 2 дня 12 часов и 30 минут.

R1\_Lo(dhcp–config)# **lease 2 12 30**

1. 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.

R1\_Lo(config)# **ip** **dhcp** **excluded-address 192.168.1.97 192.168.1.101**

R1\_Lo(config)# **ip** **dhcp pool R2\_Client\_LAN**

R1\_Lo(dhcp–config)# **network 192.168.1.96 255.255.255.240**

R1\_Lo(dhcp–config)# **default-router 192.168.1.97**

R1\_Lo(dhcp–config)# **domain-name ccna-lab.com**

R1\_Lo(dhcp–config)# **lease 2 12 30**

Изображение выглядит как текст

Автоматически созданное описание

# Шаг 2. Сохраните конфигурацию.

Сохраните текущую конфигурацию в файл загрузочной конфигурации.

R1\_Lo# **copy running-config startup-config**

# Шаг 3. Проверка конфигурации сервера DHCPv4

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

Изображение выглядит как текст

Автоматически созданное описание

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

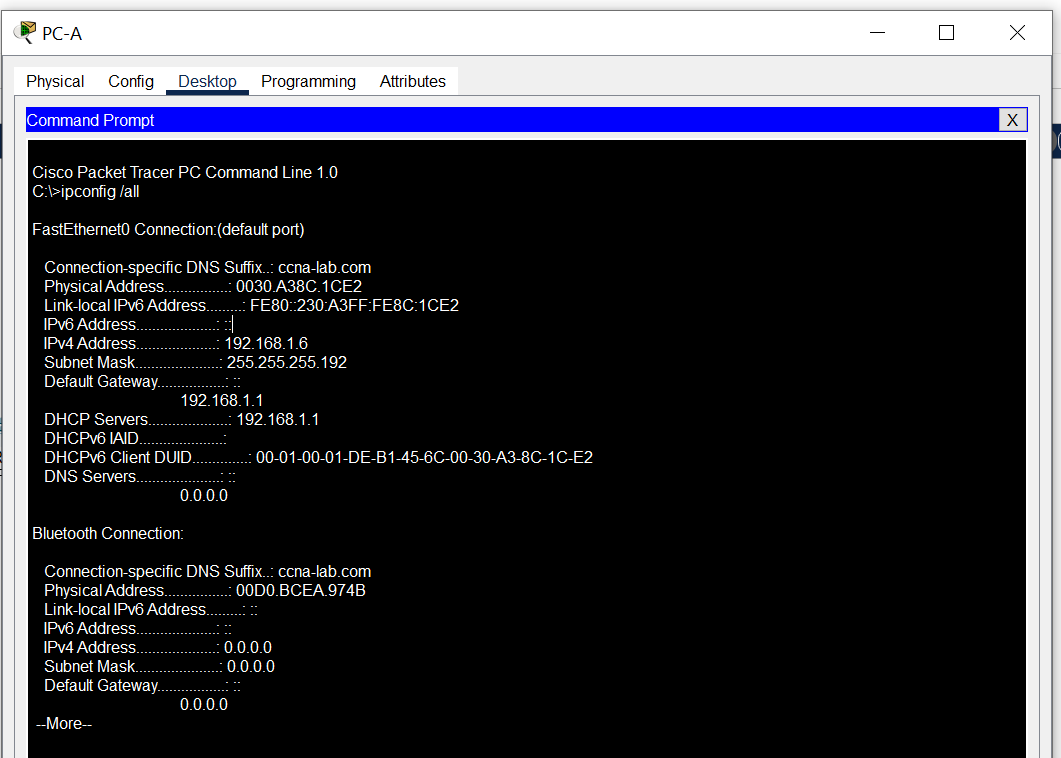
Изображение выглядит как логотип

Автоматически созданное описание

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.

Изображение выглядит как текст

Автоматически созданное описание

**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.

Изображение выглядит как текст

Автоматически созданное описание

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

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

Изображение выглядит как текст

Автоматически созданное описание

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

Изображение выглядит как текст

Автоматически созданное описание

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

Изображение выглядит как текст

Автоматически созданное описание

Изображение выглядит как текст

Автоматически созданное описание

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

Изображение выглядит как текст

Автоматически созданное описание

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

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

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

Протокол DHCP (Dynamic Host Configuration Protocol) предназначен для автоматической настройки IP-адресов и других параметров сетевой конфигурации устройствам, подключаемым к сети. DHCP может автоматически назначать IP-адреса, маски подсети, шлюзы по умолчанию, DNS-серверы и другие параметры, которые необходимы устройствам для подключения к сети и взаимодействия с другими устройствами.

Основные преимущества протокола DHCP:

* Автоматическое назначение IP-адресов: DHCP позволяет автоматически назначать IP-адреса устройствам, что упрощает процесс подключения к сети и уменьшает вероятность ошибок при настройке сетевой конфигурации.
* Централизованная управляемость: DHCP-сервер может централизованно управлять сетевыми настройками и динамически назначать IP-адреса, что обеспечивает более эффективное использование доступных ресурсов.
* Предотвращение конфликтов IP-адресов: DHCP может предотвратить конфликты IP-адресов, когда два или более устройства пытаются использовать один и тот же IP-адрес.
* Улучшенная безопасность: DHCP может автоматически назначать IP-адреса только устройствам, которые имеют правильные учетные данные или зарегистрированы в системе, что повышает уровень безопасности сети.
* Легкость администрирования: DHCP упрощает процесс администрирования сети, поскольку устройства могут быть быстро и легко настроены на работу в сети без необходимости ручной настройки каждого устройства.

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

Протокол DHCP работает по принципу клиент-сервер. DHCP-сервер предоставляет клиентам сетевую конфигурацию, которая включает IP-адрес, маску подсети, шлюз по умолчанию, DNS-серверы и другие параметры. Когда клиент подключается к сети, он отправляет широковещательное сообщение DHCP Discover на порт 67, чтобы обнаружить DHCP-сервер в сети.

Сообщение DHCP Discover использует тип рассылки "broadcast", что означает, что сообщение отправляется всем устройствам в сети. Это сделано для того, чтобы сообщение достигло DHCP-сервера, даже если клиент не знает его IP-адрес.

После получения сообщения DHCP Discover, DHCP-сервер отправляет ответное сообщение DHCP Offer клиенту, которое содержит предложение сетевой конфигурации. Если клиент согласен на получение предложенной сетевой конфигурации, он отправляет DHCP Request сообщение, чтобы запросить конфигурацию у DHCP-сервера.

После получения DHCP Request сообщения, DHCP-сервер подтверждает назначение IP-адреса, отправляя DHCP Acknowledge сообщение клиенту. Теперь клиент может использовать назначенный IP-адрес и другие параметры сетевой конфигурации для подключения к сети.

Принцип работы DHCP основан на обмене сообщениями между клиентом и сервером, в которых клиент запрашивает сетевую конфигурацию, а сервер предоставляет ее. Тип рассылки "broadcast", используемый в сообщении DHCP Discover, позволяет сообщению достигнуть DHCP-сервера, даже если клиент не знает его IP-адрес.

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

Для получения IP-адреса при использовании протокола DHCPv4, необходимо выполнить следующие шаги:

* Когда устройство подключается к сети, оно отправляет сообщение DHCP Discover на порт 67, в котором запрашивает IP-адрес и другие параметры сетевой конфигурации.
* DHCP-сервер получает сообщение DHCP Discover и отправляет ответное сообщение DHCP Offer на порт 68, в котором предлагается IP-адрес и другие параметры сетевой конфигурации.
* Если устройство согласно на предложенную сетевую конфигурацию, оно отправляет сообщение DHCP Request на порт 67, в котором запрашивает подтверждение назначения IP-адреса.
* DHCP-сервер получает сообщение DHCP Request и отправляет ответное сообщение DHCP Acknowledge на порт 68, в котором подтверждается назначение IP-адреса и других параметров сетевой конфигурации.
* Устройство принимает сообщение DHCP Acknowledge и использует назначенный IP-адрес и другие параметры сетевой конфигурации для подключения к сети.

Для настройки DHCPv4 сервера необходимо выполнить следующие действия:

* Установить и настроить DHCP-сервер на серверном компьютере.
* Настроить пул адресов IP-адресов, доступных для назначения клиентам.
* Настроить опции сетевой конфигурации, такие как маску подсети, шлюз по умолчанию, DNS-серверы и другие.
* Настроить время аренды IP-адресов, чтобы клиенты могли автоматически обновлять свою сетевую конфигурацию.
* Настроить безопасность сервера DHCPv4, чтобы предотвратить несанкционированный доступ к сетевой конфигурации клиентов.

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

Сообщение DHCP Request использует широковещательную рассылку на порт 67 для запроса подтверждения назначения IP-адреса и других параметров сетевой конфигурации. Это связано с тем, что устройство, запрашивающее IP-адрес, еще не имеет адреса и не может установить точное соединение с DHCP-сервером.

Для продления аренды IP-адреса при использовании протокола DHCPv4 необходимо выполнить следующие шаги:

* Когда время аренды IP-адреса подходит к концу, устройство отправляет сообщение DHCP Request на порт 67, в котором запрашивается продление аренды IP-адреса.
* DHCP-сервер получает сообщение DHCP Request и отправляет ответное сообщение DHCP Acknowledge на порт 68, в котором подтверждается продление аренды IP-адреса и других параметров сетевой конфигурации.
* Устройство принимает сообщение DHCP Acknowledge и продлевает аренду IP-адреса и других параметров сетевой конфигурации.

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

DHCPv4-ретрансляция (DHCP relay) позволяет использовать единственный DHCP-сервер для назначения IP-адресов и других параметров сетевой конфигурации для устройств, которые находятся в разных подсетях. Без DHCPv4-ретрансляции, DHCP-запросы не смогут достичь DHCP-сервера в другой подсети.

DHCPv4-ретрансляция принимает DHCP-запросы, отправленные устройствами в локальной сети и пересылает их на DHCP-сервер. DHCP-сервер затем отправляет ответные сообщения обратно через DHCPv4-ретранслятор, который пересылает сообщения на устройства в локальной сети.

Назначение GUA (Global Unicast Address) для IPv6 может быть следующим:

* Индивидуальный адрес: назначается конкретному устройству в глобальной сети.
* Адрес сайта: назначается всем устройствам в пределах одного сайта, обычно используется для организации локальных сетей.
* Маршрутизируемый многозначный адрес: используется для отправки пакетов на все устройства в определенной группе или подсети.
* Адрес любого каста: используется для отправки пакетов на любое устройство в глобальной сети.
* Адрес мультикаст-группы: используется для отправки пакетов на все устройства в определенной мультикаст-группе.
* Локальный адрес: используется для связи между устройствами в пределах одного сайта без маршрутизации в глобальной сети.

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

SLAAC (Stateless Address Autoconfiguration) - это метод автоматической конфигурации IP-адресов для устройств в IPv6-сетях. При использовании SLAAC, устройство самостоятельно генерирует свой IPv6-адрес, используя информацию, полученную от сообщений RA (Router Advertisement), которые отправляются маршрутизатором в локальную сеть.

Когда устройство подключается к сети IPv6, оно отправляет сообщение Neighbor Solicitation (NS) для проверки, не используется ли уже адрес, который оно планирует использовать. Затем устройство ждет сообщений RA от маршрутизатора, которые содержат информацию о подсети и другие настройки, включая флаги.

Флаги в сообщениях RA имеют следующие значения:

* Managed address configuration (M-Flag): если флаг установлен в "1", то устройства в сети должны использовать DHCPv6 для получения IP-адресов. Если флаг установлен в "0", то устройства могут использовать SLAAC для получения адресов.
* Other configuration (O-Flag): если флаг установлен в "1", то устройства в сети должны использовать DHCPv6 для получения других настроек, таких как DNS-серверы, NTP-серверы и т.д. Если флаг установлен в "0", то устройства могут использовать информацию, полученную от сообщений RA.
* Autonomous address configuration (A-Flag): если флаг установлен в "1", то устройства могут использовать SLAAC для генерации своих IPv6-адресов. Если флаг установлен в "0", то устройства не должны использовать SLAAC и должны получать все свои адреса через другие методы (например, через DHCPv6).

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

DHCPv6 Stateless (без сохранения состояния) - это метод автоматической конфигурации IP-адресов для устройств в IPv6-сетях, который использует только флаг A-Flag в сообщениях RA. При использовании этого метода устройства в сети автоматически генерируют свой IPv6-адрес, используя информацию, полученную от сообщений RA, но все остальные настройки, такие как DNS-серверы, NTP-серверы и т.д., получаются через DHCPv6 сервер.

Идентификатор интерфейса при использовании SLAAC можно генерировать несколькими способами:

* Использование EUI-64: идентификатор интерфейса может быть сгенерирован путем добавления FF:FE в середину MAC-адреса устройства. Например, если MAC-адрес устройства равен 00:11:22:33:44:55, то идентификатор интерфейса будет равен 0211:22FF:FE33:4455.
* Случайная генерация: устройства могут генерировать идентификатор интерфейса случайным образом. Этот метод гарантирует, что идентификатор интерфейса уникален в пределах сети, но может затруднить идентификацию устройства в сети.
* Использование Privacy Extensions: Privacy Extensions - это функция, которая позволяет устройствам генерировать временные IPv6-адреса с помощью случайных идентификаторов интерфейсов. Это позволяет устройствам скрыть свой реальный идентификатор интерфейса и повысить конфиденциальность в сети.

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

DHCPv6 (Dynamic Host Configuration Protocol for IPv6) с сохранением состояния - это метод автоматической конфигурации IP-адресов для устройств в IPv6-сетях, который использует DHCPv6 сервер для назначения IP-адресов и других настроек устройствам в сети.

Основные шаги работы DHCPv6:

* DHCPv6 Solicit: устройство отправляет сообщение Solicit на многоадресный адрес DHCPv6 сервера (FF02::1:2). Это сообщение содержит запрос на получение настроек от DHCPv6 сервера.
* DHCPv6 Advertise: DHCPv6 сервер получает сообщение Solicit от устройства и отправляет сообщение Advertise в ответ. Это сообщение содержит предложение настройки, включая назначенный IP-адрес, маску подсети, шлюз по умолчанию, DNS-серверы и другие параметры. Сообщение Advertise отправляется на многоадресный адрес всех DHCPv6 клиентов (FF02::1:2), и каждый клиент может получить это сообщение.
* DHCPv6 Request: устройство получает сообщение Advertise от DHCPv6 сервера и отправляет сообщение Request на многоадресный адрес DHCPv6 сервера (FF02::1:2). Это сообщение содержит запрос на подтверждение настроек, которые были предложены DHCPv6 сервером в сообщении Advertise.
* DHCPv6 Reply: DHCPv6 сервер получает сообщение Request от устройства и отправляет сообщение Reply в ответ. Это сообщение содержит подтверждение настроек, которые были предложены DHCPv6 сервером в сообщении Advertise. Если настройки были успешно подтверждены, устройство может использовать назначенный IP-адрес и другие настройки в сети.

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?**

Клиент IPv6, который получил свой IPv6-адрес с помощью метода SLAAC, может убедиться в уникальности своего адреса, используя функцию Duplicate Address Detection (DAD). DAD - это процесс, в котором клиент отправляет Neighbor Solicitation сообщение на свой IPv6-адрес, который только что получил, чтобы проверить, используется ли этот адрес другим устройством в сети. Если в сети нет других устройств с таким же IPv6-адресом, клиент получает сообщение Neighbor Advertisement в ответ, подтверждающее, что его адрес уникален.

Для настройки сервера DHCPv6 необходимо выполнить следующие действия:

* Установить и настроить DHCPv6 сервер. Существует множество программных решений для DHCPv6 сервера, таких как ISC DHCP, Dnsmasq, Kea и другие.
* Настроить пулы адресов. DHCPv6 сервер должен настроить пулы IPv6-адресов, которые будут использоваться для назначения клиентам. Кроме того, сервер может предоставлять другие настройки, такие как DNS-серверы, шлюз по умолчанию и другие параметры.
* Настроить опции для клиентов. DHCPv6 сервер может настроить опции для клиентов, такие как доменное имя, временные интервалы и другие параметры.
* Настроить фильтры. DHCPv6 сервер может настроить фильтры, чтобы запретить или разрешить доступ для конкретных клиентов или подсетей.
* Запустить DHCPv6 сервер. После настройки DHCPv6 сервера и пулов адресов, DHCPv6 сервер должен быть запущен и настроен для автоматического назначения адресов и других настроек клиентам в сети.