Содержание:

ВВЕДЕНИЕ

Тема этого реферата – DHCP - сервер. На настоящий момент времени DHCP - сервер используется почти в любой компьютерной сети от домашних до провайдерских сетей. Основное назначение DHCP - сервера это распространение сетевых настроек с помощью протокола DHCP (Dynamic Host Configuration Protocol). Устройста получающие настройки от DHCP – сервера называют DHCP – клиентами. В самом простом и частом случае DHCP используется для распространения информации о сетевой адресации, маски подсети, основного шлюза и адресов DNS - серверов.

DHCP – сервера могут быть настроены как на специализированных операционных системах для сетевого оборудования, так и на сетевых серверных операционных системах. Самые распространенные свободные реализации DHCP – сервера для Unix это: dhcpd и ISC DHCP. Настройки DHCP – серверов может отличаться в зависимости от реализации сервера. Вся дальнейшая информация описывает общий алгоритм работы протокола DHCP и не зависит от производителя оборудования или программного обеспечения.

Протокол DHCP имеет 3 различных механизма назначения адреса:

- Ручное распределение – администратор устанавливает соответствие аппаратного (MAC) и логического (IP) адресов, а DHCP передает этот адрес устройству – клиенту.
- Автоматическое распределение – DHCP - сервер автоматически присваевает постоянный сетевой адрес клиенту, выбирая его из пула адресов. В данном механизме отсутствует понятие времени аренды адреса.
- Динамическое распределение – DHCP передает клиенту сетевой адрес из пула адресов на ограниченный период времени, по истечению которого адрес может быть перезапрошен клиентом.

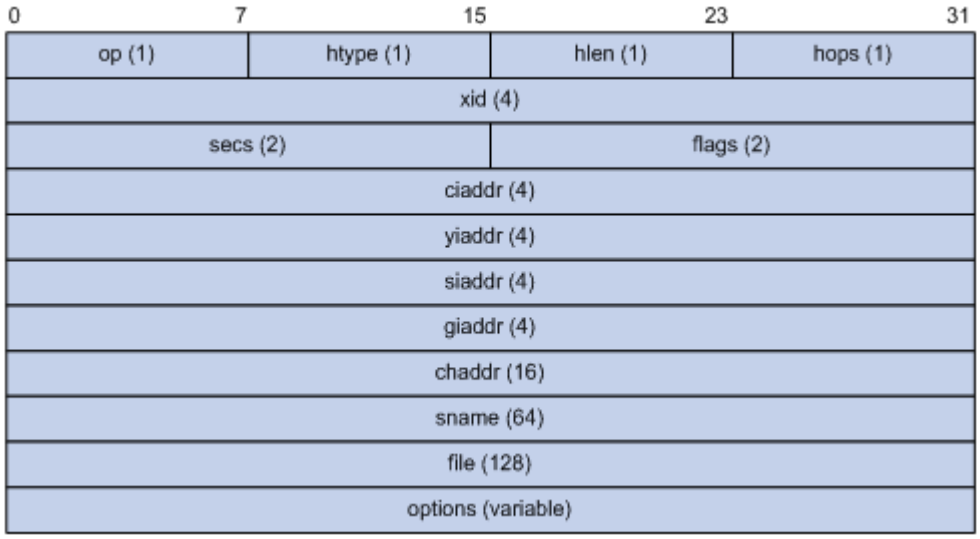
DHCPv4

DHCPv4 формат сообщений

Для всех транзакций DHCPv4 используется одинаковый формат сообщений. Сообщения прикладного уровня DHCP инкапсулируются в UDP сегмент транспортного уровня.

Сообщения DHCPv4 отправляются от клиента с 68 UDP портом, с портном назначения 67. Сообщения DHCPv4 отправляются от сервера из UDP порта 67 в порт назначения 68.[8]

Общий формат DHCP сообщений [1]:



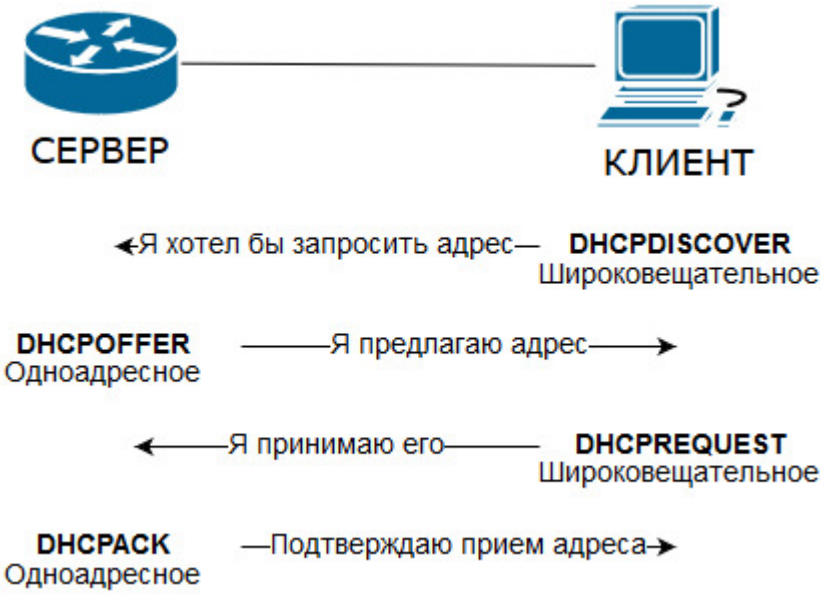
- Код операции (op) – указывает общий тип сообщения. Значение 1 – означает сообщение запрос; 2 – ответ
- Тип оборудования (htype) – определяет тип аппаратной среды. 1 – Ethernet; 15 – Frame Relay; 20 – Serial Line
- Длина физического адреса (hlen) – задает длина физического адреса
- Переходы (hops) – число использованых dhcp relay, при отправки сообщения клиентом устанавливается на 0
- Идентификатор транзакции (xid) – случайый номер установленный клиентом для согласования запоса с ответами от DHCPv4 – серверов.
- Секунды (secs) – обозначают количество секунд, пройденых с момента, когда клиент начал пытаться получить или продлить аренду. Используется DHCPv4 –

серверами для расстановки приоритетов ответов, в случае нескольких клиенских запросов.

- Флаги (flags) – устанавливается клиентом, если флаг = 0, то DHCP – сервер ответит одноадресным сообщением, если флаг = 1, то широковещательным
- IP – адрес клиента (ciaddr) – устанавливается клиентом при обновлении адреса по истечению срока аренды службы.
- “Ваш” IP – адрес (yiaddr) – устанавливается сервером для присвоения нового ipv4 – адреса клиенту.
- IP – адрес DHCP – сервера (siaddr) – адрес DHPC – сервера от которого был получен адрес
- IP – адрес шлюза (giaddr) – используется для направления DHCPv4 – сообщения при использовании dhcp relay.
- Физический адрес клиента (chaddr)
- Имя сервера (sname) – устанавливается сервером от которого был получен адрес.
- Имя файла загрузки (file) – опциональное поле, используется для указания пути до файла загрузки
- Опции (options) – опциональные параметры, например, адреса DNS – сервера, WINS – сервера.

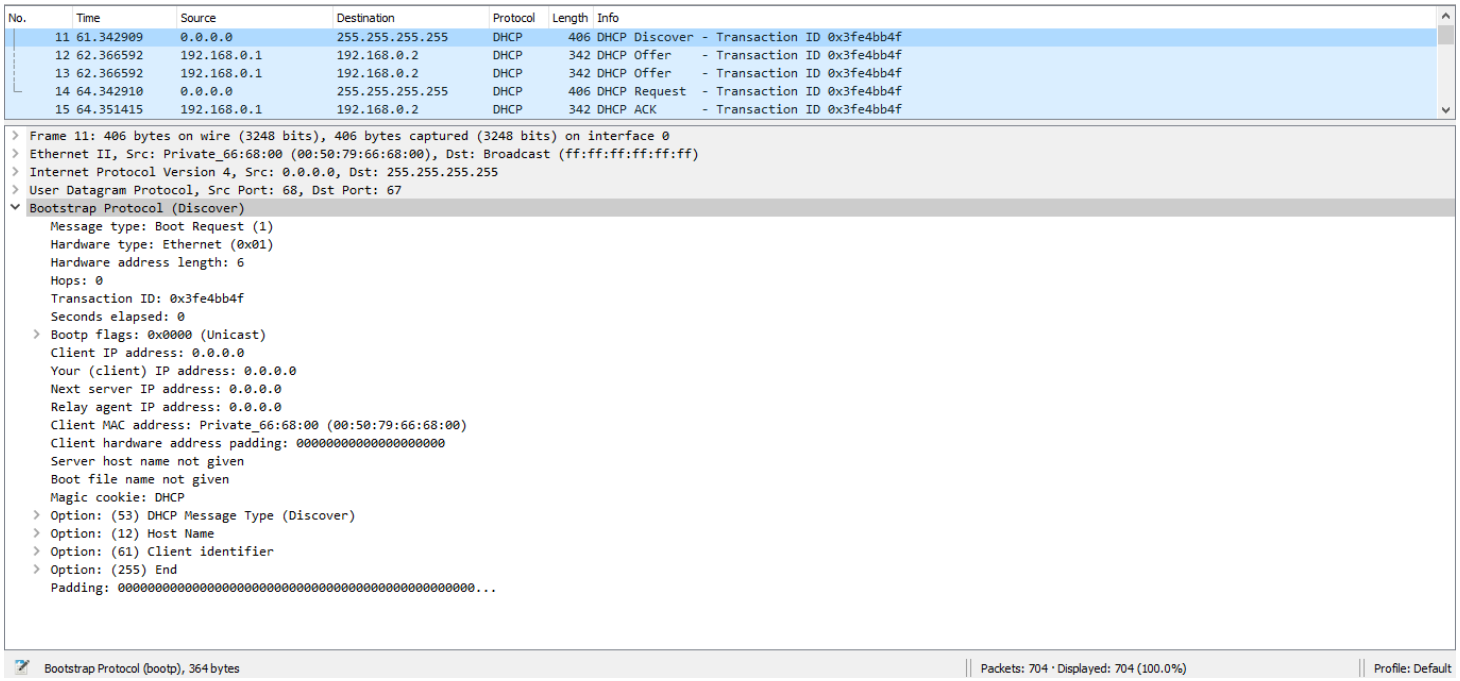
DHCPv4 обмен сообщениями

При первоначальной аренде адреса используются следующая последовательность обмена сообщениями : [8]

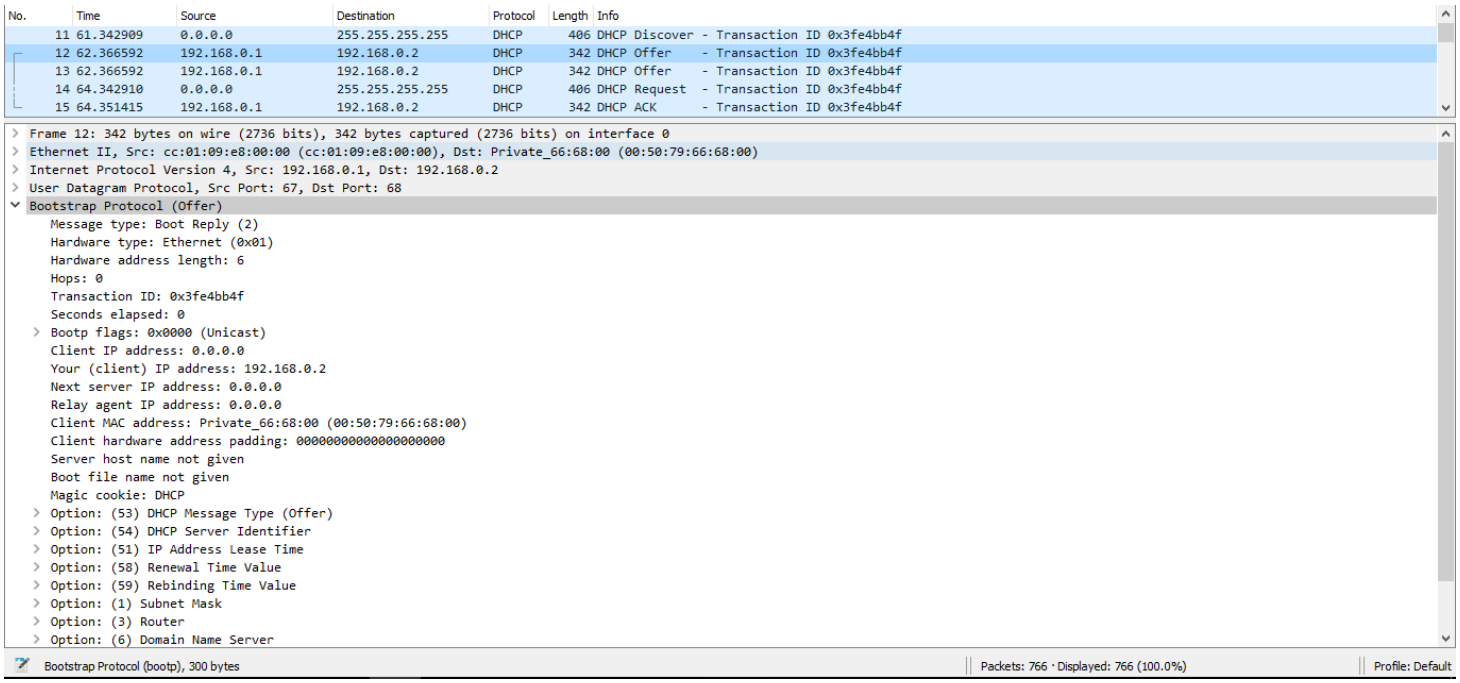


Когда срок аренды заканчивается, то клиент посылает DHCPREQUEST одноадресным сообщение непосредственно DHCP – серверу. Если DHCPACK не возвращается определенное количество времени, то клиент рассылает широковещательный DHCPREQUEST, чтобы другой сервер мог продлить срок аренды.

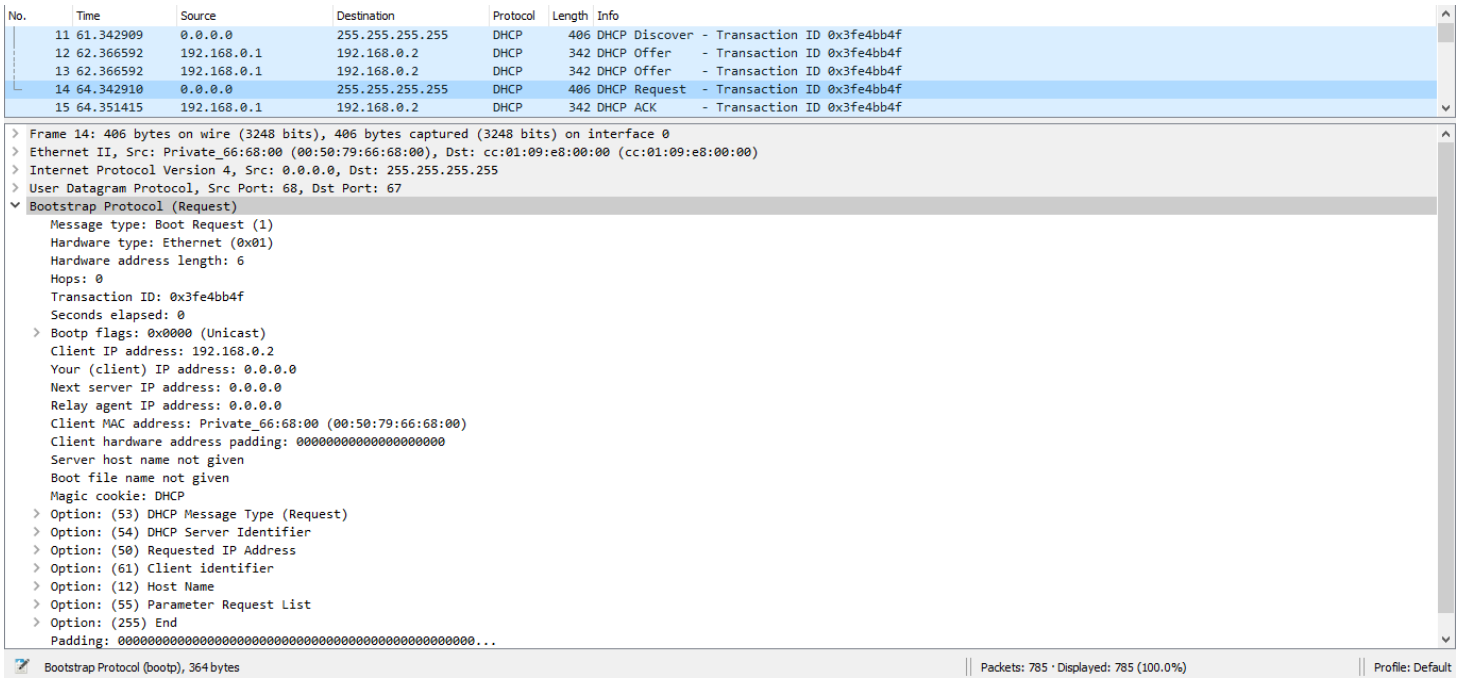
Сообщение DHCPDISCOVER при первичной аренде адреса в отображении WireShark:



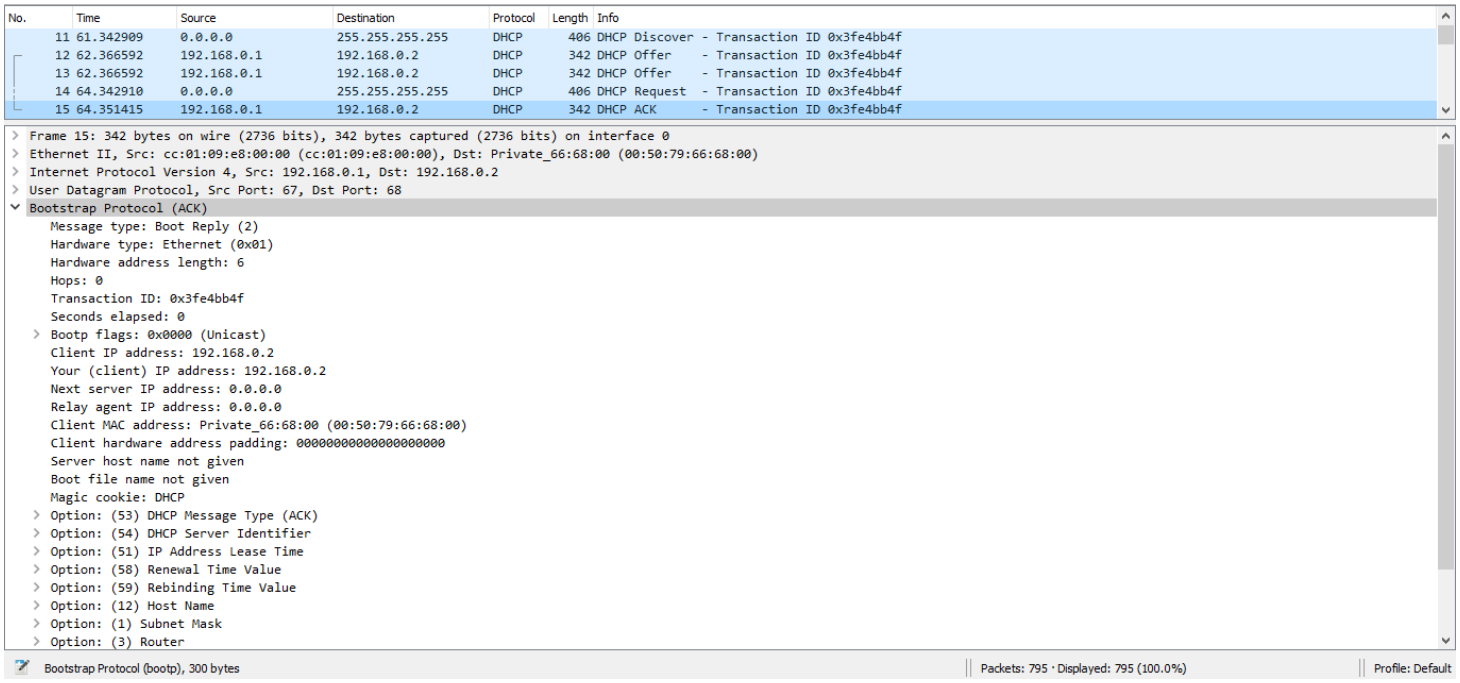
Сообщение DHCPOFFER при первичной аренде адреса в отображении WireShark:



Сообщение DHCPREQUEST при первичной аренде адреса в отображении WireShark:



Сообщение DHCPACK при первичной аренде адреса в отображении WireShark:

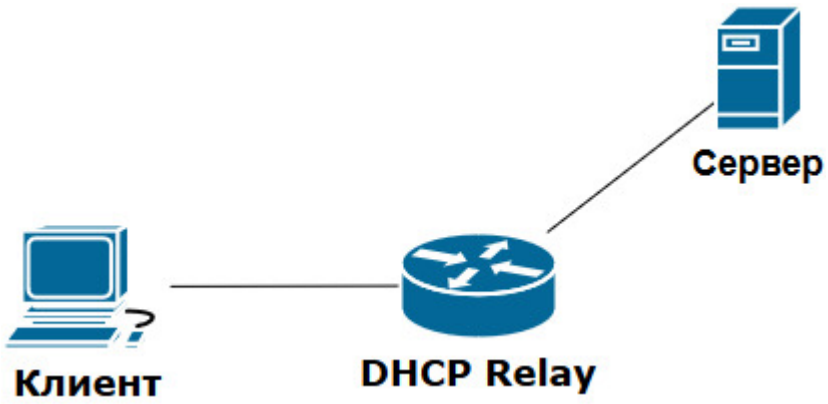


Агент ретрансляции (Relay Agent)

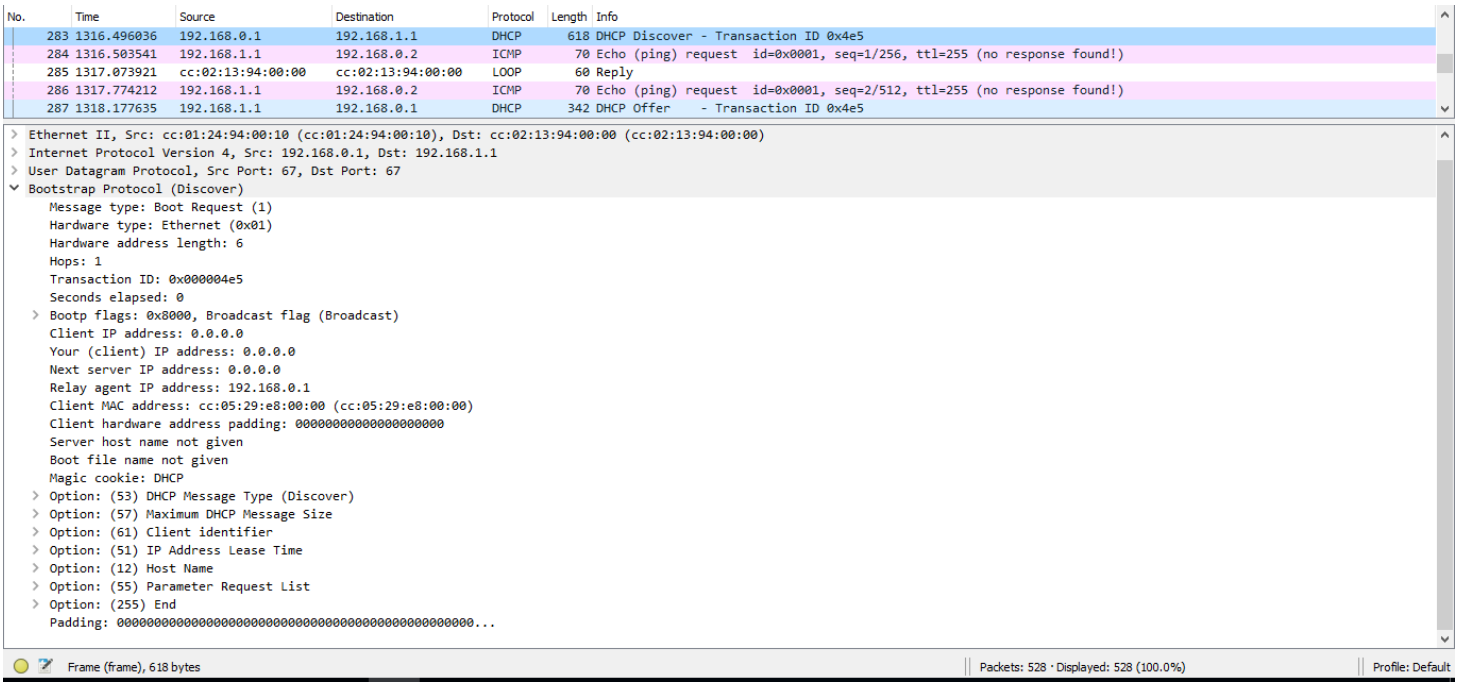
Так как DHCP сообщения используют широковещательные адреса для первичного получения настроек, то обмен сообщениями DHCP ограничен широковещательными

доменами. В случае, если DHCP – сервер находится в другой сети необходимо использовать агент ретрансляции запросов[2].

Пример сети с агентом ретрансляции:



Сообщение DHCPDISCOVER перенаправленное в другую сеть через DHCP Relay (захват кадров между DHCP Relay и Сервером):



После перенаправления в другую сеть был изменен физический адрес получателя с широковещательного на адрес DHCP – сервера. Физический адрес отправителя изменен на адрес интерфейса машрутизатора.

Сетевой адрес отправителя был изменен с 0.0.0.0 на адрес маршрутизатора со стороны клиента, а адрес назначения с широковещательного был изменен на адрес сервера.

В UDP сегменте порт источника был изменен с 68 (порт клиента) на 67 (порт сервера).

В DHCP сообщении флаг был заменен с 0 на 1. Был добавлен +1 прыжок в поле hops. Поле шлюза (giaddr) изменено на адрес интерфейса маршрутизатора, где указан DHCP relay агент. Также были добавлены некоторые дополнительные опции.

В самом простом случае агент ретрансляции использует IP – адресацию, либо поле giaddr в сообщении DHCP. В некоторых сетях необходима дополнительная информация для дальнейшего определения адресации клиента. Для добавления этой информации в DHCP – сообщение, агент ретрансляции использует дополнительную опцию 82 (DHCP Option 82).[6] Обычно это применяется при решении задачи привязки IP - адреса к порту коммутатора и для защиты от атак с использованием протокола DHCP.

Безопасность DHCPv4

Самые распространеные проблемы с безопасностью DHCP это[7]:

- Атака с подменой DHCP – сервера
- DHCP starvation – истощение пула адресов у DHCP – сервера

Для защиты от этих атак используется функция коммутаторов DHCP Snooping. По умолчанию коммутатор на котором включен DHCP snooping вставляет опцию 82 в DHCP-запросы. Коммутатор может изменять или вставлять опцию 82, даже если клиент и сервер находятся в одной сети.

Для правильной работы DHCP snooping, необходимо указать какие порты коммутатора будут доверенными (trusted), а какие — ненадёжными (untrusted):

Ненадёжные (Untrusted) — порты, к которым подключены клиенты. DHCP - ответы, приходящие с этих портов отбрасываются коммутатором. Для ненадёжных портов выполняется ряд проверок сообщений DHCP и создаётся база данных привязки DHCP (DHCP snooping binding database).

Доверенные (Trusted) — порты коммутатора, к которым подключен другой коммутатор или DHCP-сервер. DHCP-пакеты полученные с доверенных портов не отбрасываются.

По умолчанию коммутатор отбрасывает DHCP-пакет, который пришел на ненадёжный порт, если:

1. Приходит одно из сообщений, которые отправляет DHCP – сервер
2. Приходит сообщение DHCPRELEASE или DHCPDECLINE, в котором содержится MAC-адрес из базы данных привязки DHCP, но информация об интерфейсе в таблице не совпадает с интерфейсом, на котором был получен пакет
3. В пришедшем DHCP-пакете не совпадают MAC-адрес указанный в DHCP-запросе и MAC-адрес отправителя;
4. Приходит DHCP-пакет, в котором есть опция 82

DHCPv6

Методы динамического получения IPv6 адресов

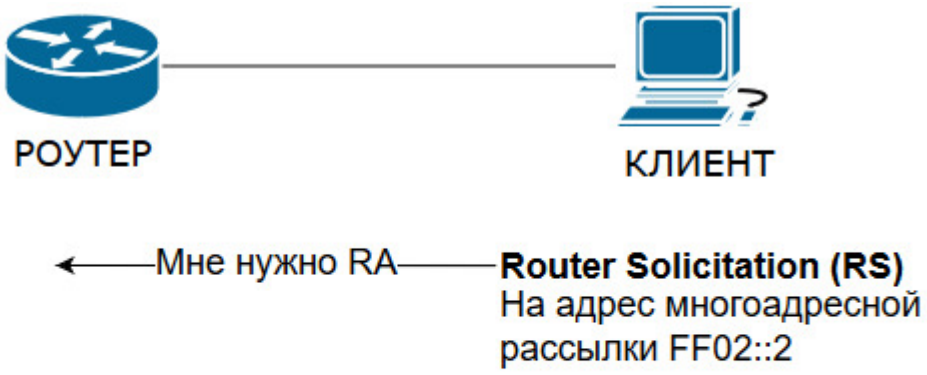
Существует 2 динамических метода получения IPv6 адресов:

- SLAAC (Stateless address autoconfiguration)
- DHCPv6

DHCPv6 подраздляется на два вида, таких как, DHCPv6 Stateless (без отслеживания состояния) и DHCPv6 Stateful (с отслеживанием состояния).

SLAAC

Механизм SLAAC используется для автоматического получения IP – адреса и сетевого префикса без использования DHCPv6 – сервера. В основе SLAAC лежит ICMPv6 с номерами сообщений относящимися к протоколу Neighbor Discovery Protocol (NDP).[4] Маршрутизатор с рабочим IPv6 интерфейсом рассылает в сеть информацию об этой сети, включающую в себя сетевую часть IP адреса и длину префикса. Кроме того, в этом сообщении содержится адрес шлюза по умолчанию.



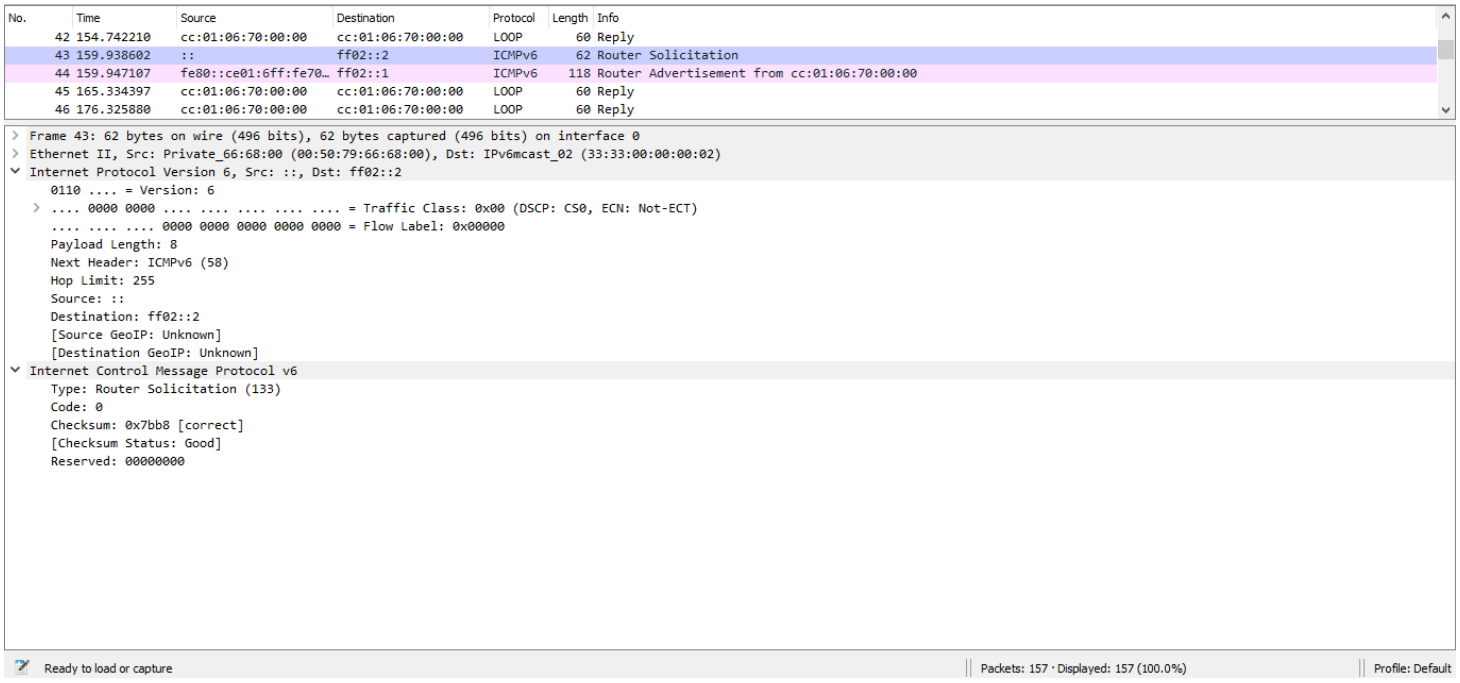
Сообщение называется Router Advertisement (RA) (ICMPv6 Type 134) и отправляется обычно раз в 200 секунд на многоадресный адрес FF02::1.[5]

Если в сети появилось новое устройство, которому необходим адрес, ему необязательно ждать 200 секунд до ближайшей рассылки, оно может направит запрос маршрутизатору Router Solicitation (RS) (ICMPv6 Type 133) и попросить его выслать настройки немедленно. Запрос маршрутизатору выполняется на адрес FF02::2.

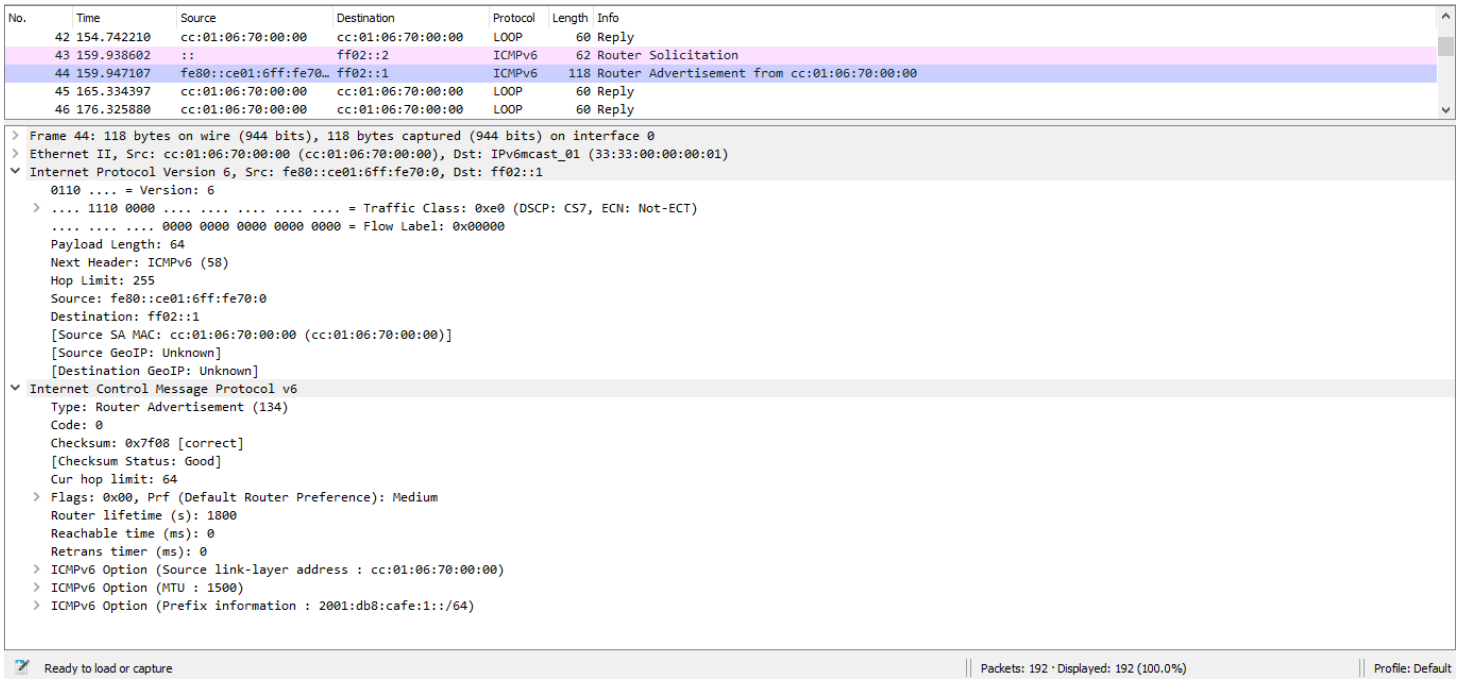
После получения сообщения RA, клиент должен создать свой идентификатор клиента (IID) с использованием полученого префикса, для этого используется процесс EUI – 64[5], либо сгенерация случайным образом.

Для устарения дублирования адресов в сети используется процесс обнаружения адресов – дубликатов (DAD)[5], который также является частью протокола обнаружения соседних устройств (NDP).

Сообщение Router Solicitation при получении префикса канала в процессе SLAAC:



Сообщение Router Advertisement при получении префикса канала в процессе SLAAC:

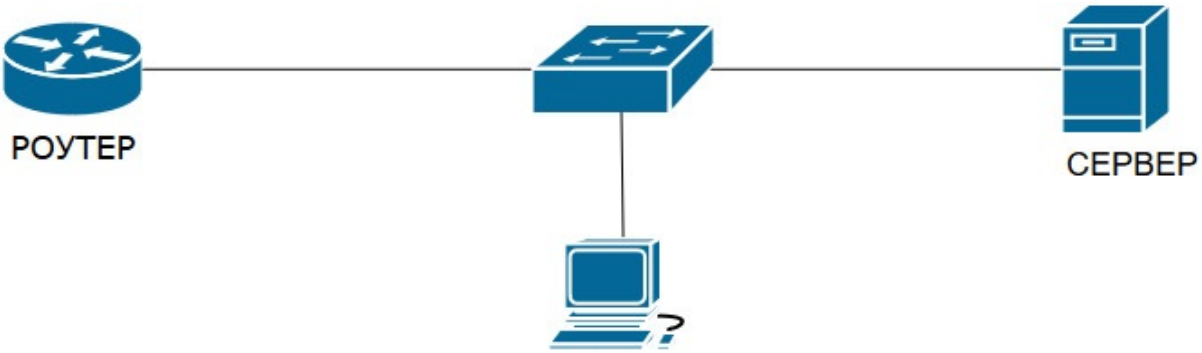


DHCPv6 без отслеживания состояния (Stateless)

Сообщения протокола DHCPv6 используют транспортный протокол UDP. Клиент отправляет сообщения на порт 547, а сервер к клиенту на порт 546.

Stateless DHCPv6 является комбинацией двух процессов, для получения префикса канала используется процесс SLAAC, а за дополнительными настройками клиент обращается к DHCPv6 – серверу.

После процесса SLAAC клиент начинат рассылать многоадресное SOLICIT сообщения на FF02::1:2. Этот адрес должен быть присвоен всем интерфейсам в сети, которые выступаю в роли DHCPv6 сервера или агента пересылки.



Процесс SLAAC:

←Мне нужно RA— **Router Solicitation (RS)**

Router Advertisement (RA) —Префикс и длина→

Процесс DHCPv6:

SOLICIT —Запрос доп. параметров→
Многоадресное сообщение на FF02::1:2

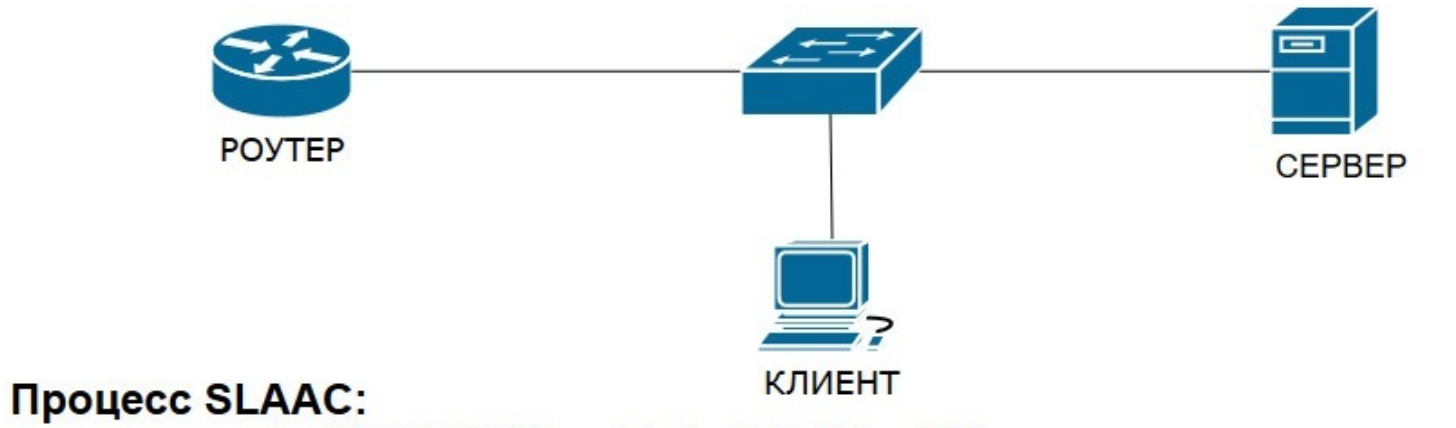
←Сервер доступен— **ADVERTISE**
Одноадресное сообщение на link-local адрес клиента

INFORMATION-REQUEST →
Одноадресное сообщение на link-local адрес сервера

← **REPLY**
Одноадресное сообщение на link-local адрес клиента

По - умолчанию в процессе SLAAC пакеты RA отсылаются с флагами M = 0 и O = 0. Для запроса клиентом дополнительных настроек с DHCPv6 сервера флаг O должен быть изменен на значение 1. При получении RA с этим флагом клиент начинает DHCPv6 процесс, в котором сервер DHCPv6 пришлет дополнительные настройки в сообщение INFORMATION-REQUEST.

DHCPv6 с отслеживанием соединения (Stateful)



Процесс SLAAC:

←Мне нужно RA— **Router Solicitation (RS)**

Router Advertisement (RA) —Префикс и длина→

Процесс DHCPv6:

SOLICIT —Запрос доп. параметров→
Многоадресное сообщение на FF02::1:2

←Сервер доступен— **ADVERTISE**
Одноадресное сообщение на link-local адрес клиента

REQUEST →
Одноадресное сообщение на link-local адрес сервера

← **REPLY**
Одноадресное сообщение на link-local адрес клиента

SLAAC процесс при работе DHCPv6 с отслеживанием состояния не посылает сетевой адрес в сообщении RA и менят флаг M на 1. Сетевой адрес присылается клиенту в сообщении REQUEST протокола DHCPv6. Функциональное назначение пакетов

DHCPv6 можно сравнить с пакетами DHCPv4 следующим образом: [3]

DHCPv6 тип сообщения	**DHCPv4 тип сообщения**
SOLICIT	DHCPDISCOVER
ADVERTISE	DHCPOFFER
REQUEST, RENEW, REBIND	DHCPREQUEST
REPLY	DHCPACK

ЗАКЛЮЧЕНИЕ

В данном реферате были рассмотрены основные процессы в DHCP для двух версий протокола IP.

Для DHCPv4 был рассмотрен процесс получения настроек от DHCPv4 сервера, в том числе, основной формат DHCPv4 сообщения, их поля, изменение полей в различных типах DHCPv4 сообщений, процесс пересылки DHCPv4 сообщений до DHCP – сервера в другую сеть и опция 82 для обеспечения безопасности.

Для DHCPv6 были рассмотрены процессы получения адресации без выделенного DHCPv6 – сервера (SLAAC), с помощью сообщений Router Solicitation и Router Advertisement протокола NDP использующего формат сообщений протокола ICMPv6. И два вариант получения настроек от DHCPv6 сервера: с арендой адреса Stateful (с отслеживанием соединения) и без аренды Stateless (без отслеживания соединения). Также была рассмотрена многоадресная адресация сетевых интерфейсов, использованная на сетевых интерфейсах для распределения ролей в процессе SLAAC и DHCPv6. И было представлено сравнение сообщений DHCPv4 и DHCPv6.

СПИСОК ЛИТЕРАТУРЫ

- 1. DHCP message format. Hewlett Packard Enterprise Development LP http://h22208.www2.hpe.com/eginfolib/networking/docs/switches/5120si/cg/5998-8491_l3-ip-svcs_cg/content/436042653.htm
  2. Configuring the Cisco IOS DHCP Relay Agent**.** Cisco Systems, Inc

https://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htdhcpre.html

- 1. DHCPv6 Based IPv6 Access Services. Cisco Systems, Inc https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/whitepaper_c11-689821.html
  2. IPv6 neighbor discovery http://packetlife.net/blog/2008/aug/28/ipv6-neighbor-discovery/
  3. NDP – Neighbor Discovery Protocol. https://howdoesinternetwork.com/2012/ndp-ipv6-neighbor-discovery-protocol
  4. Опция 82 DHCP. Н. Самойленко http://xgu.ru/wiki/%D0%9E%D0%BF%D1%86%D0%B8%D1%8F_82_DHCP
  5. DHCP snooping. Н. Самойленко http://xgu.ru/wiki/DHCP_snooping
  6. DHCP https://ru.wikipedia.org/wiki/DHCP