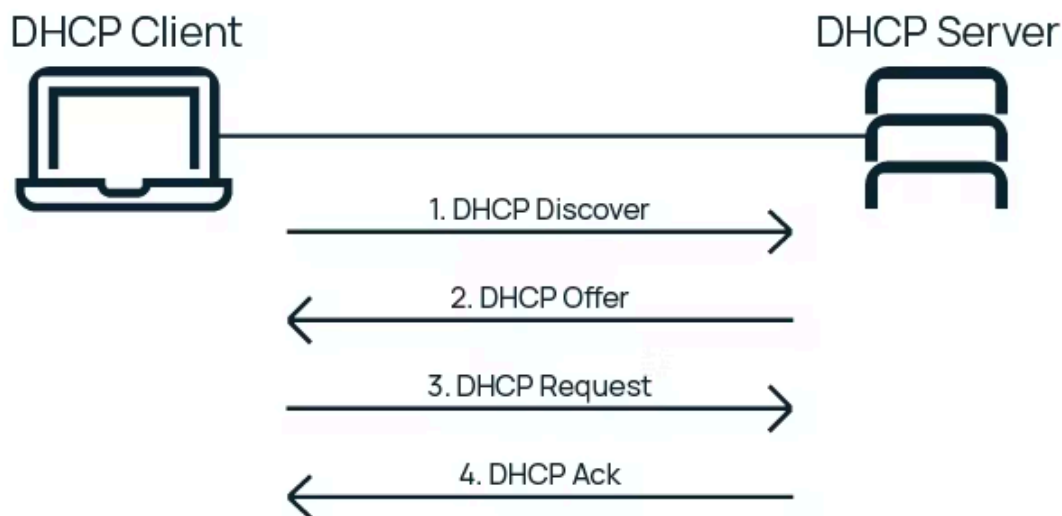

Протокол прикладного уровня модели TCP/IP, служит для назначения IP-адреса клиенту. IP-адрес можно назначать вручную каждому клиенту, то есть компьютеру в локальной сети. Но в больших сетях это очень трудозатратно, к тому же, чем больше локальная сеть, тем выше возрастает вероятность ошибки при настройке. Поэтому для автоматизации процесса назначения был создан DHCP.

Принцип работы протокола (DORA)



1. D - Discovery (поиск)

Изначально клиент находится в состоянии инициализации и не имеет своего IP-адреса. Он отправляет широковещательное сообщение DHCPDISCOVER на все устройства локальной сети. В этой же локальной сети присутствует DHCP-сервер.

В качестве DHCP-сервера может быть маршрутизатор, или коммутатор, но не стоит забывать о том, что существуют и выделенные DHCP серверы.

DHCP слушает 67 порт и ожидает широковещательное сообщение от клиента, а после его получения отправляет ответное предложение - DHCPOFFER. Клиент принимает

сообщение на 68 порту.

O - Offer (предложение)

DHCP-сервер отвечает на поиск предложением, он сообщает потенциальный IP-адрес, который может подойти клиенту. IP-адрес выделяется из выделенной области (SCOPE) доступных адресов, которая задается администратором

Если имеются адреса, которые не должны быть назначены DHCP-сервером, то область можно ограничить, указав только разрешенные адреса. Например, диапазон может задать администратор: от 192.0.0.10 до 192.0.0.254

DHCP выделяет доступные IP-адреса из области только временно, поэтому нет никакой гарантии того, что при следующем подключении у данного клиента останется прежний IP. Но всегда есть возможность назначить какому-либо клиенту определенный IP-адрес навсегда. К примеру, забронировать 192.0.0.10 за компьютером системного администратора. Такое сохранение/бронирование IP-адреса за определенным клиентом называют "резервацией"

R - Request (запрос)

Клиент получает DHCPOFFER, а затем отправляет на сервер сообщение DHCPREQUEST.

DHCPOFFER - запрос, с помощью которого он принимает предлагаемый адрес и уведомляет DHCP-сервер об этом. Широковещательное сообщение почти полностью дублирует DHCPDISCOVER, но содержит в себе уникальный IP-адрес, выделенный сервером.

Таким образом, клиент сообщает всем доступным DHCP-серверам: "всем привет, я забираю этот адрес", а DHCP-сервера помечают IP как занятый.

A - Acknowledgement (подтверждение)

Сервер получает от клиента DHCPREQUEST и окончательно подтверждает передачу IP-адреса клиенту сообщением DHCPACK. Это широковещательное или прямое сообщение утверждает не только владельца IP, но и срок, в течение которого клиент может использовать этот адрес.

Срок аренды

Срок аренды по умолчанию выставлен на 24 часа, но может достигать до нескольких дней, недель или даже месяцев. Период аренды задается в настройках самого DHCP-сервера.

3 подхода к распределению IP-адресов

1. Статическое распределение (static allocation) - почти как ввод адреса на каждом компьютере вручную. Отличие в том, что системный администратор задает нужные соответствия IP для MAC-адресов клиентов на самом DHCP-сервере. IP-адрес останется за клиентом, даже если тот выйдет из сети/отключиться/выйдет в другую сеть/etc.
 2. Автоматическое распределение (automatic allocation) - сервер закрепляет IP-адрес из области за каждым клиентом навсегда. Срок аренды при таком подходе не ограничен.
 3. Динамическое распределение (dynamic allocation) - DHCP-сервер назначает адрес из области на определенное время. Такой подход полезен, когда число доступных IP (SCOPE-адресов) ограничен.
-

Недостатки DHCP-протокола

1. Процесс DORA подразумевает рассылку сообщений широковещательного типа, когда первый откликнувшийся DHCP-сервер получает возможность предложить IP из своей области. Злоумышленник может использовать свой сервер, который даст самый быстрый ответ клиенту, тогда у него откроется возможность получить контроль над действиями пользователя в сети.
2. Надежность UDP - UDP не гарантирует доставку информации. Протокол UDP допускает потери и ошибки, которые могут сказаться и на работе DHCP, в частности, при PXE-загрузке.