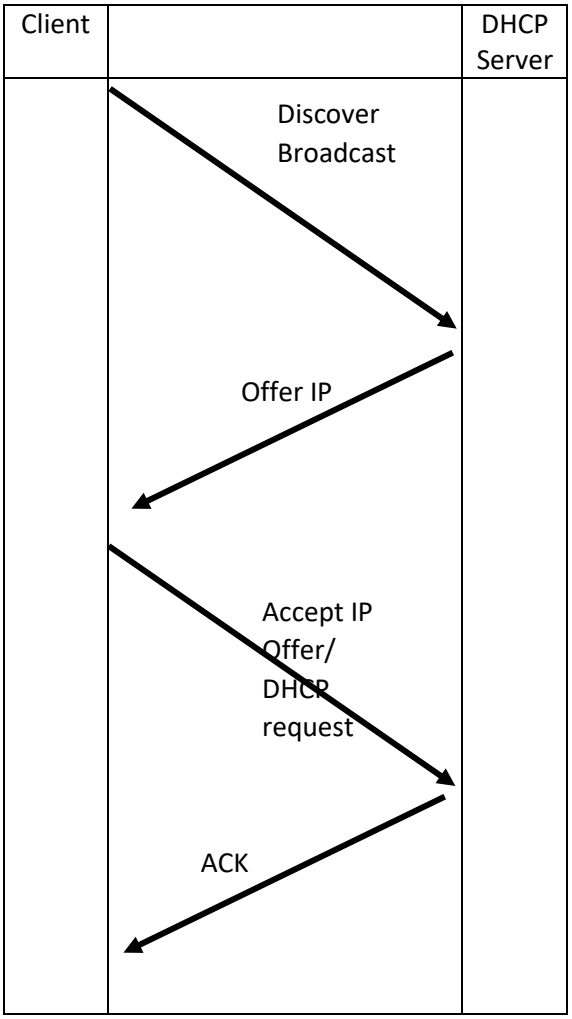
Basic Networking

DHCP v4 Handshake



A client device that is newly established on a LAN will send out a Discover Broadcast requesting an IP address.

A DHCP server will reply with an offer of an IP address for a certain lease time.

The client replies by requesting that the IP address be assigned to it (accepting the offer).

The DHCP server replies with an ACK indicating that the IP address has been assigned.

Dynamic Allocation: The addresses allocated are from a pool of addresses, and the DHCP server can reassign any IP addresses after a lease time expires.

Automatic Allocation: Like Dynamic Allocation, but clients are assigned by preference the same IP address that they've had in the past (the DHCP server keeps a table of past assignments)

Static/Manual allocation—the client is assigned an address by the DHCP server; this address was pre-allocated to that client by the sysadmin

Note that it is also possible to configure client devices themselves to ignore DHCP and instead use an IP that is statically defined in the client itself.

ARP—Address Resolution Protocol

Computer A has Computer B's IP address, but it does not have Computer B's MAC address.

- That is, Computer A's ARP table does not have a mapping between Computer B's IP address and Computer B's MAC address
- Note that Computer A could have found Computer B's IP address through the DNS lookup of a url, or it could simply have been given Computer B's IP address.
- Let's assume Computer B is on the same LAN as Computer A, then Computer A requires Computer B's MAC address to send a packet to Computer B.
    - So Computer A sends out an ARP request inside an Ethernet frame with the broadcast destination MAC address (FF:FF:FF:FF:FF:FF).
    - (If Computer B had not been on the same LAN as Computer A, then Computer A would send the packet to the default gateway/router)

Computer B sends an ARP reply containing its MAC address.

- Computer A then add the mapping between Computer B's MAC address and Computer B's IP address to its ARP table.

The contents of the ARP table can be seen on linux by doing an "arp –a" command.

Network Address Translation (NAT)

NAT is used in IPv4. One of its main purposes was to reduce the number of IP addresses being used.

<u>Versions of NAT:</u>

One to one NAT (static NAT)—maps one public IP address to one internal IP address. Each internal IP address has a separate public IP address, so this does not save on quantity of IP addresses. Main purpose of one to one NAT is to map between networks that have incompatible addressing.

Dynamic NAT—IPs from a pool of public IPs are mapped to internal addresses as needed.

Port Address Translation (PAT)—a single public IP address is shared between multiple internal (private) IPs. Each private IP is given a port number at the router. The router maintains a table that maps each private IP address/port number to its assigned external port number. Then

these external port numbers are included as the source port numbers on the outgoing TCP headers, while all outgoing IP headers use the single public IP address. When response packets come back, the router maps the external port number using its table to the internal private IP address/internal port number.

For example, one internal IP address/internal port number might be 192.168.122.3:45000, and its corresponding external (public) address/external port number might be:142.44.32.7:20022. Another internal address/internal port number might be 192.168.122.29:50000, and its corresponding external (public) address/external port number might be:142.44.32.7:20023. (Note that both use the same external (public) IP address: 142.44.32.7.

Port Forwarding

Some reasons for port forwarding are:

- Make a web server public that is running on a private network behind a router.
- SSH to a device that is on a private network behind a router.