ARP, RARP and DHCP

DHCP: Dynamic Host Configuration Protocol

It's a method for assigning Internet Protocol addresses permanently or to individual computers in an organization's network.
It gives you the IP address and the subnet mask, router(gateway), DNS/IP. And so allows you to connect to your LAN and outside.
DHCP is capable of allocating static and dynamic addresses. But how to keep track of machines that are static IP addresses. You use the MAC address to identify, that it is the same machine requesting.
But how does a new server know where is the DHCP server? The new server just broadcasts. But we don't even know the broadcast IP/subnet mask. We instead do a MAC broadcast ff:ff:ff:ff:ff:ff. This is hardwired. This message goes to all levels on the LAN. Only the DHCP responsds to this limited broadcast.

How does DHCP work?

1. When a client needs a TCP/IP operation, it broadcasts a request for address information.
2. The DHCP server will not reallocate the address during the lease period and will attempt to return the same address everytime the same client requests an address.
3. The client can extend its lease or send a message to the server before the lease expires it that it no longer needs the addres, and it can be reassigned.

Lease period is given to make sure some IP address isnt just sitting on the IP address indefinitely. This is assuming you mostly have a limited amount of IP addresses.

Dynamic addresses are traced back using what time that machine used IP address. Then the DHCP server's log can be used to trace back. By using DHCP, there is no chance of IP address conflict

When the server is not available, the whole network goes down. It becomes a critical infrastructure in the network.

You have 2 DHCP for your home connection, one at the ISP(MAN/WAN DHCP), and one at the router(LAN DHCP).

DHCP Operations

1. `DHCPDISCOVER`: When client wants to reach the DHCP server. Broadcasted to the ff:ff:ff:ff:ff:ff MAC address.
2. `DHCPOFFER`: The DHCP server returns the request with this message. This message is not a broadcast, it is a unicast. It only goes to the client who requested. We don't want to broadcast all the time.
3. `DHCPREQUEST`: Unicast to the DHCP server, to accept the IP address. It'll choose one of the many DHCP server's responses, if many of them accept. The DHCP server responds in positive with a `DHCPACK`.
4. When the lease period is about to be expired, (50%) you can renew it. It can affirm or not allow with a `DHCPNACK` message.
5. `DHCPRELEASE`: Tells the DHCP to release that IP address.
6. `DHCPINFORM`: Request more information or configuration params from the server
7. `DHCPDECLINE`: Decline request from the DHCP server.

If the client doesn't get back the IP address immediately, the protocol says that the client should wait for atleast 10 seconds before sending the next `DHCPDISCOVER` message, because its a broadcast message. Situation of too many broadcasts in the network is called a broadcast storm. E.g: electricity comes back, everyone tries asking for IP addresses of server, and the networks slow down.

Clients use port 68 to send DHCP messages, and the DHCP server uses port 67. UDP protocol, because you dont want a stream of information, just messages.

We can use sockets API, to make a DHCP address.

ARP and RARP: mapping with MAC address

ARP takes logical address and returns mapping address.

IP address is a **logical address** given to a machine so that it can communicate globally. It is implemented in software.

The MAC address is unique to a machine (48 bit). You can give it in software, but it uniquely identifies the machine.

The mapping can be static(save mappings in table), or dynamic(dynamic ip address(dhcp)). We need a protocol to map between the IP address and the MAC address.

We need the ARP protocol, because ethernet communication happens on the link layer, and that requires the MAC addresses. You need to know the MAC address of the first hop router.

Whenever a machine needs to find the physical address of another machine in the network, it sends an ARP query packet(has the physical and IP address of the sender and the IP address of whose physical address it is looking for).

The packet is broadcast over the network. Only the recipient recognizes, its IP address, and sends back the ARP response packet(recipient IP and physical address) in a unicats manner. (just like DHCP). The machine cache's MAC addresses in a ARP table. But this needs to be refreshed, if the addresses stored are dynamic(DHCP).

ARP Packet format

- **HTYPE(Hardware Type) 16b**: The type of the network on which ARP is running. Ethernet is given type 1
- **PTYPE(Protocol Type) 16b**: IPv4 is (0800)_16.
- **HLEN(Hardware Length) 8b**: Ethernet has value 6.
- **PLEN(Protocol Lenght) 8b**: IPv4 the value is 4.
- **OPER(Operation) 16b**: Type of packet. ARP request is 1, ARP reply is 2.
- **SHA(Sender hardware address) varlen**
- **SPA(Sender protocol address) varlen**
- **THA(Target hardware address) varlen**
- **TPA(Target protocol address) varlen**

Operation

1. IP asks ARP to create a request ARP message, filling the sender physical and IP address, and the target IP address. Target physical address is filled with 0s
2. The message is passed to data link layer where it is encapsulated with the physical address of the sender and the physical broadcast address.
3. Broadcast
4. Target machine replies with ARP message that contains its physical address

Proxy ARP

A proxy ARP is an ARP that acts on behalf of a set of hosts. Basically it acts as the MAC for a small set of hosts. It knows the MAC addresses of the set of hosts it serves. Helps in reducing traffic of broadcast

RARP

Gets my IP Address when have my MAC address. Diskless machines, booted from ROM, have very small booting information(airport kiosks). They only know their MAC address. RARP helps here. Same as ARP but i leave the sender protocol address empty. DHCP can be bigger, so useful for the usecase of these small machines. It is low level, supplies only IP address, and cannot be used with dynamic IP addresses.
