DHCP (RFC 2131)

- Deliver host-specific configuration parameters from DHCP server to host.

- Allocate network address to nodes:
  
  - Automatic allocation: permanent assignment.
  
  - Dynamic allocation: for a limited period of time.
  
  - Manual allocation: DHCP used only to convey assignment to host.
**DHCP Goals**

- Must ensure address uniqueness in the network.
- Must work across routers, or through BOOTP relay agents.
- Client must be prepared to receive multiple responses to configuration requests.
- Retain client configuration across client and server reboots.
Configuration Parameter Repository

- DHCP server stores a (key, value) pair for each client.

- Key used to identify a client.

- Default key = (IP-subnet number, hardware-address).

What if client changes network card or moves to another subnet?

Client can explicitly supply another identifier.
Dynamic Allocation of Network Address

- Client requests an address lease for a period of time.

- DHCP servers guarantee not to reallocate address during the lease.

- Client can extend its lease.

- Client can release an address before lease ends.

- Servers can choose to grant a shorter lease than requested.
Address Conflict Avoidance

- Servers may assign an address previously used by another client (address reuse).

- Servers may choose the least recently used address.

- Server should perform conflict detection using ICMP echo requests.

- Client should probe received address (e.g., with ARP).
**Time**

- Time represented in units of seconds.

- 0xFFFFFFFF represents infinite time.

- Time always expressed in relation to client’s clock (Why?)

- Client lease expiration time =
  
  Time when client sent DHCPREQUEST + lease duration in DHCPACK.
Timer Values

- T1: default is $0.5 \times \text{lease duration}$.

- T2: default is $0.875 \times \text{lease duration}$.

- In RENEWING state: retransmit DHCPREQUEST after half of remaining time until T2.

- In REBINDING state: retransmit after half of remaining lease time (minimum = 60 seconds).
DHCP Thread Models (for IPv6)

- Rogue server providing incorrect information to client.
- Accidentally misconfigured server providing incorrect information.
- Invalid client masquerading as valid client.
- Denial of Service attack: exhaustion of valid addresses, or exhaustion of CPU or network bandwidth.
Countering DHCP Threats

**Authentication:** optional information helps identify source and confirm integrity of message (e.g., which hash function used).

**Replay detection:** use monotonically increasing counter.

**Configuration token protocol:** matching received token with mutually agreed upon token.

**Shared secret key:** one key per (client, DHCP server) pair (scalability problems).