Revision on DHCP

Josh Wilcox (jw14g24)

April 16, 2025

Table of Contents

1. Introduction to DHCP
    - The Problem DHCP Solves
    - Overview of DHCP
        - Allocation of IP Addresses
2. DHCP for IPv4
    - Operation
    - Information Provided by DHCP
3. DHCPv6
    - The Need for DHCPv6
    - Differences Between DHCPv4 and DHCPv6
    - Stateless Address Autoconfiguration (SLAAC)
    - DHCPv6 for Additional Information

Introduction to DHCP

Subsections of ¨Introduction to DHCP¨

- The Problem DHCP Solves
- Overview of DHCP
  - Allocation of IP Addresses

- DHCP is a protocol that **automatically** configures **addresses** on a network
- DHCP can handle IP addresses within **local networks** - meaning that a certain device in one home could potentially have the same IP address in a different home - it's just they would never interact due to how DHCP is on a per-network basis

The Problem DHCP Solves: Manual Configuration Challenges

- **Manual IP Configuration Challenges:** Every device needs a unique IP address, subnet mask, default gateway, and DNS server information. Manually configuring each device is:
  - **Inefficient & Time-Consuming:** Requires administrator intervention for every device joining or leaving. Tracking assigned addresses to prevent duplicates is complex and scales poorly, especially in large networks.
  - **Error-Prone:** High risk of typos when entering addresses, assigning duplicate IPs (causing network conflicts), or setting incorrect gateway/DNS details, leading to connectivity problems.
- **Why Automatic Configuration (DHCP) is Required:**
  - **Efficiency:** Eliminates manual setup for each device, saving significant administrative time.
  - **Accuracy:** Reduces human error, ensuring correct and consistent network settings.
  - **Scalability:** Easily manages large pools of IP addresses and accommodates network growth or changes.
  - **Mobility:** Simplifies network access for devices that frequently connect and disconnect (e.g., laptops, phones).

Overview of DHCP

Subsections of ¨Overview of DHCP¨

- Allocation of IP Addresses

- Networks contain a DHCP server which manages various aspects of the **internet layer**
- The DHCP server manages **IP settings** on its **local network**
  - Assigning IP addresses automatically and *dynamically*
  - Default Gateway
  - Name servers
  - Time servers

Overview of DHCP - **Allocation of IP Addresses**

Dynamic Allocation

- Network Admin reserves a **range** of IP addresses specially for the DHCP server to provide
- Then, each DHCP client on LAN can request an IP address directly from the DHCP server during network initialisation.
- The DHCP Server **leases** IP addresses
    - The leases have a controllable time period
    - Allows DHCP to reclaim and reallocate IP addresses **dynamically**

Automatic Allocation

- Similar to *Dynamic Allocation* - Except the DHCP sever **keeps a table** of past IP assignments
- **Prefers** to assign the **same IP address** as before

Manual Allocation

- Slightly takes away from the point of DHCP, but allows for *static* definition of IP addresses on devices
- An admin manually maps MAC addresses directly to IP addresses.
- A DHCP server can fall back onto other methods if this fails

DHCP for IPv4

Subsections of ¨DHCP for IPv4¨

- Operation
- Information Provided by DHCP

Operation

- DHCP is **Connectionless** - Uses UDP
  - Server listens on port 67
  - Client listens on 68
  - (For memory - Two numbers before the funny number)
- The operation of DHCP consists of four categories:
  - **Discovery**
    - DHCP client **broadcasts** a `DHCPDISCOVER` message on the **subnet** using the address `255.255.255.255`
    - This message could include a flag that **requests an IP address**
  - **Offering**
    - Once the server receives the `DHCPDISCOVER` - it reserves an IP address for that client and sends a `DHCPOFFER` to offer an IP lease.
    - This `DHCPOFFER` would include the address, subnet mask, lease duration, and IP address of the server
  - **Requesting**
    - A response to the DHCP offer
    - Confirms the offered address
    - A client can receive offers from multiple servers - but can only accept one offer
  - **Acknowledging**
    - `DHCPACK` packet is sent to client - including lease duration and any other information requested
    - Acknowledges that the IP config process is complete
- The operation of DHCP is often abbreviated as `DORA`

Information Provided by DHCP

- **IP Address:**
  - **What:** A unique numerical label assigned to each device participating in a computer network that uses the Internet Protocol for communication.
  - **Why:** Essential for identifying the device on the network and enabling it to send and receive data packets. Without a unique IP, communication is impossible.
  - **Example:** `192.168.1.101`
- **Subnet Mask:**
  - **What:** A 32-bit number that masks an IP address and divides the IP address into network address and host address.
  - **Why:** Used by the device to determine which part of the IP address represents the network and which part represents the host. This helps determine if a destination IP is on the local network or a remote network (requiring the default gateway).
  - **Example:** `255.255.255.0` (Indicates the first three octets define the network)
- **Default Gateway:**
  - **What:** The IP address of the router on the local network that serves as the exit point to other networks (including the internet).
  - **Why:** When a device needs to send data to an IP address outside its own local subnet, it sends the packet to the default gateway, which then forwards it towards the destination.
  - **Example:** `192.168.1.1` (Often the IP address of the local router)
- **DNS Server Addresses:**
  - **What:** The IP addresses of one or more Domain Name System (DNS) servers.
  - **Why:** DNS servers translate human-readable domain names (e.g., `www.google.com`) into machine-readable IP addresses (e.g., `142.250.179.196`). This allows users to access internet resources using names instead of memorizing IP addresses.
  - **Example:** `8.8.8.8`, `1.1.1.1` (Public DNS servers provided by Google and Cloudflare, respectively)

DHCPv6

Subsections of ¨DHCPv6¨

- The Need for DHCPv6
- Differences Between DHCPv4 and DHCPv6
- Stateless Address Autoconfiguration (SLAAC)
- DHCPv6 for Additional Information

The Need for DHCPv6

- Just as DHCP automates IPv4 configuration, **DHCPv6** provides automatic configuration for devices using **IPv6**.
- While IPv6 offers **Stateless Address Autoconfiguration (SLAAC)**, DHCPv6 provides more **control** and **additional configuration options** beyond just an IP address.
- Needed for environments requiring centralized address management, specific DNS servers, or other network parameters not provided by SLAAC alone.

Differences Between DHCPv4 and DHCPv6

- **Integration with Router Advertisements (RAs):** DHCPv6 often works alongside IPv6 Router Advertisements. RAs can indicate whether a host should use DHCPv6 for addresses (**Managed** flag) or other information (**Other** flag), or rely solely on SLAAC.
- **Identifiers:** DHCPv6 uses a **DHCP Unique Identifier (DUID)** to identify servers and clients, rather than relying solely on MAC addresses like DHCPv4. DUIDs are designed to be stable even if hardware changes.
- **Message Types:** The core message exchange differs:
  - Client sends `Solicit` (like DHCPDISCOVER)
  - Server responds with `Advertise` (like DHCPOFFER)
  - Client sends `Request` (like DHCPREQUEST) or `Information-Request` (if only seeking options)
  - Server responds with `Reply` (like DHCPACK)
- **Ports:** Uses UDP ports 546 (client) and 547 (server/relay).
- **Addressing:** Uses link-local IPv6 addresses for communication.

Stateless Address Autoconfiguration (SLAAC)

- **Alternative Configuration:** SLAAC allows IPv6 hosts to configure their own IP addresses **without a DHCPv6 server**.
- **Process:**
  - Host listens for **Router Advertisement (RA)** messages from local routers.
  - RAs contain the **network prefix** (e.g., `2001:db8:abcd:1234::/64`).
  - Host generates the **interface identifier** (the host part of the address) to combine with the prefix.
- **Interface ID Generation Methods:**
  - **EUI-64 (RFC 4862):** Originally derived from the device's MAC address. Predictable and raises **privacy concerns** as the MAC address is globally unique and embedded in the IP.
  - **Stable Privacy Addresses (RFC 7217):** Generates a **pseudo-random** but stable interface ID per network prefix. Prevents tracking based on MAC address while keeping the address consistent on that specific network.
  - **Privacy Extensions (RFC 4941):** Generates **temporary, random** addresses for outbound connections. These change frequently to enhance privacy and make tracking difficult.
- **Multiple Addresses:** A host can (and often does) have multiple IPv6 addresses simultaneously: a link-local address, a stable SLAAC address (EUI-64 or RFC 7217), and one or more temporary privacy addresses.

DHCPv6 for Additional Information

- **Complementing SLAAC:** Even when using SLAAC for address configuration, a network might use DHCPv6 to provide other essential details.
- **Stateless DHCPv6:** A host uses SLAAC for its IP address but queries a DHCPv6 server (via an `Information-Request` message) for options like:
  - DNS Server Addresses
  - NTP (Network Time Protocol) Server Addresses
  - Domain Search List
- This mode is indicated by routers setting the **'O' (Other configuration)** flag in their RAs, while the **'M' (Managed address configuration)** flag is off.
- **Stateful DHCPv6:** If the 'M' flag is set in the RA, the host uses DHCPv6 for both address assignment and other options (similar to DHCPv4).
- **Coexistence:** A host can potentially have both a SLAAC-generated address and a DHCPv6-assigned address, along with other addresses like link-local and privacy extensions.