IP Addresses: How They Work, The Types, and Their Uses

Introduction

IP addresses, short for Internet Protocol addresses, are unique, numerical identifiers, for computers, tablets, phones, servers, and anything that is connected to wifi. IP addresses serve two purposes: they identify devices on the network, and provide the device's location.

Structure

There are two types of IP addresses that are used on the internet today: IPv4 and IPv6

- IPv4:
  - The most widely used format
  - Made up of 4 sets of numbers (0-255) separated by periods
  - Supports 4,294,967,296 unique addresses
- IPv6:
  - Developed to combat limitations of IPv4
  - Uses a 128-bit format with 8 groups of 4 hexadecimals numbers (0-9, A-F)
  - 340 undecillion unique IP addresses (2^{128})

Functions

- **Location**: Every device on a network, wired or wireless, is assigned an IP address so that routers can find the best possible path to or from that device
- **Identification**: An IP address uniquely identifies each device on the internet enabling communication.

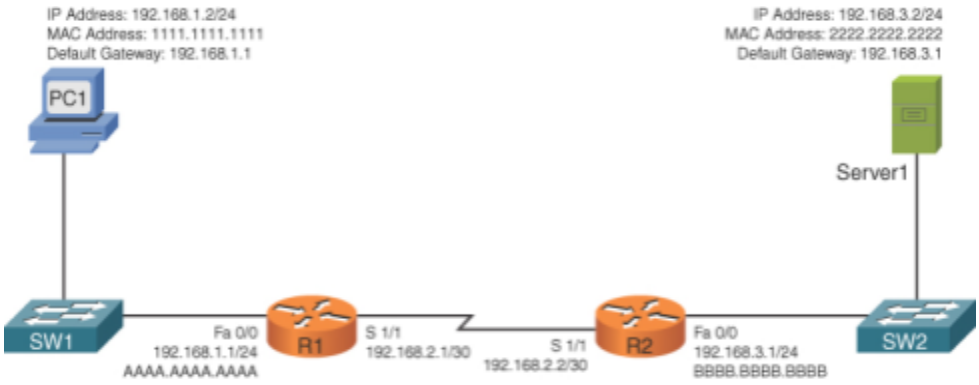

Figure 1: IP addresses and their functions in action.

1. Image Credit:
https://www.pearsonitcertification.com/content/images/chap10_9780137449941/elementLinks/10fig01_alt.jpg

Types

There are two main types of addresses, Private and Public.

- **Public addresses** are accessible directly from the internet. They are used for communication and routing between devices and networks. This is analogous to a home address.
- **Private addresses,** however, are IPs that are used within a home, school, and different business and are not accessible from the internet. This is analogous to a room in a house or apartment and these addresses were created for a variety of reasons such as reusability, security, local communication, and conservation of IPs. Since home networks frequently have devices connecting and disconnecting throughout the day, assigning public IPs to each device would be inefficient.

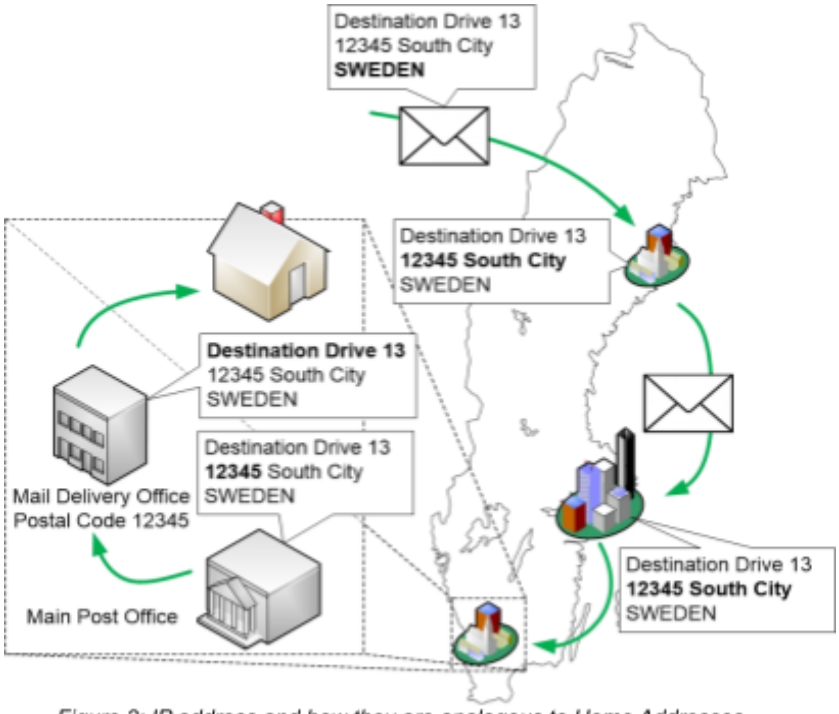

Figure 2: IP address and how they are analogous to Home Addresses

2. Image Credit:
https://www.homenethowto.com/wp-content/uploads/routing-introduced-as-post-delivery.jpg

Static VS Dynamic IPs

In addition to the previously mentioned types, IPs can be classified further as Static or Dynamic.

- **Static IP addresses** remain constant, and are set manually to a device. These IPs are useful when a device or website requires a fixed address. It should be noted that Static IPs are less secure and easier to track.

- **Dynamic IP addresses** however change every time a device connects to a network. This is done automatically by the network through DHCP (Dynamic Host Configuration Protocol), which is a protocol that automatically assigns IP addresses and other communication parameters to a device, without manual intervention.

Static*:*

- Advantages: Ideal for servers, websites, and other services that always need to be on and accessible.
- Disadvantages: Often more expensive, and less secure.

Dynamic*:*

- Advantages: More secure and more cost effective.
- Disadvantages: May have more of a delay due to having to wait until an IP is assigned.

Classes of IPv4 Addresses

IPv4 Addresses are grouped into different classes to manage their use case. They are determined based on the size and use case of the network. There are 5 different classes ranging from A - E. These are separated by their classification and how they differ on their Network ID and Host ID.

- Class A: Used for large networks, that require a significant number of IPs
    - Example: Amazon and Google
- Class B: Used for medium-sized networks
    - Example: Universities like PSU
- Class C: Used for small networks
    - Example: Small businesses that have under 256 devices connected to them.
- Class D: Used specifically for Multicasting, where one sender broadcasts data to multiple receivers
    - Example: Streaming services like Netflix
- Class E: Reserved for research and experimental purposes
    - Example: Organizations like NASA or academic institutions conducting experiments.

The image below, shows how the IPs are classes based on the Network ID, which tells the router, what specific network, and the Host ID which identifies the specific device.

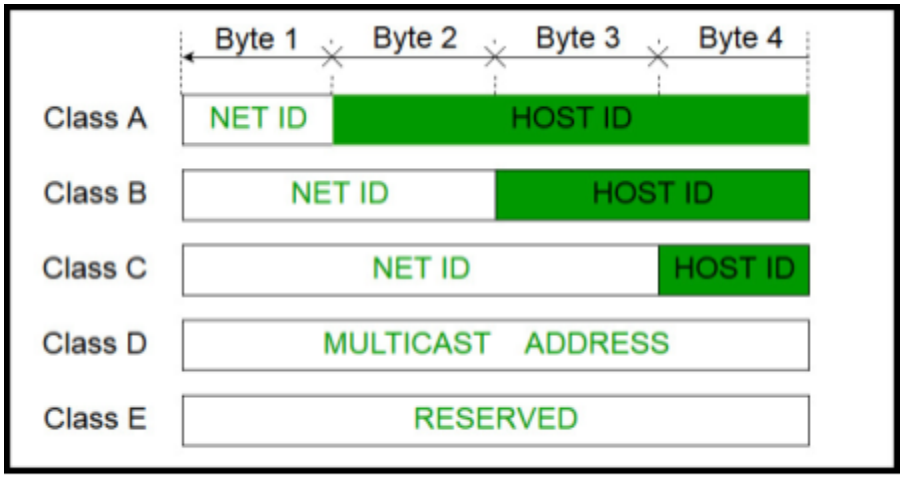

Figure 3: Structure of different IPv4 Classes

3. Image Credit:
https://media.geeksforgeeks.org/wp-content/cdn-uploads/IP_addressing_3.jpg

DHCP

A protocol (set of rules that define a process) that automatically assigns IPs to devices that connect to its network. Each IP is assigned for a limited amount of time, (lease time) before it is taken back by the protocol and then stored or reassigned to another device. DHCP assigns IPs from a limited pool to ensure no two devices have the same IP. This protocol helps simplify management by automating the IP assignment process. The DHCP protocol is analogous to a hotel front desk, each person is a device that is assigned a room (IP) and a length of stay (lease time), there is a list of available rooms (IP pool), to ensure that no two guests get the same room.

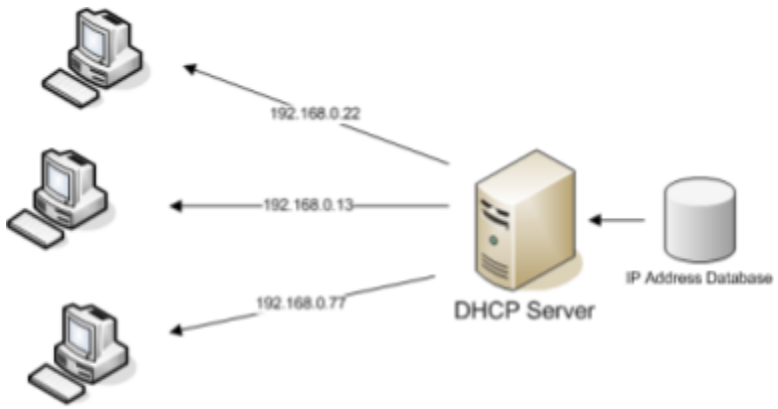

Figure 4: Illustration of how DHCP assigns IPs

4. Image Credit:
https://miro.medium.com/v2/resize:fit:528/1*1KIknnLKXpXptCyVRf6KCQ.png

Subnetting

Subnetting is the process of dividing a large network into smaller and more manageable subnetworks. This is done for several reasons such as:

- Simplified IP management
- Improved network performance
- Enhanced Security

Subnet Mask

Subnetting makes use of a subnet mask by determining which part of the IP represents the network and host ID and then masking the IP address, based on this. To create the additional subnetworks bits can be borrowed from the Host ID to extend the Network ID. This is expressed through the formula: 2^n where n is the number of bits borrowed. For example if 2 bits are borrowed then $2^2 = 4$, which indicates that 4 new subnets can be created.

NAT

Network Address Translation (NAT), is a technique used to map multiple private IPs to a single public IP. This is done for multiple reasons such as IP conservation, security, flexibility, and for more support of private IPs. There are three main types of NAT:

- Static: Where the private IP is converted to a Public IP, a one to one mapping.
- Dynamic: Where the NAT chooses a different IP based on the available Public IPs
- Port Address Translation (PAT): A type of Dynamic NAT where it enables the mapping of several private IPs to one public IP.

This is done by modifying the chunk of data before it passes through the router and to the internet and changing the IP address to a Public one.

Conclusion

In conclusion, IP addresses are the backbone of the internet; without them, any communication is impossible. IPs make communication, and data routing (how data is transported across the internet) possible. Understanding the structure of IPv4 and IPv6 addresses, as well as NAT's and Subnet's is critical for understanding IT, and network management, as well as creating efficient networks.