## What is an IP address?

An IP (Internet Protocol) address is a unique numerical identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves two main functions:

* Identifying the host or network interface: An IP address identifies the specific device or network interface on the internet or a local network.
* Providing a location for the device: Like a postal address, an IP address provides the necessary information for data packets to be routed from the source device to the destination device.

IP addresses are binary numbers, but they are usually expressed in human-readable notation, such as dotted-decimal notation for IPv4 (e.g., 192.168.0.1) or hexadecimal notation for IPv6 (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

There are two main versions of IP addresses:

* Text

  Description automatically generatedIPv4 (Internet Protocol version 4): IPv4 addresses are 32-bit numbers, which allows for a total of 4,294,967,296 unique addresses. Due to the rapid growth of internet-connected devices, IPv4 addresses are being depleted.  
  the Format of the IPV4   
  The format of an IPv4 address is a 32-bit number divided into four 8-bit octets, separated by dots. Each octet is represented by a decimal number ranging from 0 to 255.   
  Example x.x.x.x, where each “x” is represents an octet (8 bits) in decimal notation.  
  For example, consider the IP address: 192.168.0.1   
  In binary, this address would be represented as: 11000000.10101000.00000000.00000001  
  Each octet in binary:
  + - 1st octet: 11000000 (192 in decimal)
    - 2nd octet: 10101000 (168 in decimal)
    - 3rd octet: 00000000 (0 in decimal)
    - 4th octet: 00000001 (1 in decimal)

IPv4 addresses are divided into network and host portions based on the subnet mask. The subnet mask determines which part of the IP address represents the network and which part represents the host.

For example, with a subnet mask of 255.255.255.0 (or /24 in CIDR notation), the first three octets (192.168.0) represent the network portion, while the last octet (1) represents the host portion.  
For example, with a subnet mask of 255.255.255.0 (or /24 in CIDR notation), the first three octets (192.168.0) represent the network portion, while the last octet (1) represents the host portion.

IPv4 addresses are also divided into five classes (A, B, C, D, and E) based on the value of the first octet:

Class A: 0.0.0.0 to 127.255.255.255 (first octet range: 0-127)

Class B: 128.0.0.0 to 191.255.255.255 (first octet range: 128-191)

Class C: 192.0.0.0 to 223.255.255.255 (first octet range: 192-223)

Class D: 224.0.0.0 to 239.255.255.255 (used for multicast)

Class E: 240.0.0.0 to 255.255.255.255 (reserved for future use)

Classes A, B, and C are used for unicast addresses, while Class D is used for multicast addresses. Class E is reserved for experimental purposes.

* IPv6 (Internet Protocol version 6): IPv6 addresses are 128-bit numbers, providing a much larger address space than IPv4. It allows for approximately 340 undecillion (3.4 × 10^38) unique addresses, which should suffice for the foreseeable future.  
  Pv6 (Internet Protocol version 6) is the most recent version of the Internet Protocol, designed to address the limitations of IPv4 and provide a larger address space. The format of an IPv6 address is quite different from that of an IPv4 address.

An IPv6 address is a 128-bit number represented as eight 16-bit hexadecimal blocks separated by colons. Each block contains four hexadecimal digits (0-9 and a-f).  
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX  
Where each 'X' represents a hexadecimal digit.

For example, consider the IPv6 address: A8FB:7A88:FFF0:0FFF:3D21:2085:66FB:F0FA

To simplify the representation, there are two rules for abbreviation:

* + Leading zeros in each block can be omitted.
  + Consecutive blocks of zeros can be replaced by a double colon (::), but this can only be done once in an address.

IPv6 addresses are divided into two parts:

* Network part: The leftmost 64 bits (first four blocks) represent the network.
* Interface Identifier (host part): The rightmost 64 bits (last four blocks) represent the host or interface identifier.

IPv6 addresses can be categorized into three types:

* Unicast: Identifies a single interface. Packets sent to a unicast address are delivered to the specific interface.
* Multicast: Identifies a group of interfaces. Packets sent to a multicast address are delivered to all interfaces in the group.
* Anycast: Assigned to multiple interfaces, typically belonging to different nodes. Packets sent to an anycast address are delivered to the nearest interface (based on routing distance).

Some special IPv6 addresses include:

* Loopback address: ::1 (equivalent to 127.0.0.1 in IPv4)
* Unspecified address: :: (used as a source address when a host doesn't have an address yet)
* Link-local addresses: Start with FE80:: and are used for communication within a local network segment.

Comparison IPV4 and IPV6

When a device connects to a network, it is assigned an IP address by a DHCP server or manually configured with a static IP address. This IP address is used to identify the device and enable communication with other devices on the network or the internet.

Address Size:

* IPv4: 32-bit addresses, allowing for approximately 4.3 billion unique addresses.
* IPv6: 128-bit addresses, providing approximately 340 undecillion (3.4 × 10^38) unique addresses.

Notation:

* IPv4: Dotted-decimal notation, with four octets separated by dots (e.g., 192.168.0.1).
* IPv6: Hexadecimal notation, with eight 16-bit blocks separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Header Structure:

* IPv4: Header includes 12 basic fields and optional extension headers, with a variable length of 20-60 bytes.
* IPv6: Header has a fixed length of 40 bytes, with optional extension headers for added functionality.

Fragmentation:

* IPv4: Routers can fragment packets if they exceed the maximum transmission unit (MTU) of the link.
* IPv6: Routers do not fragment packets; fragmentation is handled by the source device using the Path MTU Discovery (PMTUD) mechanism.

Quality of Service (QoS):

* IPv4: Uses the Type of Service (ToS) field for QoS, which has limited functionality.
* IPv6: Includes a Flow Label field for improved QoS handling and support for real-time applications.

Security:

* IPv4: Security features like IPsec are optional and implemented as add-ons.
* IPv6: IPsec is built into the protocol, providing better security support.

Network Address Translation (NAT):

* IPv4: Widely uses NAT to conserve limited address space, which can cause complications for certain applications.
* IPv6: NAT is not necessarily due to the vast address space, enabling true end-to-end connectivity.

Multicasting:

* IPv4: Uses Internet Group Management Protocol (IGMP) for multicast group management.
* IPv6: Uses Multicast Listener Discovery (MLD) protocol, which is an integral part of the protocol.

Configuration:

* IPv4: Requires manual or DHCP configuration for addresses, which can be complex in large networks.
* IPv6: Supports stateless address autoconfiguration (SLAAC), allowing devices to configure their addresses automatically.

Adoption:

* IPv4: Widely adopted and still the most common version of the Internet Protocol.
* IPv6: Gradually being adopted to address the limitations of IPv4, especially the depletion of address space.

IPv6 has benefits over IPv4, it

* has no need for NATs (network address translation)
* removes risk of private IP address collisions
* has built in authentication
* allows for more efficient routing.
* Zero compression

There are two types of IP address

Private IP address

Private IP addresses are used within private networks and are not globally unique. They are typically used for devices within a local network, such as computers, printers, or smartphones.

Private IP addresses are defined by the Internet Assigned Numbers Authority (IANA) and fall within specific ranges (e.g., 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)

Private IP addresses are reserved for internal use behind a router or other NAT device. The following blocks are reserved for private IP addresses.

|  |  |  |
| --- | --- | --- |
| Class A | 10.0.0.0 to 10.255.255.255 | 16 million possible addresses |
| Class B | 172.16.0.0 to 172.31.255.255 | 1 million possible addresses |
| Class C | 192.168.0.0 to 192.168.255.255 | 65,600 possible addresses |

Private IP addresses (which are internal value only) allow for an entirely separate set of addresses within a network. The address space allocated to allow organizations to create their own private network.

They allow access to the network without taking up a public IP address space.

Devices using these private IP addresses cannot be reached by internet users.

When a computer is assigned a private IP address, the local devices see this computer via its private IP address.

The devices residing outside of your local network cannot directly communicate via the private IP address but uses your router's public IP address to communicate.

Network Address Translation (NAT) is used to translate private IP addresses to public IP addresses when devices communicate with the internet, enhancing security by hiding the internal network structure.

Public IP address?

Public IP addresses are globally unique and are assigned to devices directly connected to the internet. It allows direct access to the Internet. A web server, email server and any server device need to directly access the Internet are candidate for a public IP address.

Public IP addresses are the ones allocated by a user’s ISP to identify the location of their device. Devices using these IP addresses are accessible from anybody using the internet

Public IP addresses are used by

* DNS servers
* network routers
* directly-controlled computers

Public IP address is classified into to

* A **dynamic** IP address, as the name suggests, changes over time. Your ISP assigns them, but unlike other IP address types they will change every time you reboot your device, add a new device to your network, or change your network configuration. The changes rarely have any impact on your connection, and a dynamic IP address is the go-to in most households.
* A **static** IP address, contrary to dynamic IP, never changes. They are typically assigned to servers that host websites or provide email or FTP services. However, they can also be given to public organizations that need stable connections and consistent web addresses. Some Individuals use them for gaming or VOIP connections as these also need very stable connections.  
  Static IP Addresses are rarely used for individual households as they have some drawbacks:
* ISPs charge extra for assigning a static IP;
* They require additional security measures as they are more susceptible to brute force attacks;
* They are easier to track by data mining companies.

Subnetting

Subnetting is the process of dividing a larger network into smaller subnetworks (subnets) to improve network performance, security, and management.

Subnetting allows network administrators to allocate IP addresses efficiently and create logical divisions within a network based on factors such as departments, locations, or device types.

The goal of subnetting is to create a fast, efficient, and resilient computer network. As networks become larger and more complex, the traffic traveling through them needs more efficient routes. If all network traffic were traveling across the system at the same time using the same route, bottlenecks and congestion would occur resulting in sluggish and inefficient backlogs.

Subnets are defined by a subnet mask, which determines the number of bits used for the network portion and the host portion of an IP address.

Creating a subnet allows you to limit the number of routers that network traffic has to pass through.

Benefits of subnetting

* Easier maintenance;
* Advanced network security so that one subnet can’t access the other one;
* Reduced network traffic;
* When you can subnet your network, you don’t need to acquire additional IP addresses from ISPs (internet service providers).

# What is a Subnet Mask?

A subnet mask is a way of splitting a network up into smaller mini networks without wasting IP addresses.

In a standard home/small office network your router can normally support up to 250 devices and you can use subnetting to separate parts of the network from each other, whilst still allowing all devices to access the internet.

**Why do we need subnet masks?**

Breaking a large network up into smaller network reduces the network traffic because network broadcasts only go out other parts of the subnet, not the whole network. Without this a large network would be susceptible to a broadcast storm, where large amounts of broadcasts can seriously impede the performance of a network.

Diagram

Description automatically generatedHaving subnets of a larger network is more secure and also easier to troubleshoot as only part of a network would be affected by network issues.

Thus we can write the default subnet mask for a class A, B and C networks

Graphical user interface, text, application

Description automatically generated

### ***Using a subnet mask***

When an IP packet arrives on a router, the router examines the destination address to decide what to do. The router has an internal table (the routing table) which stores all the networks it knows about and the associated interface which leads to that network. The router thus needs to know the destination network of the packet so it can use this as a lookup in the routing table.

When a packet originates on an end device, the end device will need to know if the destination is on the same local network or off on a different network. It does this by examining its own local address to see which network it is on, and then compares this to the destination network of the packet. If the two match, the destination is on its own Local Area Network (LAN). If not it is on a different network and the packet should be forwarded to the default router (sometimes called the gateway).

A combination of the IP address and a subnet mask will translate into a network address.

A web address consist of 3 parts

[www.searchfacts.com](http://www.searchfacts.com)

1. Before the dot, --Sub domain
2. Between the dots --Domain Name
3. After the dot--- Domain extension (Top Level)

Diagram, timeline

Description automatically generated

The last section of a domain name is known as the Top-Level Domain (TLD)

A picture containing calculator

Description automatically generated is the most general part of the domain. They are sometimes called domain suffixes or extensions and are meant to communicate the purpose or location of a website. The Internet Corporation for Assigned Names and Numbers (ICANN) controls registries that make TLDs available.

There are several types of TLD

Text

Description automatically generatedThe second-level domain (SLD), sometimes referred to as 2LD, is the section preceding the TLD.The SLD is often the most valuable portion of the domain name because it makes up the main identity for users. The maximum length of an SLD is 63 characters, but generally, you want to pick an SLD that is short, branded and memorable.

Logo

Description automatically generated

A subdomain is an optional part of a URL that creates a completely separate section of your website. If a URL has a subdomain, it will precede the domain name with a period.

Websites might use subdomains to test or stage web development, to create new directories to separate and store web files, or to communicate unique segments of a website to the end user.

Domain Name System

Using IP addresses whether the decimal numbers or binary are difficult for us to use and remember. Just imagine if we have to remember the IP address of all the web pages we want to use on the internet, this would prove to be mightily impossible for most of us.

To get around this issue a text-based name that represents one or more IP address is used called a Domain name system

The domain name system (DNS) is the method that the Internet uses to store domain names and their corresponding IP addresses.

When you specify a domain name, a DNS server translates the domain name to its associated IP address so that data and information can be routed to the correct computer.

Entering the domain name google.com will be mapped to the server’s IP address 74.125.239.116 and then the browser will try to contact that IP directly to get the required information

How does a DNS work?

The process of DNS resolution involves converting a hostname (such as www.example.com) into a computer-friendly IP address (such as 192.168.1.1). An IP address is given to each device on the Internet, and that address is necessary to find the appropriate Internet device - like a street address is used to find a particular home. When a user wants to load a webpage, a translation must occur between what a user types into their web browser (example.com) and the machine-friendly address necessary to locate the example.com webpage.

In order to understand the process behind the DNS resolution, it’s important to learn about the different hardware components a DNS query must pass between. For the web browser, the DNS lookup occurs "behind the scenes" and requires no interaction from the user’s computer apart from the initial request.

## There are 4 DNS servers involved in loading a webpage:

* **DNS recursor** - The DNS recursor is a server designed to receive queries from client machines through applications such as web browsers. Typically, the recursor is then responsible for making additional requests in order to satisfy the client’s DNS query.  
  The resolver starts the sequence of queries that will lead to a URL being translated into the necessary IP address.
* **Root nameserver** - The root server is the first step in translating (resolving) human readable host names into IP addresses. It serves as a reference to other more specific locations.
* **TLD nameserver** - The top level domain (TLD) nameserver (TLD) is the next step in the search for a specific IP address, and it hosts the last portion of a hostname ( example.com, .org. edu).
* **Authoritative nameserver** - This nameserver is the last stop in the nameserver query. If the authoritative name server has access to the requested record, it will return the IP address for the requested hostname back to the DNS Recursor (that made the initial request.

Diagram

Description automatically generated

The following are the steps taken to use a DNS to find a web page

1. A user types ***‘example.com’*** into a web browser and the query travels into the Internet and is received by a DNS recursive resolver.
2. The resolver then queries a DNS root nameserver (.).
3. The root server then responds to the resolver with the address of a Top-Level Domain (TLD) DNS server (such as .com or .net), which stores the information for its domains. When searching for example.com, our request is pointed toward the .com TLD.
4. The resolver then makes a request to the .com TLD.
5. The TLD server then responds with the IP address of the domain’s nameserver, example.com.
6. Lastly, the recursive resolver sends a query to the domain’s nameserver.
7. The IP address for example.com is then returned to the resolver from the nameserver.
8. The DNS resolver then responds to the web browser with the IP address of the domain requested initially.

Once the 8 steps of the DNS lookup have returned the IP address for example.com, the browser is able to make the request for the web page:

1. The browser makes a [HTTP](https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/) request to the IP address.
2. The server at that IP returns the webpage to be rendered in the browser (step 10).

Diagram

Description automatically generated