IP addressing and Subnetting

Prepared by : EMAN FATIMA

1/2/25

Data Communication and Networking

Semester Project Report: IP Addressing and Sub-netting

Table of Contents

1. **Introduction**
    - Objective
    - Scope of the Project
    - Importance of IP Addressing and Sub-netting
    - History of IP addressing
2. **IP Addressing Basics**
    - What is an IP Address?
    - Static or Dynamic IP addressing.
    - IP datagram
    - IPv4 and IPv6

    IPv4
    - IPv4 address structure(32 bits, 4 octets)
    - IPv4 address types
        - Uni-cast ,Multicast, Broad-cast
    - IPv4 address notation(Dotted Decimal Notation)

    IPv6
    - IPv6 address structure(128 bits, 8 hextets)
    - IPv6 address types
        - Uni-cast ,Multicast, Any-cast
    - IPv6 address notation(Colon Hexadecimal)
    - IPv6 address shortening and abbreviation
3. **Sub-netting Concepts**
    - What is Sub-netting?
    - Purpose of sub-netting (improved network organization and security)
    - Subnet Mask
    - Network classes
4. **Types of subnetting**
    - Variable length subnet Mask (VLSMs)
    - Fixed Length subnet Mask (FLSMs)
5. **Classless Inter-Domain Routing (CIDR)**
    - Definition of CIDR
    - Purpose of CIDR(Improved network routing and addressing)
    - CIDR notation and Benefits
6. **Static IP Address Configuration**
    - Importance of Static IP's
    - Configuring Static IP on Devices
    - Assigning Static IP's in a Network
7. **Practical Implementation**
    - Setting Up a Simple Network
    - Configuring Static IPs and Sub-nets for Multiple Devices
    - Testing Connectivity and troubleshooting tips
8. **Tools and Resources**

- Tools Used (e.g., Network Simulator or Real Devices)
- Resources for Further Reading

9. **Conclusion**
    - Summary of Findings
    - Benefits of Proper IP Addressing and Subnetting

Introduction

Objective:

The objective of this project is to demonstrate the concepts of IP addressing and subnetting by configuring static IPs and subnets for multiple devices. The project will cover both theoretical and practical aspects of IP addressing and subnetting, with an emphasis on real-world applications for network configuration.

Scope of the Project:

This project will:

- Define the basics of IP addressing and subnetting.
- Show how to configure static IP addresses on various devices.
- Walk through the process of subnetting an IP address range for a network.
- Provide practical steps to implement the network setup using static IPs and subnets.

Importance of IP Addressing and Subnetting:

- Efficient IP addressing ensures proper communication between devices.
- Subnetting helps to organize networks, optimize IP address usage, and improve network security.

History of IP addressing and sub-netting:

The history of IP addressing and subnetting dates back to the **1960s** with **ARPANET.** The first IP addressing scheme emerged in the 1970s, followed by subnetting in the **1980s.**

Classful IP addressing was introduced in the **1980s** and replaced by **Classless Inter-Domain Routing (CIDR)** in the **1990s**. 'IPv6' was developed in the **1990s** to address the limitations of 'IPv4'. Modern subnetting techniques enable complex network designs with **variable-length subnet masks (VLSMs),** ensuring efficient, scalable, and secure networks. This evolution has shaped the modern internet.

IP Addressing Basics

An Internet Protocol (IP) address is a unique identifier for devices on a network. It is required for communication over the internet or a local network.

Static IP addressing

A static IP address is a fixed IP address assigned to a device or network that remains the same over time. Static IP addresses are manually configured by a network administrator or **ISP**.

Dynamic IP Addressing

A dynamic IP address is a temporary IP address assigned to a device or network that changes over time. Dynamic IP addresses are automatically assigned by a DHCP (Dynamic Host Configuration Protocol) server.

Key Features:

Feature	Static Routing	Dynamic Routing
Route Configuration	Manual configuration	Automatic configuration
Route Updates	No automatic updates	Automatic updates
Scalability	Limited scalability	High scalability
Flexibility	Low flexibility	High flexibility
Route Discovery	No route discovery	Automatic route discovery
Network Changes	Requires manual updates	Adapts to network changes
Security	More secure due to manual configuration	Less secure due to automatic updates
Complexity	Simple to implement	Complex to implement
Suitability	Small, simple networks	Large, complex networks

IP Datagram

IP Datagram Structure

- **Version (4 bits):** Indicates the IP version (e.g., IPv4 or IPv6).
- **Header Length (4 bits):** Specifies the length of the IP header.
- **Type of Service (8 bits):** Defines the quality of service (QoS) for the datagram.
- **Total Length (16 bits):** Specifies the total length of the datagram.
- **Identification (16 bits):** Identifies the datagram for reassembly purposes.
- **Flags (3 bits):** Indicates whether the datagram can be fragmented.
- **Fragment Offset (13 bits):** Specifies the offset of the fragment within the original datagram.
- **Time to Live (8 bits):** Sets the maximum number of hops the datagram can take.
- **Protocol (8 bits):** Identifies the transport-layer protocol (e.g., TCP or UDP).
- **Header Checksum (16 bits):** Verifies the integrity of the IP header.
- **Source IP Address (32 bits):** Specifies the IP address of the sender.
- **Destination IP Address (32 bits):** Specifies the IP address of the recipient.
- **Options (variable length)**: Provides additional information for routing and debugging purposes.

- **Data (variable length):** Contains the actual data being transmitted.

Key Concepts

Fragmentation:

The process of dividing a large datagram into smaller fragments to accommodate network limitations.

Reassembly:

The process of reassembling fragmented datagrams at the receiving end.

Header checksum:

A mechanism to ensure the integrity of the IP header during transmission.

IPv4 and IPv6

IPv4:

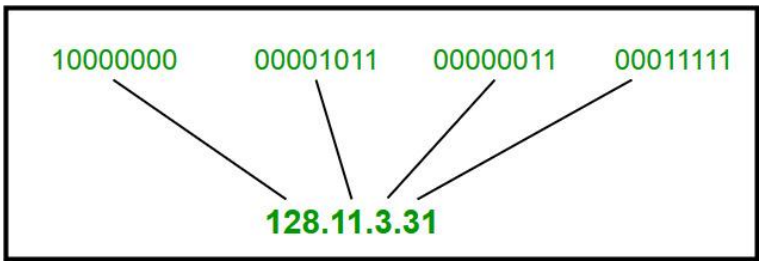
IPv4 or internet protocol version 4 is the original addressing system of the internet introduced in 1983.

Example:

192.168.1.1 is a common IPv4 address , you might find in a home network.

IPv4 address structure:

It uses a 32-bit address scheme which theoretically allows for over 4 billion unique addresses(2^32). IPv4 addresses are typically displayed in decimal format divided into 4 octets separated by dots.



IPv4 address types:

Depending on how many devices an address represents, it can be classified in three types:

- **Uni-cast addresses:**

  A unicast address represents a single device in the network.
- **Multicast addresses:**

  A multicast address represents a group of devices in the network.
- **Broadcast addresses:**

  A broadcast address represents all devices in the network.

IPv4 address notation (Dotted Decimal Notation)

IPv4 addresses are typically written in dotted decimal notation, which consists of four numbers separated by dots (.).

Format:

xxx.xxx.xxx.xxx

Where xxx represents a decimal value between 0 and 255.

Example:

192.0.2.1

Octet Representation	**Binary Representation**	**Hexadecimal Representation**
Each of the four numbers in the dotted decimal notation represents an octet (8 bits) of the IPv4 address.	IPv4 addresses can also be represented in binary form, which consists of 32 bits (0s and 1s).	IPv4 addresses can also be represented in hexadecimal form, which consists of eight hexadecimal digits.
Breakdown: 1st octet: 192 2nd octet: 0 3rd octet: 2 4th octet: 1	**Format:** xxxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx Where x represents a binary digit (0 or 1). **Example:** 11000000.00000000.00000010.00000001	**Format:** xxxxxxxx Where x represents a hexadecimal digit (0-9, A-F). **Example:** C0000201

IPv6

IPv6 stands for Internet Protocol version 6. IPv6 is the new version of Internet Protocol, which is way better than IPv4 in terms of complexity and efficiency.

The well-known IPv6 protocol is being used and deployed more often, especially in mobile phone markets. IPv6 was designed by the **Internet Engineering Task Force (IETF)** in **December 1998** with the purpose of superseding IPv4 due to the global exponentially growing internet of users.

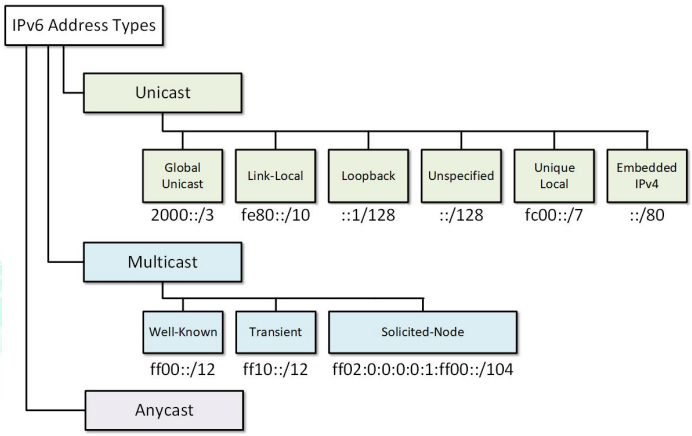
IPv6 address structure:

IPv6 is written as a group of 8 hexadecimal numbers separated by colon (:). It can be written as 128 bits of 0s and 1s.

IPv6 address types:

An IPv6 address is a 128-bit network layer identifier for a single interface of IPv6 enabled node. There are three main types of addresses as shown below:

- **Unicast** - A network layer identifier for **a single interface** of IPv6 enabled node. Packets sent to a unicast address are delivered to the interface configured with that IPv6 address. Therefore, it is **one-to-one** communication.
- **Multicast** - A network layer identifier for **a set of interfaces**, belonging to different IPv6 enabled nodes. Packets sent to a multicast address are delivered to all interfaces identified by that address. Therefore, it is **one-to-many** communication.
- **Anycast** - A network layer identifier for **a set of interfaces**, belonging to different IPv6 enabled nodes. Packets sent to an anycast address are delivered to the "closest" interface identified by that address. "Closest" typically means the one with the best routing metric according to the IPv6 routing protocol. Therefore, it is **one-to-closest** communication.
- ~~**Broadcast**~~ - There are no broadcast addresses in IPv6. Broadcast functionality is implemented using multicast addresses.



IPv6 Address Notation(Colon Hexadecimal)

IPv6 addresses are typically written in hexadecimal notation, with eight groups of four hexadecimal digits separated by colons (:).

Format:

xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx

Example:

2001:0db8:85a3:0000:0000:8a2e:0370:7334

Where x represents a hexadecimal digit (0-9, A-F).

Abbreviated IPv6 Address Notation

IPv6 addresses can be abbreviated by:

1. Removing leading zeros within each group.
2. Removing consecutive groups of zeros and replacing them with a double colon (::).

Example:

2001:db8:85a3::8a2e:370:7334

Sub-netting Concepts

Subnetting is the practice of dividing a network into smaller sub-networks (subnets). This improves performance and security by reducing traffic on individual networks and managing the network efficiently.

Subnetting purposes:

Some main subnetting purposes are as:

- **Improved Network Organization**: Divides a large network into smaller, manageable subnetworks.
- **Reduced Network Congestion**: Decreases traffic by isolating subnets.
- **Enhanced Network Security:** Implements access controls and firewalls at the subnet level.
- **Better Resource Allocation:** Allocates IP addresses to specific subnets.
- **Simplified Network Troubleshooting:** Isolates issues to specific subnets.

Sub-net Mask:

The subnet mask is a 32-bit number that determines whether a host is on the local subnet or a remote network. It's essential for TCP/IP to work. The subnet mask is used to separate the network and host addresses.

Example:

For example, consider the IP address 192.168.123.132 with a subnet mask of 255.255.255.0. The binary representation of the subnet mask is;

11111111.11111111.11111111.00000000

By lining up the IP address and subnet mask, we can separate the network and host portions:

11000000.10101000.01111011.10000100 IP address
11111111.11111111.11111111.00000000 (subnet mask)

The first 24 bits are the network address, and the last 8 bits are the host address:

Network address:

11000000.10101000.01111011.00000000

Host address:

00000000.00000000.00000000.10000100

Common subnet masks include:

255.255.255.192
255.255.255.224

These subnet masks determine how the IP address is divided between the network and host portions.

NETWORK CLASSES:

Internet addresses are allocated by the Inter-NIC the organization that administers the Internet. These IP addresses are divided into classes. The most common of these are classes A, B, and C. Classes D and E . Each of the address classes has a different default subnet mask. You can identify the class of an IP address by looking at its first octet. Following are the ranges of class A, B, and C Internet addresses, each with an example address:

Class A :

Class A networks use a default subnet mask of 255. 0. 0. 0 and have **0-127** as their first octet. The address 10.52.36.11 is a class A address. Its first octet is 10, which is between 1 and 126, inclusive.

Class B :

Class B networks use a default subnet mask of 255. 255. 0. 0 and have **128-191** as their first octet. The address 172.16.52.63 is a class B address. Its first octet is 172, which is between 128 and 191, inclusive.

Class C :

Class C networks use a default subnet mask of 255.255.255.0 and have **192-223** as their first octet. The address 192.168.123.132 is a class C address. Its first octet is 192, which is between 192 and 223, inclusive.

FLSM Subnetting and VLSM Subnetting

There are two types of Subnetting:

⇒ Fixed Length subnet mask (FLSM)

⇒ Variable length subnet mask (VLSM)

Differences between FLSM Subnetting and VLSM Subnetting

The following table lists the differences between FLSM and VLSM.

FLSM	VLSM
1. All subnets are equal in size.	**1.** Subnets are variable in length.
2. All subnets have an equal number of hosts.	**2.** Subnets have a variable number of hosts.
3. All subnets use the same subnet mask.	**3.** Subnets use different subnet masks.
4. It is easy to configure and manage.	**4.** It is complex in configuration and administration.
5. It wastes a lot of IP addresses.	**5.** It wastes minimum IP addresses.
6. It is also known as classful subnetting.	**6.** It is also known as classless subnetting.
7. It supports both classful and classless routing protocols.	**7.** It supports only classless routing protocols.

Class-less Inter-Domain Routing (CIDR)

Classless Inter-Domain Routing (CIDR) is a method of IP address allocation and IP routing that allows for more efficient use of IP addresses. CIDR is based on the idea that IP addresses can be allocated and routed based on their network prefix rather than their class, which was the traditional way of IP address allocation.

CIDR representation:

It is as also a 32-bit address, which includes a special number that represents the number of bits that are present in the Block Id.

a . b . c . d / n

Where n is the number of bits that are present in Block Id / Network Id.

Example:

20.10.50.100/20

Rules for forming CIDR Blocks:

All IP addresses must be contiguous. Block size must be the power of 2 (2n). If the size of the block is the power of 2, then it will be easy to divide the Network. Finding out the Block Id is very easy if the block size is of the power of 2.

Classes in CIDR:

In Classful addressing the no of Hosts within a network always remains the same depending upon the class of the Network.

- Class A network contains 224(IP addresses) or 224 - 2 Hosts,
- Class B network contains 216(IP addresses) or 216 - 2 Hosts,
- Class C network contains 28(IP addresses) or 28 - 2 Hosts

. Nowadays IANA is using this technique to provide IP addresses. Whenever any user asks for IP addresses, IANA is going to assign that many IP addresses to the User.32 Bit Address

Static IP Address Configuration

Importance of Static IPs:

- A static IP is manually assigned and does not change, unlike a dynamic IP.
- It's used in servers, printers, routers, and other devices where a consistent IP address is needed for reliable connectivity.

Configuring Static IP on Devices:

For Windows:

1. Go to "Network & Internet Settings".
2. Select the Ethernet or Wi-Fi network.
3. Click on "Properties" and select "Use the following IP address".
4. Enter the desired IP address, subnet mask, and default gateway.

For Linux:

1. Edit the network configuration file (/etc./network/interfaces or use nmcli commands).
2. Assign the static IP and subnet mask.

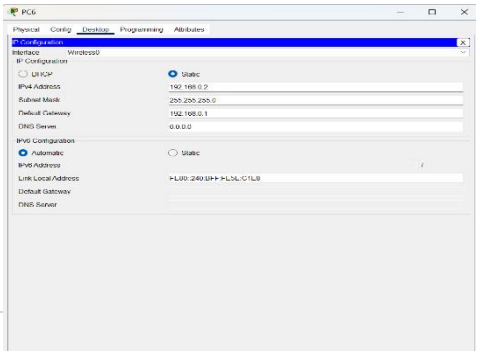
Assigning Static IPs in a Network:

Each device in the network must have a unique static IP address. The network administrator manually assigns these addresses based on the network design (subnetting).

Practical Implementation

Setting Up a Simple Network:

1. Choose an IP range(from class C generally) for your network (e.g., **192.168.1.0/24**).
2. Divide the network into smaller subnets using subnetting.
3. Assign static IP addresses to devices in each subnet.



Configuring Static IPs and Subnets for Multiple Devices

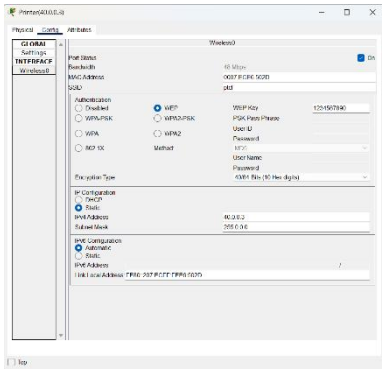
- **Device 1 (Router):**

  IP address: **192.168.1.1**
  Subnet mask :**255.255.255.0**.

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#
```

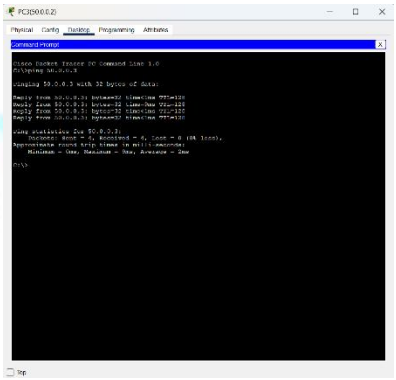
- **Device 2 (PC):**

  IP address: **192.168.1.2**
  Subnet mask: **255.255.255.0.**



- **Device 3 (Printer):**

  IP address: **192.168.1.3**
  Subnet mask :**255.255.255.0.**

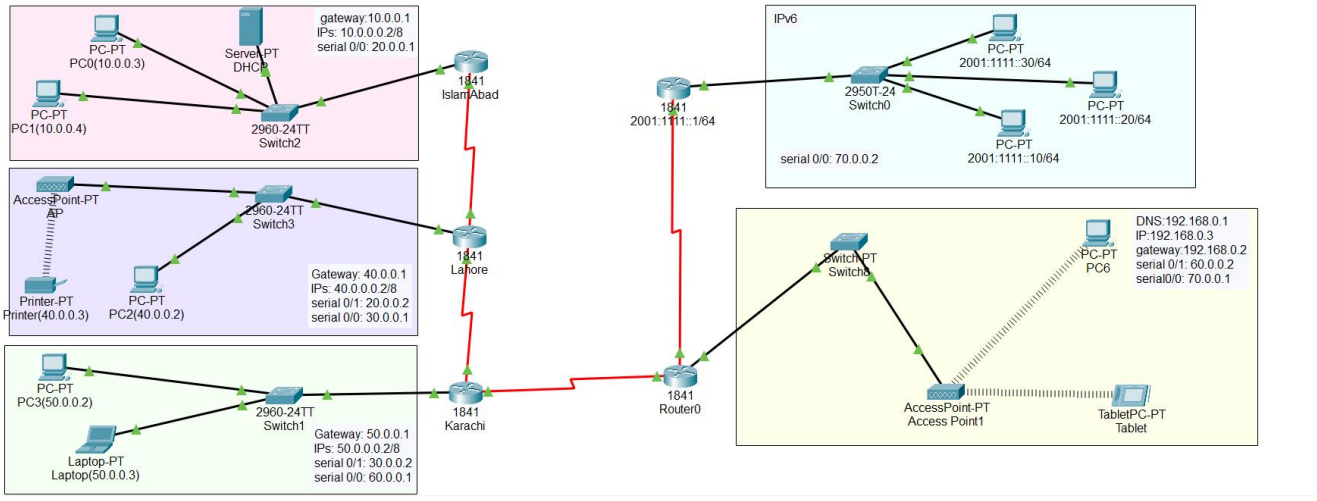


Testing Connectivity

Use the **ping** command to check if the devices can communicate with each other.

Setting Up a Simple WAN:

Click here for [WAN Configuration]



Tools and Resources

Tools used:

- **Packet Tracer/ GNS3**: Network simulators to test and visualize network configurations.
- **Wireshark**: For network traffic analysis.

Resources for Further Reading:

- "Data and computer network communication" by **SHASHI BANZIL.**
- "Data communication and Networking" by **BEHROUZ A. FOROUZAN.**
- **https://www.networkacademy.io/ccna/ipv6/ipv6-address-types.**
- **https://www.geeksforgeeks.org/differences-between-ipv4-and-ipv6/#what-is-ipv4.**
- **https://www.computernetworkingnotes.com/ccna-study-guide/flsm-subnetting-and-vlsm-subnetting.html.**

Conclusion

Summary of Findings:

- IP Addressing and Subnetting are crucial for network design and efficiency.
- Static IPs ensure reliable device identification and network management.
- Subnetting allows for better utilization of IP ranges and segmentation of networks for security and performance.

Benefits of Proper IP Addressing and Subnetting:

- Efficient use of network resources.
- Better network organization.
- Enhanced security by isolating subnets.