**ASSIGNMENT-2**

**IP Addressing**

1. **Prepare R&D Document on IP Addressing and Subnetting including IPv4 & IPv6. Understand and document IP addressing and subnetting such that you should be able to create Subnets in natural masks, subnet mask, CIDR range, count usable and total hosts in a IP address range**
2. **Prepare R&D Document on Basics of MAC Addressing and Functionality of ARP & RARP**

* **IP Addressing and Subnetting**

IP addressing is a fundamental concept in networking that allows devices to communicate over the Internet or local networks. Understanding IP addressing and subnetting is crucial for network design, management, and troubleshooting.

**1. IP Addressing**

IP Address: An Internet Protocol (IP) address is a unique identifier assigned to each device connected to a network. It serves two main functions: identifying the host or network interface and providing the location of the device in the network.

* 1. **IPv4 Addressing**:

The most widely used version of IP addressing is IPv4, which consists of 32 bits. An IPv4 address is typically represented in decimal format as four octets, separated by periods (e.g., 192.168.1.1). Each octet can range from 0 to 255.

**Structure of an IPv4 Address**

* **Network Portion**: Identifies the specific network.
* **Host Portion**: Identifies the specific device on that network.

**Classes of IPv4 Addresses**

IPv4 addresses are categorized into five classes (A, B, C, D, and E), but Classes A, B, and C are primarily used for host addressing:

* **Class A**:
  + **Range**: **1.0.0.0** to **126.255.255.255**
  + **Default Subnet Mask**: **255.0.0.0** (or **/8**)
  + **Usable Hosts**: 224-2=16777214
* **Class B**:
  + **Range**: **128.0.0.0** to **191.255.255.255**
  + **Default Subnet Mask**: **255.255.0.0** (or **/16**)
  + **Usable Hosts**: 216−2=65,534
* **Class C**:
  + **Range**: **192.0.0.0** to **223.255.255.255**
  + **Default Subnet Mask**: **255.255.255.0** (or **/24**)
  + **Usable Hosts**: 28−2=254

**1.2 IPv6 Addressing**

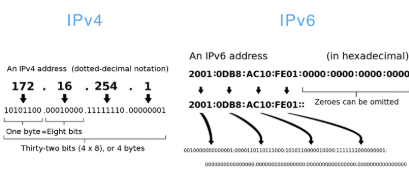
IPv6 (Internet Protocol version 6) is the successor to IPv4 and was developed to address the limitations of IPv4, particularly the exhaustion of available addresses. An IPv6 address consists of 128 bits, represented in hexadecimal format as eight groups of four hexadecimal digits (e.g., **2001:0db8:85a3:0000:0000:8a2e:0370:7334**).

**Structure of an IPv6 Address**

* **Global Routing Prefix**: Identifies the network.
* **Subnet ID**: Identifies the subnet within the network.
* **Interface ID**: Identifies the specific device.

**Benefits of IPv6**

* **Larger Address Space**: Provides a vastly larger address space than IPv4.
* **Improved Security**: Built-in IPsec support for secure communications.
* **Simplified Header Format**: Streamlined packet processing.



**2. Subnetting**

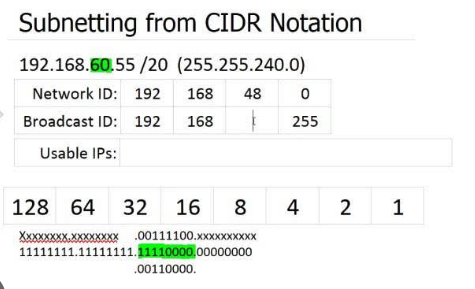
Subnetting is the process of dividing a larger network into smaller, more manageable sub-networks (subnets). This helps improve network performance, security, and efficient IP address utilization.

**2.1 Subnet Masks**

A subnet mask is a 32-bit number that divides the IP address into the network and host portions. It is typically represented in decimal format (e.g., **255.255.255.0**) or CIDR notation (e.g., **/24**).

**2.2 CIDR Notation**

CIDR (Classless Inter-Domain Routing) is a method for allocating IP addresses and IP routing that allows for more flexible subnetting than traditional class-based addressing. CIDR notation specifies the number of bits used for the network portion of the address (e.g., **192.168.1.0/24**).



**2.3 Creating Subnets**

To create subnets, follow these steps:

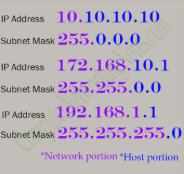
1. **Determine the Network Address**: Identify the base network address (e.g., **192.168.1.0**).
2. **Choose a Subnet Mask**: Decide how many subnets you need and select an appropriate subnet mask. For example, if you need 4 subnets, you can use a **/26** subnet mask (255.255.255.192).
3. **Calculate Subnet Ranges**: Determine the range of IP addresses for each subnet.

**Example: Subnetting 192.168.1.0/24 into 4 Subnets**

1. **Base Network**: **192.168.1.0**
2. **Subnet Mask**: **/26** (255.255.255.192)
3. **Subnet Calculation**:
   * Each subnet will have 2(32-26)=26=64 total addresses.
   * Usable addresses per subnet: 64−2=62 (subtracting network and broadcast addresses).

**Subnet Ranges:**

* **Subnet 1**:
  + **Network Address**: **192.168.1.0**
  + **Usable IPs**: **192.168.1.1** to **192.168.1.62**
  + **Broadcast Address**: **192.168.1.63**
* **Subnet 2**:
  + **Network Address**: **192.168.1.64**
  + **Usable IPs**: **192.168.1.65** to **192.168.1.126**
  + **Broadcast Address**: **192.168.1.127**
* **Subnet 3**:
  + **Network Address**: **192.168.1.128**
  + **Usable IPs**: **192.168.1.129** to **192.168.1.190**
  + **Broadcast Address**: **192.168.1.191**
* **Subnet 4**:
  + **Network Address**: **192.168.1.192**
  + **Usable IPs**: **192.168.1.193** to **192.168.1.254**
  + **Broadcast Address**: **192.168.1.255**



**2.4 Usable and Total Hosts Calculation**

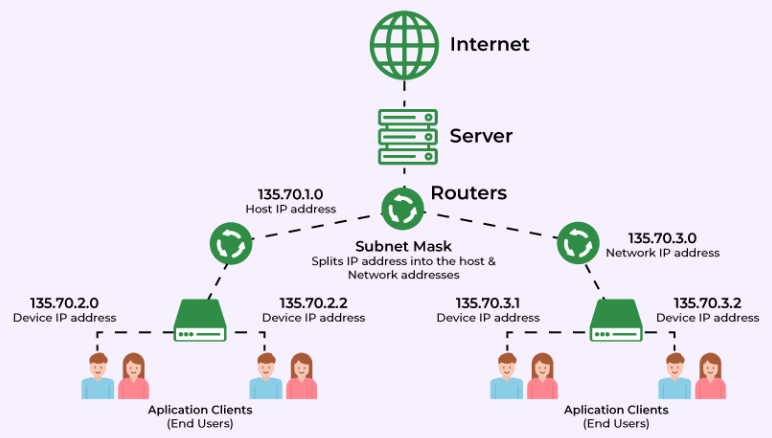
To calculate the number of usable and total hosts in a subnet, use the following formulas:

* **Total Hosts**: 2(32−n), where n is the number of bits in the subnet mask.
* **Usable Hosts**: 2(32−n)−2 (subtracting 2 for the network and broadcast addresses).

**Example Calculation for /26 Subnet Mask:**

* **Total Hosts**: 2(32−26)=26=64
* **Usable Hosts**: 2(32−26)-2=64-2=62

Understanding IP addressing and subnetting is essential for effective network design and management. This document has provided a comprehensive overview of IPv4 and IPv6 addressing, subnetting techniques, and the calculations necessary for creating subnets and determining usable hosts.



* **MAC Addressing and Functionality of ARP & RARP**
  1. **MAC Addressing**

**MAC Address** (Media Access Control Address) is a unique identifier assigned to network interfaces for communications at the data link layer of a network segment. A MAC address is typically represented as a 12-digit hexadecimal number, often displayed in six pairs separated by colons or hyphens (e.g., **00:1A:2B:3C:4D:5E**).

**1.1 Structure of MAC Addresses**

* **Length**: A MAC address consists of 48 bits (6 bytes).
* **OUI**: The first 24 bits represent the Organizationally Unique Identifier (OUI), which identifies the manufacturer.
* **NIC**: The last 24 bits are assigned by the manufacturer to the device.

**2.2 Types of MAC Addresses**

* **Unicast**: A unique address for a single device.
* **Broadcast**: An address that targets all devices on a network (e.g., **FF:FF:FF:FF:FF:FF**).
* **Multicast**: An address that targets a group of devices.
  1. **Address Resolution Protocol (ARP)**

**ARP** is a protocol used to map an IP address to a MAC address within a local area network. When a device wants to communicate with another device on the same network, it needs to know the MAC address corresponding to the IP address of the destination device.

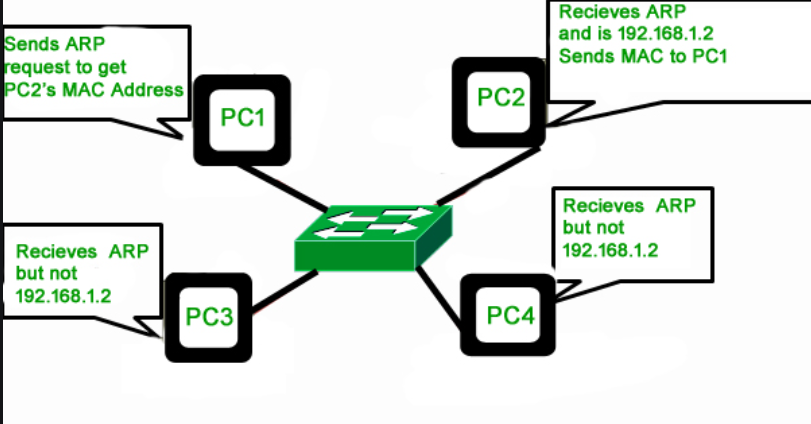
**2.1 Functionality of ARP**

1. **ARP Request**: When a device (Device A) wants to communicate with another device (Device B) and knows its IP address but not its MAC address, Device A broadcasts an ARP request packet to the network. This packet contains the IP address of Device B.
2. **ARP Reply**: All devices on the network receive the ARP request, but only Device B recognizes its own IP address. Device B then sends an ARP reply back to Device A, providing its MAC address.
3. **Caching**: Device A stores the MAC address of Device B in its ARP cache for future communications, reducing the need for repeated ARP requests.

**2.2 ARP Packet Structure**

An ARP packet consists of the following fields:

* **Hardware Type**: Specifies the type of hardware (e.g., Ethernet).
* **Protocol Type**: Specifies the protocol being used (e.g., IPv4).
* **Hardware Size**: Length of the MAC address (usually 6 bytes).
* **Protocol Size**: Length of the IP address (usually 4 bytes).
* **Opcode**: Specifies whether the packet is a request (1) or a reply (2).
* **Sender MAC Address**: MAC address of the sender.
* **Sender IP Address**: IP address of the sender.
* **Target MAC Address**: MAC address of the target (unknown in requests).
* **Target IP Address**: IP address of the target.



**3. Reverse Address Resolution Protocol (RARP)**

**RARP** is a protocol used to obtain an IP address from a known MAC address. It is primarily used by diskless workstations that need to discover their IP address when they boot up.

**3.1 Functionality of RARP**

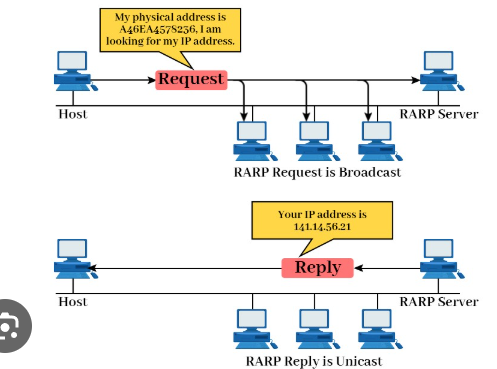
1. **RARP Request**: A device with a known MAC address sends a RARP request to the network, asking for its corresponding IP address.
2. **RARP Server**: A RARP server on the network listens for these requests. When it receives a RARP request, it checks its database to find the IP address associated with the MAC address.
3. **RARP Reply**: The RARP server sends a reply back to the requesting device, providing it with the appropriate IP address.

**3.2 RARP Packet Structure**

A RARP packet consists of similar fields to an ARP packet, including:

* **Hardware Type**
* **Protocol Type**
* **Hardware Size**
* **Protocol Size**
* **Opcode**
* **Sender MAC Address**
* **Sender IP Address** (unknown in requests)
* **Target MAC Address**
* **Target IP Address** (unknown in requests)





Understanding MAC addressing and the functionality of ARP and RARP is essential for network communication. This document has provided a comprehensive overview of MAC addressing, ARP, and RARP, highlighting their roles in facilitating communication between devices on a network.