WEEK-2 IP Addressing

IP Addressing and Subnetting IPv4 & IPv6:

IP Addresses IP addresses consist of two parts: a network identifier and a host identifier. The network ID specifies an area of the network where a device resides, while the host ID labels a specific device in that network section.

There are two main versions of IP addresses: IPv4 and IPv6.

- IPv4 Addresses IPv4 addresses are 32-bit binary strings, typically represented in dotted decimal notation (e.g., 192.0.2.2). They offer about 4.3 billion unique variations.

- IPv6 Addresses IPv6 addresses are 128-bit binary strings, typically represented in hexadecimal notation (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334). They provide more addresses and other benefits compared to IPv4.

Understand IP addressing and subnetting:

An IP address is a unique identifier assigned to a device on a network. It consists of two parts:

- **Network ID (Network Address):** Identifies the network the device is connected to.
- **Host ID (Host Address):** Identifies the specific device on that network.

IP Address Notations:

There are two main notations for IP addresses:

- **Dotted Decimal Notation (IPv4):** 192.0.2.1 (four numbers separated by dots)
- **Hexadecimal Notation (IPv6):** 2001:0db8:85a3:0000:0000:8a2e:0370:7334 (eight groups of four hexadecimal digits separated by colons)

IP Address Classes:

IPv4 addresses are divided into five classes:

Class A: 0.0.0.0 to 127.255.255.255 (large networks)

Class B: 128.0.0.0 to 191.255.255.255 (medium networks)

Class C: 192.0.0.0 to 223.255.255.255 (small networks)

Class D: 224.0.0.0 to 239.255.255.255 (multicast addresses)

Class E: 240.0.0.0 to 254.255.255.255 (reserved for future use)

WEEK-2 IP Addressing

Subnetting:

Subnetting is the process of dividing a larger network into smaller sub-networks or subnets. This is done to:

- Improve network performance: By reducing the number of devices on a network, subnetting can improve network speed and reduce congestion.
- Enhance security: Subnetting can help isolate sensitive areas of the network and limit access to specific devices or segments.
- Simplify network management: Subnetting makes it easier to manage and organize devices on a network.

Create Subnets in natural masks:

Create subnets using natural masks for each class:

Class A

Suppose we have a Class A network with the IP address 10.0.0.0 and a natural mask of 255.0.0.0. We want to create four subnets.

Subnet 1: 10.1.0.0/8 (subnet mask: 255.0.0.0)

Host range: 10.1.0.1 to 10.1.255.254

Subnet 2: 10.2.0.0/8 (subnet mask: 255.0.0.0)

Host range: 10.2.0.1 to 10.2.255.254

Subnet 3: 10.3.0.0/8 (subnet mask: 255.0.0.0)

Host range: 10.3.0.1 to 10.3.255.254

Subnet 4: 10.4.0.0/8 (subnet mask: 255.0.0.0)

Host range: 10.4.0.1 to 10.4.255.254

Class B

Suppose we have a Class B network with the IP address 172.16.0.0 and a natural mask of 255.255.0.0. We want to create four subnets.

Subnet 1: 172.16.1.0/16 (subnet mask: 255.255.0.0)

Host range: 172.16.1.1 to 172.16.1.254

Subnet 2: 172.16.2.0/16 (subnet mask: 255.255.0.0)

Host range: 172.16.2.1 to 172.16.2.254

Subnet 3: 172.16.3.0/16 (subnet mask: 255.255.0.0)

Host range: 172.16.3.1 to 172.16.3.254

Subnet 4: 172.16.4.0/16 (subnet mask: 255.255.0.0)

Host range: 172.16.4.1 to 172.16.4.254

Class C

Suppose we have a Class C network with the IP address 192.168.1.0 and a natural mask of 255.255.255.0. We want to create four subnets.

Subnet 1: 192.168.1.0/24 (subnet mask: 255.255.255.0)

Host range: 192.168.1.1 to 192.168.1.254

Subnet 2: 192.168.2.0/24 (subnet mask: 255.255.255.0)

Host range: 192.168.2.1 to 192.168.2.254

Subnet 3: 192.168.3.0/24 (subnet mask: 255.255.255.0)

Host range: 192.168.3.1 to 192.168.3.254

Subnet 4: 192.168.4.0/24 (subnet mask: 255.255.255.0)

Host range: 192.168.4.1 to 192.168.4.254

In each example, we've created four subnets using the natural mask for the respective class of IP address.

Subnet mask:

A subnet mask is a 32-bit number that determines the scope of a subnet. It is used to:

Determine the network ID: The subnet mask helps identify the network ID portion of an IP address.

Determine the host ID: The subnet mask helps identify the host ID portion of an IP address.

Subnet Mask Notations

There are two notations for subnet masks:

- **Dotted Decimal Notation:** 255.255.255.0 (four numbers separated by dots)
- **CIDR Notation:** /24 (a slash followed by the number of bits in the subnet mask)

WEEK-2 IP Addressing

Subnetting Examples:

Suppose we have a network with the IP address 192.168.1.0 and a subnet mask of 255.255.255.0. We want to create four subnets with 16 hosts each.

Subnet 1: 192.168.1.0/28 (subnet mask: 255.255.255.240)

Host range: 192.168.1.1 to 192.168.1.14

Subnet 2: 192.168.1.16/28 (subnet mask: 255.255.255.240)

Host range: 192.168.1.17 to 192.168.1.30

Subnet 3: 192.168.1.32/28 (subnet mask: 255.255.255.240)

Host range: 192.168.1.33 to 192.168.1.46

Subnet 4: 192.168.1.48/28 (subnet mask: 255.255.255.240)

Host range: 192.168.1.49 to 192.168.1.62

In this example, we've created four subnets with 16 hosts each, using a subnet mask of 255.255.255.240.

CIDR range:

Let's explore CIDR (Classless Inter-Domain Routing) ranges.

CIDR Notation

CIDR notation is a way to represent an IP address and its associated subnet mask in a compact form. It consists of an IP address followed by a slash (/) and a decimal value, known as the CIDR prefix.

Example:

IP address: 192.168.1.0

Subnet mask: 255.255.255.0

CIDR notation: 192.168.1.0/24

In this example, the CIDR prefix is 24, which means the subnet mask has 24 bits set to 1 (255.255.255.0).

WEEK-2 IP Addressing

CIDR Ranges:

Here are some common CIDR ranges:

/32: A single IP address (no subnetting)

Example: 192.168.1.1/32

/31: 2 IP addresses (1 subnet)

Example: 192.168.1.0/31

/30: 4 IP addresses (2 subnets)

Example: 192.168.1.0/30

/29: 8 IP addresses (4 subnets)

Example: 192.168.1.0/29

/28: 16 IP addresses (8 subnets)

Example: 192.168.1.0/28

/27: 32 IP addresses (16 subnets)

Example: 192.168.1.0/27

/26: 64 IP addresses (32 subnets)

Example: 192.168.1.0/26

/25: 128 IP addresses (64 subnets)

Example: 192.168.1.0/25

/24: 256 IP addresses (128 subnets)

Example: 192.168.1.0/24

/23: 512 IP addresses (256 subnets)

Example: 192.168.1.0/23

/22: 1024 IP addresses (512 subnets)

Example: 192.168.1.0/22

/21: 2048 IP addresses (1024 subnets)

Example: 192.168.1.0/21

/20: 4096 IP addresses (2048 subnets)

Example: 192.168.1.0/20

/19: 8192 IP addresses (4096 subnets)

Example: 192.168.1.0/19

WEEK-2 IP Addressing

/18: 16384 IP addresses (8192 subnets)

Example: 192.168.1.0/18

/17: 32768 IP addresses (16384 subnets)

Example: 192.168.1.0/17

/16: 65536 IP addresses (32768 subnets)

Example: 192.168.0.0/16

/15: 131072 IP addresses (65536 subnets)

Example: 192.168.0.0/15

/14: 262144 IP addresses (131072 subnets)

Example: 192.168.0.0/14

/13: 524288 IP addresses (262144 subnets)

Example: 192.168.0.0/13

/12: 1048576 IP addresses (524288 subnets)

Example: 192.168.0.0/12

/11: 2097152 IP addresses (1048576 subnets)

Example: 192.168.0.0/11

/10: 4194304 IP addresses (2097152 subnets)

Example: 192.168.0.0/10

/9: 8388608 IP addresses (4194304 subnets)

Example: 192.168.0.0/9

/8: 16777216 IP addresses (8388608 subnets)

Example: 192.168.0.0/8

/7: 33554432 IP addresses (16777216 subnets)

Example: 192.168.0.0/7

/6: 67108864 IP addresses (33554432 subnets)

Example: 192.168.0.0/6

/5: 134217728 IP addresses (67108864 subnets)

Example: 192.168.0.0/5

/4: 268435456 IP addresses (134217728 subnets)

Example: 192.168.0.0/4

/3: 536870912 IP addresses (268435456 subnets)

Example: 192.168.0.0/3

/2: 1073741824 IP addresses (536870912 subnets)

Example: 192.168.0.0/2

/1: 2147483648 IP addresses (1073741824 subnets)

Example: 192.168.0.0/1

/0: 4294967296 IP addresses (2147483648 subnets)

Example: 192.168.0.0/0

Count usable and total hosts in an IP address range:

To count the usable and total hosts in an IP address range, you can use the following steps:

Step 1: Determine the subnet mask

The subnet mask is used to determine the number of hosts in a subnet. You can represent the subnet mask in dotted decimal notation (e.g., 255.255.255.0) or in CIDR notation (e.g., /24).

Step 2: Calculate the number of bits in the subnet mask

Count the number of bits in the subnet mask. In CIDR notation, this is represented by the number after the slash (e.g., /24 means 24 bits). In dotted decimal notation, you can count the number of bits by converting each octet to binary and counting the number of 1s.

Step 3: Calculate the total number of hosts

The total number of hosts is calculated using the formula:

2^(32 - number of bits in subnet mask)

For example, if the subnet mask is 255.255.255.0 (/24), the number of bits is 24. Therefore, the total number of hosts is:

2^(32 - 24) = 2^8 = 256

Step 4: Calculate the number of usable hosts

The number of usable hosts is the total number of hosts minus 2, which are reserved for the network address and broadcast address.

Usable hosts = Total hosts - 2

Using the previous example, the number of usable hosts is: 256 - 2 = 254

WEEK-2 IP Addressing

Basics of MAC Addressing Functionality of ARP & RARP:

ARP:

ARP (Address Resolution Protocol) is a communication protocol used to map an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control (MAC) address. ARP is a crucial protocol in the TCP/IP suite that enables devices on a local area network (LAN) to communicate with each other.

Working of ARP:

Here's a step-by-step explanation of the ARP process:

ARP Request: When a device on a LAN wants to send a packet to another device, it first checks its ARP cache to see if it already has a mapping for the destination IP address. If it doesn't, it sends an ARP request packet to the destination IP address.

ARP Request Packet: The ARP request packet contains the sender's IP address, sender's MAC address, and the target IP address.

ARP Broadcast: The ARP request packet is broadcast to all devices on the LAN.

ARP Response: The device with the target IP address responds with an ARP response packet, which contains its MAC address.

ARP Response Packet: The ARP response packet is sent directly to the sender's MAC address.

ARP Cache Update: The sender updates its ARP cache with the target IP address and corresponding MAC address.

Packet Transmission: The sender can now transmit the original packet to the target device using the MAC address obtained through ARP.

ARP Cache:

The ARP cache is a table that stores the mapping of IP addresses to MAC addresses. The cache is updated dynamically as devices on the LAN respond to ARP requests. The ARP cache has a limited lifetime, and entries are removed after a certain period of inactivity.

WEEK-2 IP Addressing

ARP Message Format:

ARP messages consist of the following fields:

Hardware Type: Specifies the type of network interface (e.g., Ethernet).

Protocol Type: Specifies the protocol being used (e.g., IPv4).

Hardware Address Length: Specifies the length of the MAC address.

Protocol Address Length: Specifies the length of the IP address.

Operation: Specifies the type of ARP message (e.g., request or response).

Sender Hardware Address: The MAC address of the sender.

Sender Protocol Address: The IP address of the sender.

Target Hardware Address: The MAC address of the target device (if known).

Target Protocol Address: The IP address of the target device.

Benefits of ARP:

ARP provides several benefits, including:

Efficient use of bandwidth: ARP reduces the amount of bandwidth required for packet transmission by allowing devices to communicate using MAC addresses instead of IP addresses.

Improved network performance: ARP enables devices to quickly resolve IP addresses to MAC addresses, reducing the time it takes to transmit packets.

Simplified network configuration: ARP eliminates the need for manual configuration of MAC addresses, making it easier to set up and manage networks.

WEEK-2 IP Addressing

What is RARP:

RARP (Reverse Address Resolution Protocol) is a communication protocol used to obtain an IP address from a MAC address. It is the reverse of ARP (Address Resolution Protocol), which maps an IP address to a MAC address. RARP is used by devices on a local area network (LAN) to request their IP address from a RARP server.

Working of RARP:

Here's a step-by-step explanation of the RARP process:

RARP Request: A device on a LAN, typically a diskless workstation or a device without a configured IP address, sends a RARP request packet to the RARP server.

RARP Request Packet: The RARP request packet contains the device's MAC address and a request for its IP address.

RARP Server: The RARP server receives the request and checks its database for a matching MAC address.

RARP Response: If a match is found, the RARP server sends a RARP response packet to the device, which contains the device's IP address.

RARP Response Packet: The RARP response packet is sent directly to the device's MAC address.

IP Address Configuration: The device configures its IP address based on the response from the RARP server.

RARP Message Format:

RARP messages consist of the following fields:

Hardware Type: Specifies the type of network interface (e.g., Ethernet).

Protocol Type: Specifies the protocol being used (e.g., IPv4).

Hardware Address Length: Specifies the length of the MAC address.

Protocol Address Length: Specifies the length of the IP address.

Operation: Specifies the type of RARP message (e.g., request or response).

Sender Hardware Address: The MAC address of the sender (device).

Sender Protocol Address: The IP address of the sender (RARP server).

Target Hardware Address: The MAC address of the target device (device).

Target Protocol Address: The IP address of the target device (device).

Benefits of RARP:

RARP provides several benefits, including:

Automatic IP address assignment: RARP enables devices to automatically obtain an IP address, eliminating the need for manual configuration.

Simplified network administration: RARP reduces the administrative burden of managing IP addresses, as devices can automatically obtain an IP address from the RARP server.

Improved network reliability: RARP ensures that devices on the network have a valid IP address, reducing the likelihood of network connectivity issues.

RARP Limitations:

Limited scalability: RARP is not suitable for large networks, as it can become difficult to manage and maintain the RARP server's database.

Security concerns: RARP can be vulnerable to security threats, as devices can potentially obtain an IP address without proper authentication.