4.1. Introduction

The fundamental role of the network layer, which corresponds to level 3 of the OSI model, is to ensure the management and determination of the paths that data packets must take within a network. This crucial function of path finding requires precise identification of all hosts connected to this network. To illustrate this concept, an analogy can be drawn to how a building's location is determined using its complete postal address, including the city, street, and number. Similarly, in the context of networks, each host is identified by a specific address that encompasses crucial information for its optimal routing within the network. It is at the network layer that these addresses are used to make decisions regarding the routes to be followed for data packets. The **TCP/IP protocol model**, widely used in the architecture of the Internet, implements specific addressing system known as IPv4 addressing. This IPv4 protocol enables the management of three distinct types of traffic, each with a specific purpose:

Unicast Traffic: Unicast traffic refers to point-to-point communication between a single source host and a single destination host. In this scenario, data is sent from a sender to a specific recipient, ensuring targeted and specific communication.

Multicast Traffic: Multicast traffic refers to a form of communication where a source host sends data to a specific group of hosts that have explicitly chosen to receive the content emitted by this source. This situation is comparable to broadcasting a television channel, where only TVs tuned to that channel display the broadcasted content.

Broadcast Traffic: Broadcast traffic refers to a type of communication where a host emits data to all other hosts belonging to the same broadcast domain. This type of traffic is typically limited to broadcast networks like Ethernet. For example, the Address Resolution Protocol (ARP) uses a broadcast to query all other hosts on the network to determine the MAC address corresponding to a given IP address.

4.2. IPv4 Protocol

4.2.1. What is IPv4?

IPv4, short for Internet Protocol version 4, is the initial and currently utilized version of the IP protocol. This protocol is defined in RFC 791.

4.2.2. RFC (Request for Comments)

- A series of technical and organizational documents related to the Internet.
- RFCs serve as standards.

✓ For a complete list, visit: http://www.rfc-editor.org (English)

✓ Partial translation available at: http://abcdrfc.free.fr/ (French)

RFCs serve as foundational documents for the development and standardization of technologies used in Internet communication. They offer guidelines, specifications, and protocols that contribute to the seamless functioning of the global network. IPv4 is the foundation of modern networking, but it has its limitations, including the finite number of available IP addresses. As a result, the transition to IPv6, with its larger address space, has been undertaken to address this issue and accommodate the growing demands of connected devices and users.

4.2.3. The Role of the IP Protocol

The IP protocol resides within the Internet layer of the TCP/IP protocol suite. It is among the most crucial protocols for the functioning of the Internet, as it facilitates the creation and transportation of IP datagrams (data packets), albeit without guaranteeing their "delivery." It operates independently of the physical networks traversed. In essence, the IP protocol handles IP datagrams individually, defining their representation, routing, and forwarding.

The IP protocol determines the recipient of a message using three fields:

- ✓ **The IP address field**: Machine's address.
- ✓ **The subnet mask field**: A subnet mask enables the IP protocol to identify the portion of the IP address related to the network.
- ✓ **The default gateway field**: Enables the Internet protocol to identify which machine to forward the datagram to if the destination machine is not on the local network.

4.2.4. TCP/IP Model

TCP/IP Model consists of only 4 layers: network layer, internet layer, transport, and application layer (see figure 4.1).

Network Layer: The network layer serves essential functions within the networking architecture. It replicates the roles performed by the physical, data link, and network layers in the OSI model. This layer is responsible for various critical tasks, including:

- ✓ ***Address Mapping:*** One of its key functions is the translation between IP addresses and the corresponding network physical addresses. This process ensures that data packets can be correctly directed across different networks, bridging the gap between logical addressing (IP addresses) and physical addressing (MAC addresses).
- ✓ ***Encapsulation:*** The network layer encapsulates IP datagrams, commonly referred to as packets, in a format that is intelligible and manageable for the underlying network infrastructure. This encapsulation process ensures that data is packaged in a way that networks can efficiently transmit and route it.

Internet Layer: At the core of the TCP/IP protocol suite, the internet layer plays a pivotal role in facilitating the end-to-end communication of data. It is founded on the Internet Protocol (IP), which provides the fundamental framework for transmitting data between two distinct points in a network:

- ✓ ***Data Transmission Backbone:*** The internet layer is a cornerstone of the TCP/IP architecture, forming the backbone for transmitting data from source A to destination B. It is the IP protocol that manages the routing, addressing, and forwarding of data packets across interconnected networks.

Transport Layer: The transport layer is a vital component of the TCP/IP stack, featuring two primary protocols - TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). These protocols offer distinct approaches to data transmission:

- ✓ ***TCP (Transmission Control Protocol)***: TCP is characterized by its reliable and connection-oriented nature. It establishes a virtual connection between sender and receiver, ensuring that data is transmitted accurately and in the correct order. It offers error-checking, acknowledgment mechanisms, and flow control, making it suitable for applications where data integrity is paramount.
- ✓ ***UDP (User Datagram Protocol)***: In contrast to TCP, UDP is connectionless and offers minimal error-checking mechanisms. It is favored in scenarios where low latency and speed are prioritized over error recovery. While it doesn't guarantee the same level of reliability as TCP, its simplicity makes it a preferred choice for applications such as real-time streaming and online gaming.

Application Layer: The application layer is the uppermost layer in the TCP/IP model, fulfilling roles equivalent to the OSI application, presentation, and session layers. It encompasses a diverse range of protocols that facilitate communication between software applications on different devices:

- ✓ ***Application Protocols:*** Protocols like HTTP, FTP, SMTP, and others operate within the application layer. These protocols dictate how data should be formatted, transmitted, and received between applications. HTTP, for example, governs the transfer of web content, while SMTP is responsible for email transmission.

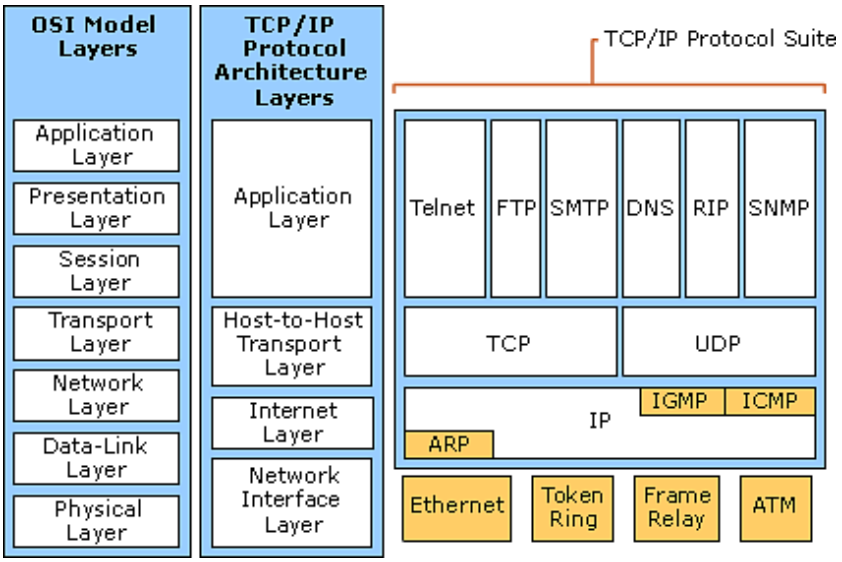

Figure 4.1: OSI vs. TCP/IP model

4.2.5. Addressing System

The IPv4 addressing system is based on encoding addresses into 32 bits, providing the capability to allocate a total of 4,294,967,296 unique addresses. These addresses are represented in the form of four numbers, each ranging from 0 to 255, combined as follows: 192.168.0.23 (for example).

Each IPv4 address is associated with a subnet mask that indicates the network to which the equipment assigned this address belongs. This mask determines which part of the IP address identifies the network, and it is typically noted in two different ways: either in modern notation, like "192.168.0.23/24," or in old notation, like "192.168.0.23/255.255.255.0." In the example "192.168.0.23/24," the "/24" also represents the C.I.D.R. (Classless Inter-Domain Routing) notation, specifying that the first 24 bits of the address constitute the network portion. In this specific case, the network's IP address would be "192.168.0.0."

The CIDR notation was introduced to simplify the management of IP addresses and routing tables. It enables a more efficient determination of network sizes and address distributions. RFC 1518 and 1519 define the specifications of this notation. It allows the expression of the number of bits used to define the network portion of the IP address.

Here are two examples of CIDR notation usage:

- "142.12.42.145/24" is equivalent to "142.12.42.145 255.255.255.0"
- "153.121.219.14/20" is equivalent to "153.121.219.14 255.255.240.0"

By using the CIDR notation, configuring routing tables becomes more concise and precise, greatly facilitating network management and the determination of data transmission routes.

4.2.6. IPv4 Frame

The IPv4 frame (Figure 4.2) header consists of 14 fields distributed as follows:

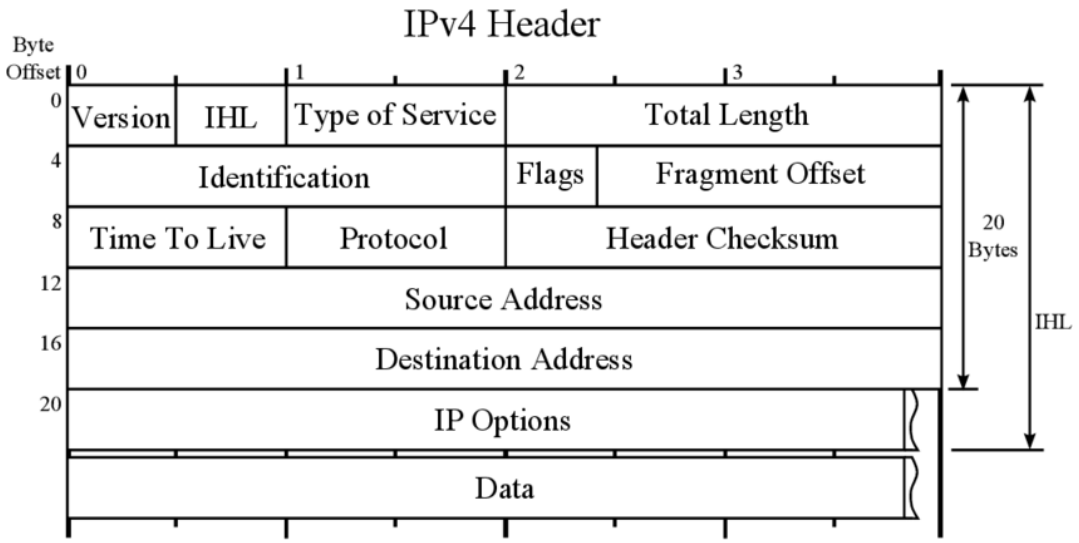

Figure 4.2: IPv4 Frame

Version (4 bits): Indicates the protocol version (here, version 4).

Header Length: Indicates the length of the datagram header.

Type of Service (8 bits): Informs routers how the datagram should be handled.

Total Length (16 bits): Specifies the total length of the datagram in bytes (header and data).

Identification (16 bits): An identifier used for reassembling the datagram.

Flags: Various control flags.

Fragment Offset: Specifies the position of the packet if it is a fragment of the datagram.

Time to Live (8 bits): Indicates the number of routers the datagram can traverse.

Protocol (8 bits): Identifies the upper-layer protocol (TCP, ICMP, etc.) used to transmit the message.

Header Checksum (16 bits): Detects transmission errors in the header.

Source IP Address (32 bits): Provides the sender's IP address.

Destination IP Address (32 bits): Provides the recipient's IP address.

Possible IP Options (less than or equal to 32 bits): Options related to tuning functionalities.

Padding: The option field doesn't have a fixed size. Padding allows this field to be a multiple of 32 bits (4 bytes).

4.3. Address Classes

The IPv4 protocol defines five address classes known simply as class A, B, C, D, or E addresses (Figure 4.3). These classes determine the number of computers and networks that can be established on a site for connection to the Internet with public addresses assigned by the Internet Service Provider (ISP). When used in a local network not connected to the Internet, it is not mandatory to adhere to this standard unless it's a matter of convention.

Class A Addresses: Class A addresses are recognizable by their binary representation, where the first bit is set to zero. These addresses range from 1.0.0.0 to 126.0.0.0, with a default subnet mask of 255.0.0.0. Class A addresses are allocated for networks with over 65,536 computers. They allocate 7 bits for network identification and 24 bits for individual machine identification.

Class B Addresses: Class B addresses start with the binary pattern '10' as their two first bits. They allocate addresses between 128.1.0.0 and 191.255.0.0, with a default subnet mask of 255.255.0.0. Class B addresses are used in intermediate networks containing between 256 (28) and 65,535 computers. They allocate 14 bits for network identification and 16 bits for each computer.

Class C Addresses: Class C addresses begin with '110' in their first three bits. These addresses allow allocation between 192.0.1.0 and 223.255.255.0, with a default subnet mask of 255.255.255.0. Class C addresses are used for small networks with fewer than 256 machines. They allocate 21 bits for network identification and 8 bits for individual computer identification.

Class D Addresses: Class D addresses have their first four bits set as '1110' and range from 224.0.0.0 to 239.255.255.255. These are multicast addresses.

Class E Addresses: Class E addresses have their first five bits set as '11110' and are reserved for future use. They range from 240.0.0.0 to 255.255.255.255.

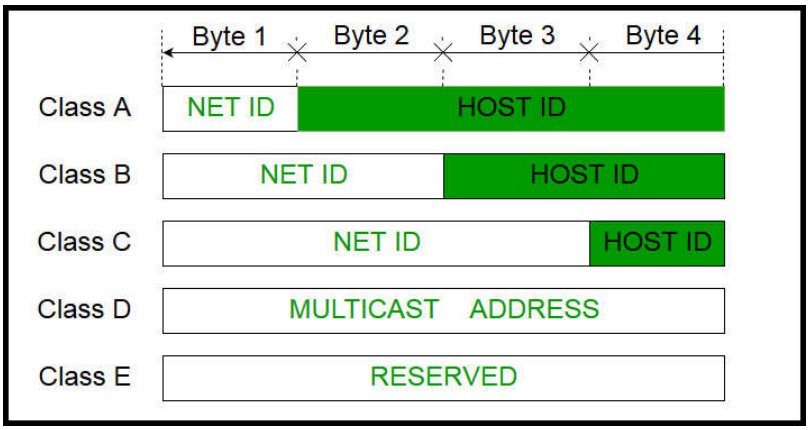

Figure 4.3: Address Classes

Each of these classes reserves private addresses for private networks that need to be connected to a public network. For Class A, private addresses start with 10.x.x.x, for Class B: 172.16.x.x to 172.31.x.x, and for Class C: 192.168.x.x. In principle, no device is allowed to communicate on a public network with a private address. These ranges are defined in RFC 1918.

Reserved Address Ranges for Local Networks:

- ***10.0.0.1 to 10.255.255.254,***
- ***172.16.0.1 to 172.31.255.254,***
- ***192.168.0.1 to 192.168.255.254,***

Reserved Test Address: ***127.0.0.1***

4.4. Subnet Masks

A default subnet mask is used for undivided TCP/IP networks, including single-segment networks. All hosts require a subnet mask, even on single-segment networks. The default subnet mask used depends on the address class.

In the subnet mask, all bits corresponding to the network ID are set to 1. The decimal value in each octet is 255. All bits corresponding to the host ID are set to 0.

Subnetting:*Why?*

- Heterogeneous use of physical layer means
- Reduction of congestion
- Saves calculation time
- Network isolation
- Enhanced security
- Optimization of reserved IP space

The mask allows segmenting a network into multiple subnets.

Example of a mask:

255.255.255.224 => 11111111.11111111.11111111.11100000

Determining a Machine's Subnet:

200.100.40.33 => 11001000.01100100.00101000.00100001

Perform a logical AND operation with the subnet masks:

200.100.40.32 => 11001000.01100100.00101000.00100000

Number of Subnets: 2 RFCs apply:

RFC 1860: $2^n - 2$, where n is the number of bits set to 1

RFC 1878: 2^n→Subnet Addresses

Number of Hosts per Subnet:

$2^m - 2$, where m is the number of bits in the host portion

4.5. Special Addresses

Several special addresses are defined by IPv4 for specific uses.

a - Loopback Address:

The loopback address corresponds to a virtual network interface found on nearly all devices. It's used for communication between processes. These processes can be games or Unix printing systems (Cups), for instance. In practice, the address of this interface is always 127.0.0.1/8. A packet sent on this interface should never appear on a network.

b - Broadcast Addresses:

Broadcast addresses correspond to the highest address on a network. For example, for the network 192.168.0.0/24, the broadcast address will be 192.168.0.255.

Broadcast Address:

Set all bits in the host part to 1

The broadcast address 255.255.255.255 is mainly used by devices that don't have an IP address on the network (for example, during auto-configuration via DHCP). Devices using this broadcast address usually announce the IP address 0.0.0.0 (no IP address).

4.6. IP Address Distribution

- **IANA** (Internet Assigned Numbers/Naming Authority):Distributes IP addresses to ISPs (Internet Service Providers).
- **InterNIC** (Internet Network Information Center):Allocates portions of the network identifier for devices directly connected to the Internet.

4.7. Associated Protocols

4.7.1. Physical Address Resolution

Physical address resolution is a crucial mechanism in computer networks that establishes a correspondence between logical addresses, such as IPv4 addresses, and physical addresses, such as MAC addresses in the context of Ethernet networks. To better understand the complexity of physical address resolution, let's take the example of Ethernet technology, widely used in local networks.

In Ethernet networks, physical addresses, also known as MAC addresses, consist of 48 bits, which is different from the length of IPv4 addresses that are encoded in 32 bits. Due to this disparity, it's not directly possible to establish a one-to-one mapping between these two types of addresses. To tackle this challenge, the Address Resolution Protocol (ARP) was designed. The ARP protocol provides an efficient and simple mechanism for this resolution.

When a computer A wants to obtain the physical address of a computer B, it sends a special frame called an ARP request over the network, asking computer B to respond with its MAC address corresponding to its IP address. All computers on the network receive this request, but only computer B recognizes its IP address in the request and responds with its MAC address. Computer A then records this mapping in an ARP table, allowing it to subsequently transmit IP datagrams to computer B using its MAC address.

It's important to note that this technology involves a second Layer 3 protocol, in addition to the IP protocol. This can increase the number of broadcast frames circulating on the network, potentially leading to network congestion.

4.7.2. ICMP Protocol

The Internet Control Message Protocol (ICMP), defined in RFC 792, plays a critical role in communications between devices within networks. ICMP messages are used for both error management and the exchange of fundamental information. These ICMP packets are exchanged in various contexts, including:

- When using the ping command, which verifies connectivity to a remote host by sending ICMP request packets and receiving responses.
- When a packet reaches the end of its lifespan and is removed from the network.
- ...

The structure of ICMP packets is relatively straightforward: they include a "type" field indicating the type of ICMP message, a "code" field providing specific details, a cyclic redundancy check (CRC) for error detection, a series of fields whose content varies based on the message type, and a section of the IP packet that led to the emission of the ICMP message.

4.7.3. IGMP Protocol

The Internet Group Management Protocol (IGMP), described in RFC 1112, plays a central role in managing multicast groups within the IPv4 protocol.

A multicast group consists of a set of devices listening on the same IP address. This technology has applications in continuous streaming, such as internet radio streams or television services via ADSL.

4.8. IP addressing with IP version 6.0

The available network IDs in IPv4 are becoming increasingly scarce. Therefore, a new version has been developed: IPv6.

The main benefits of IPv6 include the following:

■ **Larger address space**: IPv6 addresses are 128 bits, compared to IPv4's 32 bits. This larger addressing space allows more support for addressing hierarchy levels, a much greater number of addressable nodes, and simpler auto configuration of addresses.

■ **Globally unique IP addresses**: Every node can have a unique global IPv6 address, which eliminates the need for NAT.

■ **Header format efficiency**: A simplified header with a fixed header size makes processing more efficient.

■ **Improved privacy and security**: IPsec is the IETF standard for IP network security, available for both IPv4 and IPv6. Although the functions are essentially identical in both environments, IPsec is mandatory in IPv6. IPv6 also has optional security headers.

■ **Flow labeling capability**: A new capability enables the labeling of packets belonging to particular traffic flows for which the sender requests special handling, such as non default quality of service (QoS) or real-time service.

■ **Increased mobility and multicast capabilities**: Mobile IPv6 allows an IPv6 node to change its location on an IPv6 network and still maintain its existing connections. With Mobile IPv6, the mobile node is always reachable through one permanent address. A

connection is established with a specific permanent address assigned to the mobile node, and the node remains connected no matter how many times it changes locations and addresses.

IPv6 Address Format

Rather than using dotted-decimal format, IPv6 addresses are written as hexadecimal numbers with colons between each set of four hexadecimal digits (which is 16 bits); we like to call this the "coloned hex" format. The format is x:x:x:x:x:x:x:x, where x is a 16-bit hexadecimal field. A sample address is as follows:

2035:0001:2BC5:0000:0000:087C:0000:000A

IPv6 addresses are represented in 128 bits, divided into eight 16-bit fields separated by colons (:).

Each of these fields is represented in hexadecimal format (see example below).

xxxx : xxxx : xxxx : xxxx : xxxx : xxxx : xxxx : xxxx
||
0010000000000001 : 0000110110111000 : 1010110000010000 : …
||
2001 : 0DB8 : AC10 : FE01 : 0000 : 0000 : 0000 : 0000

However, a simplified representation of an IPv6 address also exists. In this representation, a maximum of three consecutive zeros at the beginning of a field can be omitted.

The network in the example below is an illustration of this representation:

2201 :0db8 :0000 :0004 :0240 :48ff :feb1 :2d65
||
2201 :0db8 : 0 : 4 :0240 :48ff :feb1 :2d65
Also, a sequence of at least two consecutive fields of the form "0000 :0000" can be represented by a single "::."

3FFE:FFFF:0:0:8:800:20C4:0
||
3FFE:FFFF::8:800:20C4:0

It is also worth noting that, in addition to the two representations already introduced, other works go even further by listing other representation formats such as hybrid and mixed representation between IPv4 and IPv6.

Now, as with IPv4 addresses, in order to ensure the two location and identification features, an IPv6 address is divided into two parts: a network part and a host part. To do this, we generally encounter the following syntax:

xxxx:xxxx : xxxx : xxxx : xxxx : xxxx : xxxx : xxxx / YY

Where YY is the number of bits used to represent the network part. However, it is important to know that, unlike IPv4, in IPv6 we speak of "prefix" and not of "network part".

Address Categories: Routable, Non-routable and Reserved

As is the case with IPv4 addressing, the IPv6 address range has also been divided into several categories. These in turn also reflect the set of characteristics seen in IPv4, such as routable, non-routable, reserved and multicast addresses. A distinction between these networks can be made based on their prefixes. Table 4 summarizes how such a distinction can be made:

Address Categories

Prefix	Characteristic
2000::/3	Global unicast addresses (routable)
fe80::/10	Link-local addresses (non-routable)
fc00::/7	Unique local addresses (non-routable)
ff00::/8	Multicast addresses
::/8	Reserved addresses

- **Unicast global addresses**: these are addresses that can be used on the Internet.
- **Link-local addresses**: these are those used by a machine to communicate with other hosts to which it is directly connected.
- **Unique local addresses**: are assigned within the same site, but are not accessible from a public network.
- **Multicast addresses**: allow communication with a group of hosts.