Internet technology from networks to streaming servers

Chapter 3: TCP/IP, DNS, NAT & IPv6

Prepared by
Alaa Mohamed

The contents of this presentation have been prepared from the study book of the course, Internet Technology from networks to streaming servers.

Why should I read this chapter?

- Learn about Addressing Process and types of addressing:
  - Physical or hardware address
  - Logical or Internet Protocol (IP) address.
- Internet Protocol Addressing Schemes:
  - Class A, Class B, Class C, Class D and Class E.
- Know the Network Architecture:
  - OSI Model
  - TCP/IP Model
- Learn about TCP/IP Layers and their functions:
  - Application Layer
  - Transport Layer
  - Internet Layer
  - Network Interface Layer

Why should I read this chapter?

- Understand DHCP process and types of IP address:
    - Static IP
    - Dynamic IP
- Learn about Domain Name System.
- Learn about IPv6 address types:
    - Unicast
    - Multicast
    - Anycast

Learning Objectives

After you have read this chapter, you should be able to:

1. Identify Internet Addressing process.
2. Discuss Internet Protocol Addressing Schemes.
3. Identify the Network Architecture.
4. Discuss TCP/IP Layers and their functions.
5. Describe DHCP process.
6. Describe Domain Name System.
7. Describe NAT Process.
8. Discuss IPv6 and IPv6 Addressing.

History

- TCP and IP delivered the basic **services** that everyone needs (as file transfer) across a very large number of client and server systems.
- Several computers in a small department can use TCP/IP (along with other protocols) **on a single LAN.**
- In 1974, Vincent Cerf and Robert Kahn developed the Transmission Control Protocol (TCP) which was further split into the Internet Protocol (IP) and TCP in 1978.
- Because the significance of TCP/IP in the history of the Internet, Cerf and Kahn are considered to be **the Father of the Internet**.
- In 1982, DoD adopted TCP/IP as the standard protocol in the Internet [14].

Internet Addressing Addresses

- **Addresses**

  provide information on how to locate something, e.g., what route to take from here to there.

- **Addressing**

  1. **Physical or hardware address**
  2. **Logical or Internet Protocol (IP) address.**

1. Physical or hardware address

- Physical address is the address which comprises of **48-bit** that is **imprinted at the time of manufacturing Network Interface Card (NIC)** to uniquely identifies the computer on the network.
- The hardware address is also known as the Media Access Control (MAC) address.
- Ex: 00 20 73 06 D3 6A , 00 8C 00 03 A4 7D
- This **MAC** address is used by computers to **identify** each other on (LAN).
- **MAC** addresses are inefficient and **cannot be used on WAN** but address system has to be employed the logical or Internet Protocol (IP) address.

2. Logical or Internet Protocol (IP)

- IP addresses is a **specific and unique** number assigned to **each host** in the Internet for identification .
- They enable communication between computers irrespective of the type of network technology used to connect the computers in which every IP address comprises of 4 bytes.
- The way in which the IP address is represented is called dotted-quad. The range of each number is between 0 and 255.

Ex: 0.0.0.0 , 255.255.255.255

Logical or Internet Protocol (IP)

- The network administrator assigns the IP addresses to a computer when installing the operating system.
- An address of a computer on a network identified by two components:

  1- **network ID** (8 bit) (which the computer is connected)

  2- **host ID** (24 bit) (the number assigned to the computer on the network)

Type	Example
Dotted Quad	129.100.23.247
Binary	10000001 01100100 00010111 11110111 (32 bits= 4 bytes)
Hexadecimal	81 64 17 F7
Decimal	2.170.820.599

IP Addressing Schemes

IP addresses are generally divided into five types of address classes to enable easy administration of a network:

- Class A
- Class B
- Class C
- Class D
- Class E

This classification is based on the number of bits fixed for the network ID and the host ID on the network.

IP Addressing Schemes

Class A

- **8 bits** are used for identifying the **network ID** and
- **24** bits for the **host ID**.
- the first bit is set to **0** and only seven bits can be used
- for the network ID
- A maximum of 2^7 class A networks can he set up.
- contains networks 1.0,0.0 to 127.255.255.255
- A total of 16,777,214 hosts call ins connected to each network.

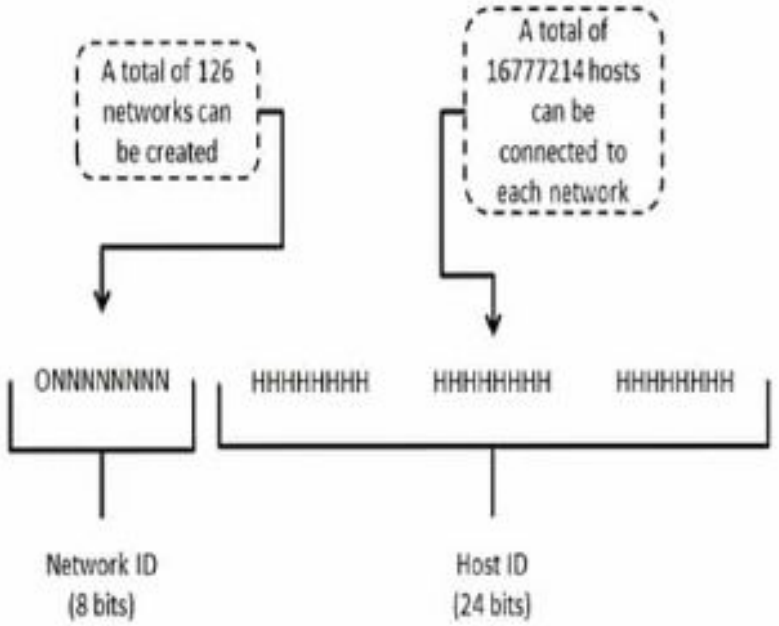


Figure 3.3: In class A addresses, the first byte is used for the network ID.

IP Addressing Schemes

Class B

- **16 bits** are used for identifying the **network ID** and **16 bits** for the **host ID**.
- the first two bits in the network ID are set to **1 and 0, 0** respectively.
- contains network 128.0.0.0 to 191.255.255.255.
- A maximum of 2^{14} class B networks can be set up and
- $2^{16} - 2$ hosts can be connected to each network.

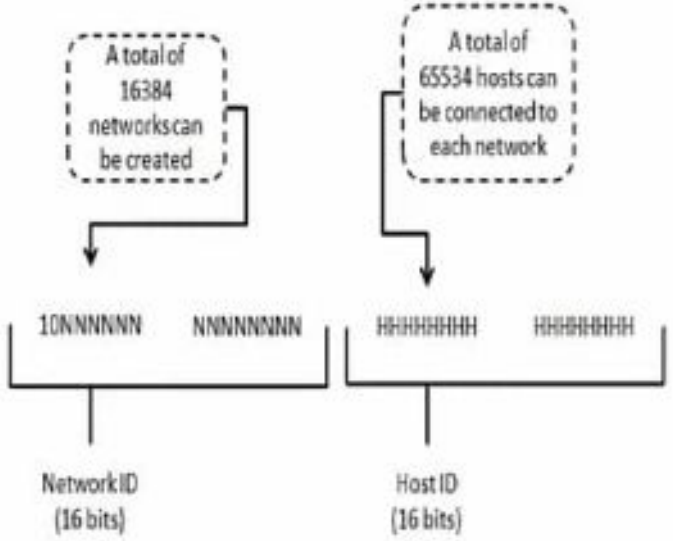


Figure 3.4: In class B addresses, the first two bytes are used for the network ID.

IP Addressing Schemes

Class C

- **24 bits** are used for identifying the **network ID** and **8 bits** for the **host ID.**
- The first three bits in the network ID are set to **1,1 and 0,** respectively.
- contains networks 192.0.0.0 to 223.255.255.255
- 2,097,152 networks can be created and each network can have a maximum of 254 hosts connected to it.

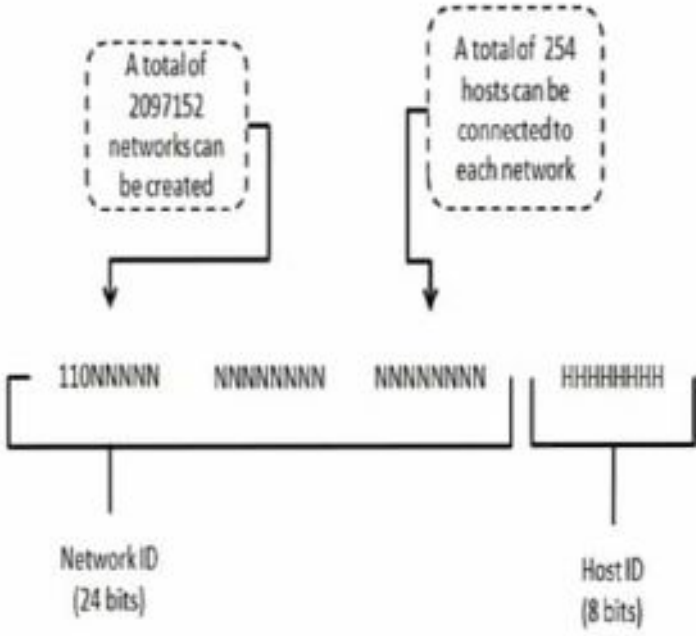


Figure 3.5: In class C addresses, the first three bytes are used for the network ID

IP Addressing Schemes

Class D

- The first four bits in the network ID are set to **1,1,1 and 0**, respectively.
- the network number can range between 224 and 239.
- Class D addresses are used **for multicasting** (multicasting refers to the process of sending messages to a group of computers on a network).

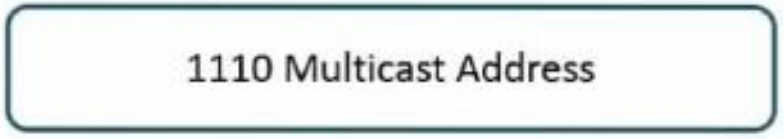


Figure 3.6: Class D addresses are reserved for multicast addresses.

Class E

- Class E addresses **are reserved for experimental purposes**.
- The network number in this scheme can range from 240 to 255.

Figure 3.7: Class E addresses are reserved for experimentation

Network Architecture

- Network architecture is the overall design of a network.
- The network design is divided into **layers**, each of which has a function separate from that of the other layers.
- The protocol stack is the **vertical** (top to bottom) arrangement of the layers each layer is governed by its own set of protocols.

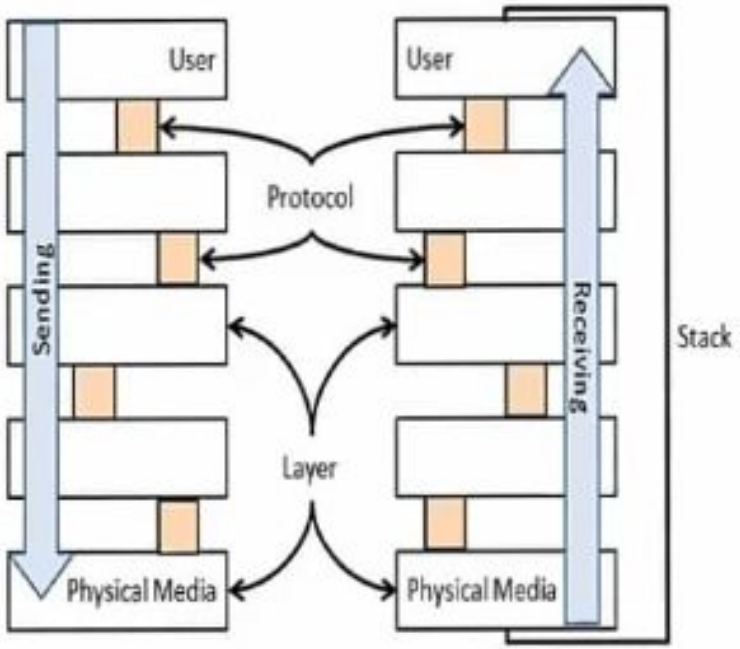


Figure 3.8: Network Architecture

The Open Systems Interconnection (OSI)

Layers in the OSI Model

- The layers in the OSI reference model are numbered from 1 to 7 starting with the Physical layer and ending with the Application layer.
- The Application layer is also referred to as Layer 7.

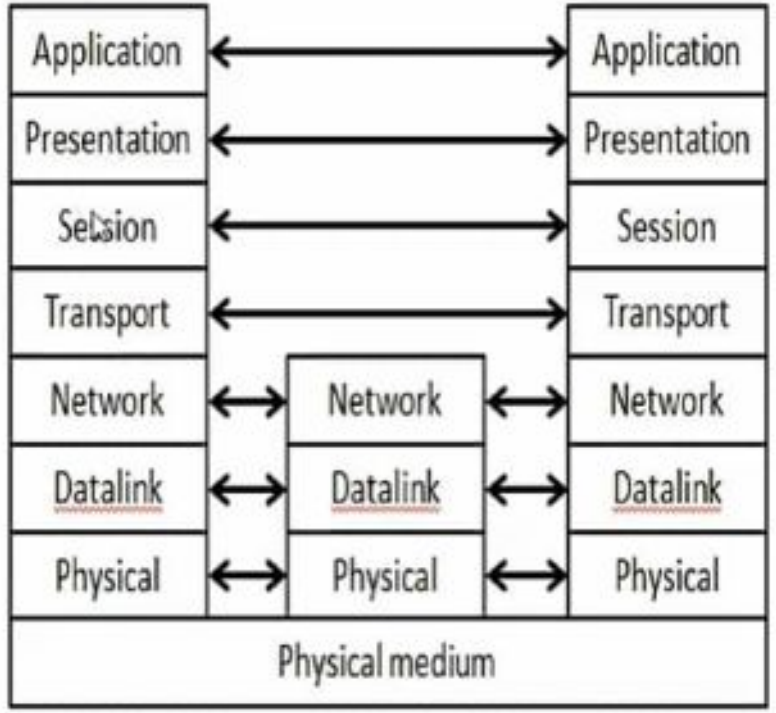


Figure 3.9: Layers in the OSI Model

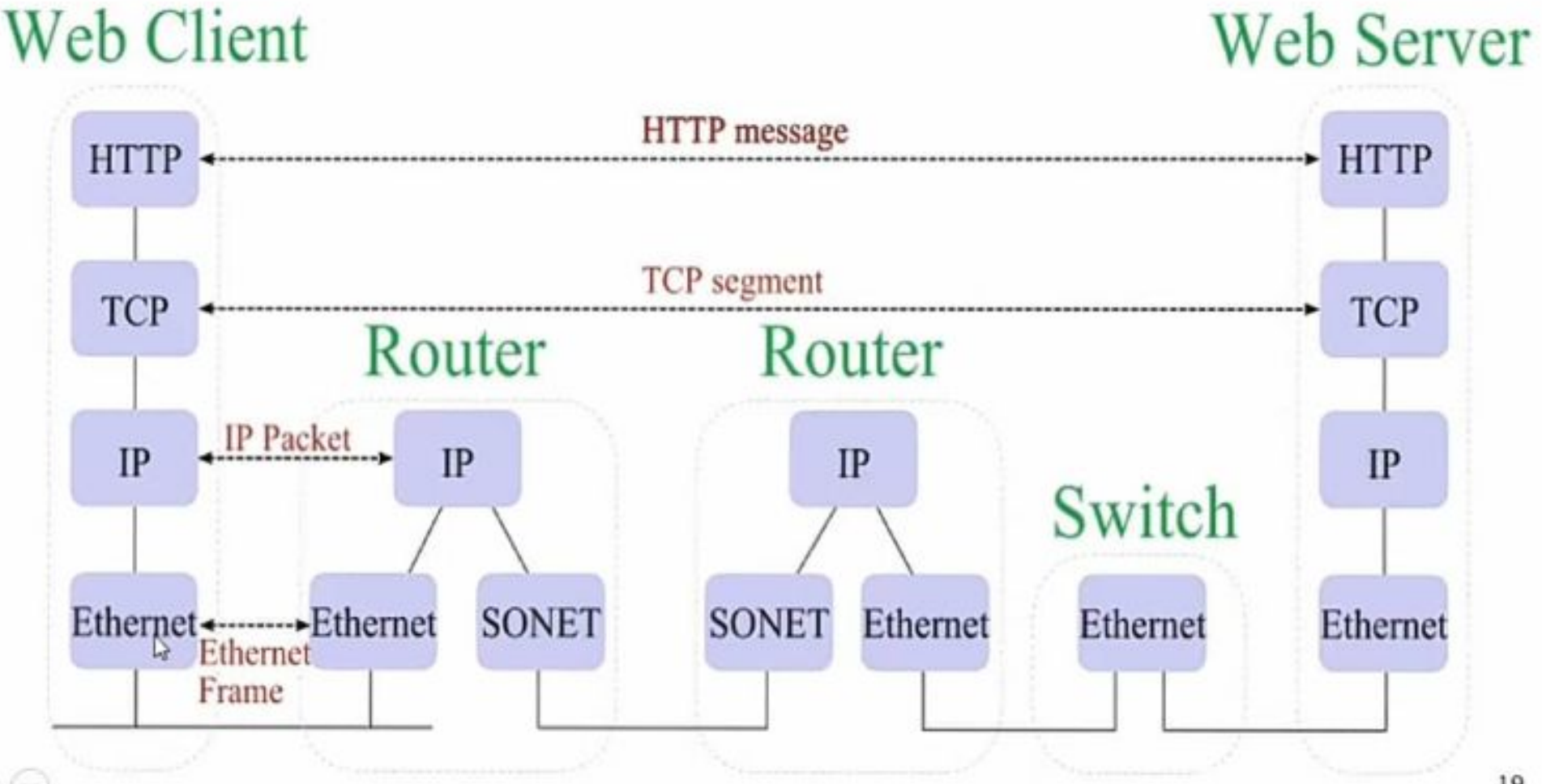
The Open Systems Interconnection (OSI)

- The functionality defined for **every layer** in the OSI reference mod implemented through **one or more protocols** that operate in a layer communicate only with the protocols in the same layer of the other computers.
- As the number of networks that were connected to the ARPAnet increased, communication among the computers became a problem.
- Common standards were required for communication.. This led to the creation of TCP and IP.

TCP/IP

- TCP
  - Controls disassembly of a message or a file into packets before transmission over Internet
  - Controls reassembly of packets into their original formats when they reach their destinations
- IP
  - Specifies addressing details for each packet

The Internet at each Hop



TCP/IP Reference Model

The TCP/IP reference model consists of **Four layers**:

1) Application
2) Transport
3) Internet
4) Network Interface

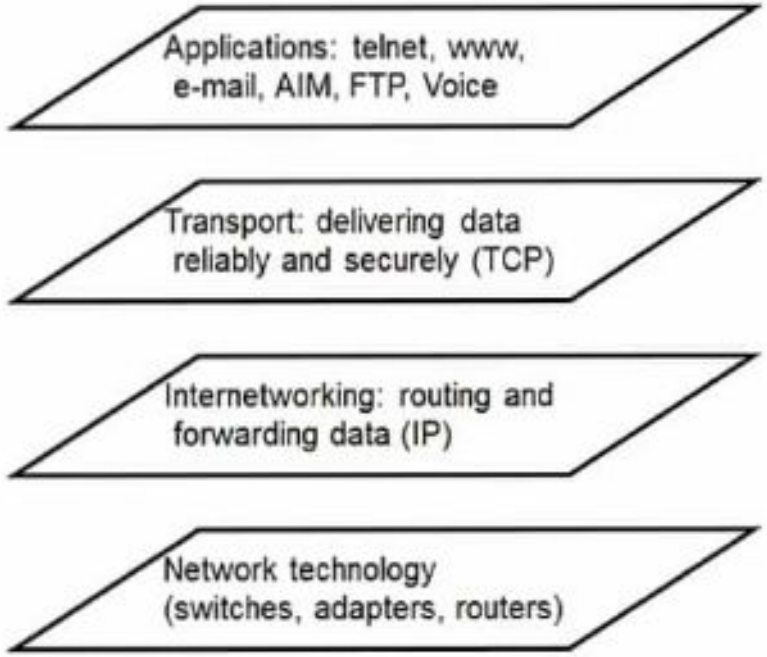
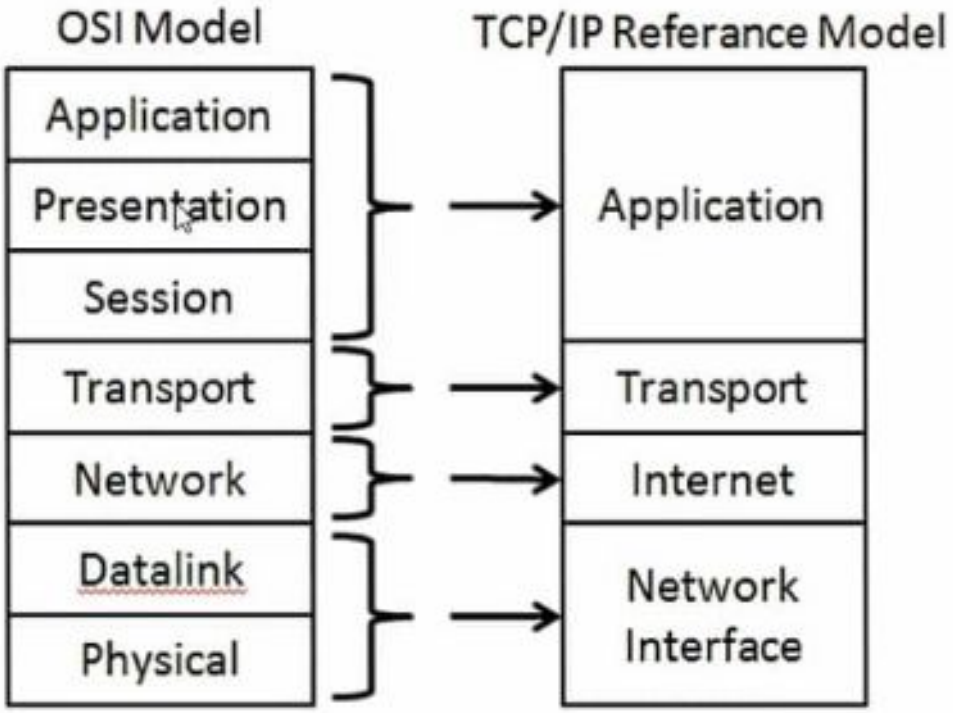


Figure 3.11: The TCP/IP reference model

OSI Model VS. TCP/IP Model



1. The Application Layer (layer process)

- **This layer responsible for**:
- Enabling users to access the network by providing a **few services** to the user.
- interacting with the operating system and the file system for data conversion and encryption.
- Some of other protocols and services available to the user are: File Transport Protocol (FTP) for transferring files, Telnet for remote login, and Simple Mail Transfer Protocol (SMTP) for exchanging mail messages

2. The Transport Layer (TCP layer)

- **Communication between computers** is handled by the Transport layer, which is comprised of Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).
- TCP is responsible for:
  - **dividing** the data into logical units called **packets** before transmitting them.
  - ensuring that data is transmitted properly to the destination.
  - retransmitting data to the destination If there is an error in data transmission.

3. The Internet Layer (IP layer)

This layer is responsible for:

- **routing** packets from **source-to- destination** across multiple networks.
- **determining** destination address if unknown

The ICMP (Internet Control Message Protocol) generates error messages if there are problems in data transmission.

4. The Network Interface Layer

This layer is responsible for:

- **dividing** the data sent by the Internet layer into logical groups **called frames**.
- accumulating all the constituent frames (The Network layer at the receiving end) and sends them to the other layers.
- ensuring that all the frames are received properly by a method called the **Cyclic Redundancy Check (CRC)**.
- exploiting the hardware address to transmit data over the physical medium.

Dynamic Host Configuration Protocol (DHCP)

Automatic Configuration

- Until 1980s, configuring a computer to connect to the Internet was a manual process.
- The protocol Bootstrap Protocol (ROOTP) was the first (TCP/IP) network configuration tool used to prevent the task of having to manually assign IP addresses by automating the process.
- The Dynamic Host Configuration Protocol (DHCP) was designed as an extension for ROOTP.

Dynamic Host Configuration Protocol (DHCP)

- The configuration of DHCP **automatically** provides the IP addresses to the network computers.
- eliminates the need of assigning the IP address individually to the client systems.
- provides range of the numbers from which DHCP allocate IP address.

Types of IP Address

There are two types of IP Address:

1. Static
2. Dynamic

1) Static IP

- Addresses are **manually assigned** to a computer by an administrator or ISP.
- These IP addresses are programmed on routers and other network equipment supplied by ISP.

Types of IP Address

2) Dynamic IP

- Addresses are assigned on LANs and broadband networks either **randomly, or arbitrarily by a server using (DHCP).**
- Even though IP addresses assigned using DHCP may stay the same for long periods of time, they can generally change.

In most current desktop operating systems, dynamic IP configuration **is enabled by default** so that a user does not need to manually enter any settings to connect to a network with a DHCP server.

Benefits:

- It avoids the administrative load of assigning specific static addresses to each user on a network.
- It also allows many users to share limited number of IP addresses available on ISP if only some of the users will be online at a particular time.

Domain Name System (DNS)

The Need for DNS

- IP addresses have a limitation that the users cannot be expected to remember the IP address to access a computer on the network.
- It's easier to use descriptive names to access a computer rather than using the IP address of the same.

Domain name

Is a **unique name** associated with a **specific IP** address by a program that runs on an Internet host computer.

Domain Name System (DNS)

- is a program, which coordinates the **IP addresses and domain names** for all computers attached to it.
- DNS enables users to type names of web sites and web pages as well as IP addresses.

  For example: www.yahoo.com instead of 112.23.345.56 .
- The last part of the domain name gives the type of organization that maintains the site for example: .com, .net, .edu, and .gov.

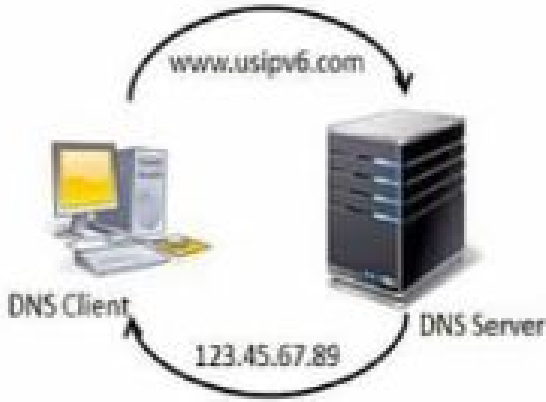


Figure 3.12: Domain Name System (DNS)

NAT & IPv6

Due to the rapid growth in popularity of the Internet, the fact that some of the methods used to allocate IP address ranges to organizations were very inefficient and the additional demands made by the strong graphical content and the growth of audio and video used by many web sites lead to that the address structure of the Internet needed to be changed.

- IPv6 (Internet Protocol version 6)
- NAT (Network address translation) help the address shortage help in solving.

Network address translation (NAT)

Network Address Translation (NAT)

- Is a method of connecting local-area network (LAN) to the Internet (or any other IP network) **using one IP address**.
- Traffic inside the network uses internal IP addresses (in the ranges 10.x.x.x, or 192.168.x.x) which do not have to be unique across the entire Internet, only on the local network.
- Traffic heading outside of the network has its IP address rewritten to one of the external IP addresses.

Network address translation (NAT)

Benefits of NAT

- solves the problems shortage of IPv4 address space.
- offers an encapsulation of an arbitrary number of local network computers and applications running on those computers.
- used to secure internal network IPs from external intrusive access.
- Ease and flexibility of network administration

Network address translation (NAT)

Internet security and NAT:

- the effective of NAT for Internet security is not particularly, they are not fundamentally intended for network security and are easily circumvented.
- NAT help with Internet security by hiding the internal IP addresses of the nodes on a network and by restricting bi-directional communications from outside the network.

NAT Techniques:

1. **Network masquerading:** a technique that hides a networks' address space behind a single IP address.
2. **Port forwarding:** a technique that allows external network traffic to pass through a specified Port to reach a specific node on the hidden internal network's address space.

DHCP Vs. NAT

NAT	DHCP
Allows multiple devices with different IPs on LAN to share a single IP on the WAN side and is used in a router which links two networks, commonly (SP (WAN) side to (LAN) side.	o is a protocol for dynamic allocation of IP addresses, Users can reserve IP addresses by MAC address to provide the situations where fixed IPs may be needed. o While commonly used with a router it would be usable in any LAN situation, and an ISP has dynamic IPs for customers (so they cannot so easily run web/mail servers).

Internet Protocol version 6 (IPv6)

- Although IPv4 has been the most successful data transmission protocol, one of the main limitations of IPv4 is the insufficient address space.
- Techniques such as **NAT** and **subnetting** that are used for conserving IP addresses are not permanent solutions to the address space problem.
- Certain limitations in IPv4 implementation have necessitated the development of a newer IP version called IPv6.

Internet Protocol version 6 (IPv6)

IP version 6 (IPv6)

is a new Internet Protocol , also called "IPng" (IP Next Generation),

which has:

- **extended IP addresses from 32 bits to 128 bits**, allowing for

  3.4×10^{38} addresses, This is in the order of 10^{29}

  times greater than IPv4

- Simplified IPv6 headers(reduction of header fields in IP packet).
- added security features.

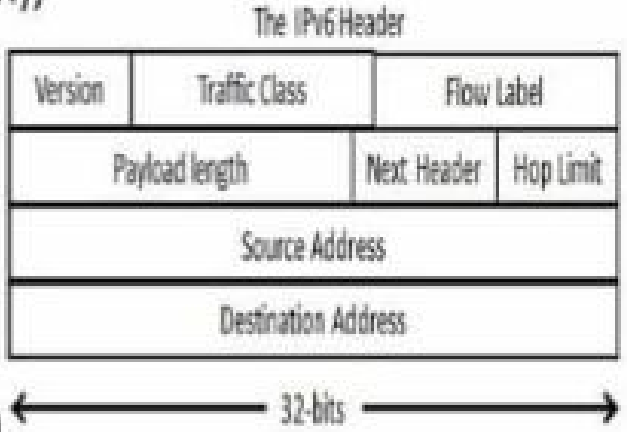


Figure 3.13: IPv6 Header

IPv6 Addressing

- The main advantages of IPv6 is the availability of a large address space that is comprised of 128-bits.
- Every host on a network that implements IPv6 is represented with an IP address of 16 bytes.

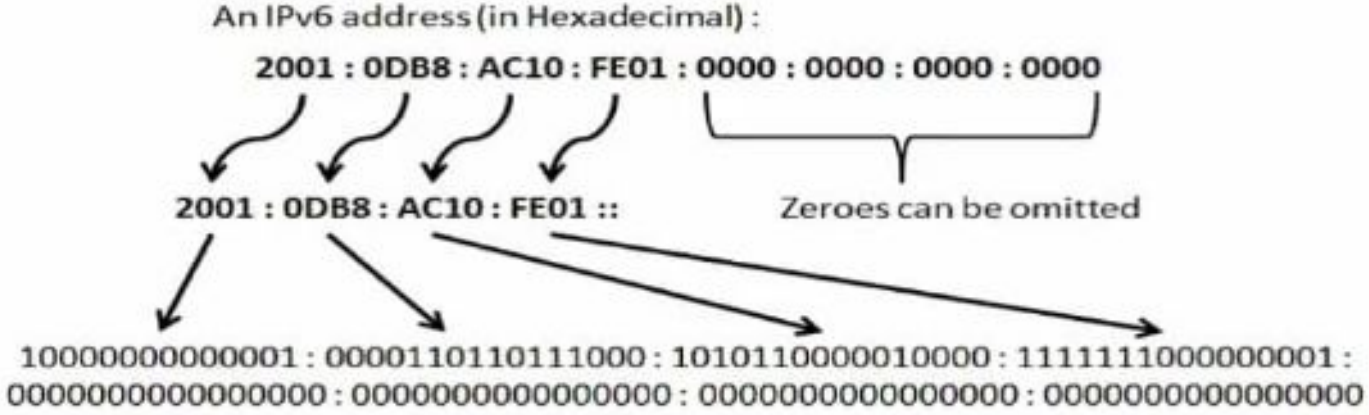


Figure 3.14 Decomposition of an IPv6 address from hexadecimal representation to its binary value.

IPv6 Addressing

- These addresses are represented in a notation called the hexadecimal colon notation.
- In this notation, the IP address is divided into eight groups of four bytes.
- The value in each group is provided in the hexadecimal notation.

An example of an IPv6 address is:

ABC3:56AC:7845:9078:6757:5645:6787:8900

- IPv6 also supports a notation called the **abbreviated notation** in which leading zeros in groups can be truncated and displayed in a concise form.

For example

1) if the IP address of a host is: ABC3:56AC:7845:0078:6757:5645:0087:ABC4

the leading zeros in the groups can be represented as: ABC3:56AC:7845:78:6757:5645:87:ABC4.

IPv6 Addressing

For Example:

2) if a group is comprised of zeros, the value of the group can be replaced with a colon.

For example, if the IP address of a host is:

- ABC3:0000:7845:0078:0000:5645:0000:ABC4

it can be abbreviated as:

- ABC3::7845:0078::5645::ABC4.

IPv6 supports three types of address:

1) unicast,
2) anycast
3) multicast IP

IPv6 Addressing

Unicast Address:

- is used to send messages to a single computer on a network.

Anycast Address:

- is used to represent a group of addresses that are represented as a single address.
- When a message is sent to an an address, the message is sent to any computer of the group.

Multicast Address:

- are used to represent a group of computers to which a message needs to be sent.
- Unlike an anycast message, a multicast message will be transmitted to all the computers in the multicast group.

Concept check

- What is Internet Addressing process and types of addresses ?
- Describe in details Internet Protocol Addressing Schemes
- Compare between OSI Model and TCP/IP Model
- Describe in details TCP/IP Layers and their functions.
- What is DHCP process ?
- What is Domain Name System ?
- Why NAT Process is developed ?
- What do you know about IPv6 ?