ST. LAWRENCE HIGH SCHOOL

A Jesuit Christian Minority Institution

STUDY MATERIAL - 7

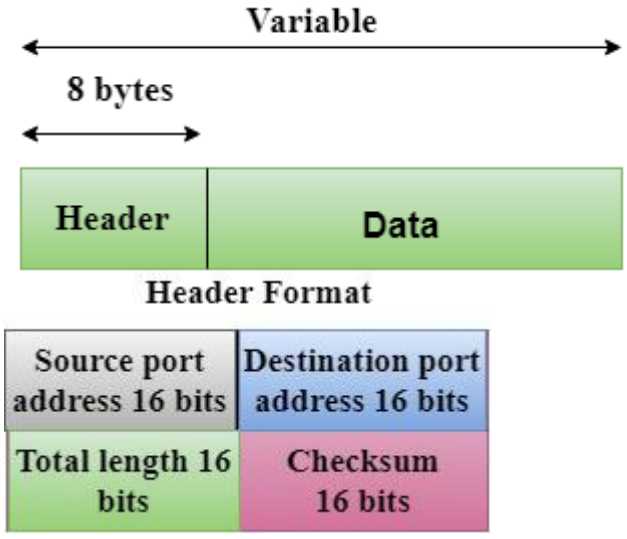
Subject: COMPUTER SCIENCE **Class - 12**

Chapter: Wide Area Network (Part -2) **Date: 12/06/2020**

Protocols used in TCP/IP model

UDP (User Datagram Packet) in Transport Layer

- It provides connectionless service and end-to-end delivery of transmission.
- It is an unreliable protocol as it discovers the errors but not specify the error.
- In UDP, the receiver does not generate an acknowledgement of packet received and in turn, the sender does not wait for any acknowledgement of packet sent. This shortcoming makes this protocol unreliable as well as easier on processing.
- UDP discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.
- **UDP consists of the following fields:**
    - **Source port address:** The source port address is the address of the application program that has created the message.
    - **Destination port address:** The destination port address is the address of the application program that receives the message.
    - **Total length:** It defines the total number of bytes of the user datagram in bytes.
    - **Checksum:** The checksum is a 16-bit field used in error detection.
- UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.



HTTP in Application Layer

HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.

HTTP works on client server model. When a user wants to access any HTTP page on the internet, the client machine at user end initiates a TCP connection to server on port 80. When the server accepts the client request, the client is authorized to access web pages.

To access the web pages, a client normally uses web browsers, who are responsible for initiating, maintaining, and closing TCP connections. HTTP is a stateless protocol, which means the Server maintains no information about earlier requests by clients.

TELNET in Application Layer

- TELNET (Terminal Network) is client-server application that allows a user to log onto remote machine and lets the user to access any application program on a remote computer.
- TELNET uses the NVT (Network Virtual Terminal) system to encode characters on the local system.
- On the server (remote) machine, NVT decodes the characters to a form acceptable to the remote machine.
- TELNET is a protocol that provides a general, bi-directional, eight-bit byte oriented communications facility.
- Many application protocols are built upon the TELNET protocol
- Telnet services are used on port no: 23.

FTP in Application Layer

- FTP stands for File Transfer Protocol. FTP is a standard network protocol used to transfer files between computers (a client and server) over a TCP/IP network.
- It is a function of Application layer and built on client-server architecture. Client controls the conversation, while server transmits the file content.
- Browser acts as a client and starts the conversation by making some request on the server. Through FTP, a client can remove, download, delete, or upload files on a server.
- When a client transfers a file to the server is called "Uploading" and server file transfer to client is called "Downloading".
- Thus, it is generally used to download files from a server over the internet and to upload files to a server using internet.

URL (Uniform Resource Locator)

URL stands for Uniform Resource Locator. It is the address of a resource, which can be a specific webpage or a file, on the internet. It is also *known as web address* when it is used with http. URL is a specific character string that is used to access data from the World Wide Web.

Every URL contains the following information:

- The scheme name or protocol.
- A colon, two slashes.
- A host normally called a domain name but sometimes as a literal IP address.
- A colon followed by a port number.
- Full path of the resource.

The URL of a web page is displayed above on the page in the address bar. A typical URL looks like this:

https://stlawrencehighschool.edu.in/teachingstaff

The above URL contains:

- **protocol**: https
- **host or domain**: stlawrencehighschool.edu.in
- **Path of the resource**: /teachingstaff

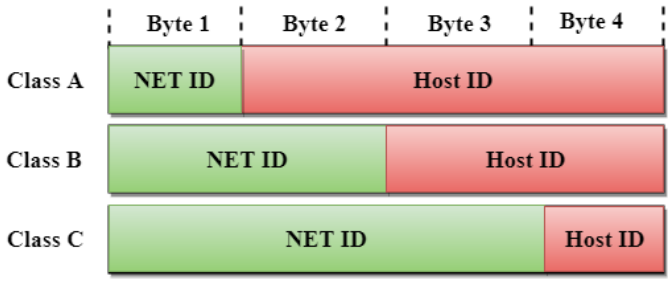
IP Addressing (Classful) Scheme

An IP address is 32-bit long. An IP address is divided into sub-classes:

- Class A
- Class B
- Class C
- Class D *(*Not in the syllabus)*
- Class E *(*Not in the syllabus)*

An ip address is divided into two parts:

- **Network ID:** It represents the number of networks.
- **Host ID:** It represents the number of hosts.



In the above diagram, we observe that each class have a specific range of IP addresses. The class of IP address is used to determine the number of bits used in a class and number of networks and hosts available in the class.

Class A

In Class A, an IP address is assigned to those networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network.

The total number of networks in Class A = 2^7 = 128 network address

The total number of hosts in Class A = 2^{24} - 2 = 16,777,214 host address

Class B

In Class B, an IP address is assigned to those networks that range from small-sized to large-sized networks.

- The Network ID is 16 bits long.
- The Host ID is 16 bits long.

In Class B, the higher order bits of the first octet are always set to 10, and the remaining14 bits determine the network ID. The other 16 bits determine the Host ID.

The total number of networks in Class B = 2^{14} = 16384 network address

The total number of hosts in Class B = 2^{16} - 2 = 65534 host address

Class C

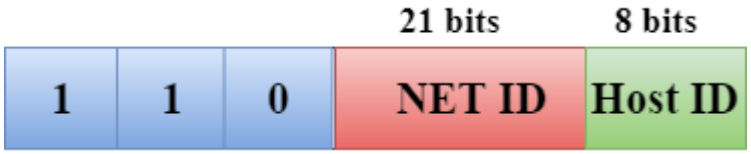
In Class C, an IP address is assigned to only small-sized networks.

- The Network ID is 24 bits long.
- The host ID is 8 bits long.

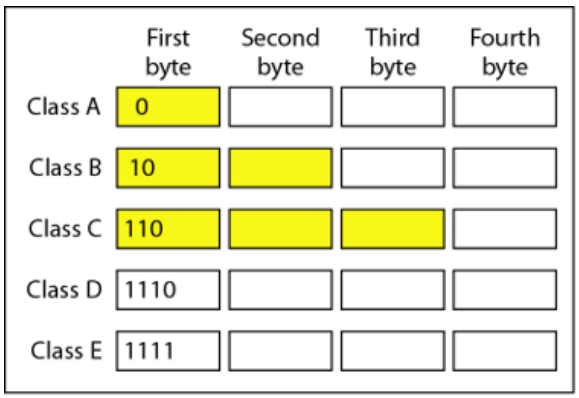
In Class C, the higher order bits of the first octet is always set to 110, and the remaining 21 bits determine the network ID. The 8 bits of the host ID determine the host in a network.

The total number of networks = 2^{21} = 2097152 network address

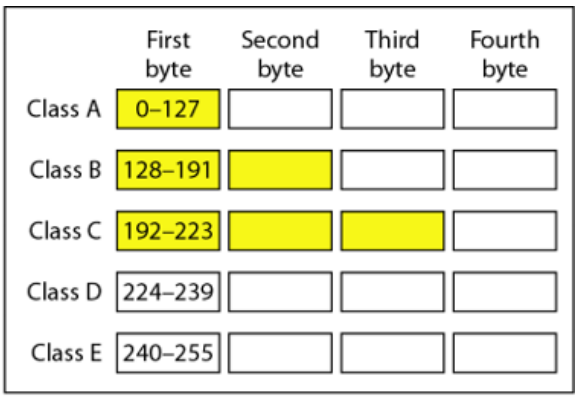
The total number of hosts = 2^{8} - 2 = 254 host address



To summarize the above points, observe the following figures carefully:



a. Binary notation



b. Dotted-decimal notation

Class	High Order Bits (First Octet)	Start Address	End Address
Class A	0xxxxxxx	0.0.0.0	127.255.255.255
Class B	10xxxxxx	128.0.0.0	191.255.255.255
Class C	110xxxxx	192.0.0.0	223.255.255.255
Class D	1110xxxx	224.0.0.0	239.255.255.2555
Class E	1111xxxx	240.0.0.0	255.255.255.255

DNS (Domain Name System) in Application Layer

An application layer protocol defines how the application processes running on different systems; pass the messages to each other.

- DNS stands for Domain Name System.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
- For example, suppose the google site has an IP address of 8.8.8.8, most people would reach this site by specifying www.google.co.in. Therefore, the domain name is more reliable than IP address.

Answer the following questions:

1. **Why is UDP unreliable?**
   Ans: In UDP, the receiver does not generate an acknowledgement of packet received and in turn, the sender does not wait for any acknowledgement of packet sent. This shortcoming makes this protocol unreliable as well as easier on processing. It is an unreliable protocol as it discovers the errors but not specify the error.

2. **What do you understand by DNS?**

   Ans: DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.

3. **Describe the TELNET protocol in brief.**
   Ans: It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.

4. **Identify the different parts of the following URL : ” https://www.w3schools.com/tags/”**
   Ans: protocol: https
   Host or domain name: www.w3schools.com
   Path of the resource: /tags

5. **State the number of networks for Class A and Class B addresses.**

Ans: Class A: 2^7 = 128 networks

Class B: 2^{14} = 16384 networks

6. Write a short note on FTP.

Ans : FTP is a standard internet protocol used for transmitting the files from one computer to another computer. When a client transfers a file to the server is called "Uploading" and server file transfer to client is called "Downloading". Thus, it is generally used to download files from a server over the internet and to upload files to a server using internet.

7. **Differentiate between TCP and UDP.**

Ans:

Transmission control protocol (TCP)	User datagram protocol (UDP)
TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission.
TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error checking mechanism using checksums.
Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in-order at the receiver.	There is no sequencing of data in UDP. If ordering is required, it has to be managed by the application layer.
TCP is comparatively slower than UDP.	UDP is faster, simpler and more efficient than TCP.
Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in User Datagram Protocol (UDP).

8. **What is the purpose of HTTP?**

Ans: HTTP allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.

9. **Which class does the following IP Addresses: {**"2.2.2.1", "128.2.2.2", "128.128.128.128" **} belong to?**

Ans :

2.2.2.1 : **Class A**

128.2.2.2 : **Class B**

128.128.128.128 : **Class B**