Computer Networking

Ronak A. Bhanushali[1], Neer M. Bhanushali[2], Mihir J. Panchal[3]
[1,2,3]*Student, K.J. Somaiya Polytechnic, Vidhyavihar*

Abstract* – A Computer Network consists of one or more machines connected together to share data, information or files over a network or with each other. This is also used to share resources with each other. It is a branch in Computer Science and Telecommunication since it relies on theoretical and practical applications related disciplines. A Computer Network extends the communication means by electronic medium with the help of various devices and technology. Computer Network can handle communications like *Email, Instant Messaging, Online Chatrooms, Voice* and *Video Calls.

I.INTRODUCTION

Computer Network plays a vital role in transfer of data from one peripheral to another or from one computer network to another. These Networks are set of computer sharinig resources located on network nodes. The networks use different types of *Protocols* to transmit data from one place to another.

II.PROTOCOLS

Some of the examples of the Network Protocols are *Internet Protocol(IP), Internet Control Messaging Protocol(ICMP), Address Resolution Protocol(ARP) etc.*

Each of these Protocols have their own particular tasks

1. Internet Protocol (IP):

It is the principal communication protocol in the Internet Protocol suite for relaying *Datagrams* across the Network boundaries. It does the task of delivering the packets from source host to destination host solely based on their respective IP addresses in the packet headers. IP addressing entails the assignment of IP address associated parameters to host interfaces. The address space is divided into networks and sub-networks, involving the designations of network or routing prefixes.

2. Internet Control Messaging Protocols(ICMP):

Internet Control Message Protocol (ICMP) is a network layer protocol used for *diagnosing* network communication issues, it is used by Network Devices. It is mainly used to determine wheather or not data is reaching its intended destination in a timely manner. Commonly, the ICMP is used on network devices like *routers etc,*

ICMP can also be used for *Distributed Denial-of-Service attacks (DDoS).*

3. Address Resolution Protocol(ARP):

This Protocol is used to *convert logical IP addresses to physical MAC address*. A MAC address is a machines permanent unique address. In this the application data is passed through all the layers within a network before being sent to the internet.

The Transport Layer provides the destination IP address with which the Internet Layer provides the destination port. The MAC address is required to uniquely identify a particular device globally.

ARP can only ask devices on its local network for the MAC address.

III.IP ADDRESSING

Another important node of Computer Network is IP Addressing.

Classful IP Addressing : It refers to IP Addresses which are divided into various different classes, to understand better we must know what is an *IP Address ?:* An IP Address is a *address information of a specific host especially outside the LAN, it is a 32-bit unique address having a address space of 2^32.* These can be further categorized into classes like Class-A, Class-B, Class-C, Class-D & Class-E. All these classes have a fixed range of IP Address. Class-D and Class-E are reserved IP Address for multicast and Experimental purposes respectively. All these IP Addresses are managed globally by *Internet Assigned Numbers Authority (IANA) and Regional Internet Registries(RIR)*

1. Class-A:

IP addresses belonging to Class-A are assigned to the networks that contain large number of hosts. Its host Id is 24 bits long, It has a network Id of 8 bits, the 24 bits host id is used to determine the host in any network. The default subnet mask for Class-A is 255.x.x.x.

2. Class-B:

IP Address belonging to Class-B are assigned to the networks that ranges from medium size to large sized networks. They have a 16 bit network Id and 16 bit host Id. The 16 bit Host ID is used to determine the host in any network. The default subnet mask for Class-B is 255.255.x.x.

3. Class-C:

IP Addresses assigned to Class-c are majorly small sized networks. They have a 24bit long network Id and 8 bit long host Id. The 8 bit host Id is used for determining the host in any network. The Default subnet mask for Class-C is 255.255.255.x.

4. Class-D:

IP Addresses belonging to Class-D are reserved for multicasting. Class-d doesn't possess any subnet-mask. And the IP Addresses in Class-D range from 224.0.0.0-239.255.255.255.

5. Class-E:

IP Addresses belonging to Class-E are reserved for Experimental purpose. IP Address of Class-E range from 240.0.0.0-255.255.255.254. This class also doesn't have any subnet-mask

IV.RULES FOR ASSIGNING HOST ID & NETWORK ID

A Host Id must be *unique* within a network, A Host ID in which all the bits are set to 0 cannot be assigned because this host ID is used to represent the network ID of the IP address, Host Id in which all the bits are et to 1 cannot be assigned because this host is reserved as a broadcast address to send packets to all.

A Network ID cannot start with a 127 because 127 belongs to Class-a address and is reserved for internal loop-back functions. All bits of Network ID set to 1 cannot be used as they are reserved as use of broadcast address and all the bits of a Network ID set to 0 are used to denote a specific host on local network and are not routed and hence not used.

V.SWITCHING TECHNIQUES

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission. Switching technique is used to connect the systems for making one-to-one communication.

1. Circuit Switching:

Circuit switching is a switching technique that establishes a dedicated path between sender and receiver. In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated. Circuit switching in a network operates in a similar way as the telephone works. A complete end-to-end path must exist before the communication takes place. Circuit switching is used in public telephone network. It is used for voice transmission. Fixed data can be transferred at a time in circuit switching technology.

2. Message Switching:

Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded. In Message Switching technique, there is no establishment of a dedicated path between the sender and receive. The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message. Message switches are programmed in such a way so that they can provide the most efficient routes. Each and every node stores the entire message and then forward it to the next node. This type of network is known as store and forward network. Message switching treats each message as an independent entity.

3. Packet Switching:

The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually. The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end Every packet contains some

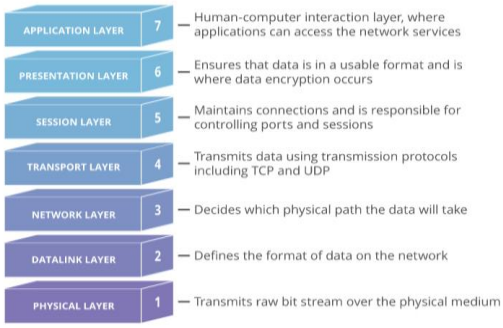
information in its headers such as source address, destination address and sequence number. Packets will travel across the network, taking the shortest path as possible. All the packets are reassembled at the receiving end in correct order. If any packet is missing or corrupted, then the message will be sent to resensd the message. If the correct order of the packets is reached, then the acknowledgment message will be sent.

VI.OSI MODEL

OSI Model (Open System Interconnection) was proposed by ISO (International Standard Organization) in 1984. It deals with connecting open systems. In simple terms, the OSI provides a standard for different computer systems to be able to communicate with each other. It is a set of technical standards, approved by the ISO, that provides a basis for data communications.

The OSI Model can be seen as a universal language for computer networking. It is based on the concept of splitting up a communication system into seven abstract layers, each one stacked upon the last.

The Seven layers are stacked as follows



Each layer of the OSI model handles a specific job and *communicates with the layers above and below itself*. *DDoS Attacks* target specify layers of a network connection.

Why does the OSI Model matter?

Although the modern Internet does not strictly follow the OSI Model (it more closely follows the simpler Internet protocol suite), the OSI Model is still very useful for troubleshooting network problems. Whether it's one person who can't get their laptop on the Internet, or a website being down for thousands of users, the OSI Model can help to break down the problem and isolate the source of the trouble. If the problem can be narrowed down to one specific layer of the model, a lot of unnecessary work can be avoided.

The Seven Layers of OSI model:

1. Physical Layer:

It is concerned with the actual physical attachment to the network i.e., its deals with the means of connecting two nodes in a network. It deals with transmitting raw bits over communication channel.

2. Data-Link Layer:

It breaks the data into frames and passes it to the network layer .

Error Control: To control transmission errors.

Flow Control: To prevent the drowning of overflow of a slow receiver by a fast transmitter.

Access Control : Control access to the shared channel A special section of the DLL called Medium Access control deals with this section.

3. Network Layer:

It has the responsibility of performing source to destination delivery of packets. Routing, Congestion Control, Quality of Service, Addressing, Integration of heterogeneous networks.

4. Transport Layer:

Control of data flow in the network, Ensuring no loss of data, Ensuring that all pieces arrive correctly at other end, Transport layer is true end to end layer.

5. Session Layer:

Keeping track of whose turn it is to transmit. Preventing two parties from attempting same critical operation at the same time. Check pointing long transaction to allow them to continue from where they were after a crash.

6. Presentation Layer:

This layer is primarily responsible for preparing data so that it can be used by the application layer; in other words, layer 6 makes the data presentable for applications to consume. The presentation layer is responsible for translation, encryption, and compression of data.

7. Application Layer:

An application layer provides user interfaces and support for services like:
Email, Remote file access, File Transfer, Shared database management.

VII.CONCLUSION

The field of Computer Networking can grow to a very high Extent if more and more public has the access to the *Network Technology*.

REFERNECE

[I] https://www.wikipedia.org/
[II] https://www.geeksforgeeks.org/