Application Layer

The Application Layer is topmost layer in the Open System Interconnection (OSI) model. This layer provides several ways for manipulating the data (information) which actually enables any type of user to access network with ease. This layer also makes a request to its bottom layer, which is presentation layer for receiving various types of information from it. The Application Layer interface directly interacts with application and provides common web application services. This layer is basically highest level of open system, which provides services directly for application process.

- **Functions of Application Layer :**
  The Application Layer, as discussed above, being topmost layer in OSI model, performs several kinds of functions which are requirement in any kind of application or communication process.
  Following are list of functions which are performed by Application Layer of OSI Model –
- Application Layer provides a facility by which users can forward several emails and it also provides a storage facility.
- This layer allows users to access, retrieve and manage files in a remote computer.
- It allows users to log on as a remote host.
- This layer provides access to global information about various services.
- This layer provides services which include: e-mail, transferring files, distributing results to the user, directory services, network resources and so on.
- Application Layer helps us to identify communication partners, and synchronizing communication.
- This layer allows users to interact with other software applications.
- In this layer, data is in visual form, which makes users truly understand data rather than remembering or visualize the data in the binary format (0's or 1's).
- This application layer basically interacts with Operating System (OS) and thus further preserves the data in a suitable manner.
- This application layer, in general, performs host initialization followed by remote login to hosts.

Features provided by Application Layer Protocols :

To ensure smooth communication, application layer protocols are implemented the same on source host and destination host.

The following are some of the features which are provided by Application layer protocols-

- The Application Layer protocol defines process for both parties which are involved in communication.
- These protocols define the type of message being sent or received from any side (either source host or destination host).
- These protocols also define basic syntax of the message being forwarded or retrieved.
- These protocols define the way to send a message and the expected response.
- These protocols also define interaction with the next level.

Transport Layer

The transport Layer is the second layer in the TCP/IP model and the fourth layer in the OSI model. It is an end-to-end layer used to deliver messages to a host. It is termed an end-to-end layer because it provides a point-to-point connection rather than hop-to-hop, between the source host and destination host to deliver the services reliably. The unit of data encapsulation in the Transport Layer is a segment.

Working of Transport Layer

The transport layer takes services from the Application layer and provides services to the Network layer.

At the sender's side: The transport layer receives data (message) from the Application layer and then performs Segmentation, divides the actual message into segments, adds the source and destination's port numbers into the header of the segment, and transfers the message to the Network layer.

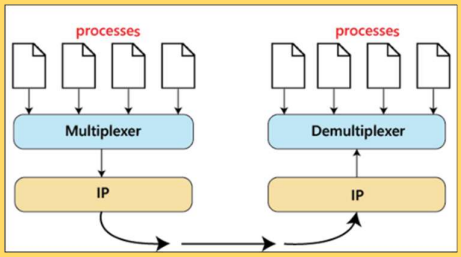
At the receiver's side: The transport layer receives data from the Network layer, reassembles the segmented data, reads its header, identifies the port number, and forwards the message to the appropriate port in the Application layer.

Responsibilities of a Transport Layer

- The Process to Process Delivery
- End-to-End Connection between Hosts
- Multiplexing and Demultiplexing
- Congestion Control
- Data integrity and Error correction
- Flow control

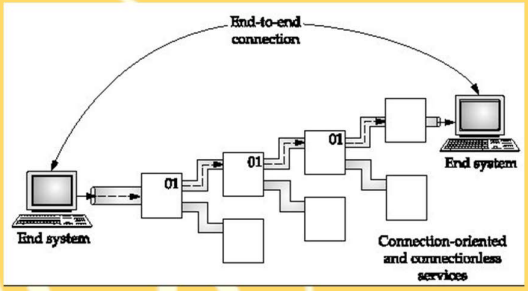
1. **The Process to Process Delivery**

   While Data Link Layer requires the MAC address of source-destination hosts to correctly deliver a frame and the Network layer requires the IP address for appropriate routing of packets, in a similar way Transport Layer requires a Port number to correctly deliver the segments of data to the correct process amongst the multiple processes running on a particular host. A port number is a 16-bit address used to identify any client-server program uniquely.



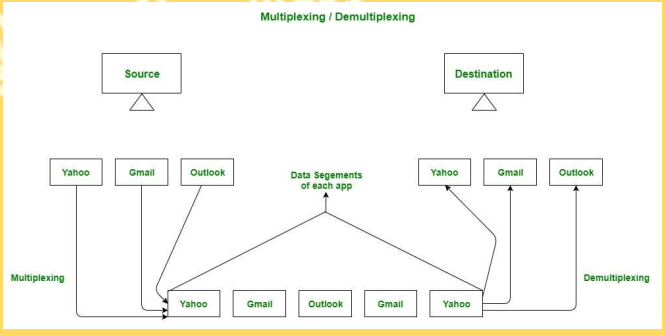
2. **End-to-end Connection between Hosts**

   The transport layer is also responsible for creating the end-to-end Connection between hosts for which it mainly uses TCP and UDP. TCP is a secure, connection-orientated protocol that uses a handshake protocol to establish a robust connection between two end hosts. TCP ensures the reliable delivery of messages and is used in various applications. UDP, on the other hand, is a stateless and unreliable protocol that ensures best-effort delivery. It is suitable for applications that have little concern with flow or error control and requires sending the bulk of data like video conferencing. It is often used in multicasting protocols.



3. **Multiplexing and Demultiplexing**

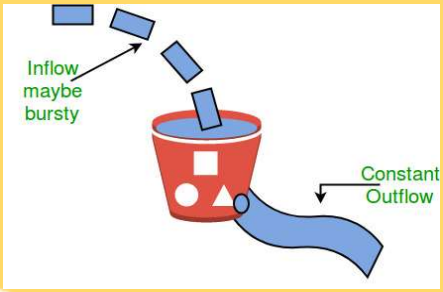
   Multiplexing(many to one) is when data is acquired from several processes from the sender and merged into one packet along with headers and sent as a single packet. Multiplexing allows the simultaneous use of different processes over a network that is running on a host. The processes are differentiated by their port numbers. Similarly, Demultiplexing one to many is required at the receiver side when the message is distributed into different processes. Transport receives the



segments of data from the network layer distributes and delivers it to the appropriate process running on the receiver's machine.

4. **Congestion Control**

Congestion is a situation in which too many sources over a network attempt to send data and the router buffers start overflowing due to which loss of packets occurs. As a result, the retransmission of packets from the sources increases the congestion further. In this situation, the Transport layer provides Congestion Control in different ways. It uses open-loop congestion control to prevent congestion and closed-loop congestion control to remove the congestion in a network once it occurred. TCP provides AIMD – additive increases multiplicative decrease and leaky bucket technique for congestion control.



5. **Data integrity and Error Correction**

The transport layer checks for errors in the messages coming from the application layer by using error detection codes, and computing checksums, it checks whether the received data is not corrupted and uses the ACK and NACK services to inform the sender if the data has arrived or not and checks for the integrity of data.

6. **Flow Control**

The transport layer provides a flow control mechanism between the adjacent layers of the TCP/IP model. TCP also prevents data loss due to a fast sender and slow receiver by imposing some flow control techniques. It uses the method of sliding window protocol which is accomplished by the receiver by sending a window back to the sender informing the size of data it can receive.

Network Layer

The network Layer is the third layer in the OSI model of computer networks. Its main function is to transfer network packets from the source to the destination. It is involved both the source host and the destination host. At the source, it accepts a packet from the transport layer, encapsulates it in a datagram, and then delivers the packet to the data link layer so that it can further be sent to the receiver. At the destination, the datagram is decapsulated, and the packet is extracted and delivered to the corresponding transport layer.

Features of Network Layer

- The main responsibility of the Network layer is to carry the data packets from the source to the destination without changing or using them.
- If the packets are too large for delivery, they are fragmented i.e., broken down into smaller packets.
- It decides the route to be taken by the packets to travel from the source to the destination among the multiple routes available in a network (also called routing).
- The source and destination addresses are added to the data packets inside the network layer.

Services Offered by Network Layer

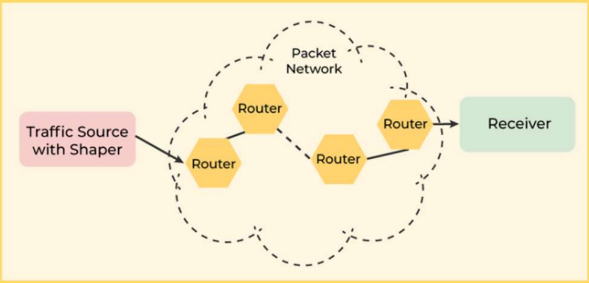
The **services** which are offered by the network layer protocol are as follows:

- Packetizing
- Routing
- Forwarding

1. **Packetizing**

   The process of encapsulating the data received from the upper layers of the network (also called payload) in a network layer packet at the source and decapsulating the payload from the network layer packet at the destination is known as packetizing.

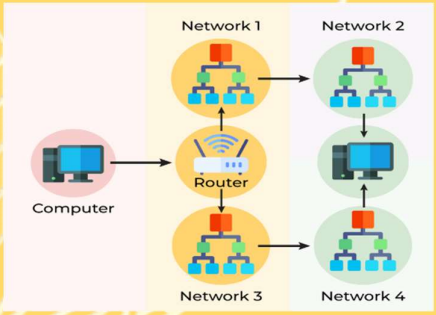
The source host adds a header that contains the source and destination address and some other relevant information required by the network layer protocol to the payload received from the upper layer protocol and delivers the packet to the data link layer.



The destination host receives the network layer packet from its data link layer, decapsulates the packet, and delivers the payload to the corresponding upper layer protocol. The routers in the path are not allowed to change either the source or the destination address. The routers in the path are not allowed to decapsulate the packets they receive unless they need to be fragmented.

2. ***Routing***

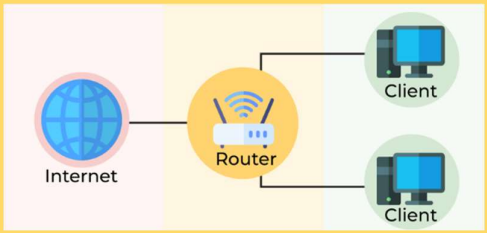
Routing is the process of moving data from one device to another device. These are two other services offered by the network layer. In a network, there are a number of routes available from the source to the destination. The network layer specifies some strategies which find out the best possible route. This process is referred to as routing.



There are a number of routing protocols that are used in this process and they should be run to help the routers coordinate with each other and help in establishing communication throughout the network.

3. ***Forwarding***

Forwarding is simply defined as the action applied by each router when a packet arrives at one of its interfaces. When a router receives a packet from one of its attached networks, it needs to forward the packet to another attached network (unicast routing) or to some attached networks (in the case of multicast routing). Routers are used on the network for forwarding a packet from the local network to the remote network. So, the process of routing involves packet forwarding from an entry interface out to an exit interface.



Difference between Routing and Forwarding

Routing	Forwarding
Routing is the process of moving data from one device to another device.	Forwarding is simply defined as the action applied by each router when a packet arrives at one of its interfaces.
Operates on the Network Layer.	Operates on the Network Layer.
Work is based on Forwarding Table.	Checks the forwarding table and work according to that.
Works on protocols like Routing Information Protocol (RIP) for Routing.	Works on protocols like UDP Encapsulating Security Payloads

Other Services Expected from Network Layer

- Error Control
- Flow Control
- Congestion Control

1. **Error Control**

   Although it can be implemented in the network layer, it is usually not preferred because the data packet in a network layer may be fragmented at each router, which makes error-checking inefficient in the network layer.

2. **Flow Control**

   It regulates the amount of data a source can send without overloading the receiver. If the source produces data at a very faster rate than the receiver can consume it, the receiver will be overloaded with data. To control the flow of data, the receiver should send feedback to the sender to inform the latter that it is overloaded with data.

   There is a lack of flow control in the design of the network layer. It does not directly provide any flow control. The datagrams are sent by the sender when they are ready, without any attention to the readiness of the receiver.

3. **Congestion Control**

   Congestion occurs when the number of datagrams sent by the source is beyond the capacity of the network or routers. This is another issue in the network layer protocol. If congestion continues, sometimes a situation may arrive where the system collapses and no datagrams are delivered. Although congestion control is indirectly implemented in the network layer, still there is a lack of congestion control in the network layer.

Advantages of Network Layer Services

- Packetization service in the network layer provides ease of transportation of the data packets.
- Packetization also eliminates single points of failure in data communication systems.
- Routers present in the network layer reduce network traffic by creating collision and broadcast domains.
- With the help of Forwarding, data packets are transferred from one place to another in the network.

Disadvantages of Network Layer Services

- There is a lack of flow control in the design of the network layer.
- Congestion occurs sometimes due to the presence of too many datagrams in a network that is beyond the capacity of the network or the routers. Due to this, some routers may drop some of the datagrams, and some important pieces of information may be lost.
- Although indirect error control is present in the network layer, there is a lack of proper error control mechanisms as due to the presence of fragmented data packets, error control becomes difficult to implement.

Datalink Layer

The data link layer is the second layer from the bottom in the OSI (Open System Interconnection) network architecture model. It is responsible for the node-to-node delivery of data. Its major role is to ensure error-free transmission of information. DLL is also responsible for encoding, decode and organizing the outgoing and incoming data. This is considered the most complex layer of the OSI model as it hides all the underlying complexities of the hardware from the other above layers.

Sub-layers of the Data Link Layer

The data link layer is further divided into two sub-layers, which are as follows:

Logical Link Control (LLC)

This sublayer of the data link layer deals with multiplexing, the flow of data among applications and other services, and LLC is responsible for providing error messages and acknowledgments as well.

Media Access Control (MAC)

MAC sublayer manages the device's interaction, responsible for addressing frames, and also controls physical media access.

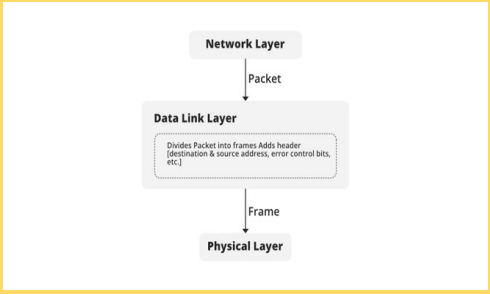
The data link layer receives the information in the form of packets from the Network layer, it divides packets into frames and sends those frames bit-by-bit to the underlying physical layer.

Functions of the Data-link Layer

There are various benefits of data link layer s let's look into it.

Framing

The packet received from the Network layer is known as a frame in the Data link layer. At the sender's side, DLL receives packets from the Network layer and divides them into small frames, then, sends each frame bit-by-bit to the physical layer. It also attaches some special bits (for error control and addressing) at the header and end of the frame. At the receiver's end, DLL takes bits from the Physical layer organizes them into the frame, and sends them to the Network layer.



Addressing

The data link layer encapsulates the source and destination's MAC address/ physical address in the header of each frame to ensure node-to-node delivery. MAC address is the unique hardware address that is assigned to the device while manufacturing.

Error Control

Data can get corrupted due to various reasons like noise, attenuation, etc. So, it is the responsibility of the data link layer, to detect the error in the transmitted data and correct it using error detection and correction techniques respectively. DLL adds error detection bits into the frame's header, so that receiver can check received data is correct or not. It adds reliability to phyiscal layer by adding mechansims to detect and retransmit damaged or lost frames.

Flow Control

If the receiver's receiving speed is lower than the sender's sending speed, then this can lead to an overflow in the receiver's buffer and some frames may get lost. So, it's the responsibility of DLL to synchronize the sender's and receiver's speeds and establish flow control between them.

Access Control

When multiple devices share the same communication channel there is a high probability of collision, so it's the responsibility of DLL to check which device has control over the channel and CSMA/CD and CSMA/CA can be used to avoid collisions and loss of frames in the channel.

Protocols in Data link layer

There are various protocols in the data link layer, which are as follows:

- Synchronous Data Link Protocol (SDLC)
- High-Level Data Link Protocol (HDLC)
- Serial Line Interface Protocol (SLIP)for encoding
- Point to Point Protocol (PPP)
- Link Access Procedure (LAP)
- Link Control Protocol (LCP)
- Network Control Protocol (NCP)

Physical Layer

The physical Layer is the bottom-most layer in the Open System Interconnection (OSI) Model which is a physical and electrical representation of the system. It consists of various network components such as power plugs, connectors, receivers, cable types, etc. The physical layer sends data bits from one device(s) (like a computer) to another device(s). The physical Layer defines the types of encoding (that is how the 0's and 1's are encoded in a signal). The physical Layer is responsible for the communication of the unstructured raw data streams over a physical medium.

Functions Performed by Physical Layer

The following are some important and basic functions that are performed by the Physical Layer of the OSI Model –

- The physical layer maintains the data rate (how many bits a sender can send per second).
- It performs the Synchronization of bits.
- It helps in Transmission Medium decisions (direction of data transfer).
- It helps in Physical Topology (Mesh, Star, Bus, Ring) decisions (Topology through which we can connect the devices with each other).
- It helps in providing Physical Medium and Interface decisions.
- It provides two types of configuration Point Point configuration and Multi-Point configuration.

- It provides an interface between devices (like PCs or computers) and transmission medium.
- It has a protocol data unit in bits.
- Hubs, Ethernet, etc. device is used in this layer.
- This layer comes under the category of Hardware Layers (since the hardware layer is responsible for all the physical connection establishment and processing too).
- It provides an important aspect called Modulation, which is the process of converting the data into radio waves by adding the information to an electrical or optical nerve signal.
- It also provides a Switching mechanism wherein data packets can be forwarded from one port (sender port) to the leading destination port.

Physical Topologies

Physical Topology or Network Topology is the Geographical Representation of Linking devices. Following are the four types of physical topology-

Mesh Topology: In a mesh topology, each and every device should have a dedicated point-to-point connection with each and every other device in the network. Here there is more security of data because there is a dedicated point-to-point connection between two devices. Mesh Topology is difficult to install because it is more complex.

Star Topology: In star topology, the device should have a dedicated point-to-point connection with a central controller or hub. Star Topology is easy to install and reconnect as compared to Mesh Topology. Star Topology doesn't have Fault Tolerance Technique.

Bus Topology: In a bus topology, multiple devices are connected through a single cable that is known as backbone cable with the help of tap and drop lines. It is less costly as compared to Mesh Topology and Star Topology. Re-connection and Re-installation are difficult.

Ring Topology: In a ring topology, each device is connected with repeaters in a circle-like ring that's why it is called Ring Topology. In Ring Topology, a device can send the data only when it has a token, without a token no device can send the data, and a token is placed by Monitor in Ring Topology.

Line Configuration

- Point-to-Point configuration: In Point-to-Point configuration, there is a line (link) that is fully dedicated to carrying the data between two devices.
- Multi-Point configuration: In a Multi-Point configuration, there is a line (link) through which multiple devices are connected.

Modes of Transmission Medium

- Simplex mode: In this mode, out of two devices, only one device can transmit the data, and the other device can only receive the data. Example- Input from keyboards, monitors, TV broadcasting, Radio broadcasting, etc.
- Half Duplex mode: In this mode, out of two devices, both devices can send and receive the data but only one at a time not simultaneously. Examples- Walkie-Talkie, Railway Track, etc.
- Full-Duplex mode: In this mode, both devices can send and receive the data simultaneously. Examples- Telephone Systems, Chatting applications, etc.

Physical Layer Protocols Examples

Typically, a combination of hardware and software programming makes up the physical layer. It consists of several protocols that control data transmissions on a network. The following are some examples of Layer 1 protocols:

- Ethernet with 1000BASE-T.
- Ethernet with 1000BASE-SX.
- Ethernet at 100BaseT.
- Synchronous Digital Hierarchy/Optical Synchronisation.
- Physical-layer variations in 802.11.
- Bluetooth.
- Networking for controllers.
- U.S. Serial Bus.

Filename: 7
Directory: C:\Users\nilad\Documents
Template: C:\Users\Nil\OneDrive\Documents\Custom Office Templates\page template.dotx
Title:
Subject:
Author: Nil
Keywords:
Comments:
Creation Date: 03-02-2024 15:01:00
Change Number: 28
Last Saved On: 09-02-2024 16:01:00
Last Saved By: Basudeb Paul Chowdhury
Total Editing Time: 136 Minutes
Last Printed On: 09-02-2024 16:01:00
As of Last Complete Printing
Number of Pages: 13
Number of Words: 3,621 (approx.)
Number of Characters: 20,646 (approx.)