Chapter 2: Network Models

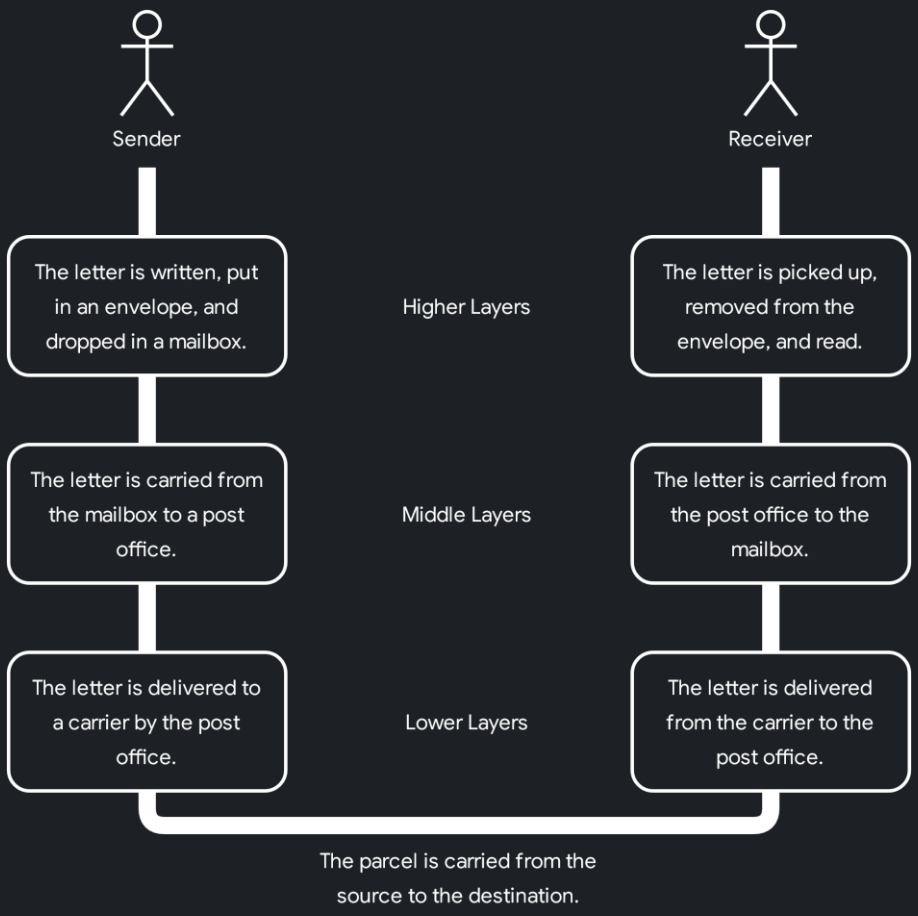
Table of Contents

A network is a combination of hardware and software that sends data form one location to another. The hardware consists of the physical equipment that carries signals from one point of the network to another. The software consists of the instruction sets that make the services we expect from the network possible.

2.1 Layered Tasks

Consider the task of sending an email. This can be broken down into several steps, each of which can be handled by a separate software package. This type of approach is called a layered approach.

Consider the image below:



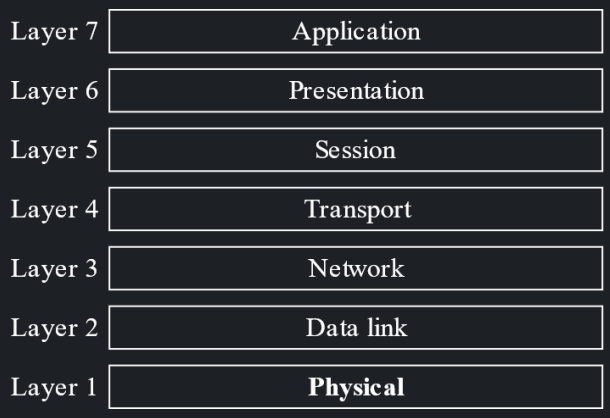
Here, we have two friends writing letters to each other. This process is broken down into several parts. First consider that the person on the left is sending a letter. This letter is recorded on a piece of paper, put in an envelope and dropped in a mail box. Afterwards, the mail is taken to the postal office. Finally, the letter is given to a carrier. On the other side, the carrier delivers the letter to the post office, then the post office delivers the letter to the final address, where the envelope is unsealed and the letter read.

Notice how the path went from top to bottom on the sender’s side, and from bottom to top on the receiver’s side. There are three layers, each of which does some different task. The top layer can be considered to be the user support layer. This is the layer that the users interact with. The bottom layer can be considered to be the communication layer, since it deals with the actual transport of the letter from one destination to another.

2.2 The OSI Model

The Open Systems Interconnection (OSI) is a layered framework that is the standard design for network systems. Note that OSI is not a protocol.

The OSI model has 7 layers.



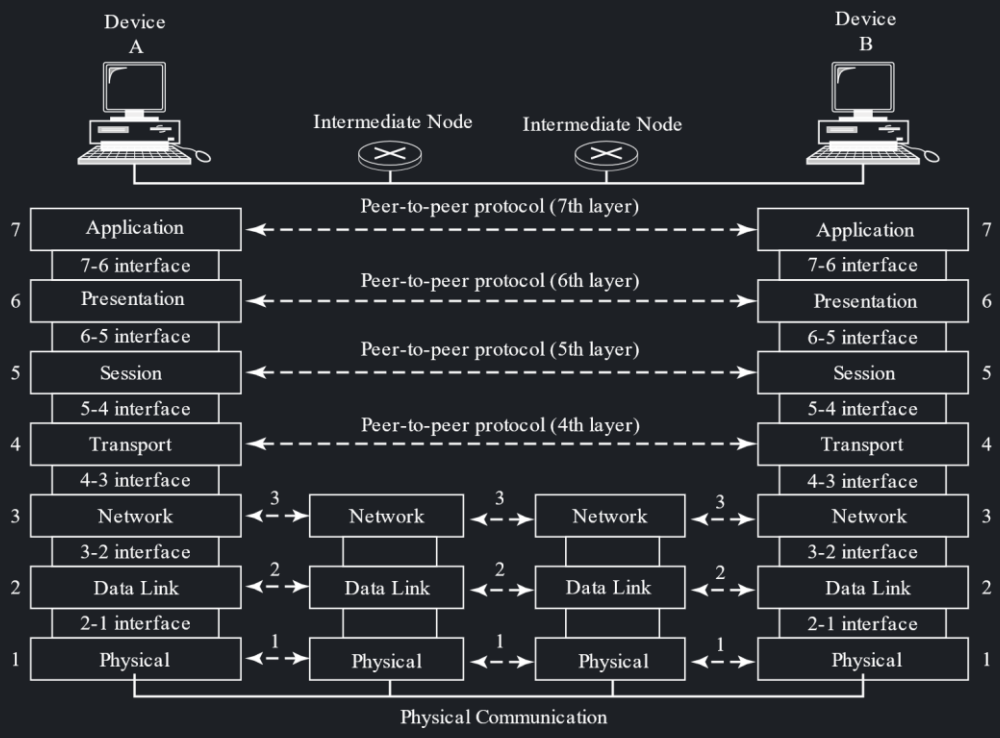
The top 3 layers are called the user support layers, and the bottom 3 are called the network support layers. The middle layer acts as a bridge between the user and network support layers.

There are a few points we need to note about this model.

- All the layers provide services to the layers above them. We shall study what these services are in a moment. There are a lot of protocols running in the different layers, but this point helps understand them. The upper layers decide which protocols must be used by the lower layers when they make use of their services. For example, an application developer will decide what his needs are, and based on that, the transport layer will have to use the TCP or the UDP protocol.
- If we want bi-directional communication, all the layers must implement opposite tasks. Going back to the first example with the letter, the top layer must be capable of writing data, as well as reading data. If the data is encrypted, the layer must be able to encrypt and decrypt data.

- At any time, there should be an identical object in the sender and receiver machines. Again, considering the first example, the top layer deals with some raw data on both the sender and receiver side. In the bottom layer, both the sender and receiver deal with the transport of a sealed envelope.

Now consider this figure.



Here, we have two devices that are communicating each other, with two intermediate devices, which can simply be routers. When a message is being sent from the device on the left, it goes down 7 layers, reaches the first router, goes up 3 layers till the network layer, comes back down, goes to another router, again goes up 3 layers and back down, and finally reaches the destination device, going up all 7 layers.

Notice how at every layer the object being dealt with is exactly the same. Also notice that the router only deals with the bottom 3 layers, which we know to be the network support layers. Because of this, routers are called layer 3 devices. Only the two main devices deal with the user interface layers and the transport layer.

Since every layer needs to interact with the layers on the same level on different devices, each layer adds some extra information onto the original message. For example, the application layer on the sender's end adds some information which the application layer on the receiver's end uses to establish some communication between those two layers. Thus, this is an end-to-end communication.

2.3 Layers in the OSI Model

Communication Between Layers

There are three types of delivery.

1. Process-to-Process Delivery
2. Host-to-Host Delivery
3. Hop-to-Hop Delivery/Node-to-Node Delivery

The application and transport layers are responsible for process-to-process delivery. The network layer is responsible for host-to-host delivery. The data link layer is responsible for hop-to-hop delivery.

Now to look at what all of this means. Consider the diagram below:

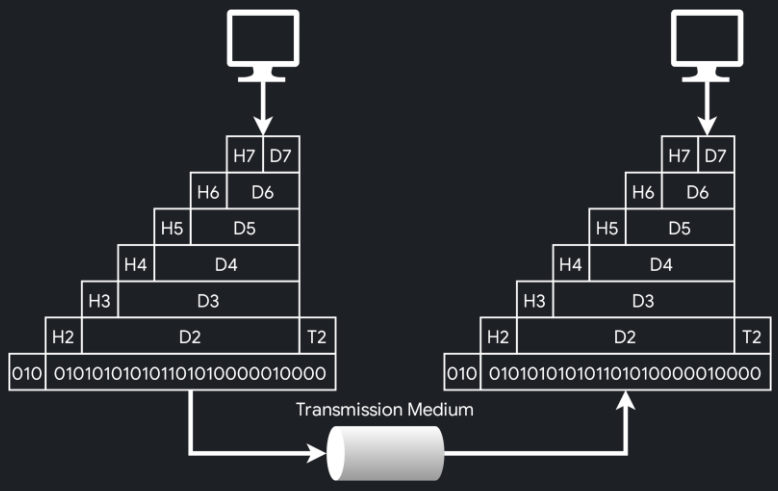
Say we have two machines that are communicating. Each machine can have several processes open on it at any time, with the data being sent from one of the processes. Say P_1 on machine A is the same application as P_4 on machine B, and they are trying to communicate. All of the data from P_1 must be delivered to P_4. Since there are multiple processes open on each machine, which process should receive the data being sent needs to be identified accurately. This is being done by the transport and application layers. The identification itself is done with the help of port addresses.

The fact that the data is going from machine A to machine B is a delivery that is handled by the network layer. We need to be able to identify the machines on either end, and this is done with the help of logical address, such as the IP address. This is unique for

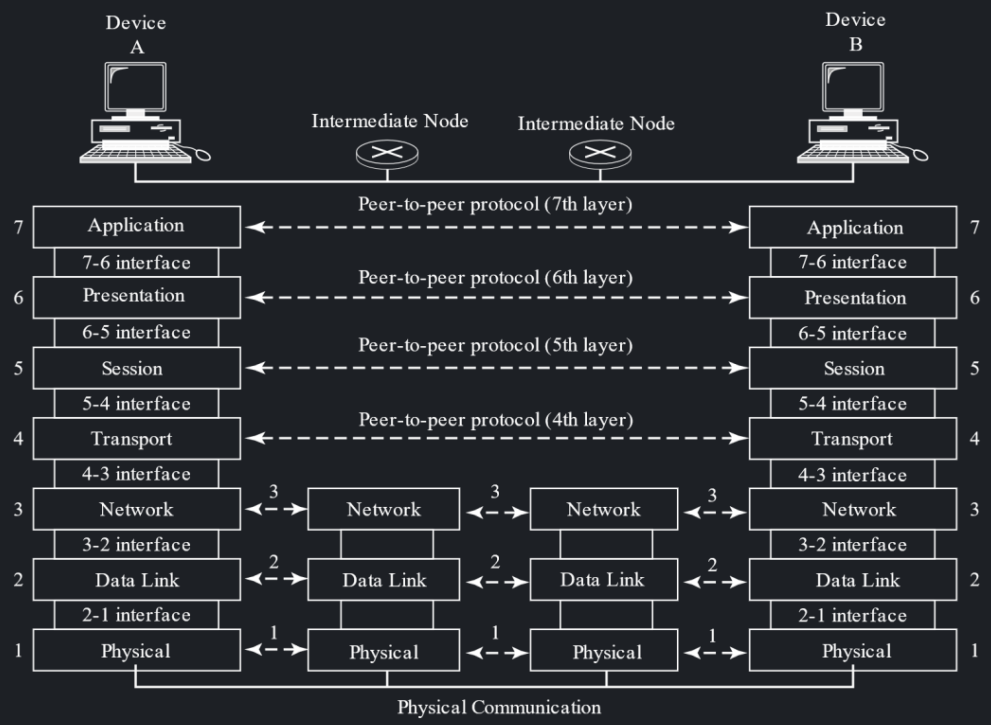
the devices on a network. The network layer is responsible for generating the packet for these logical addresses. They do not deal with which processes on the machine should be involved.

However, we cannot directly send data from one machine to another. The data goes to a switch, which sends it to a router, which sends it to another router which finally gives it to a switch on the receiver's end. This is called hop-to-hop delivery. This delivery requires each of the devices on the route to be identifiable, which is done with physical addressing. This could be the mac address of the device, which is a fixed, permanent and unique address every machine has.

Thus, when data comes from the application layer to the transport layer, it takes all of it and adds the source and destination port addresses. This goes to the network layer, which just adds the source and destination logical address. This goes to the data link layer, which adds the source and destination physical addresses. Every other layer is also adding some information, but we will look at those details later. On the receiver's side, each of the corresponding layers removes the corresponding information.



Thus, each layer is adding some information, called headers. This process is called encapsulation.



The physical layer transports the data via the communication medium to a router. The router's physical layer receives the object and passes it to the data link layer. At this point, the data is exactly the same as it was when leaving the data link layer of the source machine. The data link layer can only understand the data added by the data link layer of the source machine. This is then pushed to the network layer, which can again only read the data added by the network layer of the source machine. It uses the data to identify the destination machine, and acts accordingly to send the data to the receiver's router.

Physical Layer

The physical layer performs the actual transmission of the electromagnetic signals. The transmission of the individual bits is overseen by this layer.

The responsibilities of the physical layer include:

- Conversion of binary data into signals

- Selection of transmission mode (simplex, half-duplex or full-duplex)
- Defining the characteristics of the interface between devices and the transmission medium
- Defining the type of the transmission medium
- Controlling transmission rates
- Synchronize sender and receiver clocks so they work with the same bits at the same time
- Line configuration, or how devices are connected to the media. This can be point-to-point (2 devices directly connected) or multi-point (multiple devices connected to a single link.
- Physical topology

Data Link Layer

The data link layer is responsible for moving frames from one hop to the next. Its responsibilities all refer to these hops, not to the actual end-to-end transmission. Its responsibilities include:

- Framing – The stream of bits coming in from the network layer are divided into manageable data units, called frames.
- Physical Addressing – A header is added to each frame to define the sender and receiver of the frame.
- Flow Control – If the sender can send data faster than the receiver can receive data, the speed is regulated. This refers to intermediate devices, not the end device. Flow control for the latter is handled in the transport layer.
- Error Control – Mechanisms are added to detect and retransmit damaged or lost frames, instead of correcting them, which can be costly. It is also possible to detect duplicate frames. All of this is put in the trailer.
- Access Control – There are protocols used in this layer to determine which device in a network should have control over the link at a given time. There are several protocols related to this which we will be studying later.

The unit for the data link layer is the frame. Note that frames are changed at every hop, and the source and destination for every new frame is different. For example, if machines A and B are exchanging data, the first frame might have its source as A and destination as C, an intermediate node, the second frame might have its source as C and destination as D, another intermediate node, and finally the third frame goes from D to the actual recipient B.

Network Layer

The network layer deals with packets of data, and ensures that the actual destination is reached, even if it is on a different network. If two devices are on the same network, there might not be a need for the network layer at all.

The responsibilities of the network layer include:

- Logical Addressing – The physical addressing implemented by the data link layer only deals with devices on the same network. The network layer adds a header to the packet coming from the upper layer which includes the logical addresses of the sender and receiver. We shall discuss logical addresses a little later.
- Routing – When multiple networks are working together, the devices, or routers, that switch packets to their final destination make use of the routing mechanism of the network layer.

Essentially, the data link layer is what managed to get data from the source to the router on the network. The network layer is what allowed the router to figure out which device on which network the data needs to be sent to next, so that its final destination can be reached. There are different metrics that are used to choose which path to take, such as time, cost, etc. The information regarding which paths are optimal are stored on a routing table.

Transport Layer

The transport layer deals with process to process delivery. The network layer treats each packet as though they were completely unrelated to each other. The transport layer on the other hand, ensures all the data from a process arrives intact, and in order. It handles both error control and flow control with regards to the two end devices.

Other responsibilities of the transport layer include:

- Service-point addressing or port addressing added to the header of each segment to identify the correct process.
- Segmentation of messages into smaller parts, each containing a sequence number, and reassembly of the messages in the correct sequence. The numbered segments also help identify any lost packets and ask that they be retransmitted. The unit for the transport layer is the segment.
- Connection Control – The transport layer can either be connectionless, where all the packets are just sends each segment independently, or connection-oriented, where the transport layers of the source and destination make a connection before delivering the packets. Having a connection makes the process more reliable.
- Flow control between the end devices.
- Error control for the entire message to prevent damage, loss or duplication. Error correction occurs in the form of retransmission.

Session Layer

The session layer deals with dialogue control, which allows the two systems to enter a half-duplex or full-duplex communication, and synchronization, which breaks a very large amount of data into checkpoints so they can be individually checked.

Presentation Layer

The presentation layer deals with data translation, data encryption and data compression.

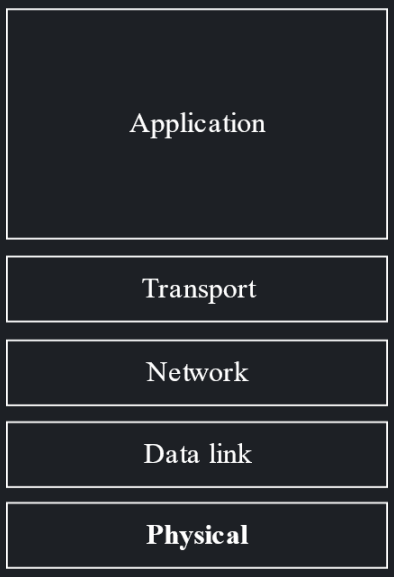
Application Layer

The application layer is the one used to interact with the network. It covers everything from e-mail to remote file access to usage of a shared database.

Layer	Uses
Application	Access network resources
Presentation	Translation, Encryption and Compression
Session	Establish, manage and terminate sessions
Transport	Provide reliable process-to-process message delivery and error recovery
Network	Move packets end-to-end
Data Link	Organize bits into frames and provide hop-to-hop delivery
Physical	Transmit bits over a medium and provide mechanical and electrical specifications

2.4 TCP/IP Protocol Suite

The only difference between the OSI model and the TCP/IP is that the Session and Presentation layers do not exist in the latter. They are part of the Application layer. Notice that we did not even discuss these two layers since they are not of much importance anyways.



In the TCP/IP protocol suite, the session, presentation and application layers are merged together to make the application layer. All the layers are similar to those in the OSI model and their functions are the same as well.

Physical and Data Link Layers

The physical and data link layers do not have any fixed protocol. Their implementation depends on the methods with which the physical connections are developed.

Network Layer

In the network layer, the dominant protocol being used is IP. IP uses four supporting protocols, ARP, RARP, ICMP and IGMP, which will be discussed later on.

Transport Layer

The transport layer has three protocols, UDP, SCTP and TCP. UDP is unreliable and SCTP is a combination of TCP and UDP.

Application Layer

In the application layer, we have a wide variety of protocols like SMTP, FTP, HTTP, DNS, SNMP, etc.

2.5 Addressing

There are four layers of addressing. Physical addressing is used in the data link and physical layers, logical addressing is used in the network layer (also called the IP layer), port addressing is used in the transport layer and specific addressing is used in the application layer.

Physical Addressing

A physical address is the address of a node as defined by its LAN or WAN, also sometimes called its MAC address. It is included in the frame used by the data link layer.

Logical Addressing

Physical addresses are not sufficient for different networks, since they may use different formats. Logical addresses, or IP addresses, use a universal format that allows each host to be identified uniquely. IP addresses are 4-bit numbers represented in decimal notation.

Physical addresses may change from hop-to-hop, but the logical address usually remains the same. Note that this simply means that the physical address given to a packet of data changes from source to destination but its logical address does not. We are not discussing the actual hosts, for which the opposite is true. The host machine's MAC address can never change, but its IP address can. We are not concerned about that for now.

IP addresses of the source and destination are added to the packet in the network layer.

Port Addressing

Port addresses are 16-bit numbers used to uniquely identify processes on a machine. For a packet of data, the port address remains the same from source to destination.

Specific Addressing

Specific addresses are used by applications. These could be things like email addresses. We will not be discussing specific addressing.