

Introduction to Computer Networking

-Aayush Tyagi

Protocol: A set of standards that computer has to follow in order to communicate properly.

Computer Networking: The name given to full scope how computer communicate with each other.

Five-layer model for networking:

- Physical layer.
- Data link layer.
- Network layer.
- Transport layer.
- Application layer.

#	Layer Name	Protocol	Protocol Data Unit	Addressing
5	Application	HTTP, SMTP, etc..	Messages	n/a
4	Transport	TCP/UDP	Segment	Port #'s
3	Network	IP	Datagram	IP address
2	Data Link	Ethernet, Wi-Fi	Frames	MAC Address
1	Physical	10 Base T, 802.11	Bits	n/a

- Physical layer: Represent the physical devices that interconnect computers, are about cabling, connectors and sending signals.
- Data link layer: Responsible for defining a common way of interpreting these signals so network devices can communicate. Most common protocol is Ethernet.
- The Ethernet standards also define a protocol responsible for getting data to nodes on the same network or link.
- Network layer: Allows different networks to communicate with each other through device known as routers. IP is the most common network layer protocol.
- Internetwork: A collection of networks connected together through routers, the most famous of these being the Internet.
- While the data link layer is responsible for getting data across a single link, the network layer is responsible for getting data delivered across a collection of networks.
- IP is the heart of the Internet and most smaller networks around the world.
- Transport layer: Sorts out which client and server programs are supposed to get that data. TCP is an example of a transport layer protocol.

- Other transfer protocols also use IP to get around, including a protocol known as User Datagram Protocol (UDP).
- TCP provides mechanisms to ensure that data is reliably delivered while UDP does not.

IP is responsible for getting data from one node to another.

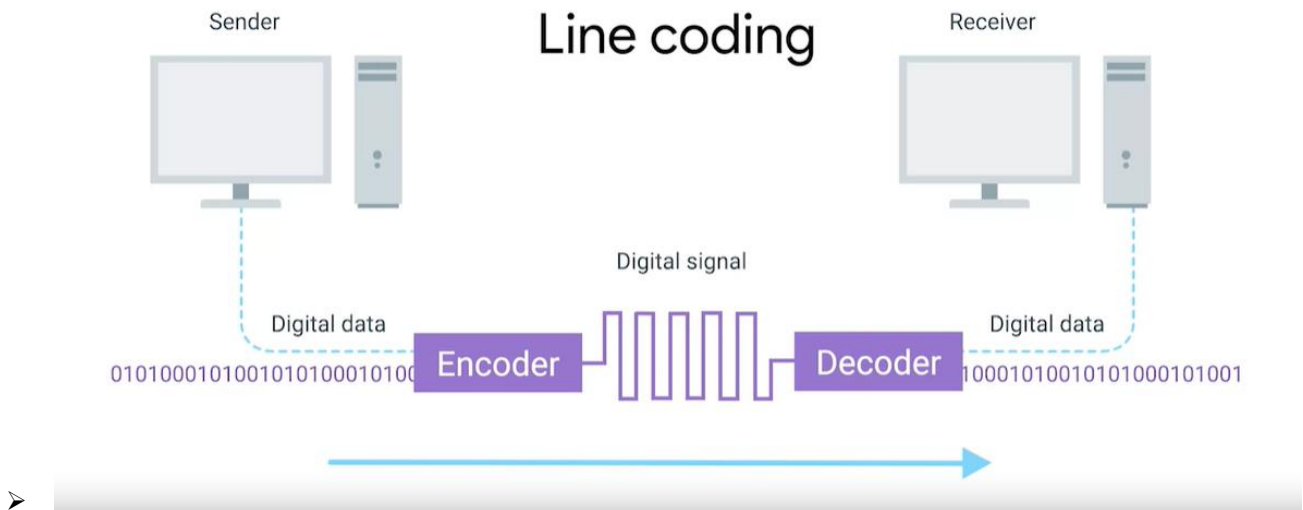
You can think of layers like different aspects of a package being delivered. The physical layer is the delivery truck and the roads. The data link layer is how the delivery trucks get from one intersection to the next over and over. The network layer identifies which roads need to be taken to get from address A to address B. The transport layer ensures that delivery driver knows how to knock on your door to tell you your package has arrived. And the application layer is the contents of the package itself.

I. The Basics of Networking Devices

- **Cables:** Connect different devices to each other, allowing data to be transmitted over them.
- Most network cables used today can be divided into two categories, **copper** and **fiber**.
- The most common form of copper twisted-pair cables used in networking are **Cat5**, **Cat5e**, and **Cat6** cables.
- **Crosstalk:** When an electrical pulse on one wire is accidentally detected on another wire.
- **Fiber cables:** Contain individual optical fibers, which are tiny tubes made out of glass about the width of a human hair. Unlike copper, which uses **electrical voltages**, fiber cables use **pulses of light** to represent the zeros and one of the data they transmit.
- **Hub:** A physical layer device that allows for connections from many computers at once.
- **Collision domain:** A network segment where only one device can communicate at a time. If multiple system try sending data at the same time, the electrical pulse sent across the cable can interfere with each other. This causes these systems to have to wait for a quiet period before they try sending their data again.
- A **switch** is very similar to a **hub** since you can connect many devices to it so they can communicate. The difference is that while a hub is a layer one or **physical layer** device, a switch is a layer two or **data link** device. This means that a switch can actually inspect the contents of the ethernet protocol data being sent around the network.
- **Hub and switches:** The primary devices used to connect on a single network, usually referred to as a **LAN**, or **local area network**.
- **Router:** A device that knows how to forward data between independent networks. Just like a **switch** can inspect Ethernet data to determine where to send things, a **router** can inspect IP data to determine where to send things.
- **Border Gateway Protocol (BGP):** Routers share data with each other via this protocol, which lets them learn about the most optimal paths to forward traffic.
- In most network topographies, each node is primarily either a server, or a client.

II. The Physical Layer

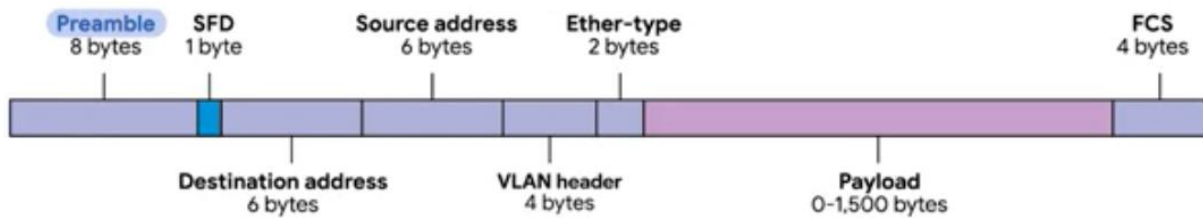
- **Bit:** The smallest representation of data that a computer can understand; it's a one or a zero.
- A standard copper network cable, once connected to devices on both ends, will carry a constant electrical charge. Ones and zeros are sent across those network cables through a process called **modulation**



- **Modulation:** A way of varying the voltage of this charge moving across the cable.
- The most common type of cabling used for connecting computing devices is known as **twisted pair**. It's called a twisted pair cable because it features pairs of copper wires that are twisted together.
- **Duplex communication:** The concept that information can flow in both directions across the cable.
- **Simplex communication:** This process is unidirectional.
- **Full duplex:** Devices on either side of a networking link can both communicate with each other at the exact same time.
- Finally they get connected at the end through RJ45 port and plug. Network ports generally attached to a device that makes up Network.

III. The Data Link Layer

- The protocol most widely used to send data across individual links is known as **Ethernet**.
- **Ethernet** and the **data link** layer provide a means for software at higher levels of the stack to send and receive data.
- If two computers were to send data across the wire at the same time, this would result in literal collisions of the electrical current representing our ones and zeros, leaving the end result unintelligible.
- Ethernet as a protocol solved this problem by using a technique known as carrier sense multiple access with collision detection.
- **CSMA/CD:** Used to determine when the communications channel are clear, and when a device is free to transmit data.
- **MAC address:** A global unique identifier attached to an individual network interface. It's a 48-bit number normally represented by six groupings of two hexadecimal numbers.
- **Hexadecimal:** A way to represent number using 16 digits.
- **Octet:** In computer networking, any number that can be represented by 8 bits.
- **Organizationally Unique Identifier (OUI):** The first three octets of a MAC address.
- If the least significant bit in the first octet of a destination address is set to **zero**, it means that ethernet frame is intended for **only the destination address**.
- If the least significant bit in the first octet of a destination address is set to **one**, it means you're dealing with a **multicast frame**.
- **Data packet:** An all-encompassing term that represents any single set of binary data being sent across a network link.
- Data packets at the Ethernet level are known as **Ethernet frames**.
- **Ethernet frame:** A highly structured collection of information presented in a specific order.



- The first part of an Ethernet frame is known as the **preamble**. A preamble is 8 bytes or 64 bits long and can itself be split into two sections.
- **Start frame delimiter (SFD)**: Signals to a receiving device that the preamble is over and that the actual frame contents will now follow.
- **Destination MAC address**: The hardware address of the intended recipient.
- **EtherType field**: 16 bits long and used to describe the protocol of the contents of the frame.
- **VLAN header**: Indicates that the frame itself is what's called VLAN frame
- If a VLAN header is present, the EtherType field follows it.
- **Virtual LAN (VLAN)**: A technique that lets you have multiple logical LANs operating on the same physical equipment.
- **Frame Check Sequence**: A 4-byte (or 32-bit) number that represents a checksum value for the entire frame.
- **Checksum value** is calculated by performing what's known as a cyclical redundancy check against the frame.
- **Cyclical Redundancy Check (CRC)**: An important concept for data integrity and is used all over computing, not just network transmissions.

