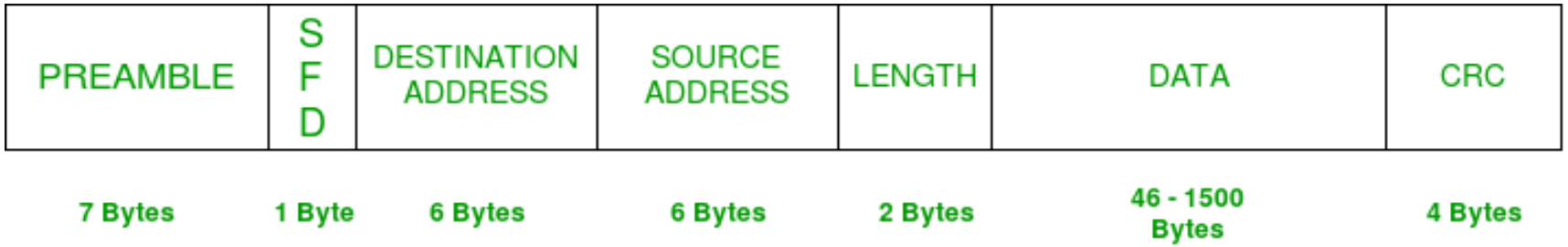
Ethernet Frame Format

- Basic frame format which is required for all MAC implementation is defined in **IEEE 802.3 standard**. Though several optional formats are being used to extend the protocol's basic capability. Ethernet frame starts with Preamble and SFD, both work at the physical layer. Ethernet header contains both the Source and Destination MAC address, after which the payload of the frame is present. The last field is CRC which is used to detect the error. Now, let's study each field of basic frame format.

- **Ethernet (IEEE 802.3) Frame Format:**
- Diagram below



IEEE 802.3 ETHERNET Frame Format

- **PREAMBLE** - Ethernet frame starts with a 7-Bytes Preamble. This is a pattern of alternative 0's and 1's which indicates starting of the frame and allow sender and receiver to establish bit synchronization. PRE (Preamble) indicates the receiver that frame is coming and allow the receiver to lock onto the data stream before the actual frame begins.
- **Start of frame delimiter (SFD)** - This is a 1-Byte field that is always set to 10101011. SFD indicates that upcoming bits are starting the frame, which is the destination address. Sometimes SFD is considered part of PRE, this is the reason Preamble is described as 8 Bytes in many places. The SFD warns station or stations that this is the last chance for synchronization.
- **Destination Address** - This is a 6-Byte field that contains the MAC address of the machine for which data is destined.
- **Source Address** - This is a 6-Byte field that contains the MAC address of the source machine. As Source Address is always an individual address (Unicast), the least significant bit of the first byte is always 0.
- **Length** - Length is a 2-Byte field, which indicates the length of the entire Ethernet frame.

- **Data** – This is the place where actual data is inserted, also known as **Payload**. Both IP header and data will be inserted here if Internet Protocol is used over Ethernet. The maximum data present may be as long as 1500 Bytes. In case data length is less than minimum length i.e. 46 bytes, then padding 0's is added to meet the minimum possible length.
- **Cyclic Redundancy Check (CRC)** – CRC is 4 Byte field. This field contains a 32-bits hash code of data, which is generated over the Destination Address, Source Address, Length, and Data field. If the checksum computed by destination is not the same as sent checksum value, data received is corrupted.

Advantages:

- **Simple format:** The Ethernet frame format is simple and easy to understand, making it easy to implement and troubleshoot Ethernet networks.
- **Flexibility:** The Ethernet frame format is flexible and can accommodate different data sizes and network topologies, making it suitable for a wide range of network applications.
- **Widely adopted:** The Ethernet frame format is widely adopted and supported by a large number of vendors and network devices, ensuring compatibility and interoperability.
- **Error detection:** The Ethernet frame format includes a cyclic redundancy check (CRC) field for error detection, which helps to ensure data integrity during transmission.
- **Support for VLANs:** The Ethernet frame format supports virtual local area networks (VLANs), which allows network administrators to logically partition a physical LAN into multiple smaller virtual LANs for improved network management and security.

Disadvantages:

- **Limited frame size:** The Ethernet frame format has a maximum frame size of 1500 bytes, which can limit the amount of data that can be transmitted in a single frame and can result in increased overhead due to fragmentation and reassembly of larger packets.
- **Broadcast storms:** Ethernet networks use broadcast transmissions to send frames to all devices on the network, which can lead to broadcast storms if too many devices send broadcast frames simultaneously, resulting in network congestion and performance issues.
- **Security vulnerabilities:** The Ethernet frame format does not include built-in security features, making Ethernet networks vulnerable to security threats such as eavesdropping and spoofing.
- **Limited speed:** Ethernet networks have a limited maximum speed, which may not be sufficient for high-speed applications or large-scale networks.
- **Limited distance:** The maximum distance between two devices on an Ethernet network is limited, which can restrict the physical coverage of the network.