Data Link Layer

- **Ethernet and MAC Addresses** :

- The Protocol most widely used to send data across individual links is known as Ethernet.

- Ethernet is Fairly old technology, It first came into being 1980 and saw its fully polished standardization in 1983.

ETHERNET :::

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 uninteligible.

Ethernet as a protocol solved this problem by using a technique known as carrier sense multiple access with collision detection.

---- We Generally abbreviate this to CSMA / CD.

CSMA / CD : Used to determine when the communications channels are clear, and when a device is free to transmit data.

CSMA / CD Works : If there’s no data currently being transmitted on the network segment, a node will feel free to send data.

- If it turns out that or more computers end up trying to send data at the same time. The Computers detect this collision and stop sending data.

- Each device involved with the collision then waits a random interval of time before trying to send data again.

- This random interval helps to prevent all the computers involved in the collision from colliding again the next time they try to transmit anything.

---- When network segment is a collision domain, it means that all devices on the segment receive all communication across the entire segment.. This means we need a way to identify which node the transmission was actually meant for..

---- This is known as Media Access Control MAC Address.

MAC Address : A Globally 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 numbers using 16 digits.

- Hexadecimal numbers employed the letters A, B, C, D, E, F to represent 10, 11, 12, 13, 14, 15.

- Another way to reference each group of numbers in a MAC address is an octet.

Octet : In Computer Networking, any number that can be represented by 8-bits.

- In this case, two hexadecimal digits can represent the same numbers that 8-bits can.

- The total number of a possible MAC addresses that could exist is 2 to the power 48.

- 281,474,976,710,656 unique possibilities.

-- A MAC Address is split into two sections :

--- The First three octets of a MAC address are known as : **Organizationally Unique Identifier (OUI)**

OUI : The first three octets of a MAC address.

-- These are assigned to individual hardware manufactures by the IEEE.. (Institute of Electrical and Electronics Engeers).

- This is a usuful bit of information to keeping your back pocket because it means that you can always identify the manufacturer of a network interface purely by its MAC Address.

--- The last three octets og MAC address can be assigned in any way that the manufacturer would like with the condition that they only assign each possible address once to keep all MAC addresses globally unique.

--- Ethernet usues MAC Addresses to ensure that the data it sends has both an address for the machine that sent the transmission, as well as the one the transmission was intended for.

In this way, even on a network segment, acting as a single collision domain, each node on that network when traffic is intended for it.

Unicast, Multicast and Broadcast

Unicast : One Device to transmit data to one other device. This is what's known as unicast.

- A Unicast transmission is always meant for just one receiving address.

At the Ethernet Level, this is done by looking at a special bit in the destination 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.

This means it would be sent to all devices on the collision domain, but only actually received and processed the intended destination.

Multicast : If the least significant bit in the first octet of a destination address is set to one, it means you are dealing with a multicast frame.

- A multicast frame is similarly set to all devices on the local network signal.

- What’s different is that it will be accepted or discarded by each device depending on criteria aside from their own hardware MAC address.

- Network interfaces can be configured to accept lists of configured multicast addresses of these sort of communication.

Broadcast : An Ethernet broadcast is sent to every single device on LAN.

- This is accomplished by using a special destination known as a broadcast address.

- The Ethernet Broadcast address is all Fs.

FF : FF : FF : FF : FF : FF

- Ethernet Broadcast are used so that devices can learn more about each other.

Dissecting an Ethernet Frame

Data Packet : An all-encompassing term that represents any single set of binary data being sent across a network link.

- The term data packet isn’t tied to any specific layer or technology. It just represents a concept.

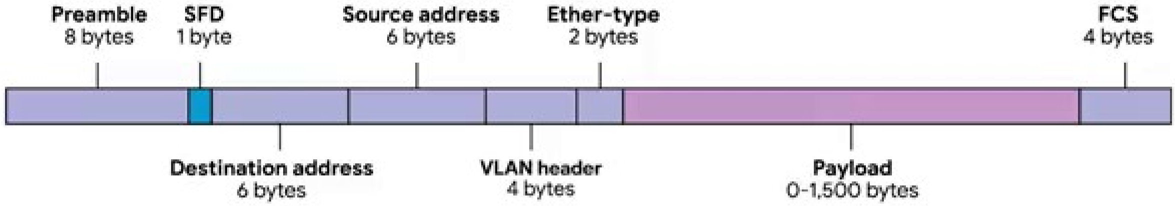
- One set of data being sent from Point – A to Point – B.

- Data Packets at the ethernet level are known as ethernet frames.

Ethernet Frame

Ethernet Frame : A highly structured collection of information presented in a specific order.

-- Almost all sections of an Ethernet frame are mandatory and most of them have fixed size.



-- The First part of an ethernet frame is known as the “Preamble”.

: **Preamble** : A Preamble is 8 bytes or 64 bits long and can itself be split into two sections.

-- The First seven bytes are a series of alternating ones and zeros.
These act partially as a buffer between frames and can also be used by the network interfaces to synchronize internal clocks they use, to regulate the speed at which they send data.

-- The Last byte in the Preamble is known as the **“SFD” (Start Frame Delimiter).**

SFD (Start Frame Delimiter) : Signals to a receiving device that the preamble is over and that the actual frame contents will now follow.

-- Immediately following the Start Frame Delimiter, comes the Destination MAC Address.

Destination MAC Address : The hardware address of the intended recipient...

-- Which is then followed by the source MAC address, or where the frame originated from.

Remember : Each MAC address is 48 bits or 6 bytes long.

EthernetType Field : It’s 16 bits long and used to describe the protocol of the contents of the frame.

-- It’s worth calling out that instead of the EthernetType field, we could also find known as VLAN header.

VLAN Frame : It indicates that the frame itself is what’s called a VLAN Frame.

- If a VLAN header is present, EtherType field follow it.

: **VLAN (Virtual LAN)** : A technique that lets you have multiple logical LANs operating on the same physical equipment.

- Any frame with a VLAN tag will only be delivered out of a switch interface configured to relay that specific tag.

- This way we can have a single physical network that operates like it’s multiple LANs.

- VLANs are usually used to segregate different forms of traffic.

Another Ethernet Frame is Data Payload :

Payload : A Payload in networking terms, is the actual data being transported, which is everything that isn’t a header.

- The data payload of a traditional ethernet frame can be anywhere from 46 to 1500 bytes long…

This contains all of the data from higher layers such as IP, transport and application layer that’s actually being transmitted.

-- Following that data we could find known as FCS (Frame Check Sequence).

FCS (Frame Check Sequence) : This is a 4 – byte (or 32 bit) number that represents a checksum value for the entire frame.

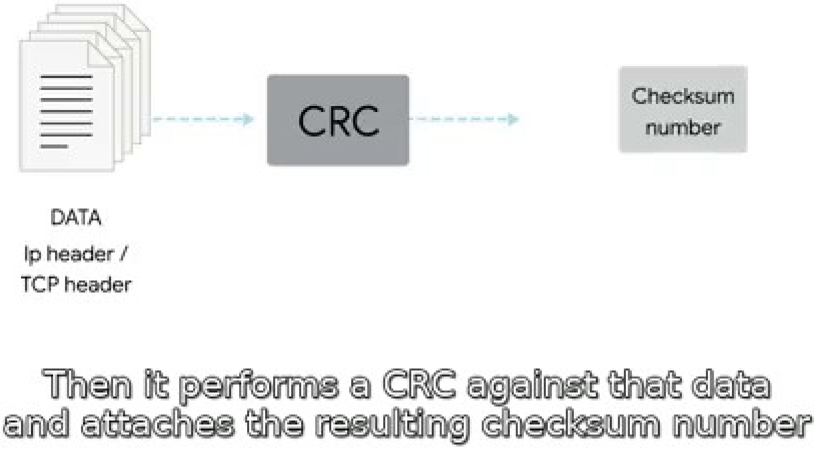
- This Checksum Value is calculated by performing what’s known as a “Cyclical Redundancy Check” against the frame.

CRC (Cyclical Redundancy Check) : An Important concept for data integrity, and is used all over computing, not just network transmissions.

- A CRC is basically a mathematical transformation that uses polynomial division to create a number that represents a large set of data.

- Anytime we perform a CRC against a set of data, you should end up with same checksum number.

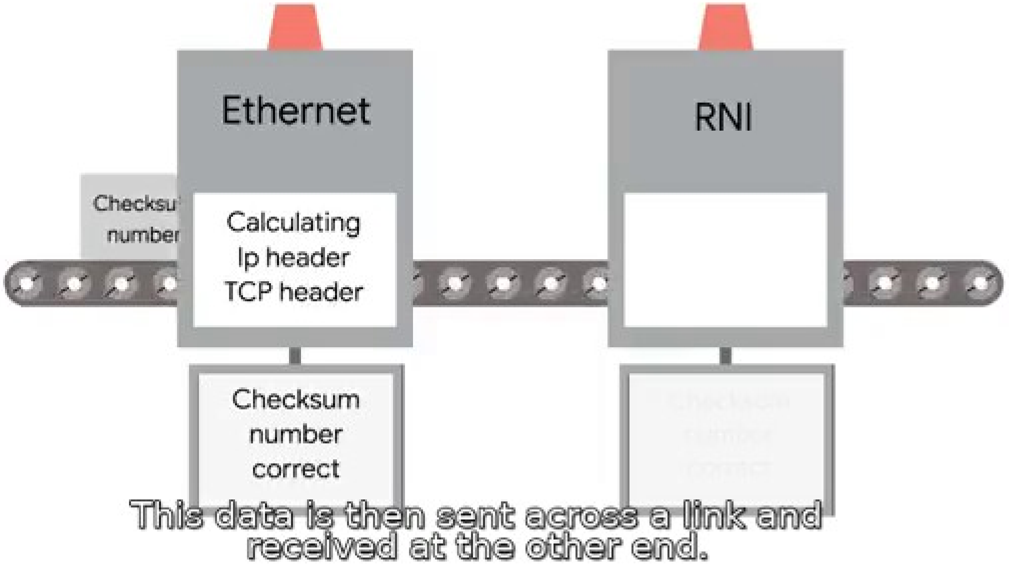
-- When a device gets ready to send an Internet frame, it collects all the information we just covered, like the destination and originating MAC addresses, the data payload and so on.



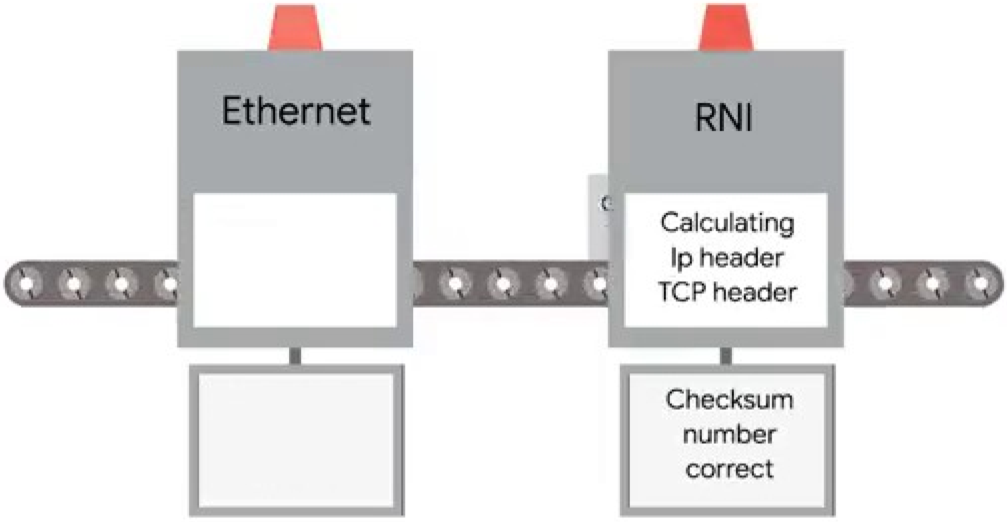
Then it performs a CRC against that data
and attaches the resulting checksum number

- Then it performs a CRC against that data and attaches the resulting checksum number as the frame check sequence at the end of the frame.

- This data is then sent across a link and received at the other end.



This data is then sent across a link and
received at the other end.



- Here, all the various fields of the Ethernet frame are collected and now the receiving side performs a CRC against that data.

- If the checksum computed by the receiving end doesn't match the checksum, in the frame check sequence field, the data is through out.

- This is because some amount of data must have been lost or corrupted during transmission.

It's then up to a protocol at a higher layer to decide if that data should be retransmitted.

-- Ethernet itself only reports on data integrity. It doesn't perform data recovery.