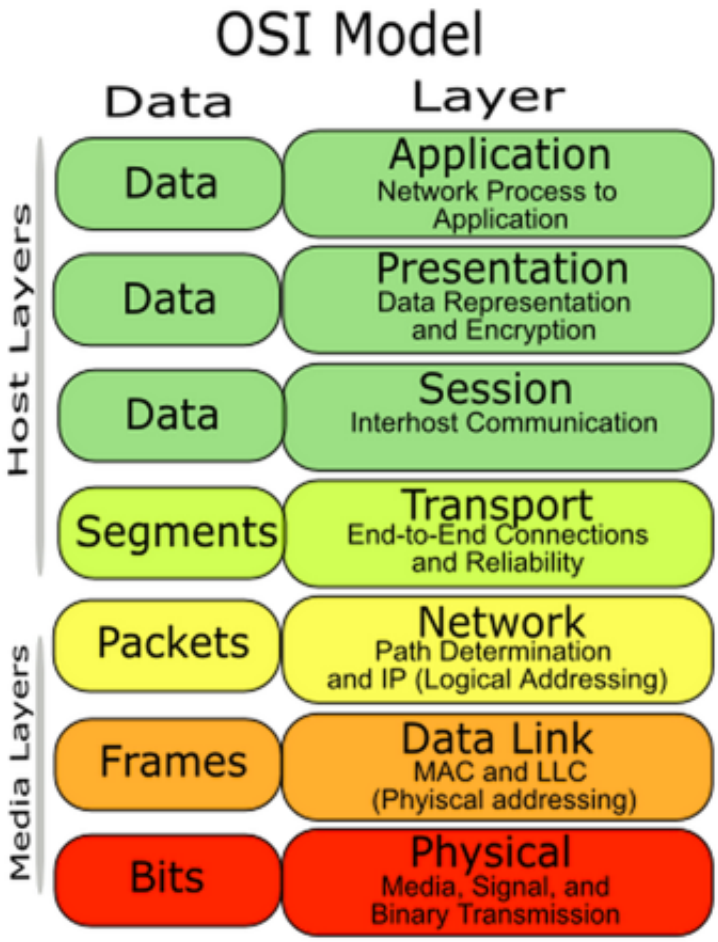
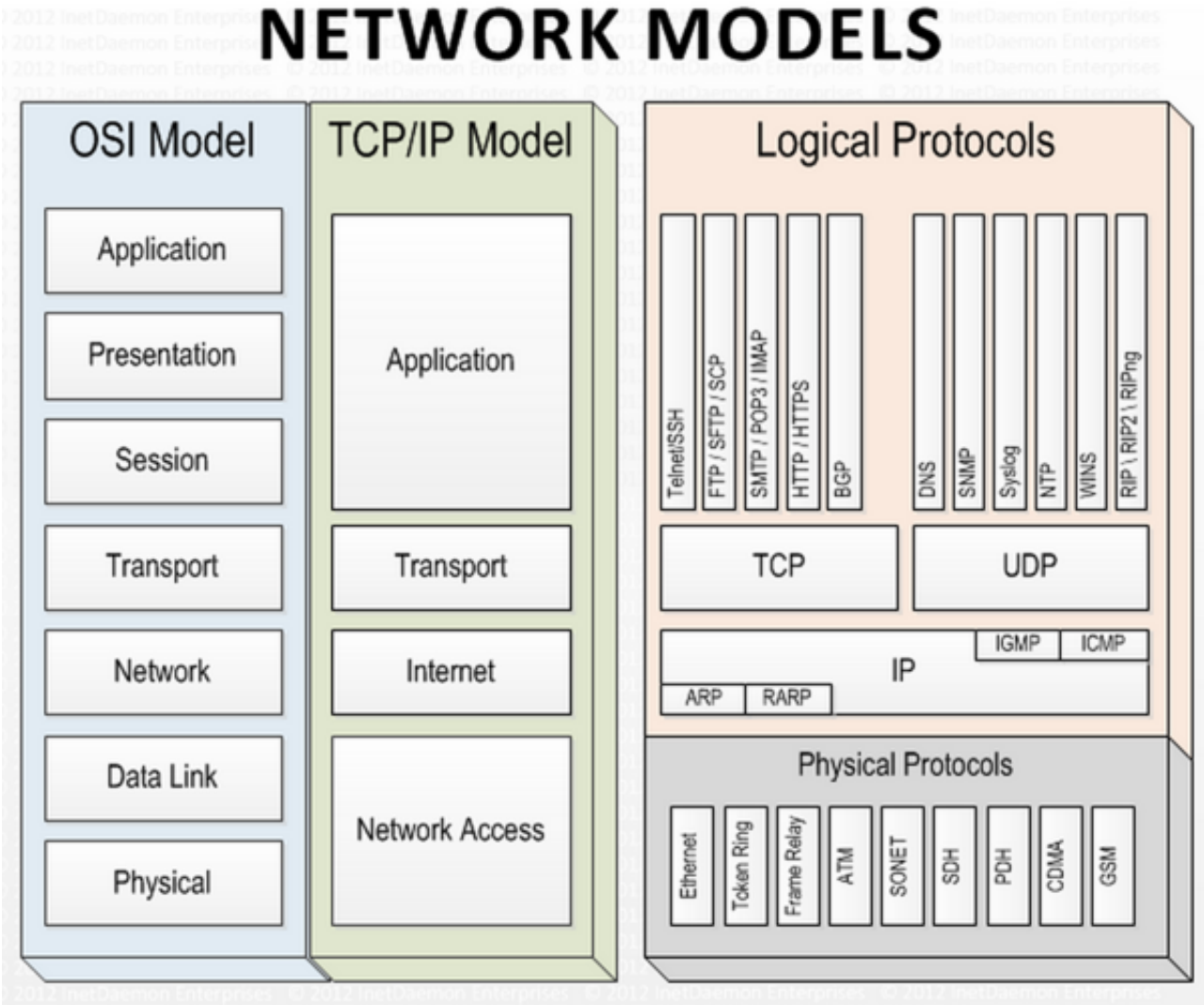
Chapter 9 - IP protocol

Take a look back at the OSI model and TCP model before this chapter.


OSI Model
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Packets
Network
Path Determination and IP (Logical Addressing)
Frames
Data Link
MAC and LLC (Phyiscal addressing)
Bits
Physical
Media, Signal, and Binary Transmission



1. ConnectionLess Operation

Connectionless communication is a data transmission method used in packet switching where a message can be sent from one end point to another without prior arrangement. **Internet Protocol (IP)** at **Network Layer** and User Datagram Protocol (UDP) at Transport Layer are connectionless protocols.

Advantages:

- **Flexible**: this is the biggest advantage of IP as the packet is not tied to any path, it can go any route.
- **Can be made robust**, i.e. can add another layer (TCP) to make a stronger structure.
- **No unecessary overhead**

2. Internet Protocol

IP is connectionless, provides a one-off bus service. All ES [1] and routers share this common network layer protocol as **Internet Protocol (IP)**. Thus all routers only need to implement up through IP (Network layer - LLC)

as they do not need to care about the content of IP datagram.

Example

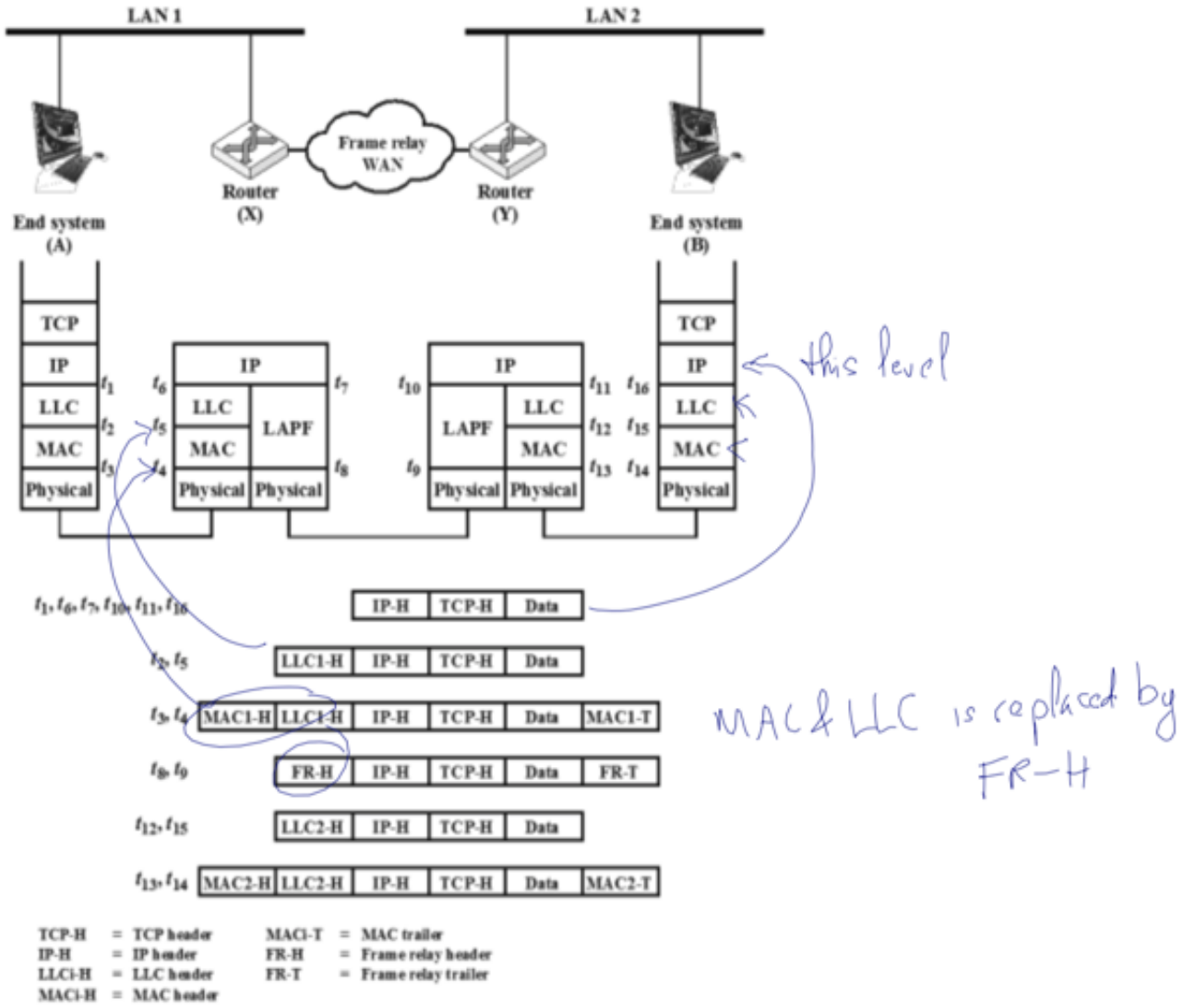


Figure 14.2 Example of Internet Protocol Operation

IP layer provides:

- Routing service for directing the packet.
- Datagram lifetime (TTL) for controlling the life/expiry of the packet.
- Fragmentation and reassembly service for data transmission.
- Error Control for error recovery.
- Flow Control for data rate and transmission control.

2.1. Routing

- IP Routing uses **routing table** to indicate the next hop to which datagram is sent to. It can be dynamic or static. Dynamic table is more flexible in dealing with error and congestion conditions.
- The technique in used is **Source Routing**, which specifies the route to be followed.

- **Route Recording**: Each time a datagram packet hops on to new router, the internet address of the router is appended to the packet's list of traverse addresses.

2.2. Datagram Lifetime (TTL)

- IP uses a field called **TTL (Time-to-live)** to indicate the datagram packet lifetime.
- TTL is initiated with an initial value called **hop count**. Each time it travels through a hop, TTL decreases 1. If TTL reaches 0 before the packet reaches destination, it will die out.

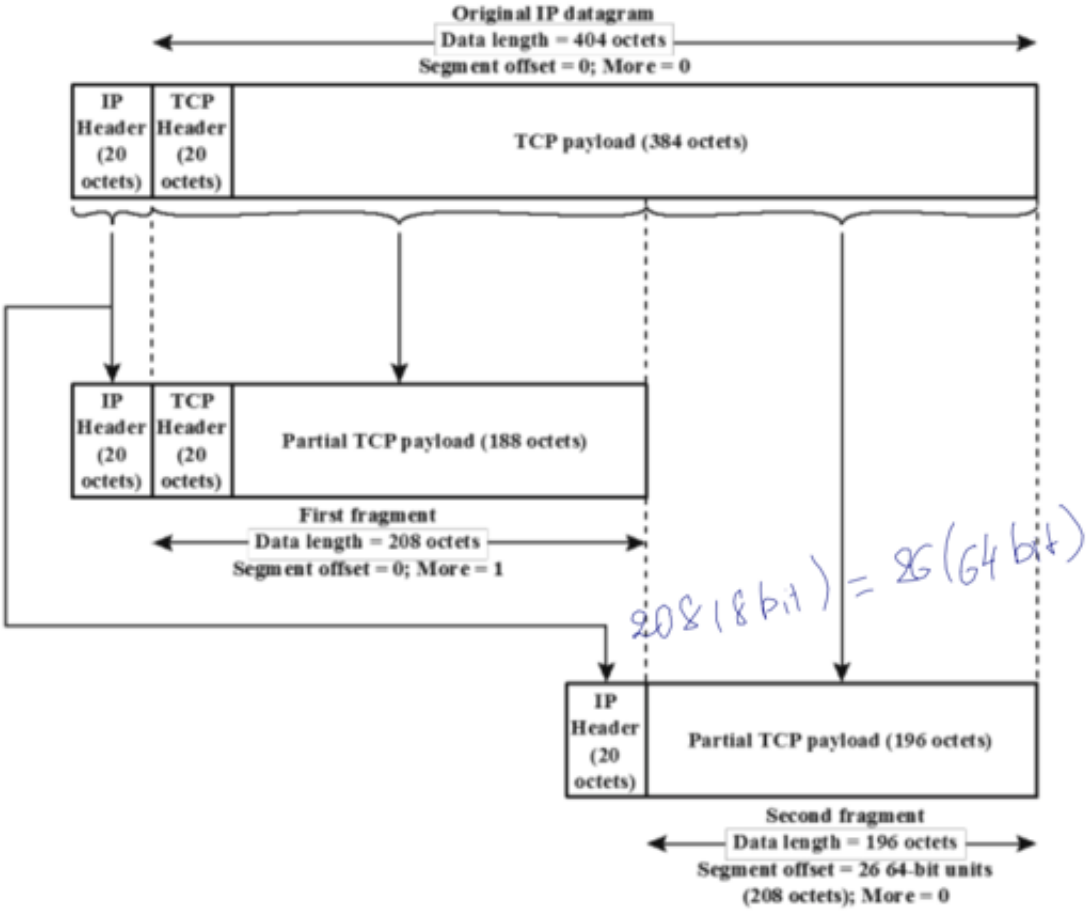
2.3. Fragmentation and Reassembly

- **Why fragmentation?** to keep the data packet to an optimal size for better transmission, error control (smaller PDU size is better), flow control (smaller buffers on routers) and fairer usage of shared facilities. The down size is more interrupts (more headers).
- Reassembly can be at intermediate node (routers) or at destination (ES). IP assembles packets at destination.
- Since IP datagrams do not come in order, IP layer provides **a sequence number** to each packet so the reassembling can be done in order.

2.3.1. IP Fragmentation

Original IP datagram is split into multiple fragments, each is a **multiple of 8 bytes**. Each fragment has the destination address, offset (position of the fragment in original datagram). Fragmentation uses these fields in the IP header:

- **Data Unit Identifier (ID)**: source address & destination address, the protocol layer that generate the data.
- **Data Length**: length of user data field (in octets-i.e. 8 bits block)
- **Offset**: position of the fragment in original datagram (in multiples of 64 bits) [2]
- **IP Flag**:
    - M: 0 (false) if no more packet following, 1 (true) if otherwise.
    - D: instruction not to fragment.



Note: 208 in octs (8 bit) is identical to 26 in 64-bit system.

2.4. Error and Flow Control

- **Error Control** is used to discard certain datagrams: expired lifetime, congestion, FCS error. Notification to source will be given in each case, except FCS (source address may be corrupted.)
- **Flow Control** is to limit the incoming rate. The target hop can send flow control packets (ICMP) to indicate its busy status & its availability (in secs) to the source. The source reset the waiting time when it receives the new availability.

2.5. IPv4

IPv4 is defined in **RFC 791**, part of the TCP/IP suite. It has **2 specifications**: specification of interface with a higher layer, and sepcification of actual protocol format and mechanism.

2.6. IP Services

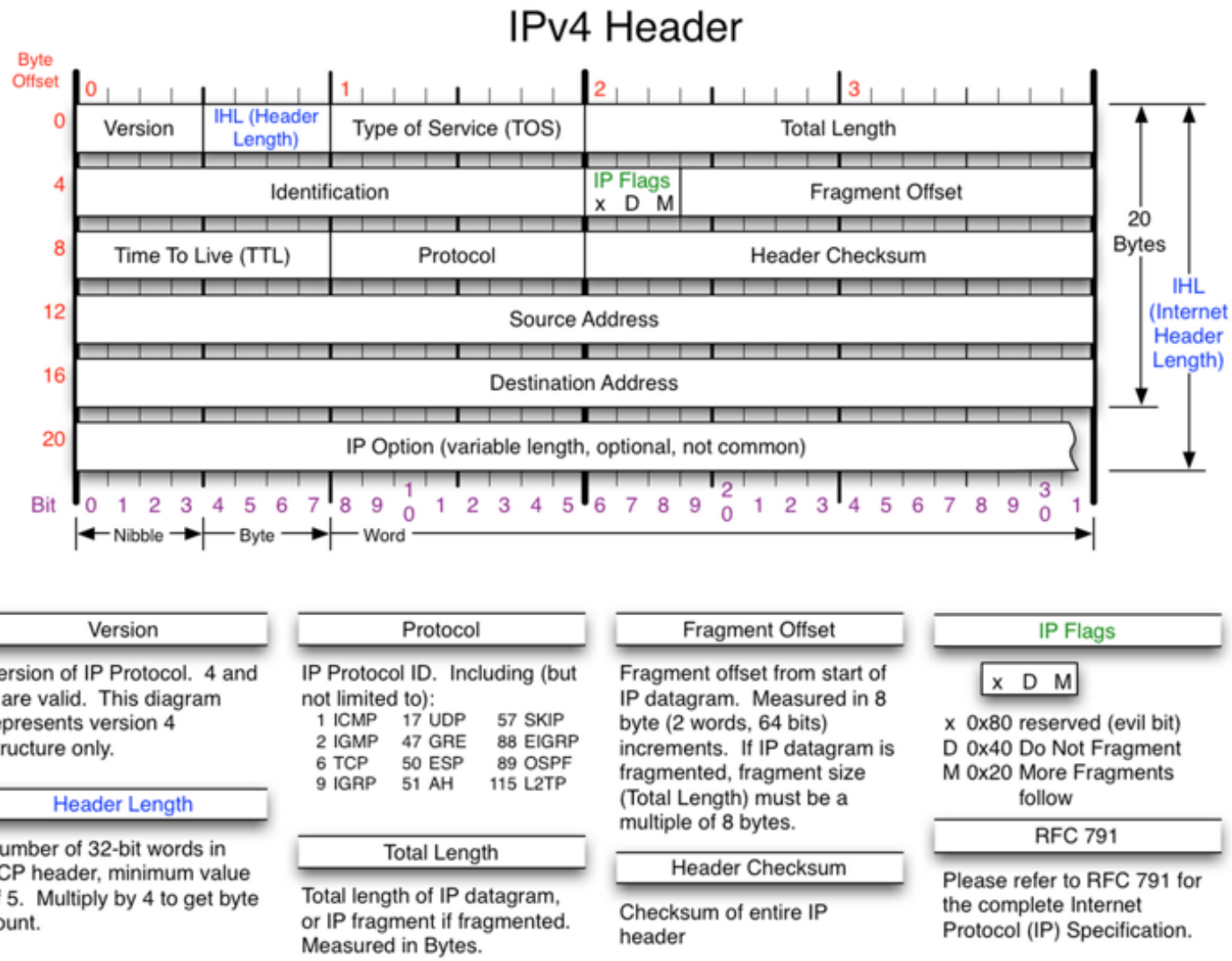
Includes its primitive implementation and functions and its parameters (data and control info passed by the sender/receiver). The parameters include (refer to the diagram for details):

- Source and dest addresses

- Protocol
- Type of Service
- Identification
- Fragment indicator (More)
- TTL
- Data Length
- Option Data
- User Data

In addition, there are IP Options: Security, Source routing, Route Recording, Stream Identification, Timestamping.

All those fields make up the IPv4 header.



Note:

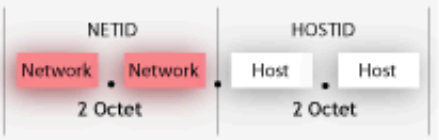
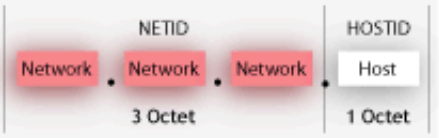
- Version (4-bit): 4
- IHL (4-bit): IP Header Length, multiple of 4 bytes.

- Total Length: total length of the packet including header, multiple of 1 byte.
- **Type of Service** is now replaced by DSCP and ECN (congestion indicator) (Wikipedia):

> - Differentiated Services Code Point (DSCP) was originally defined as the Type of service (ToS) field. This field is now defined by RFC 2474 for Differentiated services (DiffServ). New technologies are emerging that require real-time data streaming and therefore make use of the DSCP field. An example is Voice over IP (VoIP), which is used for interactive data voice exchange.
> - Explicit Congestion Notification (ECN). This field is defined in RFC 3168 and allows end-to-end notification of network congestion without dropping packets. ECN is an optional feature that is only used when both endpoints support it and are willing to use it. It is only effective when supported by the underlying network.

2.7. IPv4 Address Format

- Each IP address occupies 32-bit data length.
- Consists of the network identifier and the host identifier.
- Network identifier comes with prefix
  - Binary `0` : for class A IP address
  - Binary `10` : for class B IP address
  - Binary `110` : for class C IP address
  - Binary `1110` : for class C IP address
  - Binary `11110` : for class C IP address

CLass	First Octet Range	Default Subnet Mask	Max Hosts	Format
A	1-126	255.0.0.0	16M	
B	128-191	255.255.0.0	64K	
C	192-223	255.255.255.0	254	
D	224-239	N/A	N/A	
E	240-255	N/A	N/A	

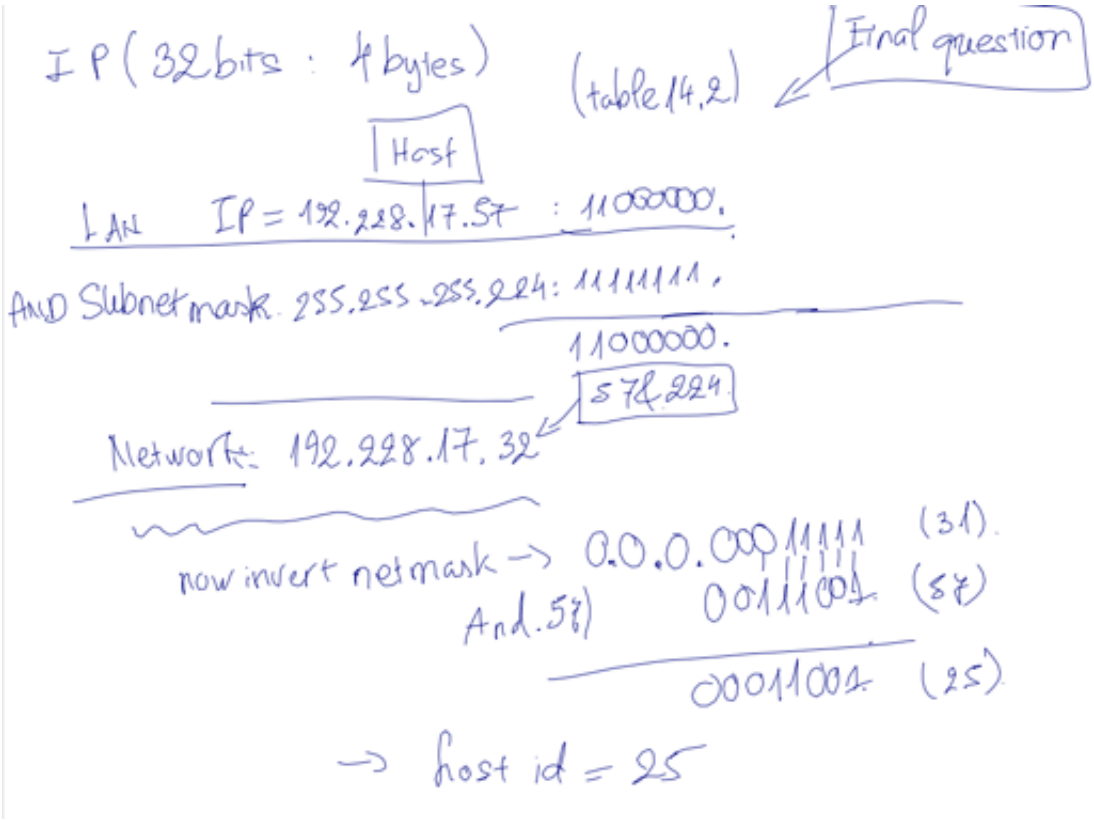
2.7.1. Calculate Network ID, Host ID base on IP Address and Netmask

Network ID:: Operate AND on the IP address and the Subnet Mask will produce the Network ID. For example:

```
192.228.17.57 AND 255.255.255.224 = 192.228.17.32
```

Host ID: Operate AND on the IP address and the bit inversion of Subnet Mask will produce the Host ID. For example:

```
192.228.17.57 AND bit-inverse(255.255.255.224) = 192.228.17.57 AND 0.0.0.31 = 25
```



3. Questions

3.1. Why we need IP address if we already have Mac Address?

3.2. Biggest advantage of IP?

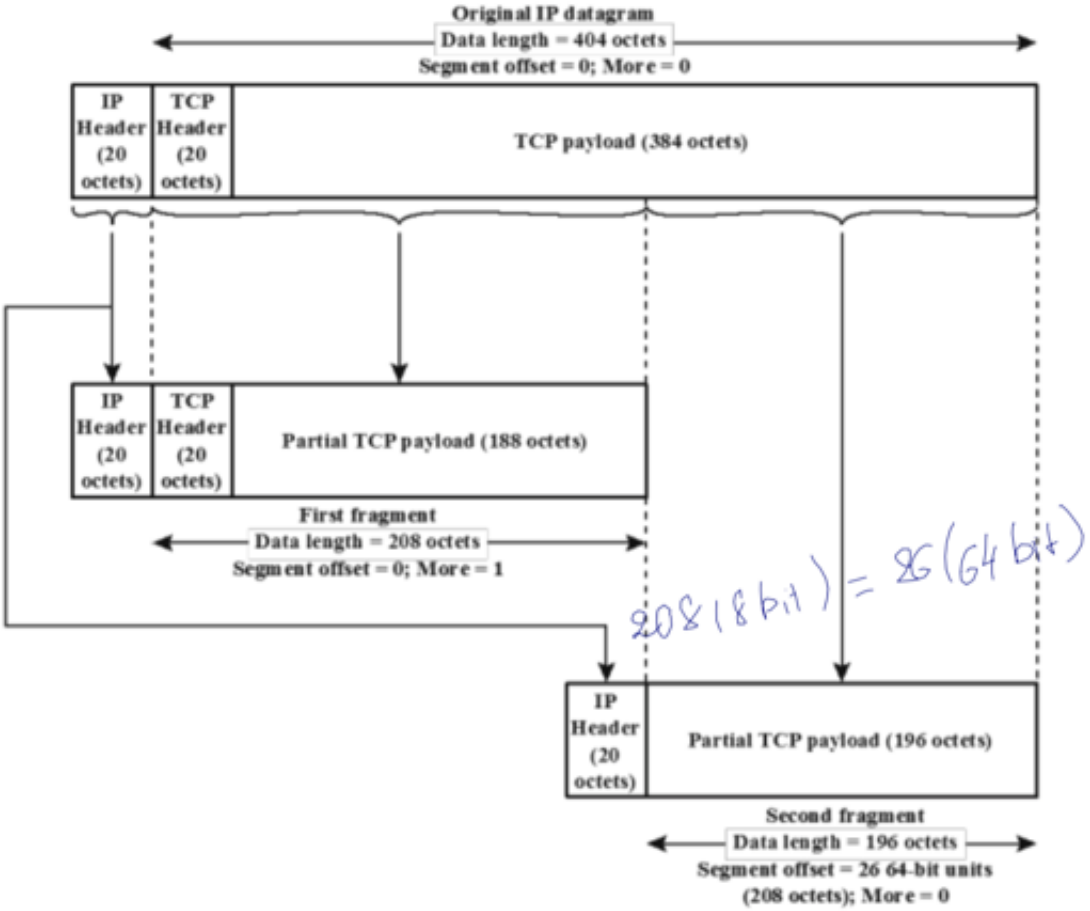
3.3. What indicates IP Datagram Life?

3.4. Which ensemble way does IP datagram use?

3.5. How does IHL measure the size of the IPv4 Header?

3.6. How does Total Length measure the size of the IPv4 data?

3.7. Calculate offset of this fragmentation.



3.8. Calculate Network ID and Host ID of IP Address and Subnet Mask

1. End System ↩
2. That's why IP fragment must be in block of 8 bytes. ↩