# CS & IT ENGINEERING

2025

## Computer Network

## IPv4 Header

By - Abhishek Sir

**Topic** Header Checksum

## Topics to be Covered

**Topic** — IPv4 Options

**Topic** — ICMP

## ABOUT ME

Hello, I'm **Abhishek**

- GATE CS AIR - 96

- M.Tech (CS) - IIT Kharagpur

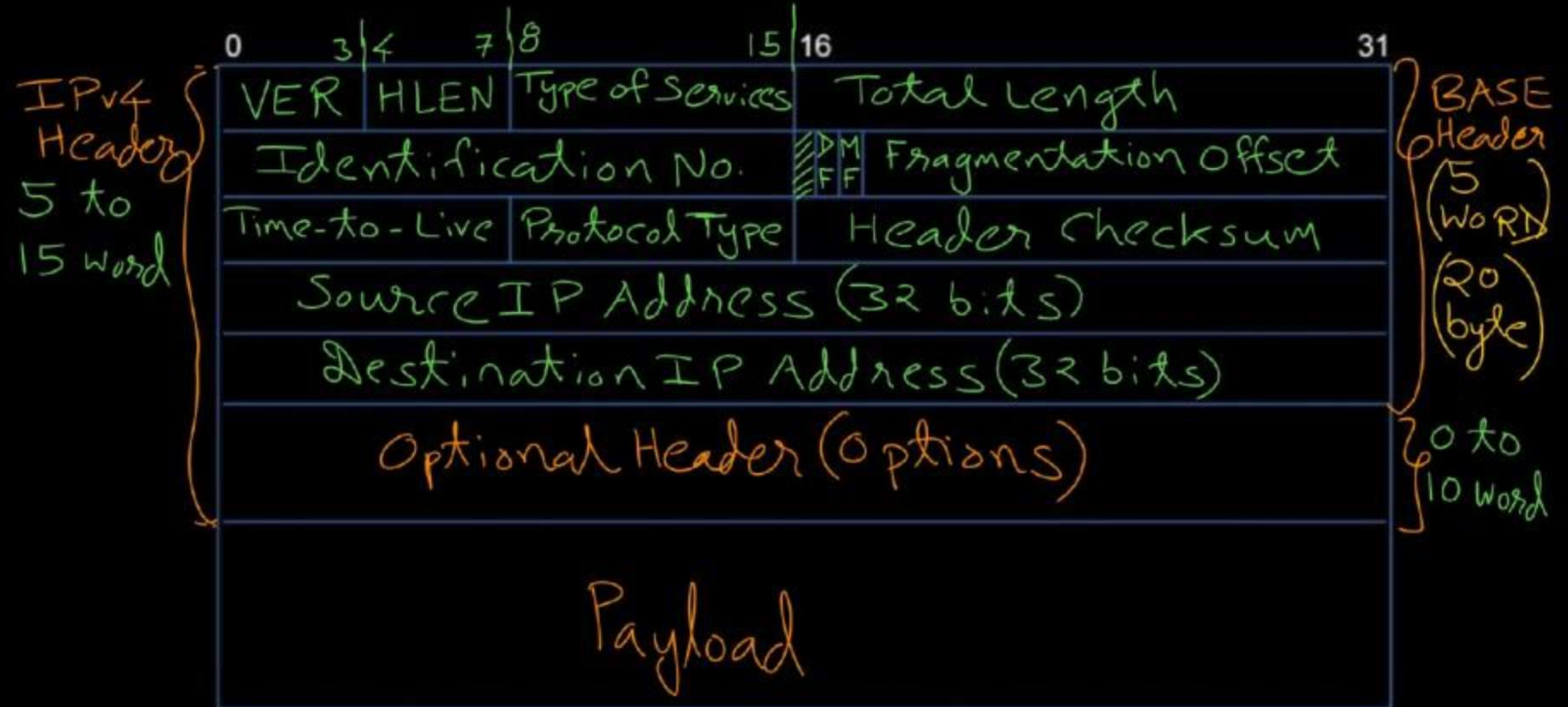- 12 years of GATE CS teaching experience

**Telegram Link :** **https://t.me/abhisheksirCS_PW**

@ABHISHEKSIRCS_PW

| | 0 3 | 4 7 | 8 15 | 16 31 |
|---|---|---|---|---|
| IPv4 Header 5 to 15 Word | VER | HLEN | Type of Services | Total Length |
| | Identification No. | | D M F F | Fragmentation Offset |
| | Time-to-Live | | Protocol Type | Header Checksum |
| | Source IP Address (32 bits) | | | |
| | Destination IP Address (32 bits) | | | |
| | Optional Header (Options) | | | |
| | Payload | | | |

BASE Header (5) (WORD) (20 byte)

0 to 10 Word

→ Checksum verification is performed at every intermediate router and destination host

→ if error is detected in IPv4 header
   (computed checksum is nonzero)
      then discards the datagram
         and no any error message is generated

→ After processing the IPv4 datagram,
   New Checksum is generated by every intermediate router, before forwarding it.

→ At intermediate Router : (for every received IPv4 datagram)

1. Verify Header Checksum,
   if error detected, discard the datagram

2. TTL = TTL – 1;   [Decrement TTL by one]
   if TTL <= 0, then discard the datagram
                and send ICMP error to source host

3. Process the datagram,
   to determine next forwarding interface

4. Update Checksum field with new generated checksum
   and forward the datagram

→ At destination host : (for every received IPv4 datagram)

1. Verify Header Checksum,
   if error detected, discard the datagram

2. TTL = TTL – 1;  [Decrement TTL by one]
   if TTL < 0, then discard the datagram
                    and send ICMP error to source host

3. Process the datagram,
   to determine higher level protocol

4. Forward the payload to higher level protocol

**#Q.** Which of the following statements is TRUE?

[GATE 2006]

(A) Both Ethernet frame and IP packet include checksum fields FALSE

(B) Ethernet frame includes a checksum field and IP packet includes a CRC field FALSE

(C) Ethernet frame includes a CRC field and IP packet includes a checksum field TRUE

(D) Both Ethernet frame and IP packet include CRC fields FALSE

Ans: C

→ Source IP Address is 32-bit field in IPv4 Header

→ Fourth word of IPv4 Header [Word size = 4 byte]

→ Assigned by source host only

→ Does not change during routing

→ May update in case of NAT device

→ Destination IP Address is 32-bit field in IPv4 Header

→ Fifth word of IPv4 Header [Word size = 4 byte]

→ Assigned by source host only

→ Does not change during routing

→ May update in case of NAT device

MSQ

#Q. Which of the following fields of an IP header is/are always modified by any router before it forwards the IP packet?

(A) Source IP Address

(B) Protocol Type

(C) Time to Live (TTL)

(D) Header Checksum

Ans: C & D

#Q. Which one of the following fields of an IP header is NOT modified by a typical IP router?

[GATE 2015, Set-1, 1-Mark]

(A) Checksum

(B) Source address

(C) Time to Live (TTL)

(D) Length

Ans: B

#Q. Host A (on TCP/IPv4 network A) sends an IP datagram D to host B (also on TCP/IPv4 network B). Assume that no error occurred during the transmission of D. When D reaches B, which of the following IP header field(s) may be different from that of the original datagram D?

(i) TTL          (ii) Checksum          (iii) Fragment Offset

[GATE 2014, Set-3, 1-Mark]

(A) (i) only

(B) (i) and (ii) only

(C) (ii) and (iii) only

(D) (i), (ii) and (iii)

#Q. In the TCP/IP protocol suite, which one of the following is NOT part of the IP header?

[GATE 2004]

(A) Fragment Offset

(B) Source IP address

(C) Destination IP address

(D) Destination port number $\Rightarrow$ TCP & UDP header

$$\boxed{Ans : D}$$

→ Also known as "Options"

→ Options are variable in size

→ Maximum size of IPv4 optional header is 10 words
[Words of 32 bits, i.e. 40 bytes]

→ if options size are not in words
than it uses padding [End-of-Option Option]

→ Options field component :-

1, Option Type    (1 byte)

2. Option Length (1 byte)

3. Option Data

HEADER

BASE Header
[5 Words]

Option Type

⟹ Options

Payload

→ Option type field are of size 8-bits

→ Option type field are divided into three sub-fields

    1. Copied         (1-bit)

    2. Option Class   (2-bits)    8 bit

    3. Option Number  (5-bits)

| Copied | Optional Class | Optional Number (5-bits) |
|--------|----------------|--------------------------|

Copied (0) : 0 to 127

Copied (1) : ~~0 to 127~~ 128 to 255

| Number | Option Type |
|:------:|:-----------:|
| 0 | End of Option [Padding] |
| 1 | No Operation |
| 7 | Record Route |
| 68 | Timestamp |
| 131 | Loose Source Route |
| 137 | Strict Source Route |

→ Option length field are of size 8-bits (1 byte)

→ Define total length of Options (in bytes)
[including option type field and option length field itself]

→ Used to record the IP address of Internet Routers
[Routers those handle the datagram along the path]

→ It can list up to "nine" router IP address

| Type = 1 00000001 | Type = 7 00000111 | Total Length = 39 00100111 | Pointer = ~~4~~ 8 00000100 |
|---|---|---|---|

12 16

First IP Address (Empty when started) Source Router IP

Second IP Address (Empty when started) $R_1$ IP

Third IP Address (Empty when started) $R_2$ IP

$9^{th}$ Last IP Address (Empty when started)

max$^m$ 9 $IP_{v4}$ Add.

Options max$^m$ $\leq 40$ byte

#Q. The maximum number of IPv4 router addresses that can be listed in the record route (RR) option field of an IPv4 header is _____ .

Ans = 9

IIT-R

→ Similar to the Record Route

→ Every router need to record the IP address and Timestamp

→ 32-bits Timestamp in milliseconds from UTC.

→ Predetermine a route for the datagram

→ Routing Path is determined by
either "Source Host" or "Centralized Server"

→ Routing Path is append in IPv4 options field by Source Host

→ Source routing are of two types :

    1. Strict Source Routing

    2. Loose Source Routing

→ Complete path from Source Router to Destination Router
  [Sequence of IP address of intermediate routers]

→ Datagram is required to follow exact defined route

→ All of the routers defined must be visited by the datagram

→ if the datagram visits a router that is not on the list
   then it discard the datagram and ICMP error message is generated

| Type = 1 | Type = 137 | Total Length = 39 | Pointer = ~~4~~ ~~8~~ 12 |
|---|---|---|---|
| 00000001 | 10001001 | 00100111 | 00000100 |

First IP Address (Filled when started) — Source Router IP

Second IP Address (Filled when started) — $R_1$ IP

Third IP Address (Filled when started) — $R_2$ IP

Last IP Address (Filled when started)

9 IP address

→ Similar to the strict source routing, but more relaxed

→ All of the routers defined must be visited by the datagram [in same order]

→ In addition, the datagram can visit other routers as well

→ Internet Control Message Protocol (ICMP)

→ To communicate network level information
[Used by Hosts and Routers]

    1. Error Reporting
      [like Unreachable Network / Host / Protocol / Port]

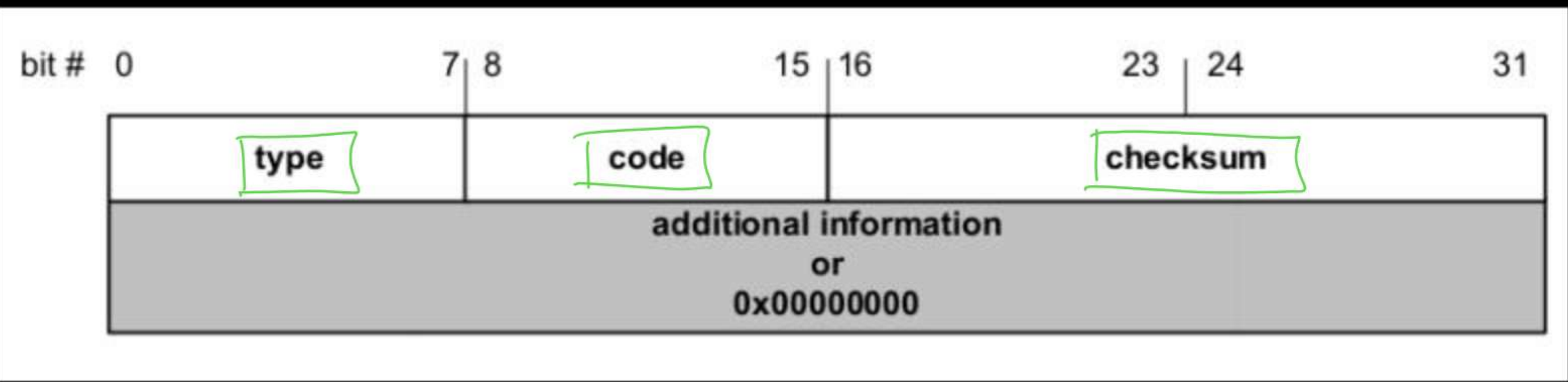    2. Echo Request / Reply
      [Used by "Ping"]

→ Network Layer Protocol

→ ICMP Messages carried in payload field of IP datagram

→ ICMP Message contains :

1. Type

2. Code

bit #  0                    7  8                    15  16                    23  24                    31

| type | code | checksum |

additional information
or
0x00000000

→ Type (1 byte) : Type of ICMP message

→ Code (1 byte) : Subtype of ICMP message

→ Checksum (2 byte) : Similar to IP header checksum
 [Checksum is calculated over entire ICMP message]

→ Each ICMP messages is at least 8 bytes long
 [If there is no additional data, 4 bytes set to zero]

(1 byte)

| Type | Description |
|------|-------------|
| 0 | Echo Reply |
| 8 | Echo Request |
| 3 | Destination Unreachable |
| 11 | Time Exceeded (TTL) |
| 30 | Traceroute |
| 4 | Source Quench |

→ ICMP error messages report error conditions

→ Whenever IP datagram is discarded at Destination Host or Intermediate Router it sent "ICMP Error Message" to Source Host

→ ICMP error messages contains complete IP header and the first 8 bytes of the IP datagram payload

| Code | Description |
|:---:|:---:|
| 0 | Network Unreachable |
| 1 | Host Unreachable |
| 2 | Protocol Unreachable |
| 3 | Port Unreachable |
| 4 | Fragmentation Required DF Flag "Set" |

#Q. A program on machine X attempts to open a UDP connection to port 5376 on a machine Y, and a TCP connection to port 8632 on machine Z. However, there are no applications listening at the corresponding ports on Y and Z. An ICMP Port Unreachable error will be generated by

[GATE 2006]

(A) Y but not Z

(B) Z but not Y

(C) Neither Y nor Z

(D) Both Y and Z

Ans: D

X

UDP

Y (UDP)
Port = 5376

$P_1 \leftarrow$ ICMP port unreachable

$K_1$

TCP

ICMP port unreachable

Z

$K_2$ TCP
Port = 8632
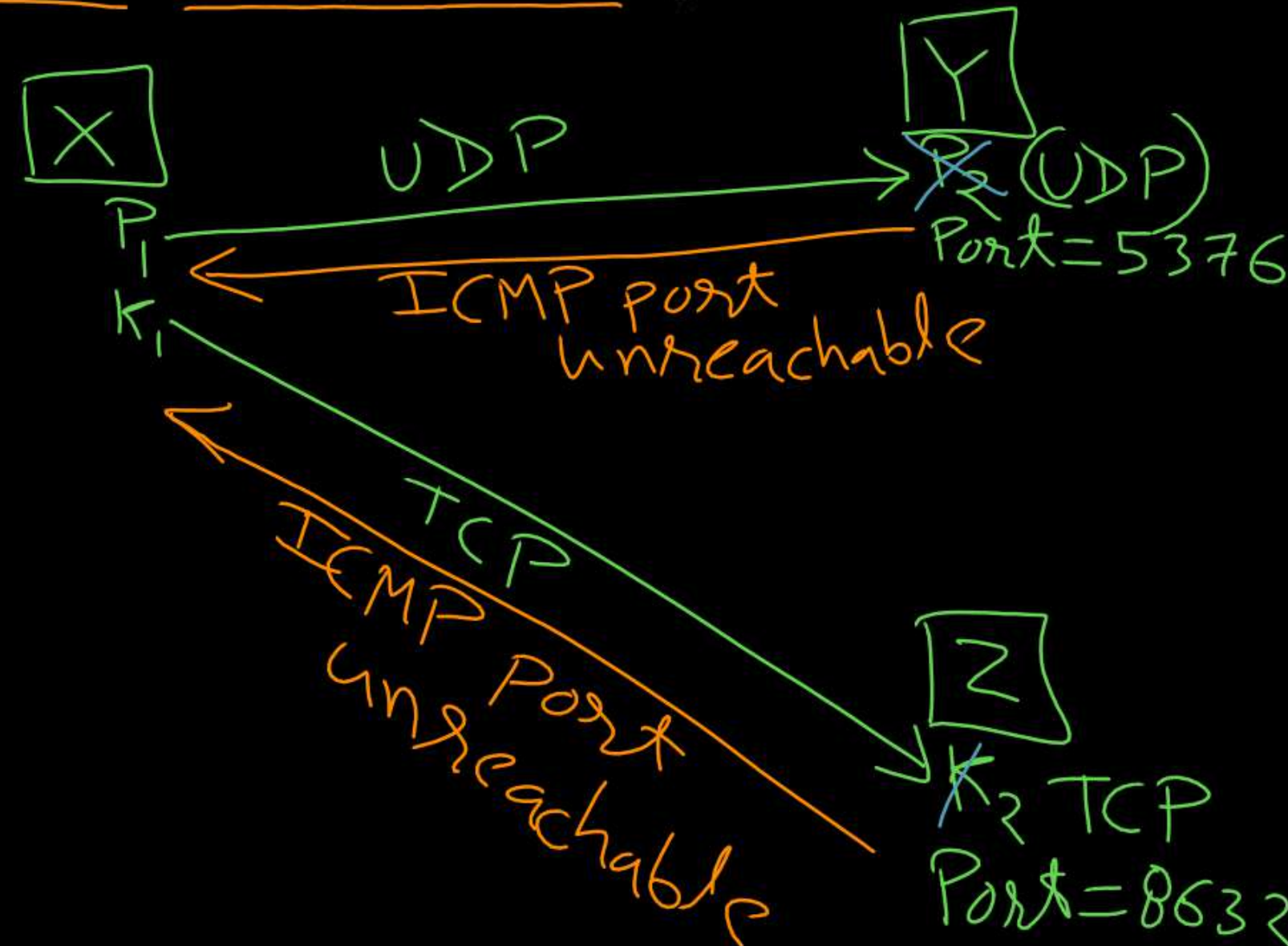
**Topic** IPv4 Options

**Topic** ICMP

THANK - YOU