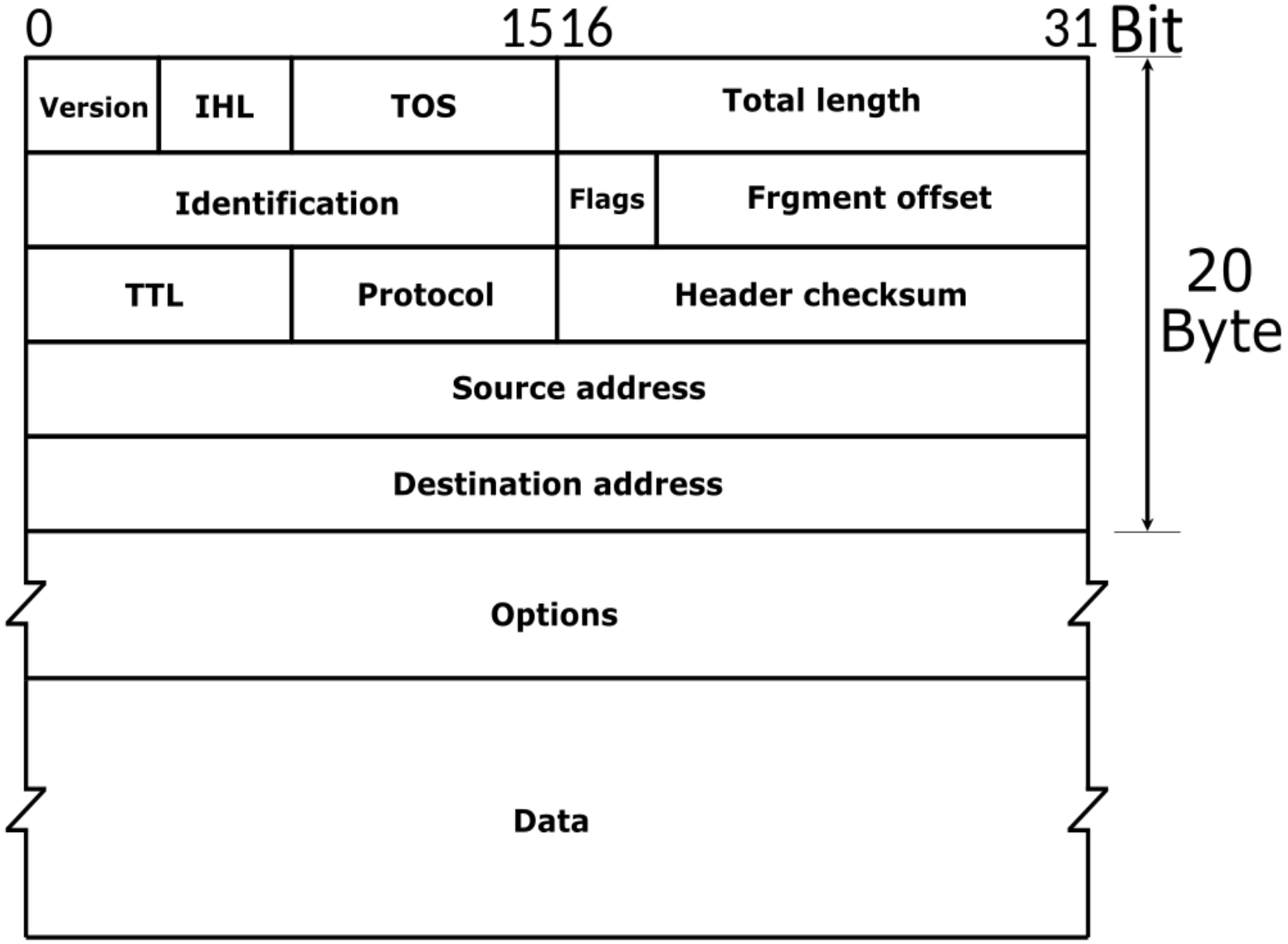
Tutorial 6: Common Questions

Objective: To answer some common questions

http://www.tcpdump.org/linktypes.html

IPv4 header length



- The IPv4 header is variable in size due to the optional field

- The length of IPv4 is determined by IHL

If the value of IHL is 5 (also the minimum value), then the length of IPv4 header is

5 × 32 bits = 160 bits = 20 bytes

The maximum value is 15, the length of the header is

15 × 32 bits = 480 bits = 60 bytes

TCP header

Similar to IPv4, the length can be determined by offset field.

TCP Header

Offsets Octet		0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port														
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved 0 0 0			NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size														
16	128	Checksum																Urgent pointer (if URG set)														
20 ...	160 ...	Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.) ...																															

- Regarding the complete TCP connections you observed:
  - the minimum, mean, and maximum time durations of the complete TCP connections
  - the minimum, mean, and maximum RTT (Round Trip Time) values of the complete TCP connections
  - the minimum, mean, and maximum number of packets (both directions) sent on the complete TCP connections
  - the minimum, mean, and maximum receive window sizes (both sides) of the complete TCP connections.

- Where it says "both directions" and "both sides", should we consider the number of packets src->dst to be separate from dst->src, or the total packets?

It’ s the total packets from both directions.

In the given basic_structures.py, there is a function called timestamp_set where we pass orig_time. What is this and how do we calculate it if need be? in get_rtt_value, we pass p. What is p

- orig_time the start time of the first packet
- p is an instance of class packet