*figure of an IP packet*

*A picture containing text, whiteboard

Description automatically generated*

1. *What are the IP addresses of your computer and the remote server?*

My computer: 192.168.86.249

Remote server: 52.114.133.166

1. *Does the Total Length field include the IP header plus IP payload, or just the IP payload?*

The Total Length field equates to the sum of the IP header and the IP payload.

1. *How does the value of the Identification field change or stay the same for different packets?* For instance, does it hold the same value for all packets in a TCP connection or does it differ for each packet? Is it the same in both directions? Can you see any pattern if the value does change?

The IP header fields are increased with every ICMP Echo request, and do not contain fields of identical value for all the packets within TCP connections. This property infers that each package will contain a different value in either direction of transmission. With each ICMP echo there will be a growth in subsequent identification fields.

1. *What is the initial value of the TTL field for packets sent from your computer? Is it the maximum possible value, or some lower value?*

Text

Description automatically generated

Initial value sent: 64

Maximum value: 128

Recommended value: 128 although some use 64

1. *How can you tell from looking at a packet that it has not been fragmented?* Most often IP packets in normal operation are not fragmented. But the receiver must have a way to be sure. Hint: you may need to read your text to confirm a guess.

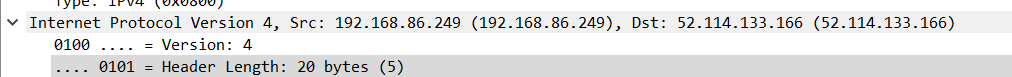
Text, letter

Description automatically generated

By identifying the flag bit of the header of the IP data packet, I was able to interpret the following:

* Reserved bit: must be 0, quite useless
* Don’t Fragment (DF): Not fragmented portion of the packet when equal to 1; 0 the contrary property
* More Fragment(MF): When equal to 0 this place holder will represent the last piece of the fragment. On the other hand when equal to 1 will contain additional pieces.

1. *What is the length of the IP Header and how is this encoded in the header length field?* Hint: notice that only 4 bits are used for this field, as the version takes up the other 4 bits of the byte. You may guess and check your text.



Length of the IP header: 20B + the length of the variable part + the length of the padding part.

The unit of the header length is fixed at 4B, which is 5\*4B = 20B.

traceroute output

Diagram

Description automatically generated

1. Divide the header into 10 two-byte (16 bit) words. Each word will be 4 hexadecimal digits shown in the packet data panel in the bottom of the Wireshark window, e.g., 05 8c
2. Add these 10 words using regular addition. You may add them with a hexadecimal calculator (Google to find one), or convert them to decimal, add them, and convert them back to hexadecimal. Do whatever is easiest.
3. To compute the 1s complement sum from your addition so far, take any leading digits (beyond the 4 digits of the word size) and add them back to the remainder. For example: 5a432 will become a432 + 5 = a437.
4. The end result should be 0xffff. This is actually zero in 1s complement form, or more precisely 0xffff is -0 (negative zero) while 0x0000 is +0 (positive zero).

Graphical user interface, text, application

Description automatically generated

4500 + 0034 + 0000 + 4000+ 3406 + e53f + 172f + 32b4 + c0a8 + 56f9 = 0xe53f