Wireshark Lab: IP

Brent Berghmans 1334252

**1. Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?**

It’s 192.168.0.198

**2. Within the IP packet header, what is the value in the upper layer protocol field?**

The value of the upper layer protocol field is ICMP.

**3. How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.**

The header has a length of 20 bytes. Because we are sending 56 bytes packets that leaves 36 bytes for the payload.

**4. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.**

The datagram is not fragmented because the value of the “Fragment offset” is zero and the “More Fragments” flag wasn’t set.

**5. Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?**

The header checksum changes and so does the identification field.

**6. Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?**

Fields that stay the same:

* Version
* Header Length
* Flags
* Protocol (ICMP)
* Source
* Destination

Fields that must stay the same:

* Version: Doesn’t really have to stay the same but it would be weird to sometimes use IPv4 and sometimes IPv6
* Header Length: Because the options do not change this should be the same for all
* Protocol: All our ping must be of ICMP
* Source: We send all our pings from the same machine
* Destination: We send all our pings to the same address

Fields that must change:

* Identification Field: Because an ID must be unique for each request
* Checksum: The checksum should change because the Identification Field changes

**7. Describe the pattern you see in the values in the Identification field of the IP datagram**

It always increments with 1.

**8. What is the value in the Identification field and the TTL field?**

Identification: 0x247c (9340)

Time To Live: 63

**9. Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?**

The Identification field changes. The TTL field stays the same.

The Identification field changes because this value needs to be unique. If it was the same that would mean it would be part of a fragmented packet. The TTL field doesn’t change because the time to live to the first hop is always the same.

**10. Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?**

Yes.

**11. Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?**

The flag 0x01 indicates “More fragments” which indicates that it has been fragmented. It is the first fragment because the “Fragment Offset” is at 0, this indicates that it is the first fragment, other fragments have a non-zero offset.

**12. Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are the more fragments? How can you tell?**

It is not the first fragment because the offset is 1480, there are no further fragments because the “More fragments” flag is set to zero.

**13. What fields change in the IP header between the first and second fragment?**

Fragment Offset, Flags, Header Checksum

**14. How many fragments were created from the original datagram?**

2 fragments.

**15. What fields change in the IP header among the fragments?**

Fragment Offset, Header Checksum.