

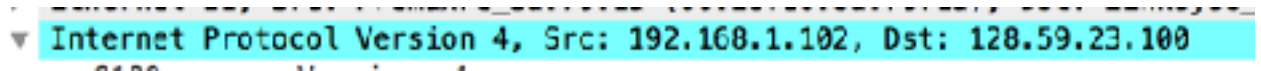
Benjamin Fondell

Introduction to Networks

November 13, 2017

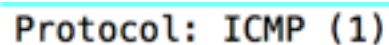
Lab 4

Note: Traceroute was not functional for my network. I will use the provided trace included with the lab. I exhausted many options to find a solution and came to the conclusion it is likely a firewall in my hardware. (router: apple time capsule , modem: zyxell z1100s, century link fiber input box.)



Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100

1. IP adress of source: 192.168.1.102



Protocol: ICMP (1)

2. Protocol: ICMP (1)

.... 0101 = Header Length: 20 bytes (5)

► Differentiated Service
Total Length: 84

3. There are 20 bytes in the IP header. The total length of is 84 bytes. Therefore 84 (total length) - 20 (header length), results in 64 bytes in the payload of the IP datagram.

Identification: 0x3200 (13000)

▼ Flags: 0x00

0... = Reserved bit: Not set

.0.. = Don't fragment: Not set

..0. = More fragments: Not set

Fragment offset: 0

4. No, the more fragments byte is not set so the datagram has not been fragmented.

5.

The identification number changes between the three datagrams associated with the trace route commands. Time to live changes as as part of the trace route program. And the header checksum changes for error detection.

6.

Constant fields:

- Header Length
- IP Version
- Source IP
- Destination IP
- Differentiated Services
- Upper Layer Protocol

Why must the following fields stay constant?:

- Header Length: Because they are all ICMP packets so they must be the same.
- IP Version: All packets must use the same version, IPv4
- Source IP: This tracks the source IP which is the same as all trace route iterations are sending from the same source.
- Destination IP: Always sending to the same destination with traceroute.
- Differentiated Services: all packets are ICMP so they must all use the same service class
- Upper Layer Protocol: All ICMP packets so all have the same upper layer protocol.

What fields must change?:

- Identification: The IP packets must be assigned different id's.
- TTL (time to live): traceroute must use different TTL for each packet as that is what finds each router at depth of the routing path.
- Header Checksum: Necessary for IP error checking and acknowledgement

```

Identification: 0x32d0 (13008)
Identification: 0x32d1 (13009)
Identification: 0x32d2 (13010)

```

7. At each Echo (ping) request the IP header identification number is incremented.

```

Identification: 0x9d7c (40316)
► Flags: 0x00
Fragment offset: 0
Time to live: 255

```

8. Identification: 40316

TTL: 255

9. In this case, Identification changes for all ICMP TTL-exceeded replies. Each identification value is unique. If they had the same identification value, that would suggest that they are fragments of a single IP datagram. The value for TTL does not change for all the responses from the first hop router because as it is the first hop router, its TTL should always be 1.

```

92 18:48:23.099003 192.168.1.102 129.20.23.100 204 514 Fragmented IP protocol (proto=ICMP 1, offset=0, ID=1289) [reassembled in #93]

```

10. Yes, the packet has been fragmented into more than one datagram.

```

▼ Flags: 0x01 (More Fragments)
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..1. .... = More fragments: Set
Fragment offset: 0
► Time to live: 1

```

11. We can tell the datagram has been fragmented because the more fragments flag is set to 1. We know this is the first segment because the offset is 0. The fragment has a total length of $1480(\text{data}) + 20(\text{header}) = 1500$ total length.

```

Internet Protocol Version 4, Src: 192.168.1.102, Dst: 128.59.23.100
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
► Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total length: 1480
Identification: 0x1219 (11349)
▼ Flags: 0x00
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..0. .... = More fragments: Not set
Fragment offset: 1480
► Time to live: 1
Protocol: ICMP (1)
Header checksum: 0x2a7a [validation disabled]
[Header checksum status: Invalid]
Source: 192.168.1.102
Destination: 128.59.23.100
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
= 12 IPv4 Fragments (2400 bytes): #92(1480), #93(1480)
► Internet Control Message Protocol

```

12. This is the second fragment. We can tell by checking the offset which is 1480. This is accurate as it is the size of the data passed in the previous datagram. There are no more fragments because the more fragments flag is set to 0.

13. The Total length, flags, fragment offset and checksum.

14. A total of 3 3 packets are created from the original datagram. This accounts for the larger byte size which must be further fragmented for to fit the maximum transmission size.

15. The feds that change for all packets are the fragment offset and the checksum. The total length and flags change between the first two packets. The last fragment has the more fragment flag set to 0 and a total length of 540. This is to account for the 3500 bytes which will require three fragments to transmit with the last fragment only partially filling the maximum transmission size.