

Xueyang (Sean) Wang
 XW1154
 04/02/2017
 CS4793
 Homework 05

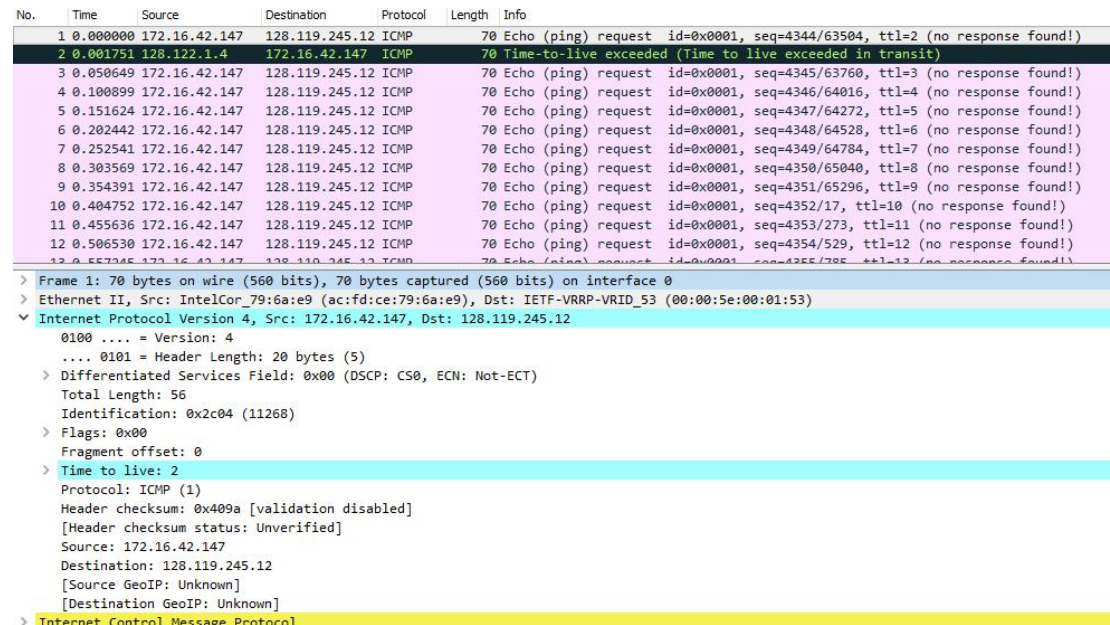


Figure 1. ICMP Echo Request Message

1. The IP address of my computer is 172.16.42.147.
2. Within the header, the value in the upper layer protocol field is ICMP (0x01)
3. There are 20 bytes in the IP header, and 56 bytes in total length. $56 - 20 = 36$ bytes in the payload of the IP data-gram.
4. The more fragments bit = 0, so the data is not fragmented.
5. Identification, time to live (TTL), and Header checksum always change.

6.

Constant across the IP datagram:

Version	IPV4
Header Length	ICMP
Source IP	Same source
Destination IP	Same destination
Differentiated Services	ICMP, same service class
Upper Layer Protocol	ICMP

Must stay constant:

Version	IPV4
Header Length	ICMP
Source IP	Same source
Destination IP	Same destination
Differentiated Services	ICMP, same service class
Upper Layer Protocol	ICMP

Must change:

Identification	IDs for IP must be different
Time to live	Traceroute increments with each packet
Header Checksum	Header changes, checksum changes as well

7. The IP header identification fields increase with each ICMP Echo(ping) request.

No.	Time	Source	Destination	Protocol	Length	Info
938	37.819s	172.16.42.147	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=4710/26130, ttl=8 (no response found!)
941	37.869s	172.16.42.147	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=4711/26386, ttl=9 (no response found!)
944	37.920s	172.16.42.147	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=4712/26642, ttl=10 (no response found!)
947	37.971s	172.16.42.147	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=4713/26898, ttl=11 (no response found!)
950	38.021s	172.16.42.147	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=4714/27154, ttl=12 (no response found!)
953	38.071s	172.16.42.147	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=4715/27410, ttl=13 (no response found!)
2	0.001751	128.122.1.4	172.16.42.147	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
19	1.120707	172.16.40.2	172.16.42.147	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
21	1.152639	128.122.1.4	172.16.42.147	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
50	2.434646	172.16.40.2	172.16.42.147	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
52	2.467585	128.122.1.4	172.16.42.147	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
70	3.652085	128.122.1.4	172.16.42.147	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
71	3.676160	172.16.40.2	172.16.42.147	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
Protocol: ICMP (1) Header checksum: 0xf8aa [validation disabled] [Header checksum status: Unverified] Source: 128.122.1.4 Destination: 172.16.42.147 [Source GeoIP: Unknown] [Destination GeoIP: Unknown]						
Internet Control Message Protocol Type: 11 (Time-to-live exceeded) Code: 0 (Time to live exceeded in transit) Checksum: 0xb6c1 [correct] [Checksum Status: Good]						
Internet Protocol Version 4, Src: 172.16.42.147, Dst: 128.119.245.12 0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 56 Identification: 0x2c04 (11268) > Flags: 0x00 Fragment offset: 0 > Time to live: 1 Protocol: ICMP (1) Header checksum: 0x419a [validation disabled] [Header checksum status: Unverified] Source: 172.16.42.147 Destination: 128.119.245.12 [Source GeoIP: Unknown] [Destination GeoIP: Unknown]						

Figure 2. ICMP TTL exceed reply

8. Identification is 11268; and time to live(TTL) is 1.

9.

The identification field changes for all the ICMP TTL exceed replies because it is a unique value. If two more IP have the same ID value, then they are fragments of a single larger IP datagram.

The TTL field remains unchanged because the TTL for the first hop router is always the same.

No.	Time	Source	Destination	Protocol	Length	Info
124	6.800763	128.119.245.12	172.16.42.147	ICMP	70	Echo (ping) reply id=0x0001, seq=4431/20241, ttl=50 (request in 123)
135	7.412761	128.119.245.12	172.16.42.147	ICMP	70	Echo (ping) reply id=0x0001, seq=4432/20497, ttl=50 (request in 134)
155	8.120690	128.119.245.12	172.16.42.147	ICMP	70	Echo (ping) reply id=0x0001, seq=4446/24081, ttl=50 (request in 154)
163	9.914580	128.119.245.12	172.16.42.147	ICMP	70	Echo (ping) reply id=0x0001, seq=4447/24337, ttl=50 (request in 162)
180	10.624s	128.119.245.12	172.16.42.147	ICMP	70	Echo (ping) reply id=0x0001, seq=4461/27921, ttl=50 (request in 179)
184	12.414s	128.119.245.12	172.16.42.147	ICMP	70	Echo (ping) reply id=0x0001, seq=4462/28177, ttl=50 (request in 183)
203	13.119s	128.119.245.12	172.16.42.147	ICMP	70	Echo (ping) reply id=0x0001, seq=4476/31761, ttl=50 (request in 200)
207	14.937s	128.119.245.12	172.16.42.147	ICMP	1514	Echo (ping) reply id=0x0001, seq=4477/32017, ttl=50 (request in 205)
239	15.623s	128.119.245.12	172.16.42.147	ICMP	1514	Echo (ping) reply id=0x0001, seq=4491/35601, ttl=50 (request in 237)
243	15.674s	128.119.245.12	172.16.42.147	ICMP	1514	Echo (ping) reply id=0x0001, seq=4492/35857, ttl=50 (request in 241)
275	16.130s	128.119.245.12	172.16.42.147	ICMP	1514	Echo (ping) reply id=0x0001, seq=4506/39441, ttl=50 (request in 273)
283	17.417s	128.119.245.12	172.16.42.147	ICMP	1514	Echo (ping) reply id=0x0001, seq=4507/39697, ttl=50 (request in 281)
215	18.132s	128.119.245.12	172.16.42.147	ICMP	1514	Echo (ping) reply id=0x0001, seq=4531/42301, ttl=50 (request in 213)
Ethernet II, Src: Cisco_bf1e:40 (58:bf:ea:bf:1e:40), Dst: IntelCor_79:6a:e9 (ac:fd:ce:79:6a:e9) Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.16.42.147 0100 = Version: 4 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) Total Length: 1500 Identification: 0x1614 (5652) > Flags: 0x01 (More Fragments) Fragment offset: 0 Time to live: 50 Protocol: ICMP (1) Header checksum: 0x00e6 [validation disabled] [Header checksum status: Unverified] Source: 128.119.245.12 Destination: 172.16.42.147 [Source GeoIP: Unknown] [Destination GeoIP: Unknown] > [2 IPv4 Fragments (1980 bytes): #207(1480), #206(500)]						
Internet Control Message Protocol Type: 0 (Echo (ping) reply) Code: 0 Checksum: 0x32e6 [correct] [Checksum Status: Good] Identifier (BE): 1 (0x0001) Identifier (LE): 256 (0x0100) Sequence number (BE): 4477 (0x117d) Sequence number (LE): 32017 (0x7d11) [Request frame: 205] [Response time: 33.108 ms]						

Figure 3. ICMP Echo Request, packet size = 2000, first

10. The message has been fragmented across more than one IP datagram.

11. The Flags is 0x01 (More Fragments), indicating that there is more. Since the offset is 0, therefore this is the first fragment in the sequence. This first datagram has a total length of 1500, including the header.

No.	Time	Source	Destination	Protocol	Length	Info
199	13.058...	172.16.42.147	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=4475/31505, ttl=13 (no response found!)
200	13.108...	172.16.42.147	128.119.245.12	ICMP	70	Echo (ping) request id=0x0001, seq=4476/31761, ttl=14 (reply in 203)
203	13.119...	128.119.245.12	172.16.42.147	ICMP	70	Echo (ping) reply id=0x0001, seq=4476/31761, ttl=50 (request in 200)
205	14.904...	172.16.42.147	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=4477/32017, ttl=255 (reply in 207)
207	14.937...	128.119.245.12	172.16.42.147	ICMP	1514	Echo (ping) reply id=0x0001, seq=4477/32017, ttl=50 (request in 205)
209	14.954...	172.16.42.147	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=4478/32273, ttl=1 (no response found!)
210	14.958...	172.16.40.2	172.16.42.147	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
212	15.005...	172.16.42.147	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=4479/32529, ttl=2 (no response found!)
213	15.007...	128.122.1.4	172.16.42.147	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
215	15.056...	172.16.42.147	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=4480/32785, ttl=3 (no response found!)
217	15.106...	172.16.42.147	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=4481/33041, ttl=4 (no response found!)
219	15.156...	172.16.42.147	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=4482/33297, ttl=5 (no response found!)
221	15.203...	172.16.42.147	128.119.245.12	ICMP	534	Echo (ping) request id=0x0001, seq=4483/33553, ttl=6 (no response found!)
> Frame 205: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface 0 > Ethernet II, Src: IntelCor_79:6a:e9 (ac:fd:ce:79:6a:e9), Dst: IETF_VRRP-VRID_53 (00:00:5e:00:01:53) > Internet Protocol Version 4, Src: 172.16.42.147, Dst: 128.119.245.12 > 0100 = Version: 4 > 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) > Total Length: 520 > Identification: 0x2c89 (11401) > Flags: 0x00 > Fragment offset: 1480 > Time to live: 255 > Protocol: ICMP (1) > Header checksum: 0x408b [validation disabled] > [Header checksum status: Unverified] > Source: 172.16.42.147 > Destination: 128.119.245.12 > [Source GeoIP: Unknown] > [Destination GeoIP: Unknown] > [2 IPv4 Fragments (1980 bytes): #204(1480), #205(500)] > Internet Control Message Protocol > Type: 8 (Echo (ping) request) > Code: 0 > Checksum: 0x2ac6 [correct] > [Checksum Status: Good] > Identifier (BE): 1 (0x0001) > Identifier (LE): 256 (0x0100) > Sequence number (BE): 4477 (0x117d) > Sequence number (LE): 32017 (0x7d11)						

Figure 4. ICMP Echo Request packet size = 2000, second

12. The fragment offset is 1480,so this is not the first fragment. And there is no more fragment flag, therefore, this is the last fragment.
13. The IP header fields that changed are: total length, flags, fragment offset, and checksum.

No.	Time	Source	Destination	Protocol	Length	Info
831	1.006362	172.18.47.57	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=17611/52036, ttl=9 (no response found!)
853	1.038792	172.18.47.57	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=17612/52292, ttl=10 (no response found!)
879	1.070990	172.18.47.57	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=17613/52548, ttl=11 (no response found!)
910	1.103497	172.18.47.57	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=17614/52804, ttl=12 (no response found!)
919	1.136628	172.18.47.57	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=17615/53060, ttl=13 (no response found!)
922	1.169717	172.18.47.57	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=17616/53316, ttl=14 (reply in 925)
925	1.184926	128.119.245.12	172.18.47.57	ICMP	1514	Echo (ping) reply id=0x0001, seq=17616/53316, ttl=50 (request in 922)
928	1.203692	172.18.47.57	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=17617/53572, ttl=255 (reply in 931)
931	1.219677	128.119.245.12	172.18.47.57	ICMP	1514	Echo (ping) reply id=0x0001, seq=17617/53572, ttl=50 (request in 928)
934	1.253690	172.18.47.57	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=17618/53828, ttl=1 (no response found!)
935	1.267543	172.18.40.2	172.18.47.57	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
939	1.304628	172.18.47.57	128.119.245.12	ICMP	554	Echo (ping) request id=0x0001, seq=17619/54084, ttl=2 (no response found!)
> Frame 925: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0 > Ethernet II, Src: Cisco-bf:fe:40 (58:bf:fe:40), Dst: IntelCor_79:6a:e9 (ac:fd:ce:79:6a:e9) > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 172.18.47.57 > 0100 = Version: 4 > 0101 = Header Length: 20 bytes (5) > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT) > Total Length: 1500 > Identification: 0xaf3c (44860) > Flags: 0x01 (More Fragments) > Fragment offset: 1480 > Time to live: 50 > Protocol: ICMP (1) > Header checksum: 0x625c [validation disabled] > [Header checksum status: Unverified] > Source: 128.119.245.12 > Destination: 172.18.47.57 > [Source GeoIP: Unknown] > [Destination GeoIP: Unknown] > [3 IPv4 Fragments (3480 bytes): #924(1480), #925(1480), #923(520)] > Internet Control Message Protocol > Type: 0 (Echo (ping) reply) > Code: 0 > Checksum: 0xe154 [correct] > [Checksum Status: Good] > Identifier (BE): 1 (0x0001)						

Figure 5. ICMP Echo Request packet size = 3500, first

14. There are three packets(fragments) after switching to 3500.
15. The changes are: fragment offset and checksum. A change in total length and in the flags when looking at the first two packets and the last packet. The first two have 1500, and the last one have 540, including header, with the more fragment bit set to 0 at the end.