Derya Tınmaz - 2380947

Wireshark Lab: ICMP

icmp

No.	Time	Source	Destination	Protocol	Length	Info
945	5.169128	144.122.149.172	8.8.8.8	ICMP	98	Echo (ping) request id=0xcc5e, seq=0/0, ttl=64 (reply in 946)
946	5.190355	8.8.8.8	144.122.149.172	ICMP	98	Echo (ping) reply id=0xcc5e, seq=0/0, ttl=248 (request in 945)
1059	6.174462	144.122.149.172	8.8.8.8	ICMP	98	Echo (ping) request id=0xcc5e, seq=1/256, ttl=64 (reply in 1060)
1060	6.195691	8.8.8.8	144.122.149.172	ICMP	98	Echo (ping) reply id=0xcc5e, seq=1/256, ttl=248 (request in 1059)
1175	7.175185	144.122.149.172	8.8.8.8	ICMP	98	Echo (ping) request id=0xcc5e, seq=2/512, ttl=64 (reply in 1176)
1176	7.195682	8.8.8.8	144.122.149.172	ICMP	98	Echo (ping) reply id=0xcc5e, seq=2/512, ttl=248 (request in 1175)
1279	8.175458	144.122.149.172	8.8.8.8	ICMP	98	Echo (ping) request id=0xcc5e, seq=3/768, ttl=64 (reply in 1298)
1298	8.197631	8.8.8.8	144.122.149.172	ICMP	98	Echo (ping) reply id=0xcc5e, seq=3/768, ttl=248 (request in 1279)
1414	9.175830	144.122.149.172	8.8.8.8	ICMP	98	Echo (ping) request id=0xcc5e, seq=4/1024, ttl=64 (reply in 1415)
1415	9.198425	8.8.8.8	144.122.149.172	ICMP	98	Echo (ping) reply id=0xcc5e, seq=4/1024, ttl=248 (request in 1414)
1532	10.1811…	144.122.149.172	8.8.8.8	ICMP	98	Echo (ping) request id=0xcc5e, seq=5/1280, ttl=64 (reply in 1533)
1533	10.2018…	8.8.8.8	144.122.149.172	ICMP	98	Echo (ping) reply id=0xcc5e, seq=5/1280, ttl=248 (request in 1532)
1651	11.1865…	144.122.149.172	8.8.8.8	ICMP	98	Echo (ping) request id=0xcc5e, seq=6/1536, ttl=64 (reply in 1652)
1652	11.2080…	8.8.8.8	144.122.149.172	ICMP	98	Echo (ping) reply id=0xcc5e, seq=6/1536, ttl=248 (request in 1651)
1770	12.1866…	144.122.149.172	8.8.8.8	ICMP	98	Echo (ping) request id=0xcc5e, seq=7/1792, ttl=64 (reply in 1775)
1775	12.2074…	8.8.8.8	144.122.149.172	ICMP	98	Echo (ping) reply id=0xcc5e, seq=7/1792, ttl=248 (request in 1770)
1948	13.1920…	144.122.149.172	8.8.8.8	ICMP	98	Echo (ping) request id=0xcc5e, seq=8/2048, ttl=64 (reply in 1974)
1974	13.2150…	8.8.8.8	144.122.149.172	ICMP	98	Echo (ping) reply id=0xcc5e, seq=8/2048, ttl=248 (request in 1948)
2083	14.1973…	144.122.149.172	8.8.8.8	ICMP	98	Echo (ping) request id=0xcc5e, seq=9/2304, ttl=64 (reply in 2084)
2084	14.2177…	8.8.8.8	144.122.149.172	ICMP	98	Echo (ping) reply id=0xcc5e, seq=9/2304, ttl=248 (request in 2083)

```
deryatinmaz@95ac ~ % ping -c 10 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=248 time=21.358 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=248 time=21.438 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=248 time=20.728 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=248 time=22.421 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=248 time=22.862 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=248 time=20.889 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=248 time=21.790 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=248 time=20.958 ms
64 bytes from 8.8.8.8: icmp_seq=8 ttl=248 time=23.206 ms
64 bytes from 8.8.8.8: icmp_seq=9 ttl=248 time=20.624 ms

--- 8.8.8.8 ping statistics ---
10 packets transmitted, 10 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 20.624/21.627/23.206/0.871 ms
```

```
deryatinmaz@95ac ~ % ip route
default via 144.122.148.1 dev en0
127.0.0.0/8 via 127.0.0.1 dev lo0
127.0.0.1/32 via 127.0.0.1 dev lo0
144.122.148.0/22 dev en0  scope link
144.122.148.1/32 dev en0  scope link
144.122.149.172/32 dev en0  scope link
169.254.0.0/16 dev en0  scope link
224.0.0.0/4 dev en0  scope link
255.255.255.255/32 dev en0  scope link
```

```
> Frame 945: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: Apple_23:4c:62 (94:f6:d6:23:4c:62), Dst: Intel_d2:46:ed (00:1b:21:d2:46:ed)
> Internet Protocol Version 4, Src: 144.122.149.172, Dst: 8.8.8.8
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4513 [correct]
    [Checksum Status: Good]
    Identifier (BE): 52318 (0xcc5e)
    Identifier (LE): 24268 (0x5ecc)
    Sequence Number (BE): 0 (0x0000)
    Sequence Number (LE): 0 (0x0000)
    [Response frame: 946]
    Timestamp from icmp data: Dec 17, 2023 21:40:17.152952000 +03
    [Timestamp from icmp data (relative): 0.000065000 seconds]
    > Data (48 bytes)
```

```
> Frame 946: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: Intel_d2:46:ed (00:1b:21:d2:46:ed), Dst: Apple_23:4c:62 (94:f6:d6:23:4c:62)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 144.122.149.172
v Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x4d13 [correct]
    [Checksum Status: Good]
    Identifier (BE): 52318 (0xcc5e)
    Identifier (LE): 24268 (0x5ecc)
    Sequence Number (BE): 0 (0x0000)
    Sequence Number (LE): 0 (0x0000)
    [Request frame: 945]
    [Response time: 21.227 ms]
    Timestamp from icmp data: Dec 17, 2023 21:40:17.152952000 +03
    [Timestamp from icmp data (relative): 0.021292000 seconds]
    > Data (48 bytes)
```

1- Request packets' source address: 144.122.149.172, destination address: 8.8.8.8
Reply packets' source address:8.8.8.8, destination address: 144.122.149.172

2- There is no port information in the packets, because ICMP packets were designed for network-layer communication between hosts and routers, excluding the need for source and destination port numbers unlike in application layer processes. Each ICMP packet is distinguished by a type and a code, collectively specifying the received message. The interpretation of ICMP messages by network software directly eliminates the requirement for port numbers to direct the message to an application layer process.

3- Type: 8 (Echo (ping) request) Code: 0
Type: 0 (Echo (ping) reply) Code: 0
3.a- The type parameter dictates the intended purpose or function of the ICMP packet. The table can be seen here.
https://networkdirection.net/articles/network-theory/icmptypes/#:~:text=The%204%2Dbyte%20ICMP%20header,field%20is%20set%20to%20zero.
3.b- The code field serves the purpose of identifying the specific error that has been triggered among the mentioned errors. The table can be seen here.
https://networkdirection.net/articles/network-theory/icmptypes/#:~:text=The%20code%20field%20is%20used,these%20errors%20has%20been%20raised.&text=When%20a%20packet%20is%20sent,the%20IP%20header%20is%20set.
3.c- Type 8 in request is Echo, type 0 in reply is Echo Reply. Code 0 in both request and reply packets indicates time to live exceeded in transit, means that a data packet, in its journey toward the destination, has traversed an excessive number of routers, leading to its discard.

4- header 20 bytes + data 48 bytes = 68 bytes per request packet
68 bytes * 10 request packets = 680 bytes in total
header includes source, destination addresses, time-to-live, protocol information..
data part include type(specifies the type of ICMP message), code(provides additional information or context for the ICMP type), checksum (used for error-checking the header and data), identifiers (helps match responses to the originating request), sequence numbers(for tracking messages), time stamps..

5- To block outgoing ping requests from my machine to IP address 8.8.8.8, I should remove the rule:
default via 144.122.148.1 dev en0
This rule specifies the default gateway for outbound traffic. By removing this rule, my machine won't have a default route to forward packets to destinations outside the local network (144.122.148.0/22). Without a default route, the machine won't know how to reach external networks, including the internet.

As a result, when the machine attempts to send ping requests to 8.8.8.8, it won't have a route to the destination, and the packets will be dropped. Removing the default gateway essentially isolates the machine from the external network, preventing it from sending requests to destinations beyond the local network.

6.a- Source: Apple_23:4c:62 (94:f6:d6:23:4c:62)
6.b- Destination: Intel_d2:46:ed (00:1b:21:d2:46:ed), it belongs to Intel machine

```
> Frame 945: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
v Ethernet II, Src: Apple_23:4c:62 (94:f6:d6:23:4c:62), Dst: Intel_d2:46:ed (00:1b:21:d2:46:ed)
  > Destination: Intel_d2:46:ed (00:1b:21:d2:46:ed)
  > Source: Apple_23:4c:62 (94:f6:d6:23:4c:62)
    Type: IPv4 (0x0800)
```

6.c- It is "Type: IPv4 (0x0800)" in all the packets. IPv4, or Internet Protocol version 4, is the fourth version of the Internet Protocol, the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv4 is the most widely used version of the Internet Protocol.

eth.type == 0x0800

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	144.122.242.203	144.122.243.255	NBNS	92	Name query NB M33.KREBSON.RU<00>
2	0.000008	144.122.187.244	144.122.187.255	NBNS	92	Name query NB WPAD<00>
3	0.000010	144.122.187.244	144.122.187.255	NBNS	92	Name query NB WPAD<00>
4	0.000011	144.122.242.203	144.122.243.255	NBNS	92	Name query NB M36.KREBSON.RU<00>
5	0.000094	144.122.149.192	144.122.151.255	UDP	82	57621 → 57621 Len=40
6	0.000190	144.122.129.17	144.122.131.255	UDP	86	57621 → 57621 Len=44
7	0.000450	144.122.149.192	144.122.151.255	UDP	82	57621 → 57621 Len=40
8	0.000501	144.122.242.203	144.122.243.255	NBNS	92	Name query NB M4.KREBSON.RU<00>
9	0.000742	144.122.180.251	144.122.183.255	UDP	305	54915 → 54915 Len=263
10	0.001012	144.122.242.203	144.122.243.255	NBNS	92	Name query NB M41.KREBSON.RU<00>
11	0.001017	144.122.242.203	144.122.243.255	NBNS	92	Name query NB M32.KREBSON.RU<00>
12	0.001231	144.122.242.203	144.122.243.255	NBNS	92	Name query NB M24.KREBSON.RU<00>
13	0.001764	144.122.220.106	144.122.223.255	UDP	305	54915 → 54915 Len=263
14	0.001771	144.122.124.146	144.122.125.255	UDP	305	54915 → 54915 Len=263
15	0.001772	144.122.183.47	144.122.183.255	UDP	86	57621 → 57621 Len=44
16	0.001859	144.122.242.203	144.122.243.255	NBNS	92	Name query NB M12.KREBSON.RU<00>
17	0.001978	144.122.134.188	144.122.135.255	NBNS	92	Name query NB WPAD<00>
18	0.002214	144.122.242.203	144.122.243.255	NBNS	92	Name query NB M40.KREBSON.RU<00>
19	0.002218	144.122.242.203	144.122.243.255	NBNS	92	Name query NB M17.KREBSON.RU<00>
20	0.002467	144.122.134.188	144.122.135.255	NBNS	92	Name query NB WPAD<00>
21	0.002978	144.122.179.121	144.122.179.255	UDP	305	54915 → 54915 Len=263
22	0.002985	144.122.134.188	144.122.135.255	NBNS	92	Name query NB WPAD<00>
23	0.102362	144.122.134.188	144.122.135.255	NBNS	92	Name query NB WPAD<00>
24	0.102369	144.122.180.230	144.122.183.255	UDP	82	57621 → 57621 Len=40
25	0.102370	144.122.183.245	144.122.183.255	UDP	305	54915 → 54915 Len=263
26	0.102459	144.122.27.104	144.122.27.255	NBNS	110	Registration NB DESKTOP-KOR92G4<20>
27	0.102760	144.122.27.104	144.122.27.255	NBNS	110	Registration NB DESKTOP-KOR92G4<00>
28	0.102765	144.122.27.104	144.122.27.255	NBNS	110	Registration NB WORKGROUP<00>
29	0.102829	144.122.209.114	144.122.211.255	NBNS	92	Name query NB D34B<00>
30	0.103282	144.122.180.90	144.122.183.255	UDP	305	54915 → 54915 Len=263
31	0.103288	144.122.209.114	144.122.211.255	BROWSER	250	Domain/Workgroup Announcement WORKGROUP, NT Workstation, Dom…
32	0.103369	144.122.187.93	144.122.187.255	NBNS	92	Name query NB ELFWS<00>

eth.type != 0x0800

No.	Time	Source	Destination	Protocol	Length	Info