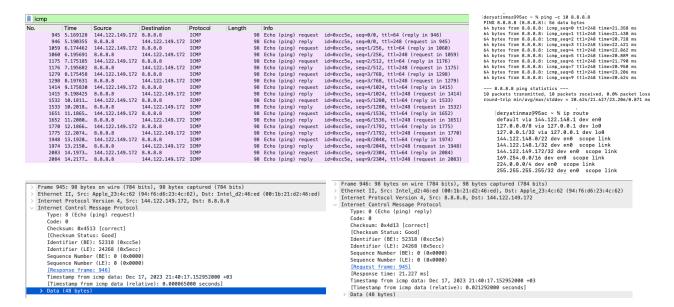
Wireshark Lab: ICMP



- 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)

Verthernet 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.

