https://heilmeier.eu/icmpv4.pcapng
https://heilmeier.eu/icmpv6.pcapng

SharkFest'26 Europe

More than just Ping. A closer look at ICMPv4/6

Uli Heilmeier



Sponsored by: PROFI TAP DEEP NETWORK OBSERVABILITY, cPacket, TCP/IP training, endace Record. Respond.

Ping

- Monty Python's The Meaning of Life
- Sonar
- Table tennis

Legacy ICMP



IANA

www.iana.org/assignments/icmp-parameters

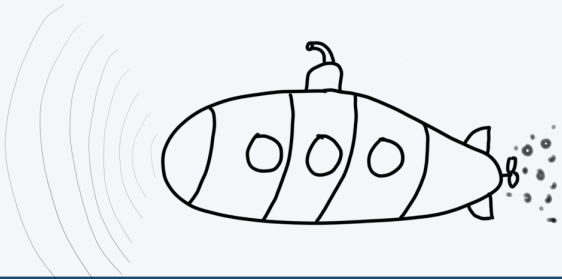
Type	Name	Reference
0	Echo Reply	RFC 792
1	Unassigned	
2	Unassigned	
3	Destination Unreachable	RFC 792
4	Source Quench (Deprecated)	RFC 792; RFC 6633
5	Redirect	RFC 792
6	Alternate Host Address (Deprecated)	RFC 6918
7	Unassigned	
8	Echo	RFC 792
9	Router Advertisement	RFC 1256
10	Router Solicitation	RFC 1256
11	Time Exceeded	RFC 792
12	Parameter Problem	RFC 792
13	Timestamp	RFC 792
14	Timestamp Reply	RFC 792
15	Information Request (Deprecated)	RFC 792; RFC 6918
16	Information Reply (Deprecated)	RFC 792; RFC 6918
17	Address Mask Request (Deprecated)	RFC 950; RFC 6918
18	Address Mask Reply (Deprecated)	RFC 950; RFC 6918
19	Reserved (for Security)	Solo
20-29	Reserved (for Robustness Experiment)	Zaw-Sing Su
30	Traceroute (Deprecated)	RFC 1393; RFC 6918
31	Datagram Conversion Error (Deprecated)	RFC 1475; RFC 6918
32	Mobile Host Redirect (Deprecated)	David Johnson; RFC 6918
33	IPv6 Where-Are-You (Deprecated)	Bill Simpson; RFC 6918
34	IPv6 I-Am-Here (Deprecated)	Bill Simpson; RFC 6918
35	Mobile Registration Request (Deprecated)	Bill Simpson; RFC 6918
36	Mobile Registration Reply (Deprecated)	Bill Simpson; RFC 6918
37	Domain Name Request (Deprecated)	RFC 1788; RFC 6918
38	Domain Name Reply (Deprecated)	RFC 1788; RFC 6918
39	SKIP (Deprecated)	Tom Markson; RFC 6918
40	Photuris	RFC 2521
41	ICMP messages utilized by experimental mobility protocols such as Seamoby	RFC 4065
42	Extended Echo Request	RFC 8335
43	Extended Echo Reply	RFC 8335
44-252	Unassigned	
253	RFC3692-style Experiment 1	RFC 4727
254	RFC3692-style Experiment 2	RFC 4727
255	Reserved	Jon Postel

File

https://heilmeier.eu/icmpv4.pcapng

Echo (icmp.type==8) and Echo Reply (icmp.type==0)

```
icmp.ident==0xfa50
```



Destination Unreachable (icmp.type==3)



```
tcp.stream == 1

ip.addr == 10.255.255.2

tcp.stream == 3

tcp.port==445

udp.port==33444
```

Filtering layered messages

```
ip.src#2==10.1.1.100
```



Codes	Description	Reference
0	Net Unreachable	RFC 792
1	Host Unreachable	RFC 792
2	Protocol Unreachable	RFC 792
3	Port Unreachable	RFC 792
4	Fragmentation Needed and Don't Fragment was Set	RFC 792
5	Source Route Failed	RFC 792
6	Destination Network Unknown	RFC 1122
7	Destination Host Unknown	RFC 1122
8	Source Host Isolated	RFC 1122
9	Communication with Destination Network is Administratively Prohibited	RFC 1122
10	Communication with Destination Host is Administratively Prohibited	RFC 1122
11	Destination Network Unreachable for Type of Service	RFC 1122
12	Destination Host Unreachable for Type of Service	RFC 1122
13	Communication Administratively Prohibited	RFC 1812
14	Host Precedence Violation	RFC 1812
15	Precedence cutoff in effect	RFC 1812

```
[*]—[client1]—[~]
└──> nc -v 10.127.127.127 12712
nc: connect to 10.127.127.127 port 12712 (tcp) failed: Host is unreachable

[x]—[client1]—[~]
└──> ping -c2 10.127.127.127
PING 10.127.127.127 (10.127.127.127) 56(84) bytes of data.
From 10.0.1.1 icmp_seq=1 Time to live exceeded
From 10.0.1.1 icmp_seq=2 Time to live exceeded

--- 10.127.127.127 ping statistics ---
2 packets transmitted, 0 received, +2 errors, 100% packet loss, time 1060ms


[x]—[client1]—[~]
└──> sudo traceroute -m 10 -n -l 10.127.127.127
traceroute to 10.127.127.127 (10.127.127.127), 10 hops max, 46 byte packets
 1  10.1.1.1  0.008 ms  0.002 ms  0.001 ms
 2  10.0.1.1  0.003 ms  0.001 ms  0.001 ms
 3  10.1.1.1  0.002 ms  0.002 ms  0.002 ms
 4  10.0.1.1  0.001 ms  0.001 ms  0.001 ms
 5  *  10.1.1.1  0.016 ms  0.005 ms
 6  10.0.1.1  0.011 ms  0.006 ms  0.004 ms
 7  10.1.1.1  0.004 ms  0.003 ms  0.003 ms
 8  10.0.1.1  0.003 ms  0.004 ms  *
 9  10.1.1.1  0.009 ms  0.003 ms  0.001 ms
10  10.0.1.1  0.002 ms  0.002 ms  0.003 ms
```

Time Exceeded (icmp.type==11)

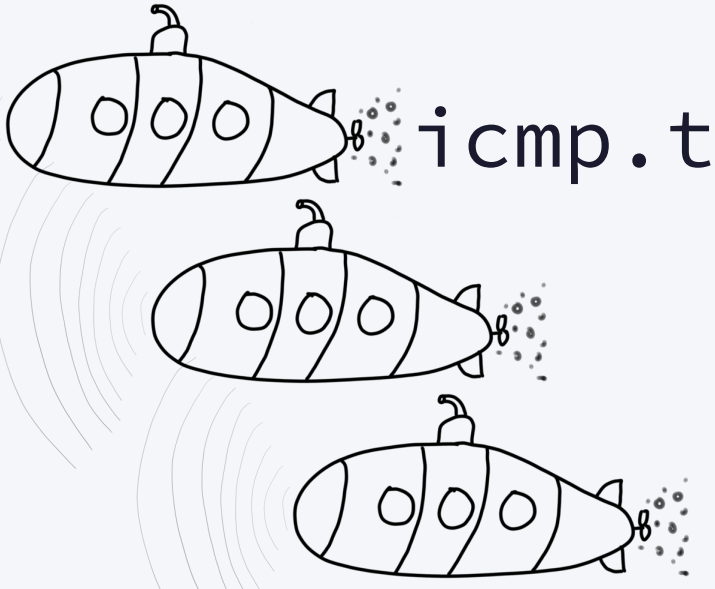
```
udp.port==58985

icmp.ident == 169

frame.number>1231
```



Extended Echo



```
icmp.type in {42,43}
```

Redirect (icmp.type==5)




```
ip.addr==10.10.10.10 and udp
```

ICMPv4 take-aways

- ICMP messages can be triggered by ICMP, UDP, TCP…
- Most of the time payload reference the triggering frame
- Dest unreachable and Time exceeded are important
- Deprecated and harmful types should be blocked

ICMPv6



IANA

Type	Name	Reference
0	Reserved	
1	Destination Unreachable	RFC 4443
2	Packet Too Big	RFC 4443
3	Time Exceeded	RFC 4443
4	Parameter Problem	RFC 4443
5-99	Unassigned	
100	Private experimentation	RFC 4443
101	Private experimentation	RFC 4443
102-126	Unassigned	
127	Reserved for expansion of ICMPv6 error messages	RFC 4443
128	Echo Request	RFC 4443
129	Echo Reply	RFC 4443
130	Multicast Listener Query	RFC 2710
131	Multicast Listener Report	RFC 2710
132	Multicast Listener Done	RFC 2710
133	Router Solicitation	RFC 4861
134	Router Advertisement	RFC 4861
135	Neighbor Solicitation	RFC 4861
136	Neighbor Advertisement	RFC 4861
137	Redirect Message	RFC 4861
138	Router Renumbering	RFC 2894
139	ICMP Node Information Query	RFC 4620
140	ICMP Node Information Response	RFC 4620
141	Inverse Neighbor Discovery Solicitation Message	RFC 3122
142	Inverse Neighbor Discovery Advertisement Message	RFC 3122
143	Version 2 Multicast Listener Report	RFC 9777
144	Home Agent Address Discovery Request Message	RFC 6275
145	Home Agent Address Discovery Reply Message	RFC 6275
146	Mobile Prefix Solicitation	RFC 6275
147	Mobile Prefix Advertisement	RFC 6275
148	Certification Path Solicitation Message	RFC 3971
149	Certification Path Advertisement Message	RFC 3971
150	ICMP messages utilized by experimental mobility protocols such as Seamoby	RFC 4065
151	Multicast Router Advertisement	RFC 4286
152	Multicast Router Solicitation	RFC 4286
153	Multicast Router Termination	RFC 4286
154	FMIPv6 Messages	RFC 5568
155	RPL Control Message	RFC 6550
156	ILNPv6 Locator Update Message	RFC 6743
157	Duplicate Address Request	RFC 6775
158	Duplicate Address Confirmation	RFC 6775
159	MPL Control Message	RFC 7731
160	Extended Echo Request	RFC 8335
161	Extended Echo Reply	RFC 8335
162-199	Unassigned	
200	Private experimentation	RFC 4443
201	Private experimentation	RFC 4443
202-254	Unassigned	
255	Reserved for expansion of ICMPv6 informational messages	RFC 4443

File

https://heilmeier.eu/icmpv6.pcapng

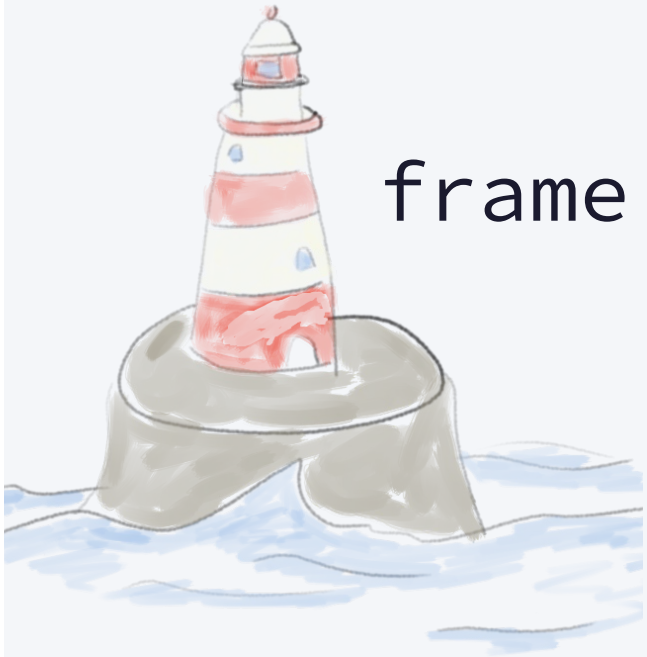
Neighbor Solicitation (135) and Neighbor Advertisement (136)



```
frame.number in {18,19}
```

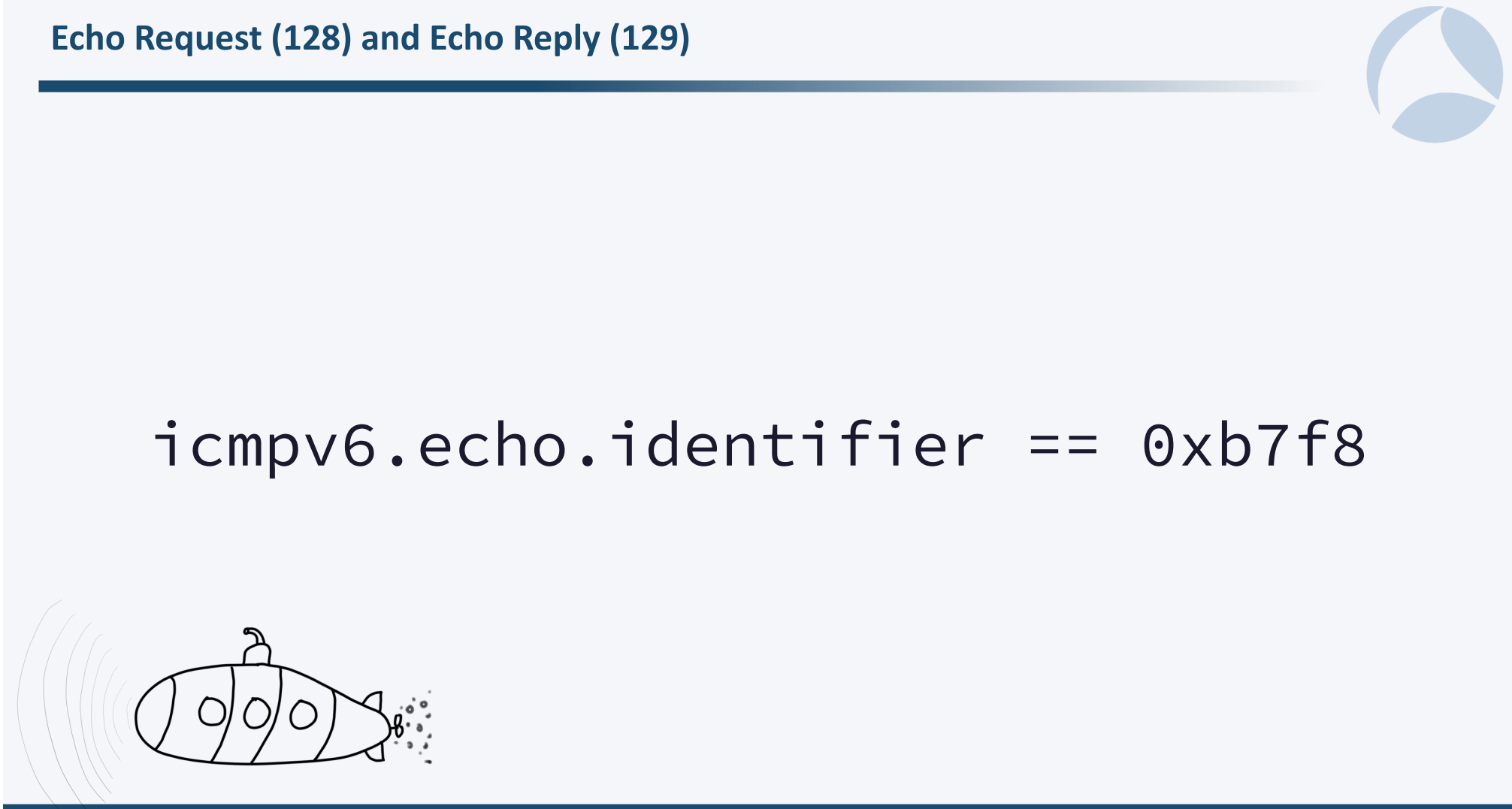


Router Solicitation (133) and Router Advertisement (134)



```
frame.number in {9,10,16}
```

Echo Request (128) and Echo Reply (129)



```
icmpv6.echo.identifier == 0xb7f8
```

Time Exceeded (3)



```
udp.port==45537
```

Destination Unreachable (1)



```
ipv6.stream == 13

udp.stream eq 12
```

Packet Too Big (2)


```
tcp.stream == 3
```



ICMPv6 take-aways

- ICMPv6 is the foundation for L2 / broadcast domain
- ARP and IGMP has moved into ICMPv6
- Dest Unreachable Fragmentation Needed is a own type Packet Too Big
- Harmful types should be blocked (like RA snooping)

Thank You!

WIRESHARK

@uhei@chaos.social
uh@heilmeier.eu