

Capitulo 18:

Analizar el protocolo de control de mensajes de Internet

(ICMPv4/ICMPv6)

Alumno: Uc Uc César Enrique

El proposito de ICMP

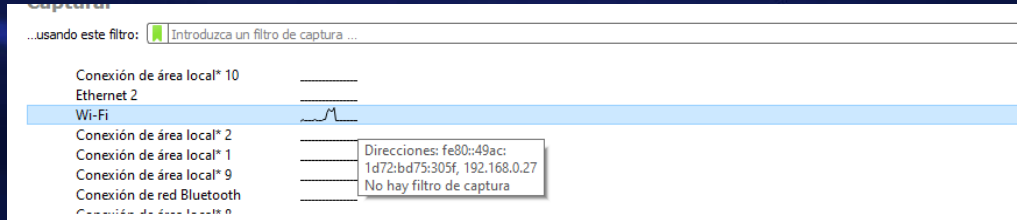
El ICMP se utiliza como sistema de mensajería para errores, alertas y notificaciones en general de una red IP. Hay muchos tipos de mensajes ICMP, algunos son:

- Echo Message: utilizado por ping y traceroute para probar la conectividad de un extremo a otro. Demasiados de estos podrían indicar un proceso de reconocimiento o posiblemente un ataque de denegación de servicio.
- Redirect Message: utilizado por los enrutadores para que la fuente sepa que hay una mejor ruta hacia un destino. Si este paquete no es enviado por un enrutador, debe considerarse sospechoso.
- Destination Unreachable Message: se utiliza para decirle al host de origen que su paquete no se pudo entregar por alguna razón; la razón se indica en el mensaje Destino inalcanzable. Una gran cantidad de estos paquetes de respuesta podría indicar que se está realizando un escaneo de puerto UDP fallido o que un servicio no se está ejecutando correctamente.

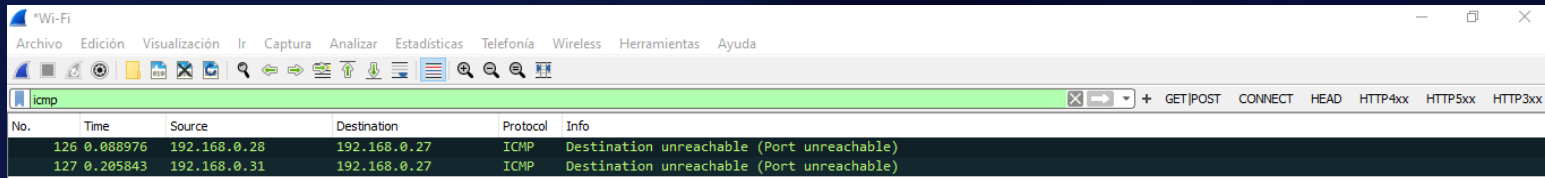
Analizar el tráfico normal ICMP

Es difícil definir el tráfico ICMP "normal", ya que es subjetivo para cada red. Algunos miembros del personal de la red utilizan pings para pruebas de conectividad, mientras que algunas empresas restringen las solicitudes / respuestas de eco ICMP.

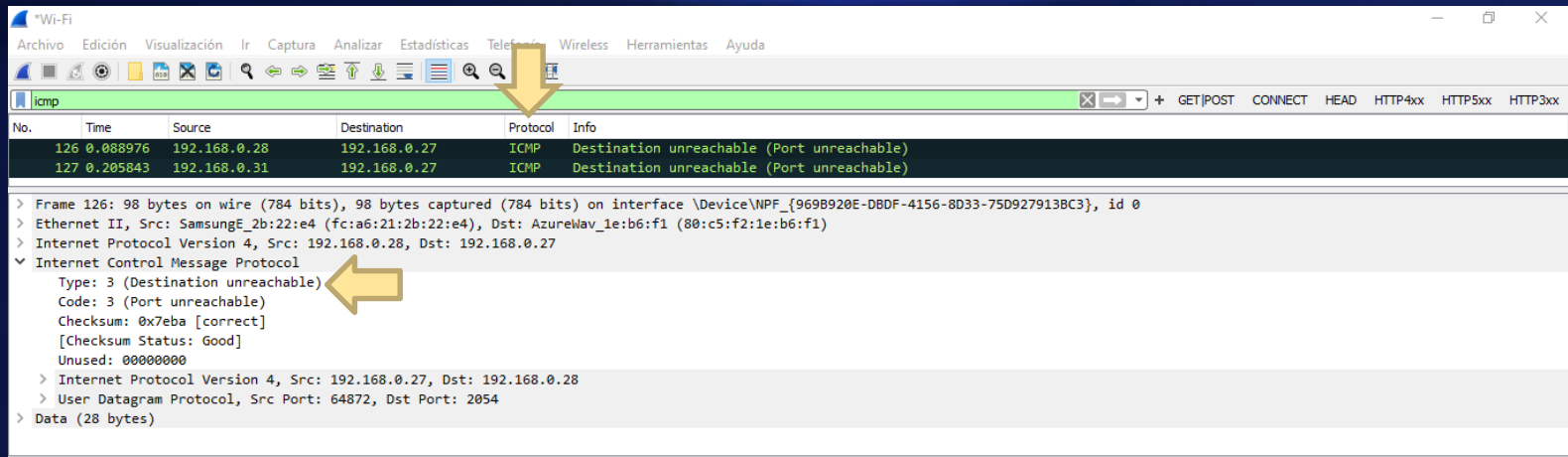
Ejemplo: Empezamos a capturar los paquetes en WireShark



Detenemos la captura de paquetes y escribimos el filtro “icmp”



Como podemos observar, nos señale el Protocol ICMP y nos muestra que es de tipo 3: Destination unreachable



The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes Archivo, Edición, Visualización, Ir, Captura, Analizar, Estadísticas, Televisión, Wireless, Herramientas, and Ayuda. The toolbar contains various icons for file operations, capture, analysis, and display. The packet list pane shows two ICMP packets:

No.	Time	Source	Destination	Protocol	Info
126	0.088976	192.168.0.28	192.168.0.27	ICMP	Destination unreachable (Port unreachable)
127	0.205843	192.168.0.31	192.168.0.27	ICMP	Destination unreachable (Port unreachable)

The packet details pane for the selected ICMP packet (No. 126) shows the following structure:

- > Frame 126: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF_{969B920E-DBDF-4156-8D33-75D9279138C3}, id 0
- > Ethernet II, Src: SamsungE_2b:22:e4 (fc:a6:21:2b:22:e4), Dst: AzureWav_1e:b6:f1 (80:c5:f2:1e:b6:f1)
- > Internet Protocol Version 4, Src: 192.168.0.28, Dst: 192.168.0.27
- > Internet Control Message Protocol
 - Type: 3 (Destination unreachable)
 - Code: 3 (Port unreachable)
 - Checksum: 0x7eba [correct]
 - [Checksum Status: Good]
 - Unused: 00000000
- > Internet Protocol Version 4, Src: 192.168.0.27, Dst: 192.168.0.28
- > User Datagram Protocol, Src Port: 64872, Dst Port: 2054
- > Data (28 bytes)

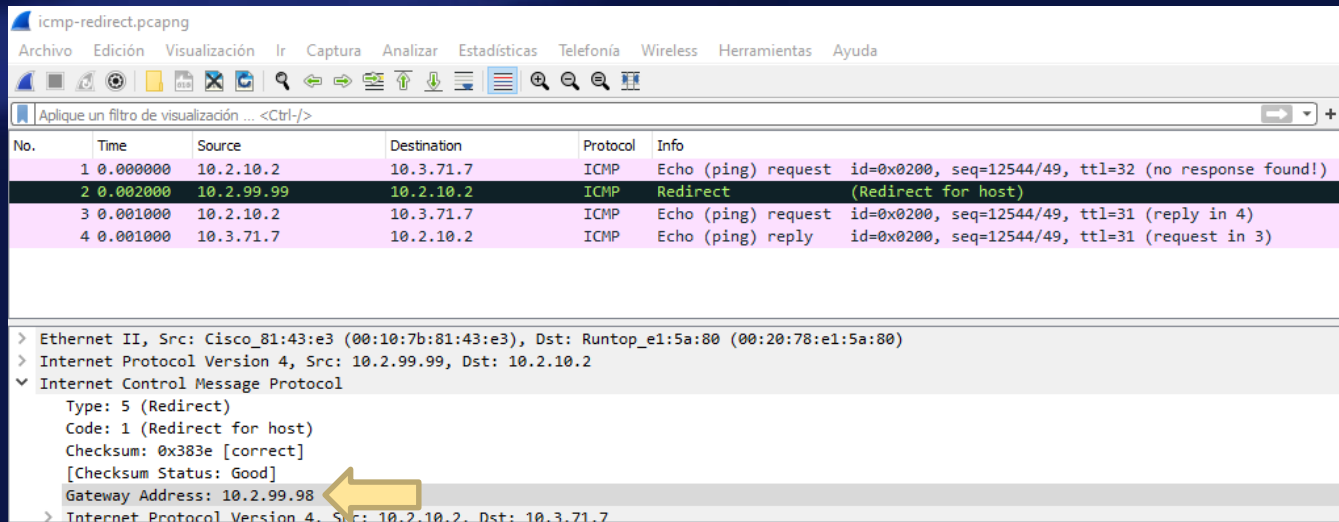
Analizar problema ICMP

Un problema común de ICMP es una prueba de eco que no recibe una respuesta, lo que implica que no hay conectividad a un objetivo. Identificar el punto donde se cae el tráfico ICMP requiere mover el sistema Wireshark a lo largo del ruta hasta llegar al punto donde se produce la pérdida de paquetes.

Sin embargo, el propio ICMP puede ayudar a localizar muchos otros problemas de red y problemas de seguridad.

Analizar problema ICMP

Ejemplo:



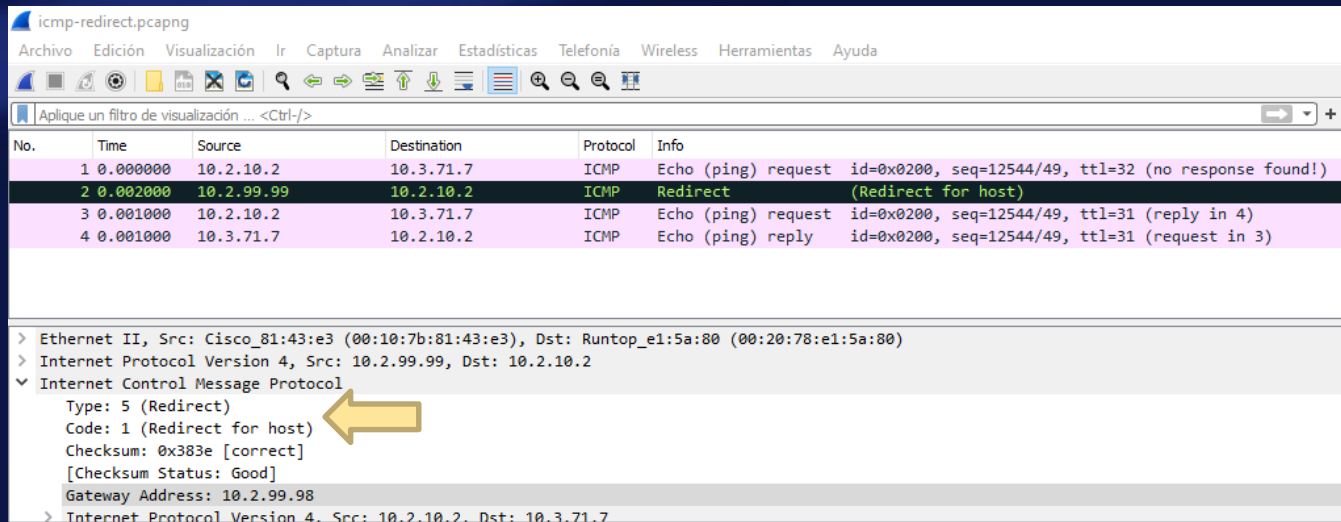
The image shows a Wireshark packet capture of an ICMP Redirect packet. The packet list table at the top shows four packets: a ping request, a redirect packet, another ping request, and a ping reply. The details pane for the selected packet (packet 2) shows the Ethernet II header, Internet Protocol Version 4 header, and Internet Control Message Protocol details. The ICMP details show it is a Redirect (Type 5, Code 1) for host 10.2.10.2, with a gateway address of 10.2.99.98. A yellow arrow points to the Gateway Address field.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.2.10.2	10.3.71.7	ICMP	Echo (ping) request id=0x0200, seq=12544/49, ttl=32 (no response found!)
2	0.002000	10.2.99.99	10.2.10.2	ICMP	Redirect (Redirect for host)
3	0.001000	10.2.10.2	10.3.71.7	ICMP	Echo (ping) request id=0x0200, seq=12544/49, ttl=31 (reply in 4)
4	0.001000	10.3.71.7	10.2.10.2	ICMP	Echo (ping) reply id=0x0200, seq=12544/49, ttl=31 (request in 3)

> Ethernet II, Src: Cisco_81:43:e3 (00:10:7b:81:43:e3), Dst: Runtop_e1:5a:80 (00:20:78:e1:5a:80)	
> Internet Protocol Version 4, Src: 10.2.99.99, Dst: 10.2.10.2	
▼ Internet Control Message Protocol	
Type: 5 (Redirect)	
Code: 1 (Redirect for host)	
Checksum: 0x383e [correct]	
[Checksum Status: Good]	
Gateway Address: 10.2.99.98	
> Internet Protocol Version 4, Src: 10.2.10.2, Dst: 10.3.71.7	


Muestra un paquete ICMP Redirect apuntando a otra puerta de enlace en 10.2.99.98. Este paquete se envía cuando un enrutador receptor identifica un enrutador mejor para el remitente.

Analizar problema ICMP



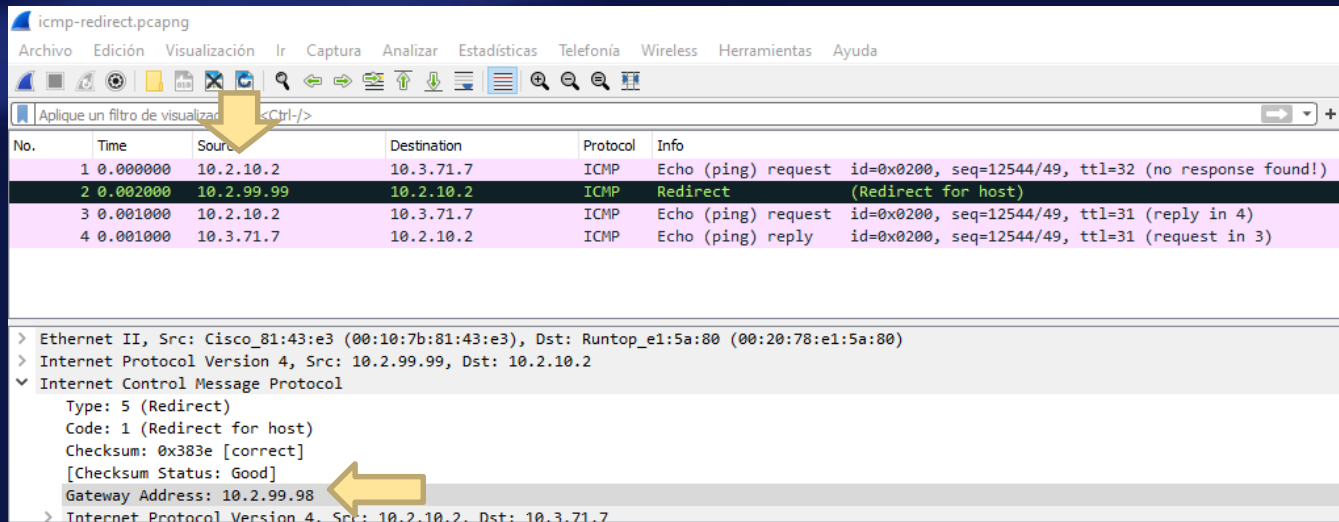
The image shows a Wireshark packet capture of an ICMP Redirect packet. The packet list at the top shows four packets: a ping request (No. 1), a redirect packet (No. 2), another ping request (No. 3), and a ping reply (No. 4). The packet details pane for packet 2 is expanded, showing the Ethernet II header, Internet Protocol Version 4 header, and the Internet Control Message Protocol (ICMP) section. The ICMP section is further expanded, showing the Type (5) and Code (1) fields, which are highlighted by a yellow arrow. The packet is identified as a Redirect for host with a gateway address of 10.2.99.98.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.2.10.2	10.3.71.7	ICMP	Echo (ping) request id=0x0200, seq=12544/49, ttl=32 (no response found!)
2	0.002000	10.2.99.99	10.2.10.2	ICMP	Redirect (Redirect for host)
3	0.001000	10.2.10.2	10.3.71.7	ICMP	Echo (ping) request id=0x0200, seq=12544/49, ttl=31 (reply in 4)
4	0.001000	10.3.71.7	10.2.10.2	ICMP	Echo (ping) reply id=0x0200, seq=12544/49, ttl=31 (request in 3)

> Ethernet II, Src: Cisco_81:43:e3 (00:10:7b:81:43:e3), Dst: Runtop_e1:5a:80 (00:20:78:e1:5a:80)	
> Internet Protocol Version 4, Src: 10.2.99.99, Dst: 10.2.10.2	
▼ Internet Control Message Protocol	
Type: 5 (Redirect)	
Code: 1 (Redirect for host)	
Checksum: 0x383e [correct]	
[Checksum Status: Good]	
Gateway Address: 10.2.99.98	
> Internet Protocol Version 4, Src: 10.2.10.2, Dst: 10.3.71.7	

El enrutador receptor genera un ICMP Redirect (Type 5/Code 1) packet con un enrutador recomendado para usar.

Analizar problema ICMP



The image shows a Wireshark packet capture of an ICMP Redirect message. The packet list shows four packets: an Echo (ping) request from 10.2.10.2 to 10.3.71.7 (no response), an ICMP Redirect from 10.2.99.99 to 10.2.10.2, another Echo (ping) request from 10.2.10.2 to 10.3.71.7, and an Echo (ping) reply from 10.3.71.7 to 10.2.10.2. A yellow arrow points to the second packet (the Redirect). The packet details pane shows the structure of the ICMP Redirect message: Type 5 (Redirect), Code 1 (Redirect for host), Checksum 0x383e, and Gateway Address 10.2.99.98. Another yellow arrow points to the Gateway Address field.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.2.10.2	10.3.71.7	ICMP	Echo (ping) request id=0x0200, seq=12544/49, ttl=32 (no response found!)
2	0.002000	10.2.99.99	10.2.10.2	ICMP	Redirect (Redirect for host)
3	0.001000	10.2.10.2	10.3.71.7	ICMP	Echo (ping) request id=0x0200, seq=12544/49, ttl=31 (reply in 4)
4	0.001000	10.3.71.7	10.2.10.2	ICMP	Echo (ping) reply id=0x0200, seq=12544/49, ttl=31 (request in 3)

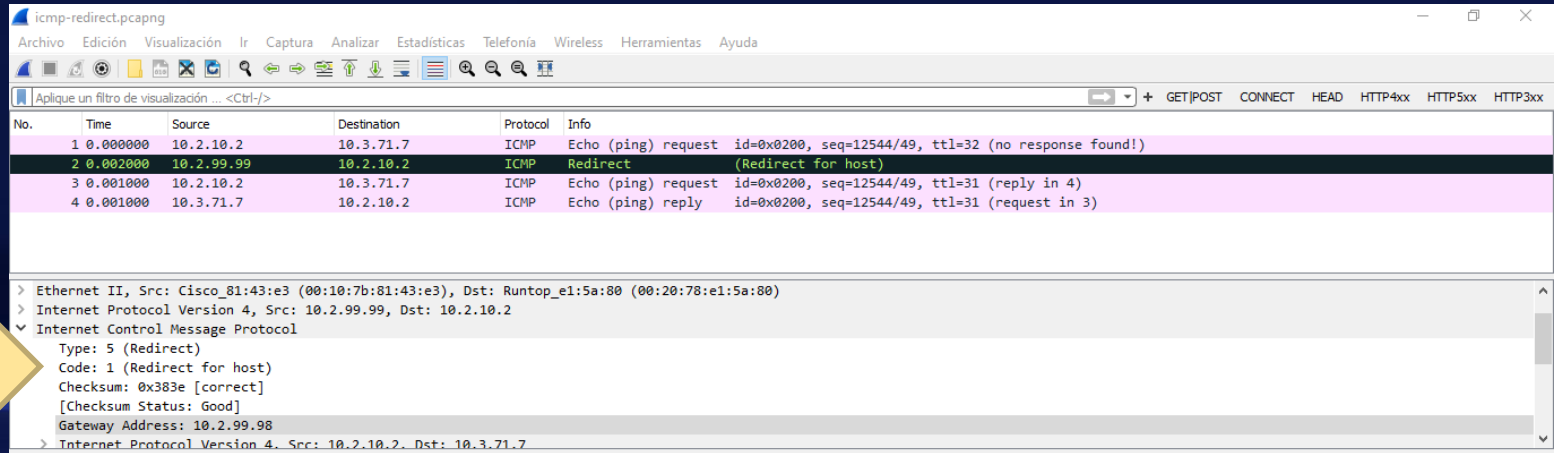
Packet Details for Packet 2:

- Ethernet II, Src: Cisco_81:43:e3 (00:10:7b:81:43:e3), Dst: Runtop_e1:5a:80 (00:20:78:e1:5a:80)
- Internet Protocol Version 4, Src: 10.2.99.99, Dst: 10.2.10.2
- Internet Control Message Protocol
 - Type: 5 (Redirect)
 - Code: 1 (Redirect for host)
 - Checksum: 0x383e [correct]
 - [Checksum Status: Good]
 - Gateway Address: 10.2.99.98
- Internet Protocol Version 4, Src: 10.2.10.2, Dst: 10.3.71.7

La próxima vez que 10.2.10.2 quiera llegar a 10.3.71.7, debería enviar sus paquetes a través del enrutador 10.2.99.98.

Disecccionar la estructura ICMP packet

Los paquetes ICMP solo contienen tres campos obligatorios después del encabezado IP: tipo, código y Checksum.



icmp-redirect.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.2.10.2	10.3.71.7	ICMP	Echo (ping) request id=0x0200, seq=12544/49, ttl=32 (no response found!)
2	0.002000	10.2.99.99	10.2.10.2	ICMP	Redirect (Redirect for host)
3	0.001000	10.2.10.2	10.3.71.7	ICMP	Echo (ping) request id=0x0200, seq=12544/49, ttl=31 (reply in 4)
4	0.001000	10.3.71.7	10.2.10.2	ICMP	Echo (ping) reply id=0x0200, seq=12544/49, ttl=31 (request in 3)

> Ethernet II, Src: Cisco_81:43:e3 (00:10:7b:81:43:e3), Dst: Runtop_e1:5a:80 (00:20:78:e1:5a:80)

> Internet Protocol Version 4, Src: 10.2.99.99, Dst: 10.2.10.2

> Internet Control Message Protocol

- Type: 5 (Redirect)
- Code: 1 (Redirect for host)
- Checksum: 0x383e [correct]
- [Checksum Status: Good]
- Gateway Address: 10.2.99.98

> Internet Protocol Version 4, Src: 10.2.10.2, Dst: 10.3.71.7

Algunos paquetes ICMP contienen campos adicionales para proporcionar información o detalles sobre el mensaje.

Tipos de mensaje ICMP

Existe una lista definida de los tipos de mensaje ICMP que pueden ser mostrados en el network. Esta lista esta basada en el documento IANA.

Link: <https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml>

Type 0: Echo Reply [RFC 792]
Type 1: Unassigned
Type 2: Unassigned
Type 3: Destination Unreachable [RFC 792]
Type 4: Source Quench [RFC 792]
Type 5: Redirect [RFC 792]
Type 6: Alternate Host Address
Type 7: Unassigned
Type 8: Echo [RFC 792]
Type 9: Router Advertisement [RFC 1256]
Type 10: Router Solicitation [RFC 1256]
Type 11: Time Exceeded [RFC 792]
Type 12: Parameter Problem [RFC 792]
Type 13: Timestamp [RFC 792]
Type 14: Timestamp Reply [RFC 792]

Type 15: Information Request [RFC 792]
Type 16: Information Reply [RFC 792]
Type 17: Address Mask Request [RFC 950]
Type 18: Address Mask Reply [RFC 950]
Type 19: Reserved (for Security)
Types 20-29: Reserved (for Robustness Experiment)
Type 30: Traceroute [RFC 1393]
Type 31: Datagram Conversion Error [RFC 1475]
Type 32: Mobile Host Redirect
Type 33: IPv6 Where-Are-You
Type 34: IPv6 I-Am-Here
Type 35: Mobile Registration Request
Type 36: Mobile Registration Reply
Type 37: Domain Name Request
Type 38: Domain Name Reply
Type 39: SKIP
Type 40: Photuris
Types 41-252: Unassigned
Type 253: RFC3692-style Experiment 1
Type 254: RFC3692-style Experiment 2

Códigos

Muchos tipos de paquetes ICMP tienen varios valores de campo de código posibles. La siguiente lista proporciona las descripciones de los campos de código más comunes.

Tipo 3: Destination Unreachable

Codes	Description	Reference
0	Net Unreachable	[RFC792]
1	Host Unreachable	[RFC792]
2	Protocol Unreachable	[RFC792]
3	Port Unreachable	[RFC792]
4	Fragmentation Needed and Don't Fragment was Set	[RFC792]
5	Source Route Failed	[RFC792]
6	Destination Network Unknown	[RFC1122]
7	Destination Host Unknown	[RFC1122]
8	Source Host Isolated	[RFC1122]
9	Communication with Destination Network is Administratively Prohibited	[RFC1122]
10	Communication with Destination Host is Administratively Prohibited	[RFC1122]
11	Destination Network Unreachable for Type of Service	[RFC1122]
12	Destination Host Unreachable for Type of Service	[RFC1122]
13	Communication Administratively Prohibited	[RFC1812]
14	Host Precedence Violation	[RFC1812]
15	Precedence cutoff in effect	[RFC1812]

Códigos

Tipo 5: Redirect

Codes	Description	Reference
0	Redirect Datagram for the Network (or subnet)	
1	Redirect Datagram for the Host	
2	Redirect Datagram for the Type of Service and Network	
3	Redirect Datagram for the Type of Service and Host	

Tipo 11: Time Exceeded Code

Codes	Description	Reference
0	Time to Live exceeded in Transit	
1	Fragment Reassembly Time Exceeded	

Función básica ICMPv6

RFC 4443 define el propósito y la funcionalidad de ICMPv6. La estructura del paquete ICMPv6 es la misma que la estructura de paquetes ICMP.

Existe una lista definida de los tipos de mensaje ICMPv6 que pueden ser enviados por la red. Esta lista es basada en el documento IANA.

Link:<https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml>

• ICMPv6 "Code" Fields

- [Type 0 - Reserved](#)
- [Type 1 - Destination Unreachable](#)
- [Type 2 - Packet Too Big](#)
- [Type 3 - Time Exceeded](#)
- [Type 4 - Parameter Problem](#)
- [Type 128 - Echo Request](#)
- [Type 129 - Echo Reply](#)
- [Type 130 - Multicast Listener Query](#)
- [Type 131 - Multicast Listener Report](#)
- [Type 132 - Multicast Listener Done](#)
- [Type 133 - Router Solicitation](#)
- [Type 134 - Router Advertisement](#)
- [Type 135 - Neighbor Solicitation](#)
- [Type 136 - Neighbor Advertisement](#)
- [Type 137 - Redirect Message](#)
- [Type 138 - Router Renumbering](#)
- [Type 139 - ICMP Node Information Query](#)
- [Type 140 - ICMP Node Information Response](#)
- [Type 141 - Inverse Neighbor Discovery](#)
- [Type 142 - Inverse Neighbor Discovery](#)
- [Type 144 - Home Agent Address Discovery](#)
- [Type 145 - Home Agent Address Discovery](#)
- [Type 146 - Mobile Prefix Solicitation](#)
- [Type 147 - Mobile Prefix Advertisement](#)
- [Type 157 - Duplicate Address Request Code Suffix](#)
- [Type 158 - Duplicate Address Confirmation Code Suffix](#)
- [Type 160 - Extended Echo Request](#)
- [Type 161 - Extended Echo Reply](#)

Función básica ICPMv6

Ejemplo:

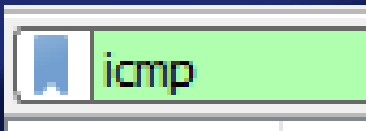
De acuerdo a lista anterior, podemos observar que el tipo de mensaje es el 128: Echo Request

```
> Frame 1: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface unknown, id 0
> Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 192.88.99.1
> Internet Protocol Version 6, Src: 2002:1806:addc::1806:addc, Dst: 2607:f0d0:2001:e:1::120
▼ Internet Control Message Protocol v6
  Type: Echo (ping) request (128)
  Code: 0
  Checksum: 0xf109 [correct]
  [Checksum Status: Good]
  Identifier: 0x0001
  Sequence: 31
  [Response In: 2]
> Data (32 bytes)
```

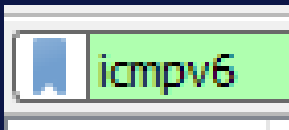
← Aquí nos muestra el número de tipo.

Filtros en tráfico ICMP y ICMPv6

La sintaxis de filtro de captura para ICMP es simplemente



La sintaxis de filtro de captura para ICMPv6 es simplemente



Para encontrar algún tipo de captura de ICMP en específico la sintaxis es

