WIKIPEDIA

ICMPv6

Protocolo de Mensajes de Control de Internet Version 6 (**ICMPv6** o **ICMP para IPv6**) es una nueva versión de ICMP y es una parte importante de la arquitectura IPv6 que debe estar completamente soportada por todas las implementaciones y nodos IPv6. ICMPv6 combina funciones que anteriormente estaban subdivididas en varias partes de diferentes protocolos tales como ICMP, IGMP o ARP y además introduce algunas simplificaciones eliminando tipos de mensajes obsoletos que estaban en desuso actualmente.

Índice

Sumario

Como IPv6 es una nueva versión de IPv4, utiliza el protocolo ICMP como fue definido para IPv4 en RFC 792 (al cual nos referiremos como ICMPv4) con algunos cambios significativos. IGMP también ha sido implementada dentro de ICMPv6. El valor del campo "Cabecera Siguiente" de la cabecera del paquete IPv6 para ICMPv6 es 58 (ver IPv6).

Este artículo explica el formato de un conjunto de mensajes de control utilizados en ICMPv6, pero no explica los procedimientos para utilizar estos mensajes para llevar a cabo una determinada función. Otros tipos de mensajes como los mensajes Neighbor Discovery deben ser descritos en artículos adicionales.

ICMPv6 es un protocolo de propósito múltiple y está diseñado para realizar funciones tales como detectar errores encontrados en la interpretación de paquetes, realizar diagnósticos, realizar funciones como Neighbor Discovery y detectar direcciones IPv6 multicast. Por esta razón, los mensajes ICMPv6 están subdivididos en dos clases: mensajes de error y mensajes informativos. Los mensajes ICMPv6 son enviados dentro de paquetes IPv6 los cuales a su vez pueden llevar las extensiones de cabecera de IPv6.

ICMPv6 (ICMP para IPv6)

El protocolo ICMPv6 es utilizado por los nodos IPv6 para detectar errores encontrados en la interpretación de paquetes y para realizar otras funciones de la capa de internet como el diagnóstico (ICMPv6 ping).

Formato de los Paquetes

Los paquetes ICMPv6 tienen el formato **Tipo, Código y Checksum**.

Los 8 bits del campo **Tipo** indican el tipo de mensaje. Si el bit de mayor peso tiene el valor 0 (valores entre 0 y 127) entonces es un mensaje de error, por el contrario si el bit de mayor peso es 1 (valores entre 128 y 255) entonces es un mensaje informativo.

Los 8 bits del campo **Código** dependen del tipo de mensaje, y son usados para crear un nivel adicional de clasificación de mensajes, de tal forma que los mensajes informativos en función del campo Código se pueden subdividir en varios tipos.

El campo **Checksum** es usado para detectar errores en los mensajes ICMP y en algunos de los mensajes IPv6.

Mensajes de Error

Los mensajes de error de ICMPv6 son similares a los mensajes de error de ICMPv4. Se dividen en 4 categorías: destino inaccesible, paquete demasiado grande, tiempo excedido y problemas de parámetros.

```
1    Destination Unreachable (Destino Inalcanzable)
2    Packet Too Big (Paquete Demasiado Grande)
3    Time Exceeded (Tiempo Agotado)
4    Parameter Problem (Problema de Parámetros)
```

Mensajes Informativos

El segundo tipo de mensajes ICMP son los mensajes informativos. Estos mensajes se subdividen en tres grupos: mensajes de diagnóstico, mensajes para la administración de grupos multicast y mensajes de Neighbor Discovery.

```
128  Echo Request (Solicitud de Eco)
129  Echo Reply (Respuesta de Eco)
```

Cada mensaje ICMPv6 está precedido por una cabecera IPv6 y cero o más extensiones de cabecera IPv6. La cabecera ICMPv6 es identificada por un valor 58 en "Cabecera Siguiente" en la cabecera inmediatamente predecesora. (Nota: el valor del campo "Cabecera Siguiente" es distinto del valor utilizado para identificar ICMP para IPv4)

Formato General de los Paquetes

Paquete ICMPv6

Bit offset	0–7	8–15	16–31
0	Type	Code	Checksum
32	Message body		

El campo Tipo indica el tipo de mensaje. Este valor determina el formato de la información a recibir.

El campo Código depende del tipo de mensaje. Es usado para crear un nuevo subnivel de clasificación de los mensajes.

El campo Checksum es usado para detectar la corrupción de los datos en los mensajes ICMPv6 y en parte de las cabeceras IPv6.

Determinación de la Dirección de un Paquete

Cuando un nodo envía un mensaje ICMPv6 debe especificar la direcciones IPv6 origen y destino en la cabecera de la dirección IPv6 antes de calcular el checksum. Si el nodo tiene más de una dirección unicast, éste debe elegir la dirección origen como sigue:

(a) Si el mensaje es una respuesta a un mensaje enviado a una de las direcciones unicast del nodo, la dirección origen de la respuesta debe esa misma dirección.

(b) Si el mensaje es una respuesta a un mensaje enviado a cualquier otra dirección, tal como:

- una dirección de un grupo multicast,
- una dirección anycast implementada por el nodo, o
- una dirección unicast que no pertenece al nodo

la dirección origen del paquete ICMPv6 debe ser una dirección unicast perteneciente al nodo. La dirección debería ser elegida de acuerdo con las reglas que serán utilizadas para seleccionar la dirección origen de cualquier paquete originado por el nodo, dada la dirección de destino del paquete. Sin embargo, debería ser seleccionada en una forma alternativa si va a derivar en una opción más informativa de la dirección accesible desde el destino del paquete ICMPv6.

Cálculo del Campo Checksum

El checksum es un conjunto de 16 bits complemento a uno, de la suma del complemento a uno del mensaje ICMPv6 a partir del campo Tipo del mensaje ICMPv6 hasta el final, precedido por una pseudo-cabecera de la cabecera IPv6, tal y como se especifica en IPv6.

Para calcular el Checksum, el campo Checksum es inicializado a cero.

El valor "Cabecera Siguiente" usado en la "pseudo-cabecera" es 58. (Nota: La inclusión de una pseudo cabecera en el checksum ICMPv6 es un cambio desde IPv4; observa IPv6 para entender completamente este cambio).

La pseudo-cabecera utilizada para calcular el checksum es la siguiente:

Pseudo-cabecera ICMPv6

Bit offset	0 - 7	8–15	16–23	24–31
0	Dirección origen			
32				
64				
96				
128	Dirección destino			
160				
192				
224				
256	Longitud ICMPv6			
288	Ceros			Siguiente cabecera

ICMPv6 Mensajes de Transmisión

Un nodo que reenvía un mensaje ICMPv6, debe determinar tanto la dirección IPv6 origen como la destino para el mensaje ICMPv6. Especial cuidado se debe tener en la elección de la dirección de origen. Si un nodo tiene más de una dirección unicast, debe elegir la dirección origen del mensaje como sigue:

- Si el mensaje es una respuesta a un mensaje enviado a una de la direcciones unicast del nodo, la dirección origen de la respuesta debe ser esa misma dirección.
- Si el mensaje es una respuesta a un mensaje enviado a un grupo multicast o anycast al cual el nodo pertenece, la dirección origen de la respuesta debe ser una dirección unicast perteneciente a la interfaz en la cual el paquete multicast o anycast fue recibido.
- Si el mensaje es una respuesta a un mensaje enviado a una dirección que no pertenece al nodo, la dirección origen de la respuesta debe servir para comprobar el error (por ejemplo, la dirección unicast perteneciente a la interfaz en la cual el reenviado del paquete falló).
- En otros casos, se deben examinar las tablas de enrutamiento del nodo para determinar que interfaz debe ser usada para transmitir el mensaje a su destinatario, y la dirección unicast perteneciente a esa interfaz debe ser usada como dirección origen del mensaje.

Cuando un nodo ICMPv6 recibe un paquete, debe realizar acciones en función del tipo de mensaje. El protocolo ICMPv6 debe limitar el número de mensajes de error enviados a un mismo destinatario para evitar sobrecarga en la red. Por ejemplo, si un nodo reenvía los paquetes erróneos, ICMP debe señalar el error al primer paquete y luego hacerlo periódicamente, de acuerdo con un periodo prefijado o en función de una carga máxima de la red. Un mensaje de error ICMP nunca debe ser enviado en respuesta a otro mensaje de error ICMP.

Tipos de mensaje ICMP

Tipo		Código	
Valor	**Significado**	**Valor**	**Significado**
1	Destination Unreachable	0	no route to destination
		1	communication with destination administratively prohibited
		2	beyond scope of source address
		3	address unreachable
		4	port unreachable
		5	source address failed ingress/egress policy
		6	reject route to destination
		7	Error in Source Routing Header
2	Packet Too Big	0	
3	Time Exceeded	0	hop limit exceeded in transit
		1	fragment reassembly time exceeded
4	Parameter Problem	0	erroneous header field encountered
		1	unrecognized Next Header type encountered
		2	unrecognized IPv6 option encountered
100	Private experimentation		
101	Private experimentation		
127	Reserved for expansion of ICMPv6 error messages		
128	Echo Request	0	
129	Echo Reply	0	
133	Router Solicitation (NDP)	0	
134	Router Advertisement (NDP)	0	
135	Neighbor Solicitation (NDP)	0	
136	Neighbor Advertisement (NDP)	0	
137	Redirect Message (NDP)	0	
138	Router Renumbering	0	Router Renumbering Command
		1	Router Renumbering Result
		255	Sequence Number Reset
139	ICMP Node Information Query	0	The Data field contains an IPv6 address which is the Subject of this Query.
		1	The Data field contains a name which is the Subject of this Query, or is empty, as in the case of a NOOP.
		2	The Data field contains an IPv4 address which is the Subject of this Query.
140	ICMP Node Information Response	0	A successful reply. The Reply

			Data field may or may not be empty.
		1	The Responder refuses to supply the answer. The Reply Data field will be empty.
		2	The Qtype of the Query is unknown to the Responder. The Reply Data field will be empty.
141	Inverse Neighbor Discovery Solicitation Message	0	
142	Inverse Neighbor Discovery Advertisement Message	0	
143	Multicast Listener Report Message v2	0	
144	Home Agent Address Discovery Request Message	0	
145	Home Agent Address Discovery Reply Message	0	
146	Mobile Prefix Solicitation	0	
147	Mobile Prefix Advertisement	0	
148	Certification Path Solicitation (SEND)		
149	Certification Path Advertisement (SEND)		
151	Multicast Router Advertisement (MRD)		
152	Multicast Router Solicitation (MRD)		
153	Multicast Router Termination (MRD)		
200	Private experimentation		
201	Private experimentation		
255	Reserved for expansion of ICMPv6 informational messages		

La tabla anterior no está completa. La lista actual de tipos y códigos ICMPv6 asignados puede encontrarse en este link: IANA: ICMPv6 Parameters (http://www.iana.org/assignments/icmpv6-parameters).

Véase también

- RFC 4443 *Especificación ICMPv6 para IPv6*

Enlaces externos

- NetworkSorcery (http://www.networksorcery.com/enp/protocol/icmpv6.htm) - Cabecera ICMPv6, Especificación campo Tipo, Código y CheckSum
- Microsoft TechNet (https://web.archive.org/web/20080229154700/http://technet2.microsoft.com/WindowsServer/es/Library/1b6e8d15-07ab-42ae-8f25-0b7acc833edf3082.mspx?mfr=true) - Breve descripción del protocolo ICMPv6