ICMP Protocol

Transcribed on July 12, 2025 at 4:35 PM by Minutes AI

Speaker 1 (00:00)

Hola a todos, bienvenidos a esta clase donde vamos a estar hablando del protocolo Icmp.

A lo largo de esta clase vamos a ver qué es el protocolo Icmp, los casos de uso en los que se utiliza este protocolo Icmp, también el formato de los datagramas icmp y terminaremos viendo los diferentes mensajes de control que existen dentro de este protocolo.

Antes de hablar del protocolo Icmp, recordaros que anteriormente habíamos comentado que el protocolo ip es un protocolo no orientado a conexión, es decir, no existe una comunicación ni una conexión previa entre origen y destino.

Y también comentaros que el protocolo ip era un protocolo de una naturaleza no confiable, es decir, no podemos confiar en él en que vaya a entregar y vaya a entregar también en orden los paquetes ip.

Necesitamos recurrir al protocolo Icmp en algunas ocasiones para que sirva este de complemento al protocolo ip y suministrarnos información sobre los aspectos de entrega del paquete e información como errores.

Los mensajes icmp se encapsulan en paquetes ip.

Por tanto podríamos resumir que el protocolo icmp es un protocolo que complementa al protocolo Ip y que lo que nos permite es informarnos sobre el estado de la red y los diferentes errores que se producen en esta.

Ahora vamos a ver los casos de uso más populares de este protocolo icmp.

Son los siguientes y seguro que os suena alguno de ellos.

Empezamos por el pin.

El pin es el uso más conocido.

Aquí lo que hacemos es enviar un mensaje de tipo echo request, un mensaje de tipo echo request icmp y esperamos un echo reply.

De esta forma comprobamos si el host es alcanzable y además si el host está activo.

Otro de los casos de uso es trade root y lo que hacemos es utilizar mensajes icmp y recibirlos y manejarnos correctamente los mensajes de tipo tiempo excedido con su objetivo pues lo que haremos será enviar paquetes con valores ttl gradualmente eficientes y escuchar los mensajes icmp de tiempo excedido para saber por qué enrutadores y por qué ips ha pasado nuestro paquete a lo largo del camino.

También, como comentábamos antes, icmp se utiliza para diagnosticar problemas de conectividad en la red.

Varios mensajes icmp nos proporcionan información sobre problemas de red encontrados durante la transmisión de Pan.

Otro caso de uso muy extendido es el descubrimiento de MTU de ruta.

Aquí los mensajes icmp como paquete demasiado grande se utiliza para descubrir el MTu de una ruta.

De esta forma pues determinamos el tamaño máximo del paquete que se puede transmitir sin fragmentar a lo largo de una ruta.

¿Recordáis que los paquetes IP había que fragmentarlos?

Pues de esta forma sabemos el tamaño máximo de fragmento a enviar.

Luego tenemos el error reporting.

Icmp utiliza routers y host para reportar errores encontrados durante el procesamiento de paquetes IP.

Estos errores incluyen por ejemplo, el destino inalcanzable, el tiempo excedido o el problema de parámetro que indica que hay un problema con el encabezado IP.

Por último, otro caso de uso de ICMP es el redireccionamiento.

Tenemos mensajes de tipo redirección, como veremos a continuación, que lo que nos permiten es informar a los host de una red de un mejor enrutador de siguientes para llegar a un destino particular.

Esto al final lo que ayuda es optimizar los caminos que siguen los paquetes dentro de una red.

Y esta que veis aquí es la cabecera icmp.

Fijaros que esta cabecera no reemplaza la cabecera ip, sino que la complementa y se apoya en la misma.

En cuanto a la cabecera icmp observamos los siguientes el tipo, que es el itmp tipo que veremos a continuación, el código icmp subtipo, si queréis llamarlo así, por ejemplo un eco request tendrá el tipo ocho y el código cero.

De esta forma identificamos el mensaje que queremos enviar porque recibimos de tipo icmp.

Luego tenemos el campo chetsum, que es una suma de verificación para verificar que no hay errores y es calculada a partir de la cabecera y los datos icmp.

Y por último tenemos el campo de contenido que varía dependiendo del tipo y código de mensaje icmp que enviamos o recibimos.

Este campo es de cuatro bytes.

Vamos a ver ahora los diferentes tipos y códigos que existen en los mensajes de tipo Icmp.

Al final esto es un extracto que he capturado de la tabla que contiene la llana y vamos a verla más en profundidad ahora en su hoja.

Pues ya estamos por aquí en la página de la llana, fijaros icmp parameters y por aquí tenemos fijaros los tipos de parámetros que tenemos.

En el caso del T tenemos que el cero selector reply, el un y el dos son no asignados y están reservados para en un futuro destinarlos a otra cosa, pero en el tipo tres tenemos destino inalcanzable.

Y luego más por aquí abajo, tenemos que cada tipo puede tener diferentes códigos.

En el caso del echo reply, por ejemplo, el código cero y el tipo cero pues dice directamente que es un eco reply, no nos dice nada más.

En el caso del tres que veíamos destino in, pues tenemos diferentes códigos.

Nos dice que el tipo tres y el código cero es red inalcanzable, pero si el tipo es tres y el código es un, nos dice que el host es el que es inalcanzable a la red hemos llegado pero al host no.

En el caso del dos el protocolo es inalcanzable, en el tres el puerto, bueno en general pues nos permite informarnos de los diferentes errores que existen en la conexión.

Luego tenemos por aquí el tipo cinco con cuatro códigos diferentes para mostrar información relacionada con las redirecciones.

En el ocho por aquí tenemos el echo request, aquí únicamente tenemos el código cero, por tanto un tipo ocho y código cero nos indicará un echo request o el mítico pin.

Para responder a este echo request pues volveríamos al un aquí y responderíamos con un y esto significa efecto reply.

De esta forma pues sabemos diferenciar un paquete icmp de otro.

Si queréis ver más detalles de esta tabla podéis visitar kyana org, por aquí hay parámetros y podréis ver todos los tipos que existen y también los códigos relativos a cada tipo.

Por supuesto podréis consultar el RFC, que esto es muy interesante, de cada tipo asignado y podréis ver más información de ese mensaje y de lo que ocurre en el interior.

Y con esto llegamos al final de esta clase donde hemos visto que es el protocolo icmp, cuáles son los casos de uso, donde se utiliza, también hemos visto el formato de las cabeceras de este protocolo icmp, al final es complementario el protocolo ip, por tanto viajan ambas cabeceras.

Y por último hemos visto los diferentes mensajes de control que existen para este protocolo icmp, tanto los tipos como sus respectivos códigos.

Sin más me despido y nos vemos en la siguiente clase.

Muchas gracias y hasta la próxima.