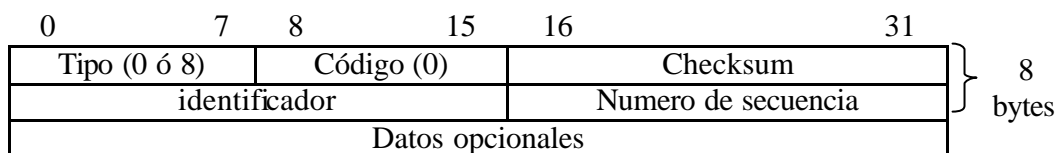


## Comando PING

El nombre “ping” es tomado de una operación sonora para encontrar algo. El programa ping fue escrito por Mike Mouss y su objetivo es probar si algún otro host es alcanzable. Para esto envía mensajes ECHO REQUEST de ICMP y espera en respuesta mensajes ECHO REPLY, también de ICMP.

Normalmente, si no se obtiene respuesta de un ping de un host, entonces tampoco se podrá acceder a una conexión Telnet o FTP. Ping es el punto de inicio para detectar un problema, pero también mide el tiempo en que recibe respuesta de un host, es una forma de saber que tan lejos se encuentra un host en específico.

Llamaremos al host que envía pings “cliente” y conoceremos al host que los recibe como “servidor”. En la mayoría de las implementaciones TCP/IP el soporte de un servidor ping se encuentra en el kernel, no es un proceso de usuario. El formato de la trama es el siguiente:



Como cualquier otra petición ICMP, el servidor debe saber el identificador y el número de secuencia de los campos, aunque los datos son opcionales.

Unix coloca en el campo identificador un ID del proceso que envía los mensajes, lo cual permite identificar las respuestas devueltas, si existen muchas entidades ejecutando un ping al mismo tiempo y al mismo host.

El número de secuencia inicia en 0 y es incrementado cada vez que se envía a un nuevo mensaje ECHO REQUEST. Ping imprime esta secuencia de cada paquete enviado, permitiendo identificar paquetes perdidos, reordenados o duplicados.

Históricamente, un programa ping, hacía una petición a la vez e imprimía cada respuesta recibida, la cual podía ser del tipo “esta vivo” o “no hay respuesta”. Si un ECHO REPLY es regresado, el número de secuencia es impreso, seguido del TTL o el tiempo en que tardó la respuesta.

Ping puede calcular el tiempo en que recibió un mensaje ECHO REPLY, insertando el tiempo en que es enviado el paquete ECHO REQUEST, como una porción de datos, cuando un ECHO REPLY es recibido, este resta el valor del tiempo actual, quedando así solamente el tiempo en que se tardó un paquete en ir y regresar.

En algunas ocasiones, el primer paquete enviado puede ser el que tarde mas en regresar una respuesta, puesto que la dirección de hardware, correspondiente a la dirección IP solicitada, no se encuentra en la caché de ARP del host que envía el paquete.

Además de la varianza que pueda existir en los tiempos en que regresa un paquete, es posible detectar un porcentaje de paquetes perdidos, esto puede ser detectado por la impresión de números de secuencia impresos mas de una vez (paquetes duplicados) o números de secuencia N+1 antes del número de secuencia N (paquetes reordenados).

En una red de área local se puede conocer la velocidad de conexión, el cual puede ser útil para calcular el tiempo real que deberían tardarse los paquetes ICMP para enviar un ping entre dos host. Suponiendo que la velocidad es 1200 bits/seg. Con 8 bits por bytes más 1 bit de inicio y 1 bit de fin, la velocidad se convierte en 120 bytes/seg. ó 8.33 mseg. por byte.

Si un paquete de ping envía 56 bytes de datos, más 8 bytes de la cabecera ICMP (64 bytes impresos en pantalla) más 20 bytes de la cabecera I, entonces quiere decir que se enviarán 86 bytes, por lo tanto, el tiempo que tardaría un paquete ping en ir y regresar es de  $(86 \text{ bytes})(8.33 \text{ mseg.})(2 \text{ veces}) = 1433 \text{ mseg.}$  El 2 veces es el tiempo de ida mas el tiempo de regreso, despreciando el tiempo de generación del mensaje en cada host por ser despreciable a medida que los ordenadores son cada vez más rápidos.

Si los mensajes ECHO REQUEST son enviados cada segundo y se ha obtenido que el tiempo en que tardaría una respuesta ECHO REPLY durará 1.4 segundos, como se calculó, probablemente detectará un mensaje perdido, sin embargo, no significa que esté perdido, sino que está en camino de regreso, puesto que mientras regresa el primer ECHO REPLY (en 1.4 segundos) ya se han enviado dos ECHO REQUEST (en 0 y 1 segundos).

### Opción grabar ruta IP (IP Record Route)

Ping da la oportunidad de observar la ruta IP grabada. Esto lo hace al colocar la opción IPRR en el datagrama Ip de salida, que contiene el mensaje ECHO REQUEST, lo cual ocasiona que cada ruteador que manipule el datagrama, añada su dirección IP a la lista en el campo opciones. Cuando el datagrama encuentra su destino final, la lista de direcciones IP es copiada en el mensaje ECHO REPLY. Finalmente, cuando ping recibe éste último mensaje, lo imprime en pantalla.

Sin embargo, la cabecera de un datagrama IP está formada por campos de 4 bits, limitada a 15 palabras de 32 bits (60 bytes), de los cuales, la cabecera IP requiere 20 bytes y 3 bytes para indicar la opción IPRR, por lo que solo restan 37 bytes para la lista de direcciones IP, lo cual se traduce en 9 direcciones IP posiblemente a almacenar.

Código	Longitud	PTR	Dir. IP 1	Dir. IP 2	Dir. IP 3	...	Dir. IP 9
1 byte	1 byte	1 byte	4 bytes	4 bytes	4 bytes	...	4 bytes
		PTR =	4	8	12	36	40

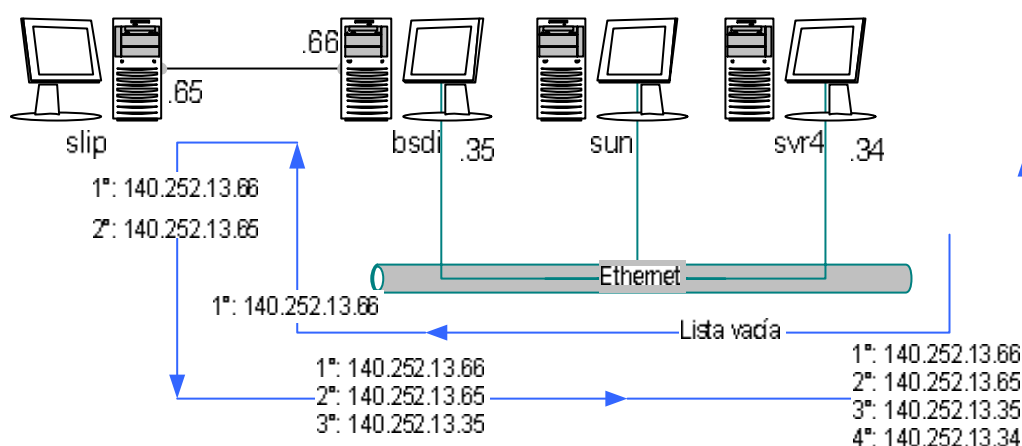
Código es igual a 7 para indicar la opción IP Record Route (IPRR).

Longitud es el número de bytes de la opción (39 en este caso).

PTR es el puntero que indica el byte siguiente para guardar la siguiente dirección. Puede tener valores de 4, 8, 12 hasta 36, el 40 indica la lista llena.

RFC 791 especifica que la dirección IP que grabará un ruteador que une a 2 o más redes diferentes, será aquella que identifique la red destino. También es de notar que cuando un host envía un mensaje ECHO REQUEST con la opción IPRR, al recibir la respuesta ECHO REPLY, este también guarda su dirección IP.

Ejemplo:



Si enviamos un ping desde 140.252.13.34 a 140.252.13.65, con la opción IPRR, la instrucción y los resultados que obtendríamos en pantalla, serían los siguientes:

\$ ping -R slip

64 bytes from (140.252.13.65) cmp\_seq=0 TTL=254 Time=280ms

RR: bsdi (140.252.13.66)  
slip (140.252.13.65)  
bsdi (140.252.13.35)  
svr4 (140.252.13.34)

Para entender mejor la secuencia, en la figura se muestra gráficamente los procesos que se llevan a cabo.

### Opción Timestamp

Código	Longitud	PTR	OF	FL	Timestamp 1	Timestamp 2	...	Timestamp 9
1 byte	1 byte	1 byte	4 bits	4 bits	4 bytes	4 bytes	...	4 bytes

Código es 0x44 para indicar la opción Timestamp

Longitud es 36 o 40 normalmente

PTR toma valores de 5, 9, 15, etc.

OF es el valor de sobreflujo (overflow)

FL es el campo de banderas, el cual puede tomar los siguientes valores:

- 0 Graba solo timestamps.
- 1 Graba cada dirección IP del ruteador por el que paso y su timestamp. En este caso, la lista se reduce a un máximo de 4 campos.
- 3 El cliente inicializa la lista con 4 pares de dirección IP y timestamp. Un ruteador graba el timestamp si la próxima dirección IP en la lista congenia con la del ruteador.

Si el ruteador no puede agregar un timestamp por la longitud, simplemente incrementa el campo OF. El comando traceroute, sin embargo, es más útil para medir los tiempos de respuesta de cada host por el que pasa el mensaje.