

Protocolo ICMP

Ing. Gilberto Sánchez Quintanilla

Introducción

- ICMP es el Protocolo de Mensajes de Control de Internet (Internet Control Message Protocol), el cual informa de condiciones de **error y control**.
- **IP** proporciona utilidad de entrega de datagramas de un extremo a otro, pero **no proporciona** ninguna utilidad para **informar de errores** de enrutamiento o entrega.

Introducción

- Cuando un protocolo encuentra un error que no se puede recuperar en el procesamiento de un paquete, puede realizar las siguientes acciones:
 - ♦ ***Descarte no informado***: Elimina el paquete infractor sin enviar una notificación al host origen. Ej.: Una NIC Ethernet comprueba cada trama para ver el error con el CRC. Si tiene error la trama, se elimina.
 - ♦ ***Descarte informado***: Elimina el paquete infractor y envía una notificación al host origen.

Introducción

- **ICMP** es un protocolo extensible que también proporciona funciones para **comprobar la conectividad IP** y ayudar en la configuración automática de los host.
- **ICMP no hace que IP sea confiable.** No existe utilidad para IP o ICMP para proporcionar secuencia o retransmisión de datagramas IP que presenten error.

Introducción

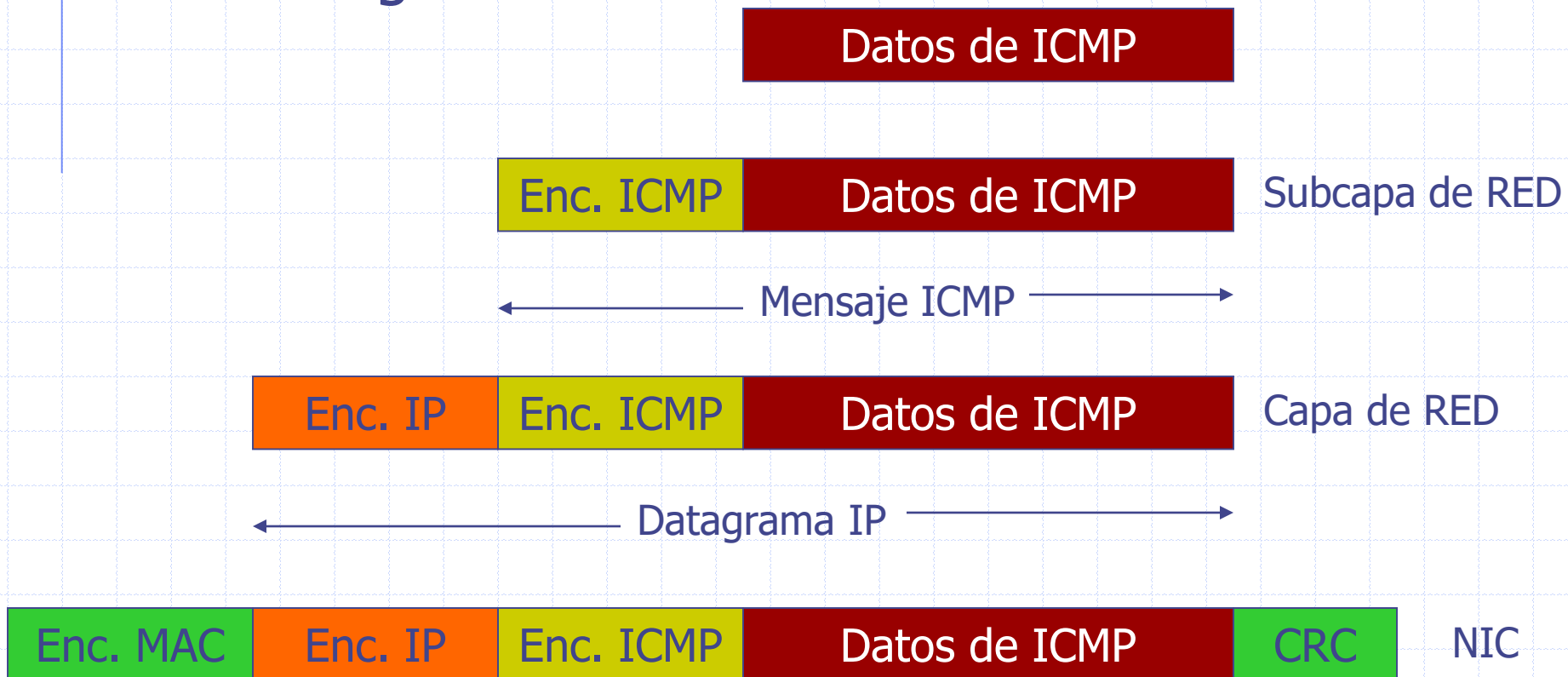
- ICMP se envía como datagrama IP
- ICMP informa de un error, pero no existe ningún requisito de cómo debe tratar el error el host emisor.
- Depende de la implementación TCP/IP interpretar el error y ajustar su comportamiento del modo correspondiente.

Introducción

- Los **mensajes ICMP** sólo se envían para el **primer fragmento** de un datagrama.
- Los mensajes de **ICMP no se envían** para problemas encontrados por **mensajes de error ICMP** o por datagramas de **difusión o multidifusión**.

Estructura de un Mensaje de ICMP

- Los mensajes de ICMP se envían como datagramas IP.

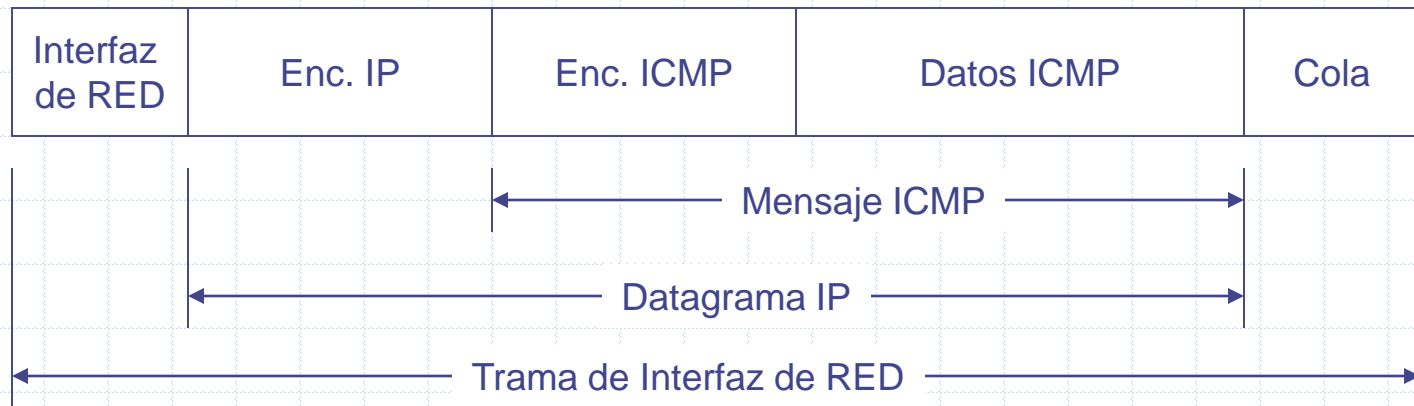


Estructura de un Mensaje de ICMP

- En el encabezado IP de los mensajes de ICMP, el campo dirección **IP origen** se configura como **el ruteador o la interfaz de host** que envía el mensaje de ICMP.
- El campo dirección **IP destino** se configura como el **host emisor del paquete infractor** (en el caso de mensajes de error de ICMP) o un **host específico**.

Estructura de un Mensaje de ICMP

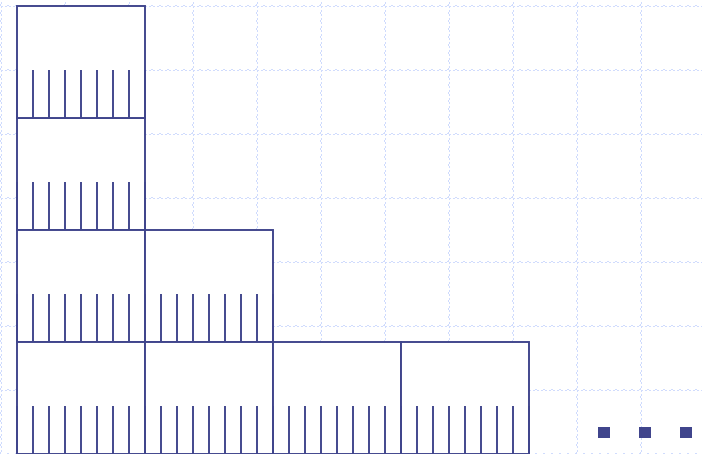
- Los mensajes de ICMP tienen la siguiente estructura



[illegible]

Código

Datos específicos del tipo



Mensaje de ICMP

■ Tipo

- ◆ Campo de 1 byte que indica el tipo de mensaje ICMP

Tipo ICMP	Descripción
0	Respuesta de ECO
3	Destino inalcanzable
4	Flujo de origen
5	Redirección
8	Solicitud de ECO
9	Anuncio de enrutador
10	Solicitud de enrutador
11	Tiempo de espera agotado
12	Problema de parametros

Mensaje de ICMP

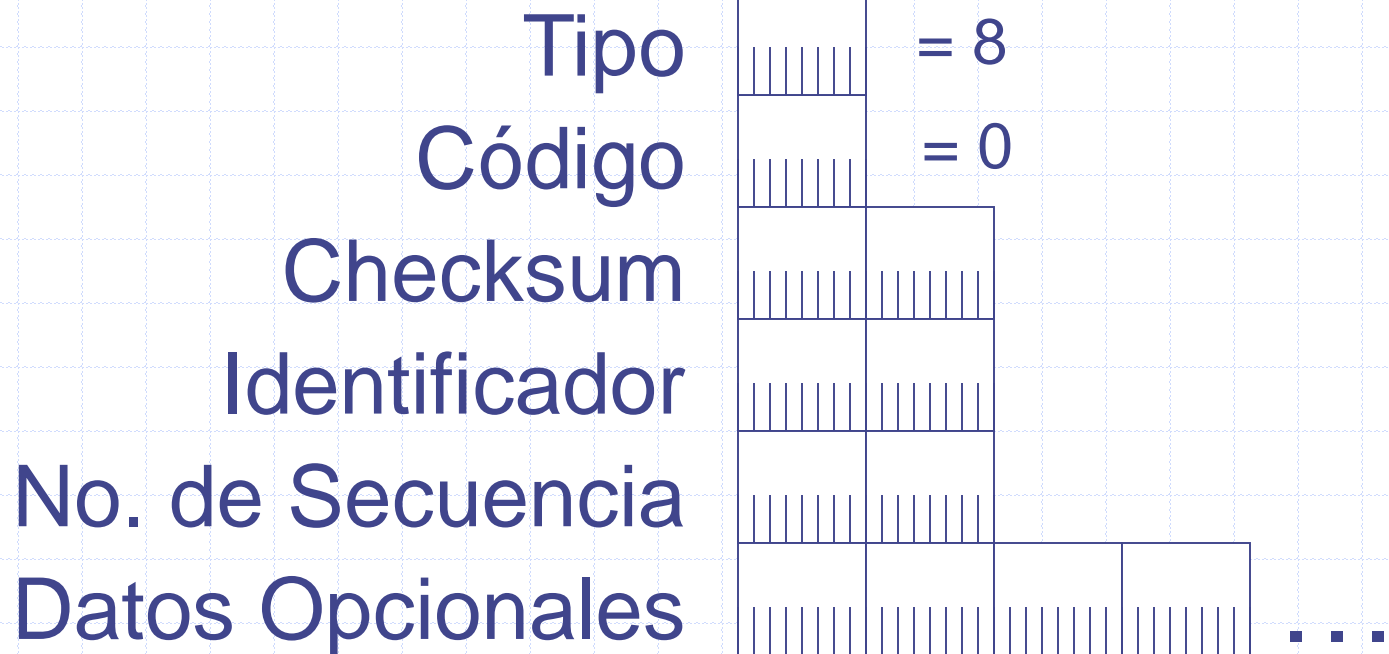
- Código
 - ◆ Campo de 1 byte que indica un mensaje ICMP específico dentro de un tipo ICMP.
- Suma de comprobación
 - ◆ Campo de 2 bytes para una suma de comprobación de 16 bits que cubre el mensaje ICMP (Enc. ICMP y datos ICMP).
- Datos específicos del tipo
 - ◆ Datos especiales para cada tipo ICMP.

Solicitud y Respuesta de ECO

- Esta es una de las utilidades más usadas, donde se envía un mensaje sencillo a un nodo IP y devuelve el mensaje de eco al remitente.
- Se utiliza para la depuración y solución de problemas de red.
- Las utilidades **ping**, **tracert** y **pathping** utilizan mensajes de eco y respuestas de eco.

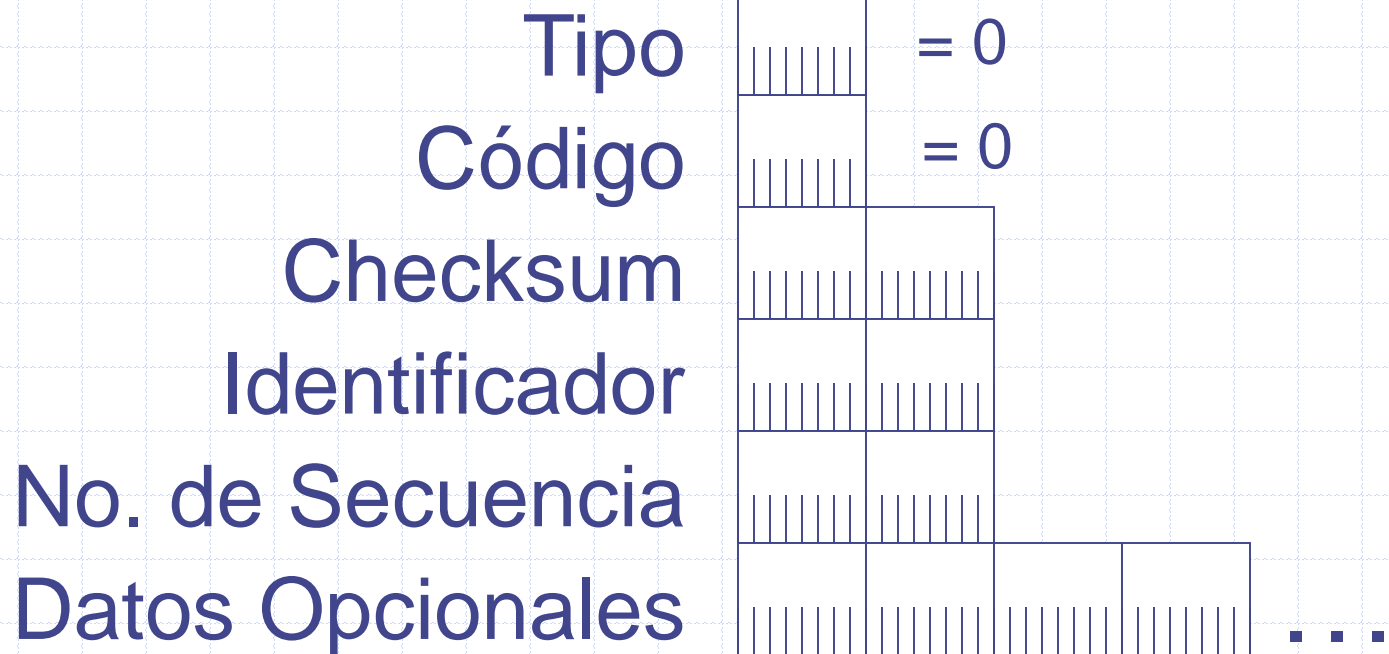
Solicitud de ECO

- Solicitud de ECO



Respuesta de ECO

- Respuesta de ECO



Solicitud y Respuesta de ECO

- Identificador

- ◆ Campo de 2 bytes que almacena un número generado por el remitente que se utiliza para **reunir la solicitud de ECO con** su correspondiente **respuesta de ECO**.

- Número de secuencia

- ◆ Campo de 2 bytes que almacena un número adicional que se utiliza para **reunir la solicitud de ECO con** su correspondiente **respuesta de ECO**.

Utilidad ping

- Es la principal herramienta de red para resolver problemas de conectividad IP.
- La utilidad ping prueba la accesibilidad, el enrutamiento de origen, la latencia de red y otros aspectos de IP.
- PING envía un mensaje de eco ICMP a un destino y registra el tiempo de recorrido completo, el número de bytes enviados y el TTL de la respuesta de eco correspondiente.

Utilidad ping

- Cuando ping termina de enviar mensajes de eco, muestra estadísticas del promedio de respuesta y el tiempo de recorrido completo.
- Al hacer ping a una dirección IP de destino, el comportamiento predeterminado es enviar 4 solicitudes de eco, fragmentables, sin ruta de origen con un campo de datos opcional de 32 bytes y espera de 1 segundo por la respuesta de ICMP correspondiente.

Utilidad ping

- En el encabezado de los mensajes de eco, generados mediante ping,
 - ◆ El campo identificador se configura con un valor múltiplo de 256(ej.: 0x0300)
 - ◆ El campo número de secuencia para el primer mensaje se elige como múltiplo de 256 y los sucesivos se incrementan en 256.
 - ◆ El campo Datos opcionales es de 32 bytes (de manera predeterminada), y esta formado por la cadena "abcdefghijklmnopqrstuvwabcdefghi"

Utilidad ping

```
C:\>ping www.upiicsa.ipn.mx
```

```
Haciendo ping a www.upiicsa.ipn.mx [148.204.115.2] con 32 bytes de datos:
```

```
Respuesta desde 148.204.115.2: bytes=32 tiempo=2ms TTL=124
```

```
Respuesta desde 148.204.115.2: bytes=32 tiempo<1m TTL=124
```

```
Respuesta desde 148.204.115.2: bytes=32 tiempo<1m TTL=124
```

```
Respuesta desde 148.204.115.2: bytes=32 tiempo<1m TTL=124
```

```
Estadísticas de ping para 148.204.115.2:
```

```
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
```

```
(0% perdidos),
```

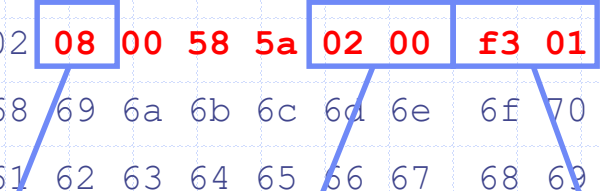
```
Tiempos aproximados de ida y vuelta en milisegundos:
```

```
Mínimo = 0ms, Máximo = 2ms, Media = 0ms
```

Utilidad ping

Solicitud de ECO de 148.204.25.27 a 148.204.115.2

0000	00	01	f4	43	c9	19	00	50	ba	b2	f3	7b	08	00	45	00	...C...P ...{...E.
0010	00	3c	09	0d	00	00	80	01	7b	fe	94	cc	19	1b	94	cc	.<..... {.....
0020	73	02	08	00	58	5a	02	00	f3	01	61	62	63	64	65	66	s...XZ.. ..abcdef
0030	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76	ghijklmn opqrstuv
0040	77	61	62	63	64	65	66	67	68	69							wabcdefg hi



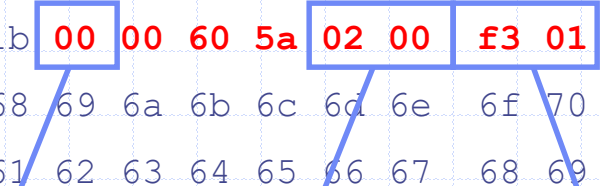
Tipo: Sol. de ECO

Identificador

No. de secuencia

Respuesta de ECO de 148.204.115.2 a 148.204.25.27

0000	00	50	ba	b2	f3	7b	00	01	f4	43	c9	19	08	00	45	00	.P...{... .C....E.
0010	00	3c	df	5c	00	00	7c	01	a9	ae	94	cc	73	02	94	cc	.<.\...s...
0020	19	1b	00	00	60	5a	02	00	f3	01	61	62	63	64	65	66`Z.. ..abcdef
0030	67	68	69	6a	6b	6c	6d	6e	6f	70	71	72	73	74	75	76	ghijklmn opqrstuv
0040	77	61	62	63	64	65	66	67	68	69							wabcdefg hi



Tipo: Resp. de ECO

Identificador

No. de secuencia

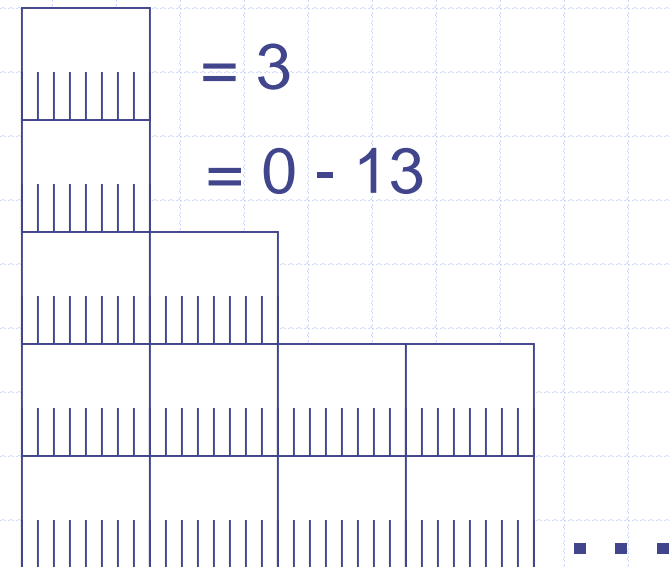
Destino inalcanzable ICMP

- Cuando se envía un datagrama, IP hace el mejor esfuerzo para entregar de la forma más conveniente de los datagramas a su destino.
- Pero pueden ocurrir errores de enrutamiento o entrega a lo largo de la ruta de acceso o en el destino.
- Cuando ocurre un error de entrega o enrutamiento, un enrutador o el destino eliminan el datagrama infractor y trata de informar el error enviando el mensaje Destino Inalcanzable, al origen.

Destino inalcanzable ICMP

- Destino inaccesible ICMP

Tipo
Código
Checksum
No utilizado
Enc. IP y primeros 8 bytes del datagrama



Destino inalcanzable ICMP

■ Códigos de destino inaccesible ICMP

- ◆ 0. Red Inalcanzable
- ◆ 1. Host Inalcanzable
- ◆ 2. Protocolo Inalcanzable
- ◆ 3. Puerto Inalcanzable
- ◆ 4. Necesita Fragmentación y se especificó DF
- ◆ 5. Error en ruta fuente
- ◆ 6. Red de destino desconocida
- ◆ 7. Host de destino desconocido
- ◆ 8. Host de origen aislado
- ◆ 9. Comunicación prohibida por el administrador con la red de destino
- ◆ 10. Comunicación prohibida por el administrador con el host de destino
- ◆ 11. Red Inaccesible por el tipo de servicio
- ◆ 12. Host inalcanzable por el tipo de servicio
- ◆ 13. Comunicación prohibida debido a un servidor de seguridad.

Destino inalcanzable ICMP

■ Puerto inaccesible

- ◆ Enviado por un host de destino cuando el puerto del encabezado UDP o TCP no coincide con una aplicación que se ejecuta en el destino.
- ◆ En la práctica, cuando no se pueden encontrar puertos TCP, TCP envía el segmento conexión reestablecida (RST).
- ◆ De este modo, los mensajes puerto inaccesible solo se envían por mensajes UDP.

Destino inalcanzable ICMP

- Ejemplo de puerto inalcanzable (Código 03)
 - ♦ Cuando un cliente DNS(Domain Name System, el cual utiliza los servicios de UDP de capa de transporte) envía un mensaje a un servidor DNS a través de un puerto 53, el servidor debe recibir los datos del cliente y responder si fuese necesario.
 - ♦ Cuando una terminal (host o servidor) recibe un mensaje con el puerto 53 y no esta prestando un servicio a través de éste, elimina el paquete y envía al origen un mensaje de ICMP indicando que el paquete fue eliminado porque el destino es inalcanzable debido a que el puerto es inalcanzable.

Destino inalcanzable ICMP

Mensaje de DNS enviado a la terminal 148.204.25.111 la cual no es un servidor de DNS

0000	00 02 d1 02 d4 ca 00 50	ba b2 f3 7b 08 00 45 00P ...{..E.
0010	00 3f 07 dc 00 00 80 11	d6 af 94 cc 19 1b 94 cc	.?.....
0020	19 6f 04 0c 00 35 00 2b	4e 6d 52 a7 01 00 00 01	.o...5.+ NmR.....
0030	00 00 00 00 00 00 03 77	77 77 06 67 6f 6f 67 6cw ww.googl
0040	65 03 63 6f 6d 02 6d 78	00 00 01 00 01	e.com.mx

Puerto: 53 DNS

Protocolo: UDP

Mensaje ICMP de error enviado por la terminal 148.204.25.111

0000	00 50 ba b2 f3 7b 00 02	d1 02 d4 ca 08 00 45 00	.P...{..E.
0010	00 38 26 2d 00 00 40 01	f8 75 94 cc 19 6f 94 cc	.8&-...@. .u...o..
0020	19 1b 03 03 aa 23 00 00	00 00 45 00 00 3f 07 dc#.. ..E..?..
0030	00 00 80 11 d6 af 94 cc	19 1b 94 cc 19 6f 04 0co..
0040	00 35 00 2b 4e 6d		.5.+Nm

Tipo:

Clase:

Inicio de encabezado del
Paquete eliminado

Dest. Inalcanzable

Puerto. Inalcanzable

Destino Inalcanzable

- Red Inalcanzable

- ◆ Enviado por el ruteador cuando no se puede encontrar una ruta para la dirección IP de destino en la tabla de ruteo.
- ◆ La dirección IP de origen de este mensaje identifica al ruteador que no puede encontrar una ruta.

Destino inalcanzable ICMP

Solicitud de eco enviada a la terminal con IP 20.20.20.20

```
0000  00 01 f4 43 c9 19 00 50  ba b2 f3 7b 08 00 45 00  ...C...P ...{...E.
0010  00 5c 08 40 00 00 0c 01  d0 52 94 cc 19 1b 14 14  .\.@.... .R.....
0020  14 14 08 00 61 fe 02 00  94 01 00 00 00 00 00 00  ....a... .....
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  .....
0060  00 00 00 00 00 00 00 00  00 00                                ..... ..
```

Mensaje ICMP de error enviado por el ruteador 12.124.219.22

```
0000  00 50 ba b2 f3 7b 00 01  f4 43 c9 19 08 00 45 20  .P...{.. .C....E
0010  00 38 00 00 00 00 f2 01  33 2b 0c 7c db 16 94 cc  .8..... 3+.|....
0020  19 1b 03 00 fc ff 00 00  00 00 45 00 00 5c 08 40  ..... ..E..\.@
0030  00 00 01 01 db 52 94 cc  19 1b 14 14 14 14 08 00  ....R.. .....
0040  61 fe 02 00 94 01                                a.....
```

Tipo:

Dest. Inalcanzable

Clase:

Red Inalcanzable

**Inicio de encabezado del
Paquete eliminado**

Destino Inalcanzable

■ Host Inalcanzable

- ◆ Enviado por un ruteador IP cuando no se ha encontrado una ruta al destino en la tabla de ruteo.
- ◆ En la Internet, se trata del mensaje más adecuado cuando un ruteador no puede determinar el próximo salto para un datagrama IP.
- ◆ La dirección IP de origen de este mensaje identifica al ruteador que no ha podido entregar el datagrama al host destino.

Destino inalcanzable ICMP

Solicitud de eco enviada a la terminal con IP 10.0.0.1

```
0000  08 00 09 72 74 e0 00 00  b4 34 b7 fa 08 00 45 00  ...rt... .4....E.
0010  00 3c 8a 03 00 00 20 01  26 aa 86 27 59 ec 0a 00  .<..... &...'Y...
0020  00 01 08 00 1b 5c 01 00  31 00 61 62 63 64 65 66  .....\\.. 1.abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                                wabcdefg hi
```

Mensaje ICMP de error enviado por el ruteador 168.156.1.33

```
0000  00 00 b4 34 b7 fa 08 00  09 72 74 e0 08 00 45 00  ...4.... .rt...E.
0010  00 38 7a a9 00 00 fc 01  ba 4a a8 9c 01 21 86 27  .8z..... .J...!.'
0020  59 ec 03 01 a7 a2 00 00  00 00 45 00 00 3c 8a 03  Y..... ..E..<..
0030  00 00 1c 01 2a aa 86 27  59 ec 0a 00 00 01 08 00  ....*...' Y.....
0040  1b 5c 01 00 31 00                                .\\..1.
```

Tipo:

Dest. Inalcanzable

Clase:

Host Inalcanzable

**Inicio de encabezado del
Paquete eliminado**

Tiempo excedido de ICMP

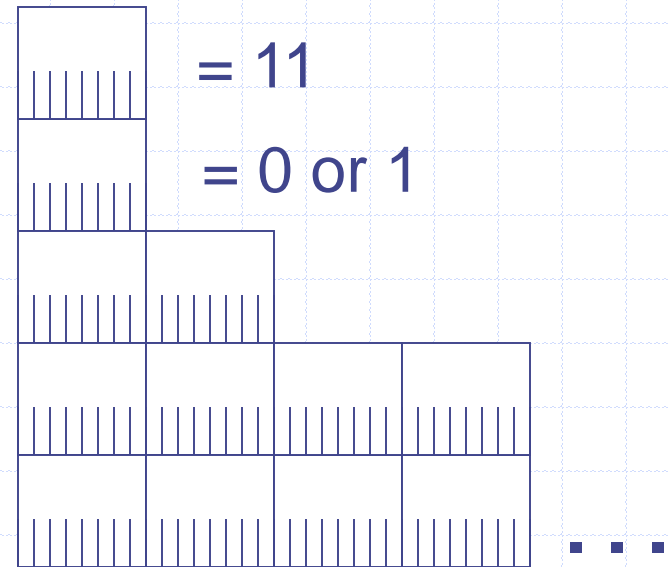
- El mensaje Tiempo Excedido de ICMP se envía en los siguientes casos:
 - ♦ Cuando un ruteador decrementa el campo TTL del encabezado IP a 0.
 - ♦ Cuando el temporizador de reensamblado de un datagrama IP fragmentado expira.

Tiempo excedido de ICMP

- Cuando el campo TTL llega a 0 en un datagrama IP, puede significar dos cosas:
 - ♦ El datagrama IP se envió con un TTL inapropiado que no reflejaba el número real de enlaces entre el origen y el destino. En este caso se debería incrementar el TTL.
 - ♦ Existe un bucle de enrutamiento en el conjunto de redes.

Tiempo excedido de ICMP

Tipo
Código
Checksum
No usados
Enc. IP y primeros 8
bytes de datos de
datagrama



Código = 0: TTL Expiro

Código = 1: Tiempo de Reensamblado Expiro

Tiempo excedido de ICMP

Solicitud de eco enviada por 148.204.25.27 a 148.204.115.2

0000	00 01 f4 43 c9 19 00 50	ba b2 f3 7b 08 00 45 00	...C...P ...{...E.
0010	00 5c 08 cf 00 00 04 01	f8 1c 94 cc 19 1b 94 cc	.\.....
0020	73 02 08 00 06 fe 02 00	ef 01 00 00 00 00 00 00	s.....
0030	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0040	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0050	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0060	00 00 00 00 00 00 00 00	00 00

TTL: 4

Mensaje ICMP de error enviado por el ruteador 148.204.0.162

0000	00 50 ba b2 f3 7b 00 01	f4 43 c9 19 08 00 45 c0	.P...{.. .C....E.
0010	00 38 00 00 00 00 3d 01	39 b0 94 cc 00 a2 94 cc	.8....=. 9.....
0020	19 1b 0b 00 f4 ff 00 00	00 00 45 00 00 5c 08 cfE..\..
0030	00 00 01 01 fb 1c 94 cc	19 1b 94 cc 73 02 08 00s...
0040	06 fe 02 00 ef 01	

Tipo:

Tiempo excedido

Clase:

TTL expiro

Inicio de encabezado del
Paquete eliminado

Utilidad tracer

- La utilidad tracer usa mensajes de ECO de ICMP para determinar la ruta o la serie de ruteadores, que sigue un datagrama IP desde un host origen hasta llegar al host destino.
- Cuando se ejecuta un tracer con una dirección IP de destino, su comportamiento predeterminado es realizar una traza de la ruta y generar un informe de los tiempos de ida y vuelta de las direcciones de las interfaces cercanas de los ruteadores.

Utilidad tracert

■ Funcionamiento de tracert

- ♦ Se envía un eco al destino con un TTL =1. Si el destino se encuentra en la misma red, este responde con la correspondiente respuesta de eco.
- ♦ Si el destino no está conectado directamente en la red, el mensaje de eco es enviado al primer ruteador.
- ♦ El ruteador determina que el datagrama es tráfico en tránsito y decrementa su TTL. Como TTL ahora vale cero, el ruteador descarta el datagrama IP y envía de vuelta un mensaje de Tiempo excedido-TTL expiro al host origen.

Utilidad tracert

- ♦ La interfaz donde recibió este datagrama IP, es la interfaz cercana.
- ♦ Tras recibir el mensaje de Tiempo excedido-TTL expiro, la utilidad tracert registra el tiempo de ida y vuelta y la dirección IP de origen (IP del ruteador).
- ♦ Tracert envía dos mensajes de eco más con TTL=1 y registra los tiempos.
- ♦ Incrementa el TTL de uno en uno, hasta que recibe la correspondiente respuesta de eco del host destino.

Utilidad tracert

```
C:\>tracert -d www.upiicsa.ipn.mx
```

Traza a la dirección `www.upiicsa.ipn.mx` [148.204.115.2]
sobre un máximo de 30 saltos:

1	<1 ms	<1 ms	<1 ms	148.204.25.254
2	<1 ms	<1 ms	<1 ms	148.204.0.129
3	1 ms	1 ms	<1 ms	10.204.0.14
4	2 ms	<1 ms	<1 ms	148.204.0.162
5	1 ms	<1 ms	<1 ms	148.204.115.2

Traza completa.