REDES DE COMPUTADORES

Grado en Ingeniería Informática
Doble Grado en Ingeniería Informática y ADE

Curso académico 2019/2020

PRÁCTICA 2. Protocolo de Mensajes de Control de Interred (ICMP)

Contenidos

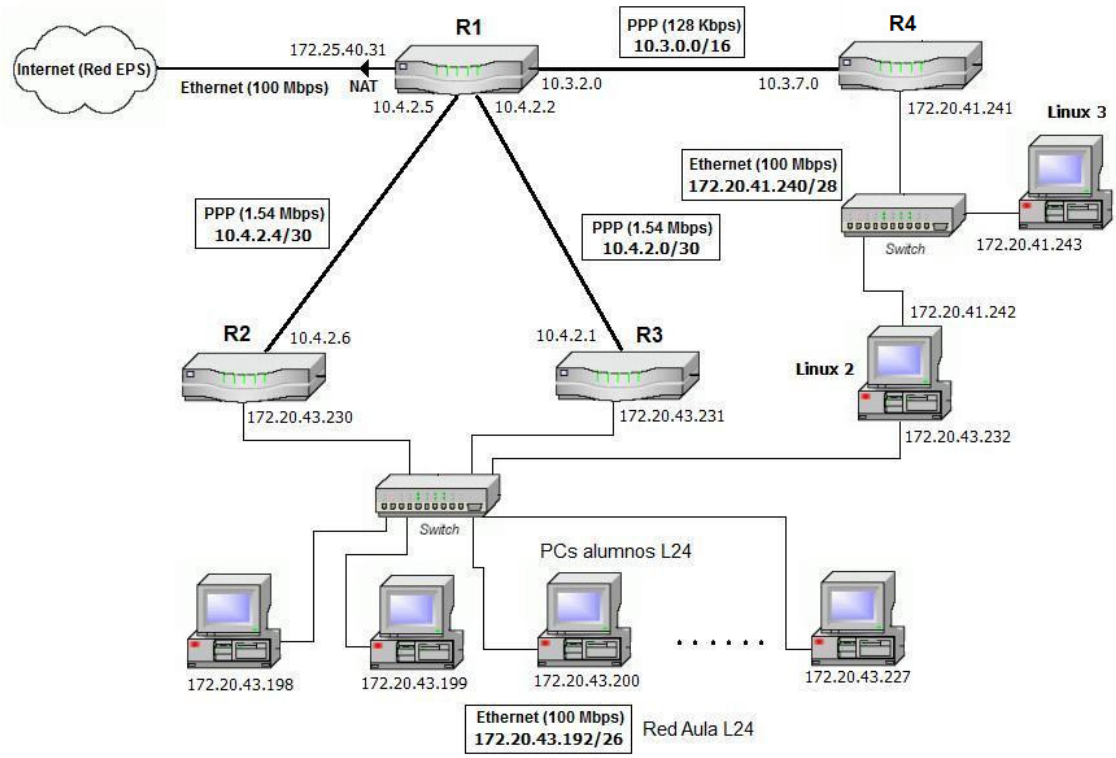
1. OBJETIVOS

El objetivo de la práctica 2 de la asignatura Redes de Computadores es el estudio del protocolo ICMP, el cual se apoya para su funcionamiento en el protocolo IP.

El alumno adquirirá conocimientos acerca de los diferentes mensajes ICMP y su utilidad a la hora de evaluar el funcionamiento de una red.

En la realización de la práctica se abordarán distintas situaciones de error en el funcionamiento de una red de datagramas basada en el protocolo IP y se evaluará de forma práctica los tiempos de respuesta en la red.

El esquema de la red del laboratorio que se dispone para la realización de las prácticas se muestra a continuación.



2. PROTOCOLO ICMP

ICMP (*Internet Control Message Protocol*, Protocolo de Mensajes de Control de Interred) es un protocolo que para su funcionamiento se apoya sobre el protocolo IP dentro de la arquitectura TCP/IP. Su misión es informar del estado y situaciones de error en el funcionamiento de la capa de red, sobre todo de aspectos como el encaminamiento, congestión, fragmentación, etc.

Los mensajes ICMP son transmitidos en el interior de datagramas (paquetes) IP, como se muestra en la siguiente figura.

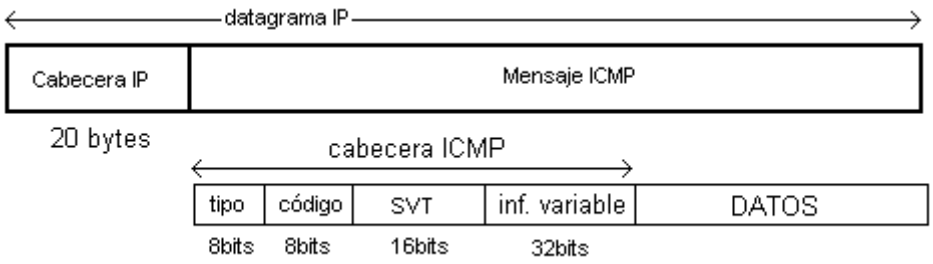


Figura 1. Encapsulación de un mensaje ICMP dentro de un paquete IP.

El mensaje ICMP consta de una cabecera, donde aparecen los campos **tipo**, **código**, **SVT** e **información variable**, y un cuerpo de datos.

A continuación se describen los diferentes **tipos** de mensajes ICMP:

- *Echo Reply*. Tipo 0
- Destino inaccesible. Tipo 3
- Cadencia de envío demasiado elevada (Control de flujo). Tipo 4

- Redirección. Tipo 5
- *Echo Request*. Tipo 8
- Aviso de Router. Tipo 9
- Solicitud de Router. Tipo 10
- Tiempo sobrepasado (ttl). Tipo 11
- Problema de parámetros o de forma. Tipo 12
- Petición 'Timestamp'. Tipo 13
- Respuesta 'Timestamp'. Tipo 14

El campo tipo se complementa con la información suministrada por el campo ***código***. En función del valor que tomen ambos, el receptor del mensaje puede obtener información muy concreta acerca de cuál es el estado de funcionamiento de la red.

El campo **SVT** se denomina secuencia de verificación de trama y consiste en una suma de control de todo el paquete ICMP.

Los siguientes 32 bits después del campo SVT, **información variable**, tienen un propósito que varía y se especifican de forma diferente para cada tipo de mensaje ICMP considerado.

Mensajes ICMP de solicitud y mensajes ICMP de error

Podemos distinguir entre dos clases de mensajes ICMP: En el caso de un mensaje ICMP de petición o solicitud, se solicita o se informa de un acontecimiento concreto que no es causa de ningún error. Una respuesta a un eco ICMP lanzado por la aplicación 'ping' o un aviso de presencia de router, serían un ejemplo de ello. En este caso, en el campo de datos del mensaje ICMP se introduce información relativa al mensaje de solicitud o información.

En el caso de un mensaje ICMP de error se informa de situaciones de error que se producen en el envío de paquetes IP en la red, como puede ser cuando el campo TTL alcanza el valor cero, una máquina es inaccesible, una fragmentación es requerida pero imposible de realizar debido al bit '**don't fragment**', etc... Es importante tener en cuenta que un mensaje de error nunca puede ser producido como consecuencia de otro mensaje de error. Si esta regla no fuese aplicada, podríamos encontrarnos sobre escenarios en los que un error ICMP provoca otro error ICMP y así sucesivamente.

Un mensaje de error ICMP contiene en el campo de datos del mensaje la cabecera IP y los 8 primeros bytes de datos del paquete IP que lo provocó. Ello permite determinar qué paquete provocó el error analizando la cabecera IP contenida en el campo de datos del mensaje ICMP.

Las situaciones expuestas a continuación **no** generan mensajes de error ICMP:

- Un mensaje de error ICMP. (Un mensaje de error ICMP puede, a pesar de todo, ser generado como respuesta a una solicitud ICMP).
- Un paquete IP destinado a una dirección IP de 'broadcast'.
- Un paquete IP enviado como 'broadcast' de la capa de enlace.
- Un paquete IP fragmentado que no sea el primero de la secuencia.
- Un fragmento de paquete IP recibido fuera de secuencia.
- Un paquete IP cuya dirección origen no está asociada a una única máquina. Esto significa que la dirección origen no puede valer 0, ni ser una dirección de broadcast o de grupo.

Estas reglas son necesarias para prevenir las 'tormentas de *broadcast*' (*broadcast storms*), que aparecían en el pasado cuando los errores ICMP se generaban como respuesta a paquetes emitidos bajo la forma de '*broadcast*'.

3. MENSAJES ECHO Y ECHO REPLY

Existe en los sistemas Unix, Linux, OS/2, Windows, etc., un programa de aplicación denominado **ping** que presenta una serie de posibilidades que lo convierten en una herramienta muy valiosa a la hora de depurar y localizar errores, pues se fundamenta en el protocolo ICMP.

Ping, a diferencia del resto de aplicaciones TCP/IP, no utiliza ninguno de los protocolos de transporte TCP o UDP. Se apoya directamente sobre IP. Este aspecto debe tenerse en cuenta, dado que la recepción de una respuesta al comando ping indica que la máquina remota está activa a nivel IP, pero no asegura que el funcionamiento de su capa TCP o UDP sea el correcto.

Ping utiliza un mensaje *Echo Request* (tipo 8) para enviar un paquete IP a su destinatario y espera el retorno de un mensaje *Echo Reply* (tipo 0) del destinatario. De este modo es capaz de evaluar tiempos de respuesta promedios.

Dispone de varias opciones, entre las que cabe destacar la posibilidad de modificar el tamaño del paquete enviado, el tiempo de vida o TTL, el valor del bit de fragmentación y el control del número de paquetes enviados entre otras.

Al ejecutar el comando

C:\> ping -l 200 172.20.43.231

se produce el envío de 4 paquetes IP hacia el router R2, cada uno de ellos incorporando 200 bytes de datos a los que habría que sumar 20 bytes de la cabecera IP y 8 de la ICMP.

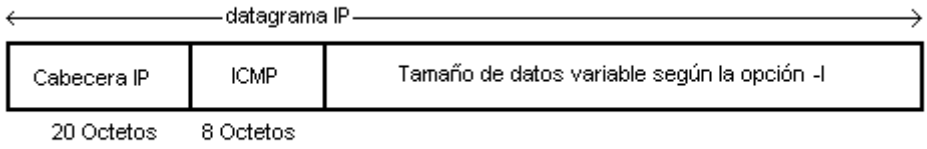


Figura 2. Formato del mensaje ICMP echo.

La respuesta que Ping proporciona en pantalla corresponde a una serie de líneas donde se indica el tiempo de respuesta del eco ICMP y el número de secuencia. Al concluir el comando, queda reflejado el número de paquetes perdidos y los tiempos mínimos, máximos y medios de respuesta (ida y vuelta). Nos permitirá conocer la tasa de error de un enlace así como la velocidad real de transmisión de forma experimental.

Algunas opciones del comando ping son:

ping -n <x> -l <y> -i <z> -f <ipaddr>

-n <x> envía <x> paquetes ICMP *Echo Request*

-l <y> envía paquetes ICMP *Echo Request* con <y> bytes de datos

-i <z> Limita la vida del paquete (campo TTL) a <z>

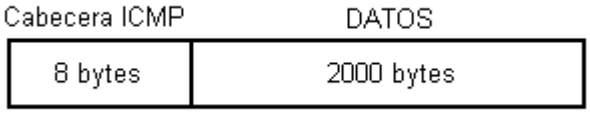
-f Activa el bit Don't fragment

<ipaddr> Dirección IP de destino

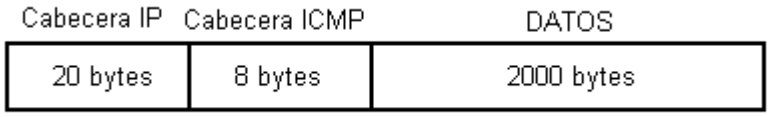
Si se envía un mensaje ICMP echo suficientemente grande, es posible que no quepa íntegro en un único paquete IP. Al ejecutar el comando

C:\> ping –n 1 -l 2000 172.20.43.231

se genera el siguiente mensaje ICMP



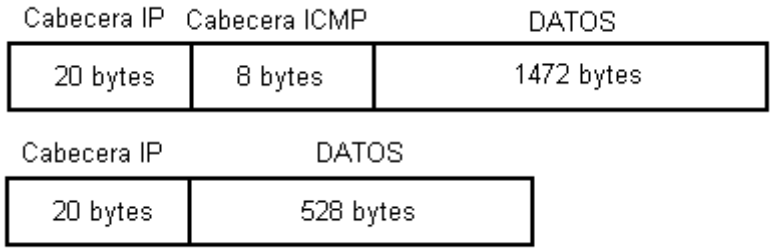
Al encapsular el mensaje ICMP en un paquete IP se obtiene



Este paquete tiene una longitud de 2028 bytes y dado que Ethernet puede enviar como mucho paquetes IP de una longitud de 1500 bytes, es necesario fragmentar el paquete. Sin embargo, Ethernet es un protocolo que no puede realizar la fragmentación de información, ya que su cabecera no incluye información relativa a la fragmentación, por lo que el nivel superior de la arquitectura (el nivel de red) será el encargado de la fragmentación. El protocolo IP sí soporta la fragmentación de información, por lo que troceará el mensaje ICMP en fragmentos de forma que todos quepan en paquetes IP de 1500 bytes de tamaño como máximo.

Para realizar la fragmentación de la información procedente del nivel superior, el protocolo IP necesita conocer cuál es el tamaño máximo de datos que pueden transportar un paquete de nivel de enlace, lo que se denomina MTU o cantidad máxima de datos en un paquete de nivel de enlace. Con este valor el protocolo IP determina cuál es la cantidad máxima de datos que puede incorporar en un paquete IP. Dado que el paquete IP consta de 20 bytes de cabecera IP y datos, la cantidad máxima de datos que transporta un paquete IP en una red Ethernet serán 1480 bytes. Por tanto, IP fragmentará el mensaje ICMP de 2008 bytes en fragmentos de 1480 bytes de tamaño máximo.

Al fragmentar IP el mensaje ICMP se obtienen dos paquetes IP:

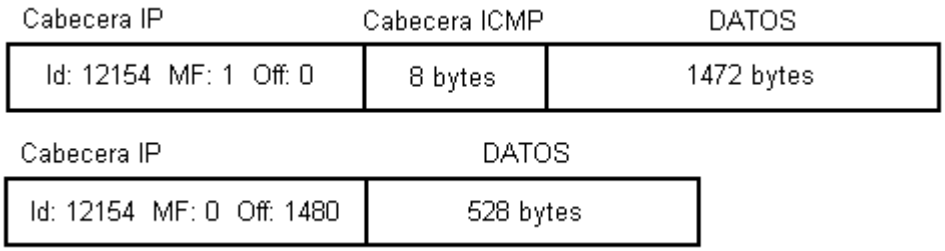


El protocolo IP divide el mensaje ICMP en dos fragmentos: uno de 1480 bytes y otro de 528 bytes correspondientes a los 2008 bytes del mensaje ICMP. En la cabecera IP de cada fragmento se indica que los dos paquetes enviados son fragmentos de un paquete del nivel

superior ICMP. Esta información se encuentra en tres campos de la cabecera: **identificación**, ***fragment offset*** y el bit ***more fragments***.

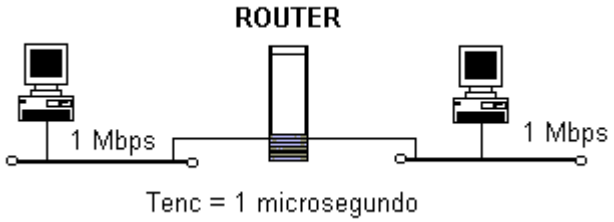
Dado que los fragmentos están asociados a un mismo paquete de información del nivel superior (un mensaje ICMP), los dos paquetes IP tienen asignado el mismo valor de identificación. Cada vez que una estación envía un paquete IP asociado a un sólo paquete del nivel superior, le asigna un número de identificación diferente. En caso de fragmentación, a cada fragmento le asigna el mismo identificador. En cada fragmento se emplea el bit *more fragments* para indicar al receptor si el paquete IP es independiente o si es un fragmento de un mensaje del nivel superior. Para ello, el bit *more fragments* toma el valor 1 en todos los fragmentos excepto en el último paquete IP enviado. Sin embargo, en una red de datagramas los paquetes IP pueden llegar desordenados, por lo que es necesario indicar en qué secuencia han de ser unidos los datos de cada paquete IP para recomponer el mensaje fragmentado. Para ello se emplea el campo *fragment offset*, que indica en qué desplazamiento en bytes dentro del mensaje original se encuentra los datos del paquete IP. En el caso de una red Ethernet, el campo *fragment offset* tomará el valor 0 en el primer fragmento, 1480 en el segundo, 2960 en el tercero y así sucesivamente.

Con este esquema de fragmentación, las cabeceras IP de los fragmentos del mensaje ICMP anterior quedarán:



Aunque el protocolo IP permite realizar la fragmentación de paquetes del nivel superior, la fragmentación produce efectos nocivos en la eficiencia de la red de comunicaciones. La razón está en que transmitir un paquete IP muy grande o el mismo en varios trozos, no produce muchas diferencias en cuanto a tiempo de transmisión de los paquetes (sólo se transmiten unos pocos bytes más debido a las cabeceras), pero sí en cuanto a tiempo de encaminamiento de esos paquetes. Un router emplea el mismo tiempo de CPU para encaminar un paquete independientemente del tamaño del mismo, pues el tiempo de decisión de encaminamiento depende de la complejidad a la hora de decidir cuál es siguiente salto en el envío de un paquete IP en la red. En las primeras redes de datagramas, las velocidades de transferencia eran bastante reducidas (poco más de 100 KBps) y la tasa de errores alta, por lo que la fragmentación era necesaria para reducir el tiempo de transmisión de la información cuando se producían errores. En caso de que un trozo del mensaje sufriera un error no hay que reenviar todo el mensaje y por tanto se pierde menos tiempo al reenviar sólo un fragmento del mismo. Sin embargo, actualmente las redes de datagramas son de gran velocidad (del orden de los cientos de Mbps) y la tasa de error es muy baja, por lo que la fragmentación de la información no supone mucha ventaja a la hora de recuperar los errores y sí que provoca graves problemas de congestión. Hoy en día, el tiempo de encaminamiento es muy significativo respecto del tiempo de transmisión y podemos verlo en el siguiente ejemplo.

Sean dos equipos en dos redes interconectados por un router. Cada red puede transmitir información a una velocidad de 1 Mbps y desean intercambiar un bloque de 1000 bits de datos. El router que interconecta las redes ha de comprobar la cabecera IP de los paquetes para determinar dónde han de ser enviados. El tiempo para decidir donde enviar un paquete (decisión de encaminamiento) depende de muchos factores (tipo de CPU del router, cantidad de memoria RAM, velocidad del bus E/S, etc) pero un valor real bastante aceptable es un tiempo de decisión de 1 microsegundo por paquete. Vamos a despreciar el tamaño de las cabeceras de los protocolos.



Si consideramos el envío de los 1000 bits en un sólo paquete, el tiempo necesario para su transmisión será la suma del tiempo de transmisión del bloque en un segmento, el tiempo de encaminamiento en el router del paquete y el tiempo de transmisión en el otro segmento: T = Ttr1 + Tenc + Tr2 = 1ms + 0.001 ms + 1 ms = 2.001 ms.

Si enviamos 100 paquetes de 10 bits cada uno, ahora el tiempo de transmisión será: T = 100*Tr1 + 100*Tenc + 100*Tr2 = 100*0.01 ms + 100*0.001 ms + 100*0.01 ms = 1 ms + 0.1 ms + 1 ms = 2.1 ms.

Efectivamente, el aumento de la fragmentación produce un retardo en la transmisión de la información que puede ser muy apreciable. De hecho, hoy en día la fragmentación se evita en lo posible para evitar retardos en el encaminamiento. Este exceso de encaminamiento en los routers produce a su vez que el tiempo de encaminamiento sea mayor, ya que la capacidad de los routers se desborda y aparecen problemas de congestionamiento en redes que tienen medios de comunicación de alta velocidad. Actualmente está en fase de implantación en Internet una nueva versión del protocolo IP: el protocolo IP version 6 (IPv6) que sustituirá a la actual IPv4 y que presenta como una de sus características más importantes el que no se permita la fragmentación de paquetes IP en los routers.

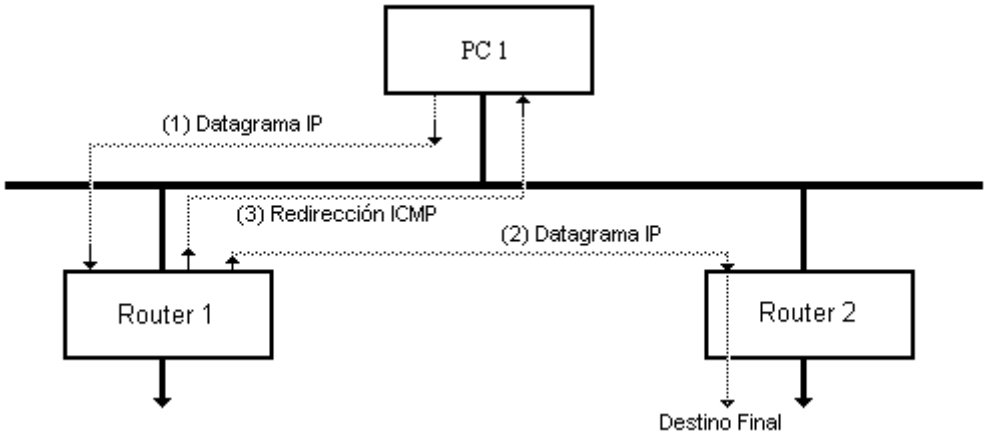
4. MENSAJE DESTINATION UNREACHABLE

El mensaje **Destination Unreachable** (tipo 3) se produce cuando un paquete IP no consigue alcanzar su destino por algún motivo. Dependiendo del valor del campo código en el mensaje ICMP se indica un motivo diferente, algunos de los cuáles son:

- **a. Código 1**. Host Unreachable (3/1). Este mensaje es enviado cuando el router encargado de enviar un paquete a la máquina de destino no puede llevar a cabo la operación. Esta situación se produce cuando un router no puede obtener mediante ARP la dirección MAC del destino, por ejemplo porque la máquina no se encuentra activa y no responde a la petición ARP.
- **b. Código 3**. Port Unreachable (3/3). Este mensaje se genera cuando un paquete IP que contiene un paquete de transporte dirigido a un número de puerto determinado, alcanza el destino y no existe ningún proceso que pueda atender la conexión del nivel de transporte.
- **c. Código 4**. Fragmentation Needed and Don't Fragment was Set (3/4). Un router entre las máquinas origen y destino precisa realizar la fragmentación de un paquete IP y no se puede llevar a cabo porque el bit don't fragment de la cabecera IP está activo.
- **d. Código 13**. Communication Administratively Prohibited. Este mensaje es generado por un router cuando un paquete IP no puede ser encaminado debido a reglas de filtrado de paquetes que existan en el router. En la práctica 4 se tratará en detalle el filtrado de tráfico IP.

5. MENSAJE REDIRECT

El mensaje **Redirect** (tipo 5) es enviado por un router hacia el emisor de un paquete IP cuando este paquete IP debería de haber sido transmitido a un router diferente. En el siguiente esquema se representa esta situación.



Siguiendo el esquema de la figura, veamos paso a paso qué ocurre en la configuración representada:

1. Suponemos que el PC 1 envía un paquete IP a un destino que está fuera de su red. El paquete IP es enviado al router 1, pues éste es la puerta de enlace por defecto del PC 1.

2. El router 1 recibe el paquete IP, interroga su tabla de rutas, y determina que el router 2 es el siguiente salto en el envío del paquete IP. En el momento de enviarlo, detecta que el interfaz de salida es el mismo que por el que recibió el paquete IP procedente del PC 1.

3. Procede por tanto a emitir un error de redirección ICMP hacia el PC 1, informándole que actualice su tabla de encaminamiento y que envíe directamente los próximos paquetes IP dirigidos al mismo destino al router 2 sin pasar por el router 1. A continuación, envía el paquete IP al router 2.

El mensaje de error ICMP Redirect sólo será enviado si la dirección IP origen del paquete reenviado (PC 1) pertenece a la misma red IP que el interfaz del router que lo reenvía (Router 1). Es decir, en una red donde no se encuentra la máquina que genera el paquete IP reenviado, el mensaje ICMP Redirect no será generado (encaminamiento en redes intermedias).

La recepción por una máquina del mensaje redirect implica una modificación en la tabla de rutas o de encaminamiento. La tabla de encaminamiento de cualquier equipo en una red TCP/IP (tanto una máquina como un router) informa al equipo de cómo enviar los paquetes IP a través de los interfaces de red que dispone. En el caso de una máquina normal, como puede ser cualquier PC del laboratorio de prácticas, la tabla de encaminamiento informa acerca de cómo enviar los paquetes IP cuando van dirigidos a nuestra propia red y cuando van dirigidos a destinos fuera de nuestra red. Esta tabla de encaminamiento puede visualizarse ejecutando el comando:

C:\netstat -rn

Este comando mostrará la siguiente información:

Tabla de rutas

Rutas Activas:

Dirección de red	Máscara de red	Puerta de enlace	Interfaz
172.20.43.192	255.255.255.192	En vínculo	172.20.43.x
0.0.0.0	0.0.0.0	172.20.43.230	172.20.43.x

En la tabla de rutas aparece información de otras rutas, pero para el propósito de estas prácticas no las tendremos en cuenta. De todas las entradas de la tabla aparecen dos fundamentales: la 172.20.43.192 y la 0.0.0.0.

La ruta 172.20.43.192 hace referencia a la red Ethernet del laboratorio a la que está conectado el alumno. Si algún paquete IP es enviado a esta red se comprueba qué puerta de enlace tiene asociada. Si la puerta de enlace asociada es la dirección IP del propio equipo (En vínculo), entonces mediante ARP se buscará la dirección MAC asociada a la dirección IP del destinatario y se enviará el paquete.

La ruta 0.0.0.0 hace referencia a cualquier destino. Esta ruta es la última que se comprueba cuando se busca una ruta que coincida con el destino al que se ha de enviar un paquete IP, e indicará la puerta de enlace por defecto de nuestro equipo. Cuando no existe ninguna ruta para el destino de un paquete, éste será enviado a la puerta de enlace por defecto. Por tanto, empleando ARP se determinará la dirección MAC de la puerta de enlace por defecto (172.20.43.230) y será enviado a ésta para que decida hacia dónde enviar el paquete.

La tabla de rutas se modifica mediante mensajes ICMP Redirect o puede modificarla el usuario directamente empleando el comando **route**. El formato de uso de este comando es:

Para añadir una ruta:

C:\route ADD dirección_de_destino MASK máscara_de_red puerta_de_enlace

Para borrar una ruta:

C:\route DELETE dirección_de_destino

Por ejemplo, si queremos que los paquetes que enviemos dirigidos a la red 10.3.0.0/16 vayan a través del router 172.20.43.231 en vez del 172.20.43.230 (el configurado por defecto) tenemos que emplear la orden:

C:\route ADD 10.3.0.0 MASK 255.255.0.0 172.20.43.231

Con el comando **netstat -rn** podemos comprobar que aparece una nueva entrada en la tabla de rutas y que si utilizamos **ping** para enviar paquetes al equipo 10.3.2.0, ARP buscará la dirección MAC de la puerta de enlace 172.20.43.231.

También podemos añadir una ruta para que cuando se envíe información a una máquina en concreto se siga otra ruta. Por ejemplo, si queremos que los paquetes dirigidos a la máquina 10.4.2.2 vayan a través del router 172.20.43.232 tenemos que emplear la orden:

C:\route ADD 10.4.2.2 MASK 255.255.255.255 172.20.43.232

Hay que tener en cuenta que estas entradas permanecerán activas en nuestra máquina hasta que no las borremos con los comandos:

C:\route DELETE 10.3.0.0
C:\route DELETE 10.4.2.2

6. MENSAJE TIME EXCEEDED

El mensaje **Time Exceeded** (tipo 11) genéricamente indica que el tiempo máximo de tránsito para un paquete IP en la red se ha sobrepasado. Dependiendo del código del mensaje éste se emplea en dos situaciones diferentes:

Código 0. *Time to Live exceeded in Transit* (11/0). Este mensaje ICMP es enviado por un router cuando el valor del campo TTL (time to live) en la cabecera IP de un paquete toma el valor 0.

Cada vez que un router recibe un paquete IP que no va dirigido a ninguno de sus interfaces decrementa el campo TTL de la cabecera IP en una unidad. Si el valor obtenido es distinto de cero, el router procede a encaminar el paquete y enviarlo al siguiente salto. Pero si al decrementar el campo TTL se obtiene el valor cero, el paquete es eliminado, pues se ha agotado el número de saltos que puede realizar el paquete en la red. Dado que el campo TTL tiene 8 bits, el número máximo de routers que puede atravesar un paquete es de 255. De esta forma se evita que existan paquetes circulando indefinidamente en la red sin alcanzar su destino. Al eliminar el router el paquete IP, éste informa al remitente del paquete IP eliminado enviando el mensaje *time to live exceeded in transit*.

La aplicación **tracert** emplea este mensaje ICMP de error para determinar la ruta que sigue un paquete IP en una red TCP/IP. Tracert envía un mensaje ICMP *Echo Request* con un valor para el campo TTL de la cabecera IP de 1. Cuando este mensaje alcanza el primer router en su camino al destino, el valor TTL se decrementa, toma el valor cero y se envía a la máquina de origen un mensaje ICMP *Time to live exceeded in transit*. Tracert visualiza entonces la dirección del router que le envía el mensaje de error como el primer salto para alcanzar el destino. A continuación vuelve a enviar un mensaje *Echo Request* con el valor del campo TTL incrementado en una unidad, es decir 2, por lo que el segundo router en el camino al destino enviará el mensaje *Time exceeded*. Este proceso se repite hasta que se recibe un mensaje *Echo Reply* del destino, visualizando las direcciones de todos los routers intermedios en el camino al destino.

Por ejemplo, al ejecutar el comando:

C:\tracert -d 10.3.7.0 (la opción **-d** es necesario especificarla para evitar resoluciones DNS)

Obtenemos la secuencia:

Traza a 10.3.7.0 sobre caminos de 30 saltos como máximo.

1 1 ms 1 ms 1 ms 172.20.43.230
2 2 ms 1 ms 2 ms 10.4.2.5
3 60 ms 45 ms 58 ms 10.3.7.0

Traza completa.

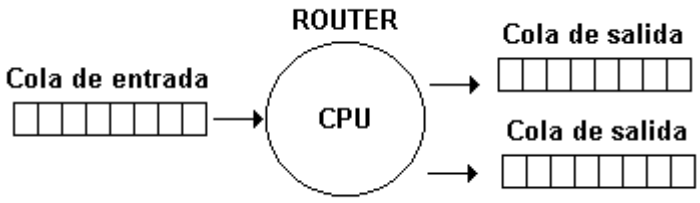
De este resultado se deduce que para enviar un paquete IP a la estación 10.3.7.0, se sigue una ruta en la red a través de los routers R2 y R1. Para cada salto se indica el tiempo de ida y vuelta de un paquete IP hasta ese punto. Aparecen tres tiempos, ya que para cada salto **tracert** envía tres paquetes ICMP *Echo Request* con el mismo valor de TTL para poder proporcionar una estadística del tiempo medio en cada salto.

Código 1. *Fragment Reassembly Time Exceeded* (11/1). Este mensaje ICMP es enviado por la máquina de destino de un paquete IP cuando en el reesamblado de los fragmentos de un paquete fragmentado, alguno de ellos no se recibe antes de un tiempo determinado.

Este mensaje es de especial utilidad para detectar congestionamiento debido a la fragmentación en redes IP. En la actualidad, la probabilidad de que un fragmento de un mensaje no alcance su destino es bastante baja, ya que para ello debería ocurrir un problema de encaminamiento puntual para un sólo paquete. Si el encaminamiento funciona adecuadamente, cuando algún fragmento llega al destino el resto de fragmentos lo hará también más tarde o más temprano. Precisamente, el que los fragmentos tarden más o menos en alcanzar el destino es la causa de generación del mensaje fragment reassembly time exceeded. Si existe una congestión alta en la red los paquetes IP llegan con gran retardo a su destino. Si los paquetes IP son independientes, se aprecia un retardo en la comunicación, pero si los paquetes IP son fragmentos de mensajes más grandes y llegan con mucho retardo al destino éstos no pueden ser reesamblados, por lo que los mensajes no son interpretados nunca en el destinatario y el usuario cree que no hay comunicación con el destino. Detectando la presencia de mensajes *fragment reassembly time exceeded* puede determinarse si el problema es de congestión o que la información realmente no alcanza su destino.

7. MENSAJE SOURCE QUENCH

El esquema básico de funcionamiento de un router se fundamenta en un nodo procesador de paquetes que dispone de una o varias colas de entrada y una o varias colas de salida de paquetes.



El router recoge en su cola de entrada los paquetes que recibe para encaminar. En un modelo de funcionamiento sencillo, el router procesa secuencialmente los paquetes de la cola de entrada y determina dónde deben ser enviados (decisión de encaminamiento) y los introduce en la cola de salida adecuada. Si el router no tiene suficiente capacidad de proceso es posible que no pueda encaminar los paquetes tan rápidamente como le llegan a la cola de entrada, por lo que el número de paquetes almacenados en la cola de entrada para ser encaminados aumenta. Esta situación es más frecuente de lo que pueda parecer, pues las redes de comunicaciones actuales son capaces de transmitir gran cantidad de paquetes por segundo. Cuando alguna de las colas de entrada de paquetes de un router se llena, éste tiene que eliminar los paquetes que le llegan en exceso y emite mensajes ICMP *Source Quench* (tipo 4) para indicar esta situación. Así, el mecanismo de control de congestión utilizado por IP se limita a enviar mensajes *Source Quench* al equipo origen de los paquetes IP eliminados, para indicarle que reduzca el flujo de paquetes que transmite y así reducir la congestión.

8. REALIZACIÓN DE LA PRÁCTICA

CADA ALUMNO DEBE EJECUTAR EL COMANDO C:\PRACREDES PARA CONFIGURAR SU EQUIPO CORRECTAMENTE.

Cuestión 1. Ping

Iniciar el programa monitor de red capturando los paquetes IP con origen o destino la máquina del alumno. A continuación ejecutar el comando:

C:\>ping –n 1 –l 500 172.20.43.231

Detener la captura en el monitor de red y visualizar los paquetes capturados. En base a los paquetes capturados determinar,

a) ¿Qué tipos de mensajes ICMP aparecen?

b) Justificar la procedencia de cada dirección MAC e IP.

c) Verificar que los tamaños de los datos y las cabeceras de los protocolos que aparecen en los paquetes ICMP (Ethernet, IP, ICMP) son los esperados.

Cuestión 2. Fragmentación

Nota sobre el monitor de red: Para interpretar correctamente la información de la fragmentación IP en el monitor de red, es necesario cambiar las opciones de visualización de Wireshark. Para ello, en el menú 'Edit' -> 'Preferences', buscar en la sección 'Protocols' el protocolo IPv4. DESACTIVAR la opción 'Reassemble fragmented IPv4 datagrams'.

Empleando el programa monitor de red de la misma forma que en la situación anterior, ejecutar:

C:\>ping –n 1 –l 2000 172.20.43.231

a) Describir los paquetes IP generados por el PC del alumno asociados a la fragmentación del mensaje ICMP Echo Request.

b) Determinar el MTU de la máquina del alumno y de la máquina 172.20.43.231.

Activando de nuevo la captura de paquetes en el monitor y ejecutar el comando:

C:\>ping –n 1 –l 1000 10.3.7.0

a) Describir los paquetes IP generados por el PC del alumno asociados a la fragmentación del mensaje ICMP Echo Request.

b) Determinar el MTU del destino analizando el tamaño de los paquetes IP recibidos desde la dirección 10.3.7.0.

Activando de nuevo la captura de paquetes en el monitor y ejecutar el comando:

C:\>ping –n 1 –l 4500 172.20.43.232

a) Determina cuántos paquetes IP se generarán desde el PC del alumno y qué valores tendrán los campos OFFSET y bits DF y MF de la cabecera IP.

b) ¿Se corresponden con los paquetes IP capturados con el monitor de red ?

Cuestión 3. Redirect

Iniciar el monitor de red con los filtros adecuados para capturar los paquetes involucrados en la situación de Redirect. A continuación ejecuta el comando:

C:\>ping -n 1 172.20.41.241

En base a los paquetes capturados contestar a las siguientes preguntas:

a) ¿Cuántos paquetes están involucrados?
b) Dibujar gráficamente el origen y destino de cada paquete en el esquema de red.
c) ¿Qué estación envía el mensaje ICMP redirect?
d) ¿Qué datos complementarios transporta el mensaje ICMP redirect?

Comprueba que al ejecutar de nuevo el comando anterior (**ping –n 1 172.20.41.241**) no aparece el mensaje ICMP Redirect y el paquete ICMP Echo Request es enviado directamente a la puerta de enlace especificada en el mensaje Redirect anterior.

Nota: Si vuelve a aparecer el mensaje ICMP Redirect, es debido a que ha expirado un temporizador en Windows 10 que almacena esa información (no se almacena en la tabla de rutas). Prueba a ejecutar varias veces seguidas el comando ping –n 1 172.20.41.241, comprobando que sólo aparece un mensaje Redirect.

Cuestión 4. Establecimiento de rutas estáticas

Con el comando **route** añade una ruta en la tabla de encaminamiento del PC del alumno para que los paquetes enviados al destino 10.3.7.0 sean encaminados a través del router R3. A continuación ejecutar el comando:

C:\>ping -n 1 10.3.7.0

Determina:

a) ¿Qué router se emplea como puerta de enlace en el mensaje ICMP Echo Request? ¿Se corresponde con el especificado en la entrada añadida con el comando route?

b) ¿Qué router se emplea como puerta de enlace en el mensaje ICMP Echo Reply?

(Recuerda borrar la entrada añadida con el comando **route (delete)**)

Con el comando **route** añade una ruta en la tabla de encaminamiento del PC del alumno para que los paquetes enviados a la red de destino 172.20.41.240/28 sean encaminados a través del router Linux 2. A continuación ejecutar el comando:

C:\>ping -n 1 172.20.41.242

Determina:

a) ¿Qué router se emplea como puerta de enlace en el mensaje ICMP Echo Request? ¿Se corresponde con el especificado en la entrada añadida con el comando route?

b) ¿ Qué router se emplea como puerta de enlace en el mensaje ICMP Echo Reply?

(Recuerda borrar la entrada añadida con el comando **route (delete)**)

Cuestión 5. Destination Unreachable

Dentro del mensaje ICMP Destination Unreachable se analizará el de código 4: Fragmentation Needed and Don't Fragment was Set (3/4). En primer lugar iniciar el monitor de red de la misma forma que en las cuestiones anteriores. Ejecutar los siguientes comandos:

C:\route delete 0.0.0.0
C:\ipconfig /release
C:\ipconfig /renew
C:\pracredes

para eliminar cualquier información almacenada en el equipo para alcanzar el destino 10.3.7.0.

C:\>ping -n 1 –l 1000 -f 10.3.7.0

En base a los paquetes capturados, indicar:

a) Identificar las direcciones IP/MAC de los paquetes involucrados.

b) ¿ Qué estación envía el mensaje ICMP Fragmentation Needed and Don't Fragment was Set (3/4) ?

c) Analiza la información de la cabecera ICMP del mensaje anterior ¿ Cuál es el valor del MTU de la red que no puede transmitir el paquete ICMP Echo Request ?

A continuación se analizará el mensaje ICMP Destination Unreachable con el código 1: Host Unreachable. Con el comando **route**, establece una ruta para alcanzar la red 172.20.41.240/28 a través del router Linux 2. Para ello ejecuta el comando:

C:\>route add 172.20.41.240 mask 255.255.255.240 172.20.43.232

A continuación, ejecuta el comando:

C:\>ping -n 1 172.20.41.244

En base a los paquetes capturados, indicar:

a) Identificar las direcciones IP/MAC de los paquetes involucrados.

b) ¿ Qué estación envía el mensaje ICMP Host Unreachable (3/1) ?

Al finalizar este ejercicio elimina la ruta añadida con el comando:

C:\route delete 172.20.41.240

Cuestión 6. Time Exceeded

Dentro del mensaje ICMP *Time Exceeded* se analizará el de código 0: *Time to Live exceeded in Transit* (11/0). En primer lugar iniciar el monitor de red para capturar paquetes IP relacionados con la máquina del alumno y ejecutar el comando:

C:\> ping –i 1 –n 1 10.3.7.0

Detener la captura y determinar:

a) ¿Qué estación envía el mensaje ICMP *Time to Live exceeded in Transit*?

b) ¿Qué paquete causó el error

c) ¿Cuántos paquetes ICMP aparecen en el monitor de red ?

Iniciar de nuevo la captura y ejecutar a continuación el comando:

C:\> ping –i 2 –n 1 10.3.7.0

Detener la captura y determinar:

a) ¿Qué estación envía el mensaje ICMP *TTL exceeded* ?

b) ¿Qué paquete causó el error ?

c) ¿Cuántos paquetes ICMP aparecen en el monitor de red ?

d) Justifica la diferencia con el caso anterior.

Emplear la aplicación **tracert** para determinar las rutas que siguen los paquetes IP dirigidos desde la red de los alumnos a diferentes destinos del laboratorio:

C:\tracert -d 10.3.7.0
C:\tracert -d 172.20.41.241
C:\tracert -d 10.4.2.5
C:\tracert -d 10.4.2.1
C:\tracert -d 10.4.2.2
C:\tracert -d 172.20.41.242

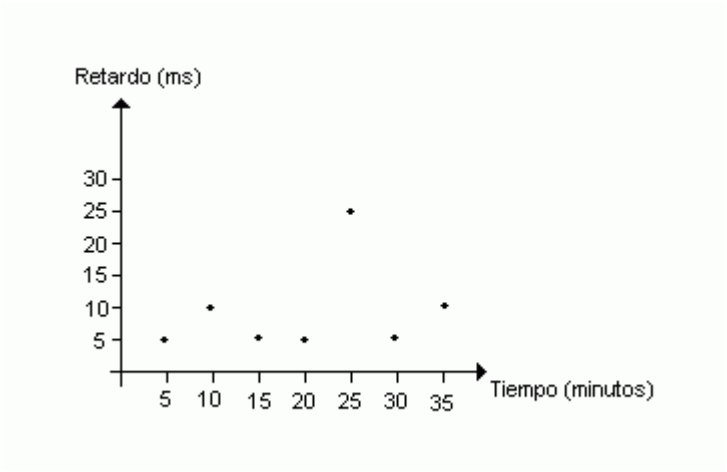
Determina las razones del comportamiento del encaminamiento al ejecutar el comando:

C:\tracert -d 10.3.4.4

Cuestión 7. Evaluación experimental del rendimiento de una red

La evaluación del rendimiento de una red de comunicaciones se puede realizar en base a distintos parámetros como son: velocidad de transmisión de datos, tasa de error, retardo en el envío de paquetes, etc. Si se considera el retardo en el envío de paquetes, es posible determinar de forma experimental el retardo medio de los paquetes que circulan por la red empleando los mensajes ICMP *Echo Request* y *Echo Reply*.

Se estudiará el retardo producido en paquetes dirigidos a dos redes distintas dentro de la topología del laboratorio. Para cada una de las redes se obtendrá una gráfica en la que se representará el retardo de un paquete (tiempo de ida y vuelta) dirigido a un determinado destino en intervalos de 1 minuto a lo largo de **30** minutos.



Los paquetes que se emplearán para determinar los retardos se generarán con la aplicación **ping**, enviando mensajes ICMP echo a una determinada dirección y con una determinada longitud. El valor de la longitud de los paquetes lo tomaremos como el tamaño máximo de paquete que puede circular de origen a destino sin ser fragmentado por el protocolo IP. En la red del laboratorio existen diferentes valores de MTU, por lo que consideraremos el MTU de menor tamaño, que es 600 bytes. Por tanto, emplearemos como tamaño para el envío de paquetes Ethernet un tamaño de 614 bytes, 600 bytes de datos (el paquete IP) y 14 bytes de cabecera Ethernet.

Con este valor de longitud se caracterizará el retardo de paquetes en la red. Para ello se utilizará el comando ping en la forma:

ping -n 1 -l longitud dirección_ip

que enviará un paquete ICMP de tipo *Echo Request* con longitud de datos **longitud** a la máquina con dirección **direccion_ip**, esperando un paquete ICMP de tipo *Echo Reply* procedente de la dirección **dirección_ip**. El comando ping nos proporciona el intervalo de tiempo desde que se envió el E*cho Request* y se recibió el *Echo Reply*. Este valor será el tiempo de ida y vuelta o retardo del paquete.

Nótese que el valor **longitud** hace referencia sólo a la longitud de los datos del paquete ping, por lo que $MTU = cab_{IP} + cab_{ICMP} + longitud$ para que la longitud total del paquete IP sea el del MTU escogido.

Una vez obtenida una muestra de *n* retardos obtenidos cada minuto durante 30 minutos (***n* = 30**), puede construirse la gráfica citada anteriormente. De esta gráfica se obtendrá el **retardo medio de la red** como la media de los retardos obtenidos.

$$\overline{retardo} = \frac{\sum_{i=1}^{n} retardo_i}{n}$$

Para determinar si una red de transmisión de datos está funcionando de forma correcta es necesario determinar la desviación de los retardos en la red respecto de la media. Cuanto mayor sea esta desviación peor será el rendimiento de la red, pues indica que el tráfico en la red no está distribuido de forma homogénea. La **desviación típica** de un conjunto de n muestras viene dada por:

$$S = \sqrt{\frac{\sum_{i=1}^{n}\left(\overline{retardo} - retardo_i\right)^2}{n-1}}$$

La desviación típica indica el valor medio en unidades de la magnitud medida (en el caso del retardo, la magnitud es el tiempo) que las muestras difieren de la media. Usualmente esta desviación se expresa en tanto por cien respecto de la media, en la forma

$$S(\%) = \frac{S}{\overline{retardo}} \cdot 100$$

Si obtenemos un valor de S en tanto por cien (%) superior a 50, la red que estamos evaluando presentará un rendimiento bajo, pues la distribución de la carga en la red no es homogénea y presenta picos de utilización.

a) Determinar la gráfica retardos-tiempo y la desviación típica de los retardos en % cuando se envían paquetes a la máquina con dirección IP **10.3.7.0**

b) Determinar la gráfica retardos-tiempo y la desviación típica de los retardos en % cuando se envían paquetes a la máquina con dirección IP **10.4.2.5**

9. DOCUMENTACIÓN COMPLEMENTARIA

- **RFC 792**. Internet Control Messages Protocol (ICMP).
- **Fragmentation Considered Harmful**. *C. Kent and J. Mogul*. In Proc. SIGCOMM '87 Workshop on Frontiers in Computer Communications Technology. August, 1987.