PRÁCTICA 4

Encaminamiento de paquetes con IP

REDES (9359)

ING. TÉCNICA EN INFORMÁTICA DE SISTEMAS

CURSO 2010/2011

(*Este documento es una versión en papel de la versión completa en formato web-SCORM publicada a través de la plataforma Moodle-UA*)

Pablo Gil Vázquez (Pablo.Gil@ua.es)
Grupo de Innovación Educativa en Automática

Universitat d'Alacant
Universidad de Alicante

4.1 Introducción

Dentro de una red local (LAN) el envío de datos entre equipos se efectúa de forma directa entre equipos mediante el protocolo de enlace (MAC Ethernet en nuestro caso) y su esquema de direccionamiento. El problema surge a nivel de red, cuando se quiere enviar datos entre equipos que pueden estar en diferentes redes, caso en donde no es aplicable el direccionamiento de enlace de forma directa. Nosotros consideraremos el caso habitual de diferentes redes interconectadas a través de *routers* (o encaminadores) y que trabajan con un protocolo de red común: IP.

Con la realización de esta práctica el alumno debe adquirir conocimientos que le permitan:

- Conocer el funcionamiento básico de un *router*: como se realiza el encaminamiento de paquetes y como son las tablas de encaminamiento.
- Aprender a organizar y a asignar las entradas de las tablas de encaminamiento en una red.
- Conocer como se realiza la gestión dinámica de tablas de encaminamiento mediante el protocolo de enrutamiento dinámico RIP.

4.2. Encaminamiento en un equipo con los protocolos TCP/IP

Un *router*, que puede interconectar dos o más redes, requiere de un método de encaminamiento que le permita determinar hacia donde debe reenviar un paquete recibido por uno de sus interfaces, o generado en el mismo equipo. Para ello debe basarse en el esquema de direcciones de máquina y de red de IP, así como en las máscaras.

A continuación se describen los pasos que sigue una máquina con TCP/IP para enviar o reenviar un paquete al destino IP correspondiente.

***A**.¿La dirección IP destino pertenece a una interfaz de red de esta máquina?*

Si es así el envío se efectúa sin necesidad de colocar datos en los niveles de enlace y físico, esto es, a través de un *loopback* interno a nivel IP. Un *loopback* hace referencia a una dirección IP interna de la propia máquina que sirve para efectuar envíos a nivel de red IP dentro de la misma máquina, sin requerir que los datos pasen al nivel de enlace. Se usa habitualmente la dirección 127.0.0.1.

De no ser así, se continúa en el siguiente paso.

***B**.¿La dirección IP destino pertenece a una red local conectada directamente a una interfaz de red de esta máquina?*

Esto se puede determinar utilizando la máscara de red definida en la máquina para cada interfaz. Mediante una operación lógica AND de la máscara de una interfaz con la dirección IP de esa interfaz se determina la dirección de la red asociada, y operando la máscara con la IP destino se determina la red destino.

Si coinciden, para alguna interfaz, el destino está en la red local de esa interfaz, y el envío se efectúa directamente tras aplicar el protocolo ARP para determinar la dirección MAC del destino.

De no ser así, se continúa en el siguiente paso.

C. *¿Tengo una ruta especifica para la dirección IP destino o para su red?*

Se debe explorar la tabla de encaminamiento buscando una entrada en la que se especifique explícitamente la dirección IP de la máquina destino, o en su omisión, una dirección de red que incluya la IP destino. Básicamente la tabla de encaminamiento (que se describe en el siguiente punto) mantiene una serie de entradas que relacionan posibles direcciones IP destino (de máquina o de red) y sus máscaras con las direcciones IP de las interfaces en las redes locales (llamados *gateways* o puertas de enlace) que dan acceso a esos destinos.

Si se encuentra alguna entrada para el destino deseado, se envía el paquete al *gateway* correspondiente dentro de la red local usando el direccionamiento de enlace. Para ello puede ser necesario desencadenar el protocolo ARP entre este equipo y el *gateway* con el objetivo de determinar su dirección MAC a partir de su IP.

De no ser así, se continúa en el siguiente paso.

D. *¿Tengo una ruta por defecto?*

Si existe una entrada de ruta por defecto, se envía el paquete a su *gateway* asociado (conocido en este caso como *default gateway*). Puede ser necesario desencadenar el protocolo ARP entre este equipo y el *gateway* con el objetivo de determinar la dirección MAC a partir de su IP.

De no ser así, este equipo considera el destino inaccesible.

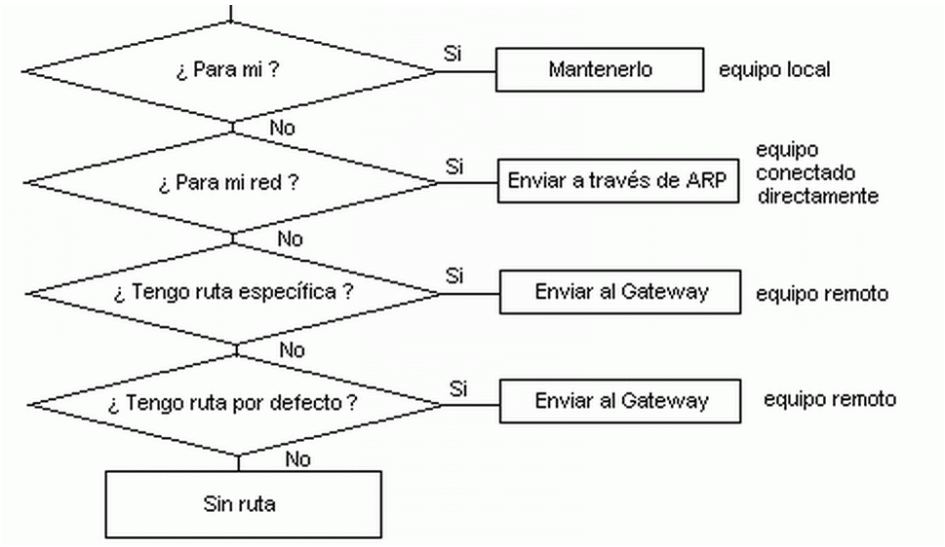


Figura 1. Pasos para encaminar un paquete en una arquitectura de protocolos TCP/IP.

En la práctica, el esquema de enrutamiento anterior es seguido por cualquier máquina con TCP/IP, sea un *router* o un simple equipo de usuario. Aunque solo tiene sentido hablar de *router* cuando se trata una máquina con más de una interfaz de red operando a nivel de red y que realiza tareas de enrutamiento, en un equipo de usuario con una sola interfaz de red, el enrutamiento funciona igual. Ahora bien, en un equipo de usuario con una sola interfaz de red, habitualmente basta con definir una sola ruta, la ruta por

defecto, esto es, especificar la IP destino del *default gateway* al que se envían los paquetes que no van dirigidos a la propia red local.

4.3. Tablas de encaminamiento

La forma elemental de una tabla de encaminamiento de un equipo sería la que muestra la siguiente figura:

IP destino	Máscara IP destino	Puerta de enlace
destino_1	máscara_1	gateway_1
destino_2	máscara_2	gateway_2
…	…	…

Figura 2. Formato de una tabla de encaminamiento.

Para una entrada, la IP destino hace referencia a una dirección de máquina o de red a la que se pueden enviar paquetes. Cada IP destino tiene su máscara asociada. La puerta de enlace de una entrada indica la dirección IP del interfaz de red al que se deben enviar los paquetes dirigidos a la IP destino correspondiente.

La herramienta o comando "**netstat**" presente en una máquina Unix (y por supuesto también en Linux) permite visualizar la tabla de encaminamiento, además de otros aspectos como estado de los *sockets* TCP/IP activos. Si se ejecuta el comando con la opción **–i** ("netstat –i") el equipo visualiza información acerca de las interfaces físicas del sistema. Por ejemplo, el resultado en una máquina Linux puede ser:

```
Kernel Interface table
Iface   MTU Met  RX-OK RX-ERR RX-DRP  TX-OK TX-ERR TX-DRP Flags
lo     3584   0    100      0      0    100      0      0  BLRU
eth0   1500   0 195051      0      0  38488      0      0   BRU
ppp0    296   0  17907      0      0   1900      0      0   BRU
```

Figura 3. Información de los interfaces de una máquina Linux.

La primera columna indica el nombre que Unix da a la interfaz instalada; "eth0" es el nombre de una tarjeta de red Ethernet, "lo" es el *loopback*, y "ppp0" es el nombre de una conexión PPP. La segunda columna indica el MTU que tiene asignado cada interfaz. El resto de columnas presentan información, como los datos transmitidos, los recibidos y los errores producidos.

En Windows, auque existe el comando **"netstat"** ejecutado en línea de comandos MS-DOS no dispone de la opción **–i**. Así que para visualizar la información física de los interfaces del sistema, se emplea el comando **"ipconfig"** en su versión de comandos. La información que se obtiene es bastante más excueta que en sistemas operativos Unix.

```
Adaptador Ethernet Conexión de área local:
Sufijo de conexión específica DNS : dfists.ua.es
Descripción. . . . . . . . . . . . : NIC PCI 3Com EtherLink XL 10/100
PCI para administración completa del equipo (3C905C-TX)
Dirección física. . . . . . . . . : 00-04-75-E3-AB-97
```

Figura 4. Información de los interfaces de una máquina Windows.

Con otras opciones se puede obtener la tabla de encaminamiento actual (opción **-r**), mostrando las direcciones IP con notación decimal (opción **-n**). Así, el resultado de ejecutar el comando "netstat –rn" en una máquina Linux podría ser:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window interface
10.3.2.0        10.3.7.0        255.255.255.255 UGH       460   0      0 ppp0
172.20.41.240   0.0.0.0         255.255.255.240 U        1500   0      0 eth0
10.3.0.0        0.0.0.0         255.255.0.0     U         460   0      0 ppp0
127.0.0.0       0.0.0.0         255.0.0.0       U        3584   0      0 lo
0.0.0.0         172.20.41.242   0.0.0.0         UG       1500   0      0 eth0
```

Figura 5. Tabla de encaminamiento de una máquina Linux.

En otras máquinas Unix el resultado puede ser algo diferente, pero la información más importante, la descrita a continuación, suele estar presente. La columna ***Genmask*** especifica la máscara asociada con cada IP destino. En el campo ***flags*** (indicadores) pueden aparecer 5 valores diferentes:

- **U** (up). La ruta está en servicio.
- **G** (gateway). El destino de la ruta se alcanza a través de una puerta de enlace. Si este flag no está activado, el destino está conectado directamente al equipo en la misma LAN.
- **H** (host). El destino hace referencia a otra máquina, esto es, el destino es una dirección de máquina completa. La no existencia de este indicador implica que la ruta incluye otra red, y el destino es una dirección de red (o de subred).
- **D** (directed). La ruta ha sido creada tras recibirse un error ICMP de redirección (mecanismo que se activa durante la emisión de un datagrama IP a un *router* cuando debería de haberse enviado a otro de la misma red).
- **M** (modified). La ruta ha sido modificada por una redirección.

El flag G tiene una especial importancia por cuanto permite distinguir entre una ruta directa y otra indirecta. La diferencia entre ellas reside en que un datagrama IP dirigido por una ruta directa posee a la vez las direcciones MAC e IP de la máquina destino, mientras que un paquete emitido sobre una ruta indirecta posee la dirección IP del destino pero la dirección MAC del próximo *router* que es la puerta de enlace.

Para el ejemplo anterior, supóngase que se desea enviar o reenviar un datagrama con la dirección 10.3.2.0. La búsqueda tendrá éxito en la primera entrada y el datagrama será enviado por la interfaz física local "ppp0" que tiene dirección 10.3.7.0. Nótese que, para las conexiones punto a punto, conviene definir el destino de forma absoluta, es decir, especificando la dirección completa de la máquina destino en cada extremo de la conexión.

Los datagramas enviados sobre el segmento de red Ethernet conectado a la interfaz eth0 están definidos por la segunda entrada donde aparece la dirección de red destino 172.20.41.240 y la puerta de enlace 0.0.0.0 para indicar que a esta red se accede directamente a través del interfaz de red "eth0" Lo mismo ocurre para la red 10.3.0.0 de la tercera entrada, sólo que con el interfaz "ppp0". La cuarta entrada

especifica el interfaz de *loopback*, y la quinta, identificada por el destino 0.0.0.0, indica que la puerta de enlace por defecto es el equipo con IP 172.20.41.242 presente en la red Ethernet. Los datagramas con direcciones que no pertenezcan a ninguno de los destinos especificados en las entradas 1 a 4 serán reconducidos a la entrada 5.

El S.O. MS. Windows (NT, 95, 98, 2000, XP...) con TCP/IP instalado también ofrece el comando "netstat", aunque con algunas variaciones en cuanto a los parámetros y al formato del resultado. Así por ejemplo, no admite el parámetro -i. El resultado de ejecutar "netstat –rn" en un equipo con sistema MS. Windows puede asemejarse al siguiente:

```
Tabla de rutas
Rutas activas:
 Dirección de red Máscara de red  Puerta de enlace  Interfaz       Métrica
 0.0.0.0          0.0.0.0         172.20.43.230    172.20.43.223     1
 172.20.43.192    255.255.255.192 172.20.43.223    172.20.43.223     1
 172.20.43.223    255.255.255.255 127.0.0.1        127.0.0.1         1
 172.20.43.255    255.255.255.255 172.20.43.223    172.20.43.223     1
 127.0.0.0        255.0.0.0       127.0.0.1        127.0.0.1         1
 224.0.0.0        224.0.0.0       172.20.43.223    172.20.43.223     1
 255.255.255.255 255.255.255.255  172.20.43.223    172.20.43.223     1
```

Figura 6. Tabla de encaminamiento de una máquina Windows.

En este caso se muestra para cada entrada la dirección destino, la máscara asociada a esa dirección, la puerta de enlace, la dirección IP del interfaz del propio equipo por el que se alcanza la puerta de enlace y el número de saltos necesarios para llegar al destino. La ruta por defecto se identifica también en este caso como la entrada con destino 0.0.0.0.

Tras la tabla de encaminamiento, el comando "netstat" de MS. Windows también se muestra el estado de los sockets TCP/IP activos.

4.4 Creación y mantenimiento de rutas estáticas

Tanto en MS. Windows (con TCP/IP) como en Unix existe el comando "**route**" que permite crear entradas estáticas en la tabla de encaminamiento o modificar y eliminar las ya existentes. Las sintaxis de este comando, en Windows, se define del siguiente modo:

- ***route [-f] [comando [addr] [MASK mask] [gateway] [METRIC cost]]***

A continuación se describen con más detalle las opciones:

- **-f**: Borra de la tabla de enrutamiento las entradas de todas las puertas de enlace.
- **comando**: Especifica uno de los cuatro comandos siguientes: **PRINT** para ver una entrada, **ADD** para agrega una entrada, **DELETE** para eliminar una entrada y **CHANGE** para modificar una entrada existente.
- **addr:** Especifica la dirección IP del equipo o red de destino.

- **MASK**: Si esta palabra está presente, el siguiente parámetro (***mask***) es interpretado como el parámetro de la máscara de red correspondiente a la dirección IP destino. Si no se especifica, se toma el valor 255.255.255.255 (dirección de máquina).
- **gateway**: Especifica la dirección IP de máquina que es la puerta de enlace.
- **METRIC**: Especifica como número de saltos para alcanzar el destino el valor de ***cost***.

Cuando el comando es PRINT o DELETE, se puede utilizar comodines para el destino y la puerta de enlace, o se puede omitir el argumento "puerta" para mostrar todas las entradas. Para añadir o modificar la entrada por defecto el valor de destino debe ser "default". Por ejemplo, "route ADD 10.3.0.0 MASK 255.255.0.0 10.3.7.0" añade una entrada de ruta para poder alcanzar la red 10.3.0.0 a través de la puerta de enlace local 10.3.7.0. Un ejemplo, de empleo del comando "route" para añadir y borrar entradas en la tabla de encaminamiento en un sistema Windows se puede observar ejecutando el script "pracredes.bat", y comprobar la tabla de encaminamiento, con el comando "route print" antes y después de la ejecución de este script.

```
route delete 0.0.0.0
route add 0.0.0.0 mask 0.0.0.0 172.20.43.230
```

En los sistemas Unix también existe la orden "route", pero con más opciones y un formato distinto de los parámetros. Como ocurre con "ifconfig", se necesitan **privilegios de root** para ejecutar este comando y se puede consultar el manual del sistema para obtener información sobre el mismo ("man route"). La sintaxis básica del comando es:

- ***route add [-net | -host] addr [gw gateway] [metric cost] [netmask mask] [dev device]***
- ***route del [-net | -host] addr***

A continuación se describen con más detalle las opciones:

- **-net** ó **-host:** Especifican si la dirección ***addr*** es un equipo ó una red de destino.
- **gw**: Especifica que la puerta de enlace de la entrada es la dirección IP de máquina ***gateway***.
- **metric**: Especifica como número de saltos para alcanzar el destino el valor de ***cost***.
- **netmask**: Especifica que la máscara de red correspondiente a la dirección IP destino es el valor dado por el parámetro ***mask***. Si no se especifica, "route" tomará la máscara que crea más apropiada.
- **dev**: Fuerza a que la nueva entrada sea por el interfaz de red indicado por ***device***.

Por ejemplo, para cambiar la entrada de la tabla de encaminamiento relativa a la puerta de enlace por defecto de forma que ésta sea la 172.20.43.231 se puede ejecutar:

```
route del default
route add default gw 172.20.43.231
```

Para añadir la entrada de encaminamiento relativa a la interfaz de *loopback* recién creada con "ifconfig" habría que ejecutar:

```
route add -net 127.0.0.1
```

Si se quisiera añadir una entrada para alcanzar la red 172.20.41.240/28 a través de la puerta 172.20.43.231 (que debe ser alcanzable a partir de otras entradas existentes), habría que ejecutar:

```
route add -net 172.20.41.240 gw 172.20.43.231 netmask 255.255.255.240
```

4.5 Enrutamiento dinámico con RIP

El protocolo de encaminamiento dinámico que vamos a estudiar es RIP (Routing Information Protocol) en su versión 2. Está definido en la RFC 2453 (descripción), en base a lo ya establecido para el protocolo RIP versión 1, definido en la RFC1058.

RIP 1 se encarga de mantener actualizadas las tablas de encaminamiento de los *routers* a través de mensajes de difusión. Se dice que es un protocolo de "vector de distancia" ya que emplea el número de saltos a un destino (o métrica) para decidir que entrada de ruta debe ser aplicada para alcanzar dicho destino. El número de saltos se puede ver como el número de *routers* que debe atravesar un paquete para llegar al destino, sin contar el origen e incluyendo el destino, o como el número de redes por las que debe pasar el paquete. Con RIP el máximo número de saltos se sitúa en 15, y por ello es utilizado en redes con dimensiones reducidas en cuanto a número de *routers*. De hecho, una métrica de 16 indica el valor infinito.

Aunque RIP 2 emplea los algoritmos básicos de RIP 1, aporta unas características nuevas muy importantes:

- Identificadores de rutas externas. Permite propagar información sobre rutas establecidas con otros protocolos de encaminamiento (como EGP o BGP) sin alterarlas. Su objetivo principal es separar rutas "internas" de la red donde funciona RIP de rutas "externas" a esa red bajo otros protocolos.
- Máscaras de subred. Permite trabajar con rutas de subredes. El gran problema que tenía RIP 1 era no disponer de esta característica, aunque su necesidad es evidente.
- Dirección del siguiente salto. En cada entrada de ruta de un mensaje RIP se puede especificar, además del número de saltos para llegar a la IP destino (como se hace en RIP 1), la dirección IP del siguiente *router* al que pueden ser enviados los paquetes, en vez de utilizar el *router* que genera el mensaje. Permite la optimización del encaminamiento en la red.
- Autentificación. Aporta mecanismos para que un *router* solo acepte mensajes RIP determinados con el objetivo de aumentar la seguridad de acceso los *routers*. Se evita así que cualquier equipo de una red pueda enviar paquetes RIP a un *router* para confundirlo. Básicamente consiste en asociar un código redundante al bloque con las entradas de rutas del paquete. Así, si algún equipo no autorizado modificase las rutas del paquete RIP, los *routers* autorizados interpretarían

dicho paquete como erróneo, al no ser ya válido el código que tiene. Para que el mecanismo sea eficaz, el código redundante se calcula aplicando claves y métodos hash.

- *Multicasting*. Los paquetes RIP 2 se envían a una dirección IP específica; la dirección IP de multicast 224.0.0.9 (de la clase especial de *multicast* de IP: 224.0.0.0/28). Solo los *routers* con RIP 2 activo hacen caso de lo recibido por esa dirección, esto es, funciona como si de un *broadcast* selectivo se tratase.

En LANs, los paquetes con direcciones multicast de destino se transportan en tramas con direcciones MAC de destino reservadas para tal uso. Esto reduce bastante la carga en la red y en los equipos, puesto que la conversión MAC-IP es directa. Así por ejemplo, un paquete IP con destino 224.0.0.9 viajará en un trama de enlace Ethernet con una dirección destino como 000746000009, donde 000746 es un código propio del fabricante de la tarjeta Ethernet y 000009 referencia la dirección de multicast de RIP 2.

Los mensajes RIP son transportados por datagramas UDP dirigidos al número de puerto 520. Un mensaje RIP tiene 4 bytes de cabecera, y utiliza 20 bytes más por cada entrada de ruta, sin contar los 20 de IP y los 8 de UDP. Así se pude señalar un máximo de 25 rutas por mensaje, conservando un tamaño no superior a 512 bytes por datagrama UDP (8+4+20x25=512). El formato del mensaje de RIP 2 se muestra en la Figura 7. Formato de mensajes RIP.

.

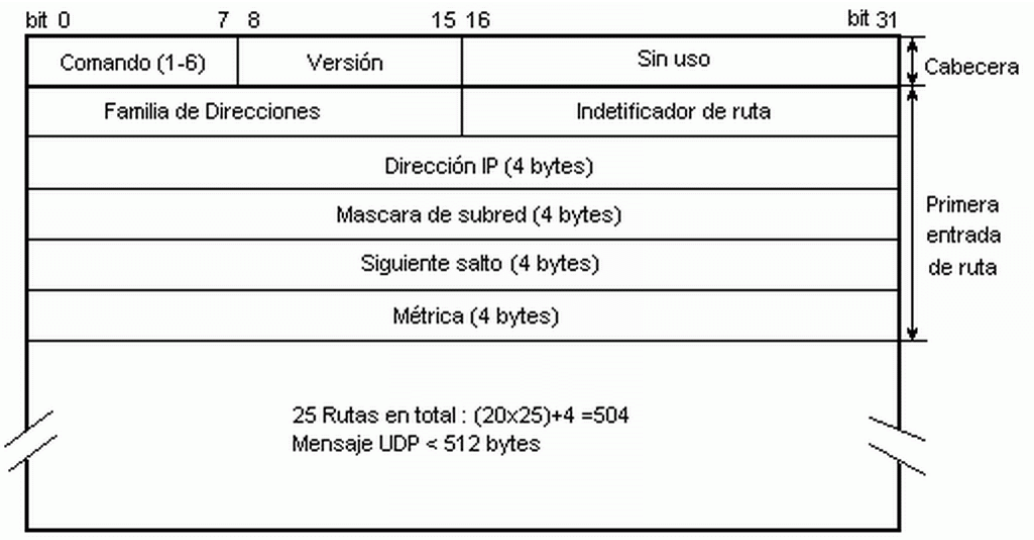


Figura 7. Formato de mensajes RIP.

Dentro de la cabecera, el campo "**comando"** indica la función del mensaje RIP, y básicamente puede tener el valor 1 (RIP r*equest* o solicitud) ó 2 (RIP r*esponse* o respuesta). Con RIP 2, en el capo versión debe aparecer el valor 2. El "**identificador de ruta**" permite separar los mensajes RIP referentes a la red donde trabaja RIP de los mensajes relativos a otros procedimientos de encaminamiento.

RIP permite trabajar con información de encaminamiento de otros protocolos que no son IP, y para identificar el protocolo al que pertenecen los datos de una entrada de rutas se usa el campo "**familia de direcciones"**, que con IP vale 2. La información referente a autentificación, cuando se utiliza, se envía

en mensajes RIP que en vez de entradas de rutas tienen un campo con la clave. Estos mensajes se identifican por que, en ellos, el valor del campo "familia de direcciones es" FFFFh.

Para un mensaje RIP 2 generado por un *router* dado, cada entrada de ruta hace referencia a una dirección "**IP destino**" de red o máquina que se puede alcanzar desde el *router*, su correspondiente "**máscara de subred**", la dirección IP del "**siguiente salto**" o *router* al que deberían enviarse los paquetes (0.0.0.0 si los paquetes deben enviarse al *router* que envía el mensaje), y el "**número de saltos**" necesario para alcanzar el destino (métrica). Este número de saltos se cuenta desde el *router* que envía el mensaje RIP.

Cuando se inicia el proceso de actualización de la tabla de rutas en un *router* con RIP 2 instalado, se envían solicitudes RIP (comando=1) por todas las interfaces activas reclamando entradas de rutas de los *routers* adyacentes. Los *routers* que las reciben envían la información de sus correspondientes tablas de encaminamiento mediante mensajes RIP de respuesta (comando=2). Además, en cada *router* con RIP, cada cierto tiempo (típicamente 30 segundos), una parte o la totalidad de la tabla de encaminamiento es enviada a los *routers* adyacentes a través de la dirección multicast 224.0.0.9 (comando = 2).

Cuando un *router* que acepta mensajes RIP 2 a la dirección de *multicast* recibe uno, examina las entradas de rutas que contiene para comprobar si debe actualizar su tabla de encaminamiento. Si en el mensaje aparece una ruta referente a un destino que no conoce, o a una entrada dinámica (que se puede actualizar) de su tabla de encaminamiento cuyo destino se podría alcanzar con menos saltos al utilizar como puerta de enlace el *router* que envió el mensaje RIP (o la IP especificada en el campo en "siguiente salto"), el *router* receptor procede a actualizar su tabla de encaminamiento. Para ello añade o modificando la entrada, colocando como puerta de enlace la dirección IP del *router* que envió el mensaje RIP (o la IP especificada en el campo en "siguiente salto").

Por cada ruta dinámica en la tabla existe un temporizador asociado. Un sistema con RIP que encuentra una ruta no actualizada desde hace cierto tiempo (3 minutos) procede a marcarla para su destrucción con el valor infinito (16). La eliminación permanente se retrasa 60 segundos más para asegurarse de que esta acción ha sido notificada al resto de la red con el tiempo suficiente.

- Si el equipo Linux1 enviase mensajes RIP 2 ¿Cuál sería el contenido de los mensajes que difundiría?

4.6 Herramientas para realizar la práctica

Monitores de red

Para analizar el tráfico de la red se dispone de varias herramientas de libre distribución en los PCs del laboratorio:

- **tcpdump.** Herramienta de captura y análisis de tráfico de una red de datos basada en línea de comandos muy potente, con muchas opciones de filtrado en tiempo de captura, y muy extendida en los ámbitos académico y profesional. En el laboratorio está instalada en el equipo

Linux2. El hecho de que funcione en línea de comandos hace que sea muy flexible, rápida de utilizar, y muy fiable en la captura de paquetes. Incluso se puede usar para crear programas que trabajen con el estado de la red. Además, su sintaxis es prácticamente un estándar para herramientas de análisis de redes de datos.

- **Wireshark**. Herramienta gráfica para captura y análisis de tráfico que reconoce gran cantidad de protocolos. Para las prácticas están disponible la versión de MS. Windows en cada PC de alumnos. Su uso es, inicialmente, más sencillo que el de "tcpdump", aunque no resulta tan flexible como esta última.

Para más información se puede ver el manual facilitado en el campus virtual, junto con la práctica 1 o cualquiera de los manuales oficiales disponibles en las páginas **tcpdump**: http://www.tcpdump.org/.**Wireshark**: http://www.wireshark.com/.

Acceso remoto a equipos del laboratorio

En el caso de necesitar acceder a los equipos **Linux 1** y **Linux 2** del laboratorio (10.3.7.0 y 172.20.43.232) para ver sus tablas de encaminamiento, la configuración de interfaces o ejecutar comandos como "ping". Para ello se pueden utilizar los servicios de ejecución remota y de terminal remoto, con el usuario "**alumnos**" con la contraseña "**alumnos**".

- Para la ejecución remota de comandos en los equipos Linux desde el PC del alumno con MS. Windows se puede utilizar el programa "**rexec**" instalado en los PCs. Este programa permite ejecutar comandos de forma remota en el equipo con la dirección IP especificada, conociendo un usuario y contraseña válidos, así como ver el resultado de estos comandos en una ventana de texto.

- Para el servicio de terminal remota, se debe usar el programa cliente "**telnet"** de M.S Windows (en línea de comando) o el popular cliente "**putty**", más avanzado que el anterior. Ambos programas permiten acceder a una consola de línea de comandos del equipo remoto, lo cual es útil para ejecutar aplicaciones interactivas como el monitor de red "**tcpdump"** disponible en el equipo Linux 2. Para este caso concreto se debe ejecutar el siguiente comando en la ventana del programa terminal:

```
sudo /usr/sbin/tcpdump [parámetros]
```

El comando "sudo" ejecuta el comando especificado tras él (se requiere el camino completo del mismo) habilitando permisos de root, lo cual es necesario para ejecutar el monitor de red.

Finalmente, es posible analizar cierta información procedente de los tres *routers* del laboratorio ejecutando el comando "**stdprac**" en el equipo Linux 2 (con "rexec", "telnet" o "putty") usando esta sintaxis:

```
stdprac [router] [comando] [texto]
```

Los parámetros son los siguientes:

- **router**. Puede ser uno de estos tres valores; "2513", "1720" o "1601", e indica el *router* sobre el que se desea obtener información.

- **comando**. Especifica que información del *router* se desea obtener. Puede especificarse "**rutas**" para obtener la tabla de encaminamiento del *router*, o "**intf**" para explorar la configuración de los interfaces del *router*.

- **texto**. Este parámetro es opcional, y hace referencia a una cadena de texto que se puede utilizar para filtrar la información devuelta por el comando, de forma que este solo muestra las líneas de la configuración que contienen el texto especificado. Por ejemplo, se puede especificar como texto una dirección IP usando los comandos "rutas" para ver solo las entradas referentes a esa dirección IP. Con el comando "intf", se puede, por ejemplo" indicar el texto MTU para ver sólo los MTUs de los interfaces.

  Además se pueden formar expresiones más complejas usando los símbolos "|" o "&" en el texto. El primero se utiliza para indicar que sólo se muestren las líneas que contienen al menos una de las cadenas indicadas.

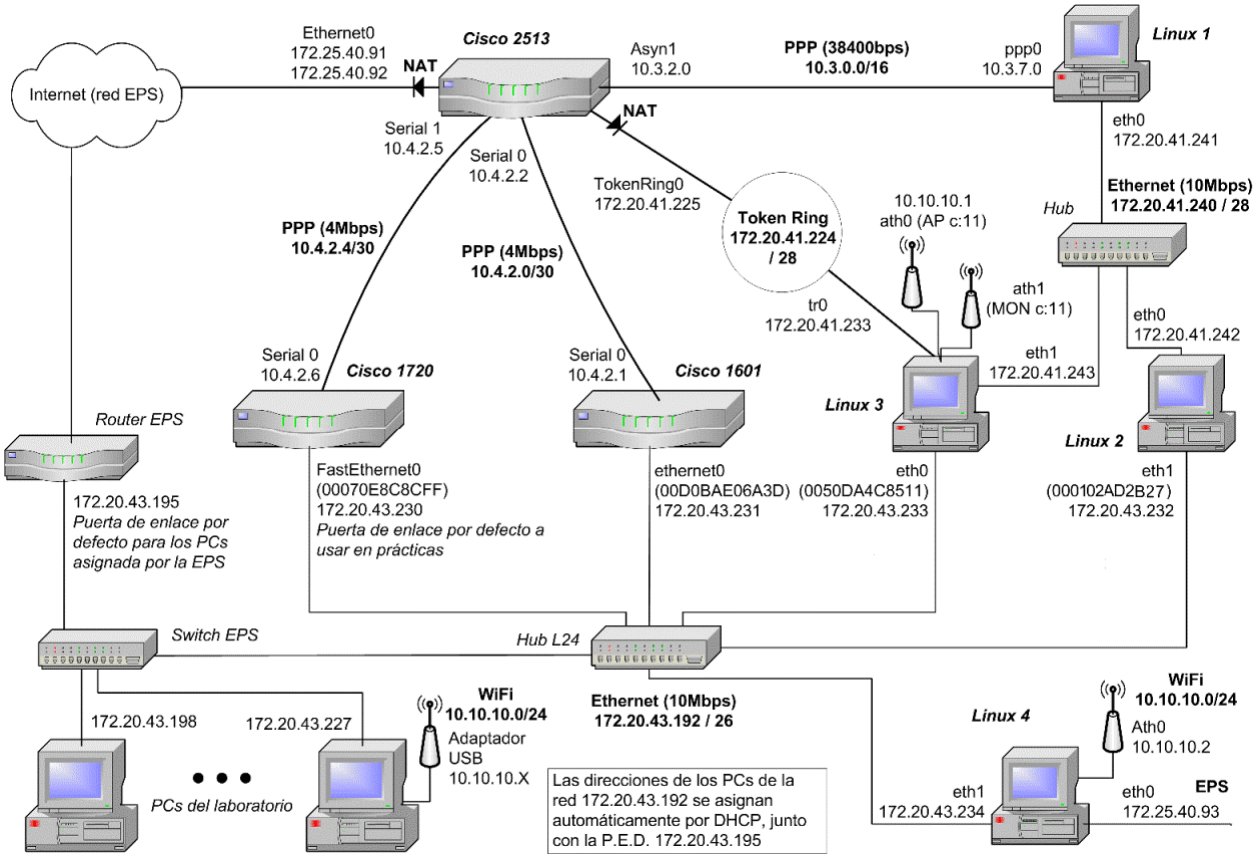


Figura 8. Topología del laboratorio L24 de la EPS. Universidad de Alicante.

4.7 Ejercicios

Cuestión 1. Tablas de encaminamiento

- Analiza la configuración de las tablas de encaminamiento de distintos equipos de la red de la figura 8 (PC del alumno, Linux 1, Linux 2 y los tres *routers*) con las herramientas descritas anteriormente. Trata de determinar la estructura de la red del laboratorio L24 con esa información pintando su esquema en papel. Luego compara la estructura de red que has determinado con el esquema de la red del laboratorio L24 facilitado por el profesor en la figura 8.

- Tablas de encaminamiento Windows: En general, en la tabla de encaminamiento de una maquina con MS-Windows, ¿Qué dirección IP tienen como puerta de enlace la entradas correspondientes a una red conectada directamente a la máquina?
- Tablas de encaminamiento Linux: Con relación a la tabla de encaminamiento de un equipo Linux, ¿A qué tipo de destino se refieren las entradas que tienen como puerta de enlace la dirección IP 0.0.0.0?
- Tablas de encaminamiento Linux: ¿De qué maneras puedes distinguir las direcciones destino que corresponden a una máquina y no a una red en la tabla de encaminamiento de una máquina Linux?
- Comandos de actualización de rutas estáticas en Windows y Linux: Modifica la tabla de encaminamiento de tu PC para alcanzar las direcciones de la red 10.3.0.0/16 pasando por los equipos Linux 2 y Linux 1. Comprueba si la modificación tiene éxito o no usando el comando "tracert" varias veces, y determinar el porqué.

  Comandos de actualización de rutas estáticas: Indicar el comando necesario para modificar la tabla de encaminamiento de tu equipo con el objetivo de hacer más corto el camino de los paquetes IP que parten de tu equipo hacia un destino situado en INTERNET, en concreto 209.85.227.106. Comprueba si la modificación tiene éxito o no usando el comando "tracert" varias veces.

Cuestión 2. Comprobación de rutas y encaminamiento

- Encaminamiento de paquetes ICMP Echo: Ejecuta el compando "ping -n 1 172.20.41.241" en tu equipo del laboratorio y determina el camino que siguen los paquetes 'Echo Request'.
- Encaminamiento de paquetes ICMP Echo Reply: Para el caso anterior, ¿qué camino siguen los paquetes 'Echo Reply'?
- Encaminamiento IP: Estudiando las tablas de encaminamiento de los diferentes equipos y el esquema de la red de la L24, determina qué camino sigue por la red del laboratorio un paquete que parte del router Cisco 1720 con destino 10.4.2.1.
- Encaminamiento IP Teniendo en cuenta que los paquetes que envía tu equipo a Internet deben seguir pasando por el Cisco 2513 ¿Cuál de estos equipos puedes usar para configurar una nueva puerta de enlace para tu equipo que sea por defecto y sea alternativa a la 172.20.43.230?
- Encaminamiento IP: Cuando accedes a un servidor de Internet (por ejemplo con HTTP) desde tu equipo del laboratorio, ¿Qué camino dentro de la red del laboratorio siguen los paquetes IP que envía el servidor a tu equipo para llegar a tu equipo? ¿Y si pruebas a configurar en tu equipo la otra puerta de enlace por defecto encontrada en el ejercicio anterior?
- Estudiando las tablas de encaminamiento de los diferentes equipos y el esquema de la red, determina qué camino sigue por la red del laboratorio un paquete que parte del *router* Cisco 1720 con destino 10.3.7.0. Después ejecuta el comando "tracert –d 10.3.7.0" desde tu equipo y examina el resultado. Observa las diferencias con la ruta obtenida, anteriormente, para la dirección 172.20.41.241.

- ¿Por dónde van los paquetes echo y echo-reply que intercambian tu equipo y el destino 10.10.10.2? Justifica la respuesta observando las tablas de encaminamiento de las máquinas de la L24 y el monitor de red.
- ¿Qué camino siguen los paquetes IP enrutados desde tu PC del laboratorio al destino 10.9.2.5? ¿Se genera algún error ICMP a causa de esos paquetes?
- Si ejecutas el comando "ping 172.20.41.233" en tu equipo del laboratorio, ¿Qué camino siguen y cuantas redes atraviesan los paquetes de "echo request"? ¿Y los de "echo reply"?
- Estudiando las tablas de encaminamiento de los diferentes equipos y el esquema de la red, determina qué camino sigue por la red del laboratorio un paquete que parte del *router* Cisco 1720 con destino 10.3.7.0. Después ejecuta el comando "tracert –d 10.3.7.0" desde tu equipo y examina el resultado. Observa las diferencias con la ruta obtenida, anteriormente, para la dirección 172.20.41.241.

Cuestión 3. Encaminamiento IP básico. Configuración de tablas estáticas

- En la siguiente topología de red se ha añadido la red LAN E al router A. Se pide, determinar unas nuevas direcciones IP y sus máscaras asociadas para todas y cada una de las redes y máquinas que constituyen la nueva topología sin que esto suponga la necesidad de que se modifique la tabla de encaminamiento del router B.

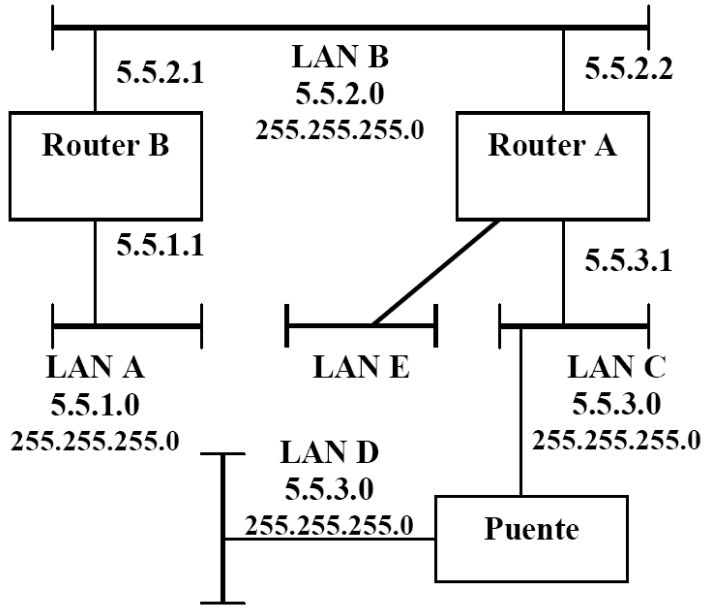


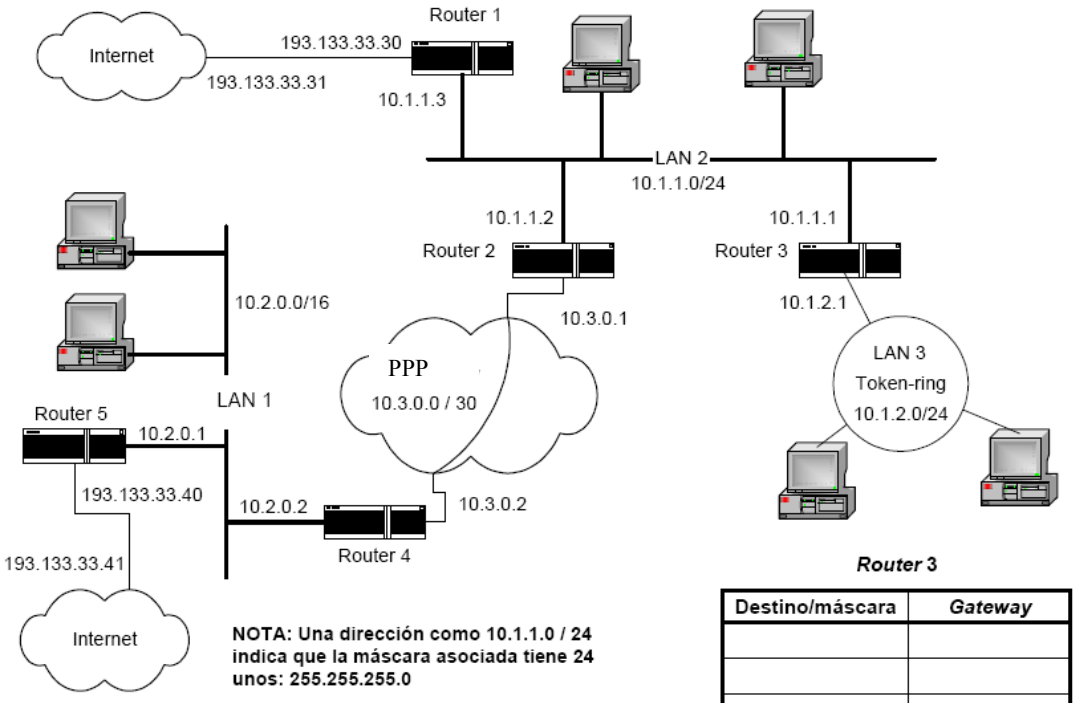
Tabla de rutas del Router B:

5.5.1.0	5.5.1.1
5.5.2.0	5.5.2.1
5.5.3.0	5.5.2.2

Direcciones IP y máscaras:

LAN A	
LAN B	
LAN C	
LAN D	
LAN E	

- Dada la siguiente estructura de red, completar las tablas de encaminamiento de los routers 1, 2, 3 y 4. Se supone que el router 5 ya está configurado correctamente. Además, se debe asegurar la conectividad IP entre las tres redes LAN del esquema, y que todos los paquetes IP destinados a otras redes se dirijan a la conexión con Internet más cercana. También, se exige que las tablas de encaminamiento deben tener el menor número de entradas posibles, pero eso sí, siempre evitando la redirección de paquetes.



Router 3

Destino/máscara	*Gateway*

Router 1

Destino/máscara	*Gateway*

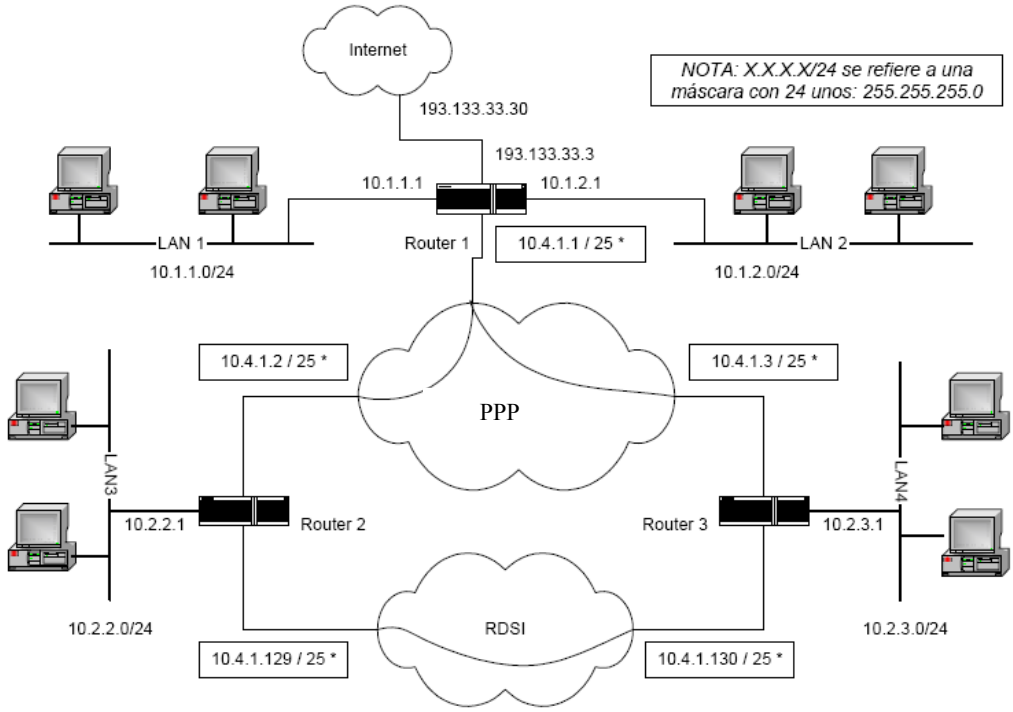
Router 2

Destino/máscara	*Gateway*

Router 4

Destino/máscara	*Gateway*

- Dada la siguiente estructura de red, asignar direcciones IP a los extremos de las conexiones, teniendo en cuenta que se dispone de la subred 10.4.1.0/24 para todas las conexiones punto a punto.
- Después, se pide completar las tablas de encaminamiento de los routers 1, 2 y 3 para asegurar la conectividad IP entre las redes LAN de modo que cualquier paquete dé un máximo de 2 saltos hasta alcanzar su destino. Además, hay que considerar:
    - Que sólo los equipos de las redes 10.1.1.0 y 10.1.2.0 deben tener acceso a Internet.
    - Que deben evitarse los bucles de paquetes.
    - Que las tablas deben tener el mínimo número de entradas necesario para realizar los encaminamientos adecuadamente.
    - Las subredes para los enlaces PPP y RDSI deben ser diferentes.



Router 1

Destino/máscara	*Gateway*

Router 2

Destino/máscara	*Gateway*

Router 3

Destino/máscara	*Gateway*

– Se dispone de dos equipos PC, uno de tipo Windows y otro de tipo Linux, cuyas tablas de encaminamiento respectivas son:

```
Dirección de red    Máscara de red   Puerta de enlace    Interfaz
        0.0.0.0          0.0.0.0         10.1.0.3    10.1.0.1
       10.1.0.0      255.255.0.0         10.1.0.1    10.1.0.1
       10.1.0.1  255.255.255.255        127.0.0.1   127.0.0.1
       10.5.0.0      255.255.0.0         10.5.0.1    10.5.0.1
       10.5.0.1  255.255.255.255        127.0.0.1   127.0.0.1
       10.3.0.0      255.255.0.0         10.1.0.2    10.1.0.1
       10.4.0.0      255.255.0.0         10.1.0.2    10.1.0.1
      127.0.0.0        255.0.0.0        127.0.0.1   127.0.0.1
```

Destination	Gateway	Genmask	Flags	Iterface
10.4.0.0	10.3.0.2	255.255.0.0	UG	eth1
10.1.0.0	0.0.0.0	255.255.0.0	U	eth0
10.3.0.0	0.0.0.0	255.255.0.0	U	eth1
127.0.0.0	0.0.0.0	255.0.0.0	U	lo
0.0.0.0	10.1.0.3	0.0.0.0	UG	eth0

- Se sabe que ambos equipos actúan como routers, para encaminar paquetes entre sí y para encaminar paquetes a Internet. También se sabe que el equipo Linux tiene dos interfaces, eth0 y eth1, cuyas direcciones IP son 10.1.0.2 y 10.3.0.1 respectivamente.
- Se pide dibujar la topología de red que hay alrededor de esos equipos, incluyendo todas las redes, equipos y máquinas de interconexión que aparecen en las tablas de encaminamiento, incluyendo sus direcciones IP, y la posible ubicación de la conexión a Internet.

Cuestión 4. Encaminamiento IP dinámico. Protocolo RIP

- Realiza una captura (de al menos 30 segundos) con el monitor de red para localizar mensajes RIP 2 en el segmento Ethernet 172.20.43.192/26. Averigua de quien proceden los mensajes RIP capturados.
- Comprobar si los mensajes RIP tienen información redundante de autentificación.
- Examinar las direcciones IP y MAC del paquete RIP procedente de la máquina CISCO 1720 para comprobar el uso de direcciones *multicast* de red y de enlace, y la correspondencia entre estas.
- ¿Concuerda toda la información sobre rutas que dispone la máquina CISCO 1720 con la que transportan los mensajes RIP procedentes del CISCO 1720?
- Actualización tablas de encaminamiento con protocolo RIP: Comprobar si en la tabla de encaminamiento del router Cisco 1601 hay alguna entrada dinámica generada por RIP. En base a ello, ¿se puede afirmar que el router Cisco 2513 está enviando paquetes RIP?