Sistemas de Transporte de Datos
Ingeniería Informática (9186)

# Manual de la Práctica 1: Encaminamiento avanzado con IP

Francisco Andrés Candelas Herías
Santiago Puente Méndez
Grupo de **I**nnovación **E**ducativa en **A**utomática

Universitat d'Alacant
Universidad de Alicante

# Práctica 1. Encaminamiento avanzado con IP

## 1. Objetivos

- Entender cómo funciona la traducción de direcciones de red NAT, conocer sus principales aplicaciones, y analizar casos avanzados de traducción.
- Conocer como se realiza la gestión dinámica de tablas de encaminamiento mediante protocolos de enrutamiento dinámico como RIP e EIGRP.
- Aprender a utilizar la asignación dinámica de puertas de enlace con HSRP.
- Conocer comandos básicos de IOS de Cisco, y como se aplican las listas de acceso.

## 2. Conocimientos básicos

### 2.1. Listas de acceso

Una lista de acceso (o **ACL**: *Access List*) es una forma de definir criterios genéricos, que se pueden aplicar a multitud de comandos del router, como los de gestión de QoS, enrutamiento de nivel de red, NAT, conmutación de nivel de enlace, gestión de usuarios... Las ACLs son actualmente la piedra angular de muchos sistemas operativos de red, tales como el IOS de Cisco. Las ACLs pueden ser estáticas o dinámicas, para definir criterios que siempre permanecen igual, o que pueden modificarse con el tiempo.

Una ACL es una colección secuencial de condiciones "permite" (*permit*) y "deniega" (*deny*) que se aplican a paquetes de datos para decidir si deben ser procesados o bloqueados. Los paquetes sobre los que trabaja una ACL dependen del comando de IOS donde se utiliza la ACL. Por ejemplo, si la ACL se utiliza en la definición de características de la entrada de una interfaz de red, entonces se permite o se bloquean los paquetes que entran por esa interfaz, pero si la ACL se utiliza en la definición de una política QoS (*Quality of Service*), entonces la ACL especifica a que paquetes se debe aplicar una restricción de velocidad y a cuáles no.

Cada ACL se identifica con un número, y las distintas condiciones de la ACL se definen como diferentes líneas en las que se indica ese número tras el comando "acess-list". Cuando una ACL debe evaluar un paquete de datos, se compara los campos existentes en dicho paquete con los atributos definidos en cada condición de la ACL, de forma secuencial. Si una condición se define con la sentencia "*permit*", y los campos del paquete de datos cumplen la condición, la ACL acabará y devolverá un valor "verdadero" al comando que la llamó. Sin embargo, si una condición se define con la sentencia "*deny*", y los campos del paquete de datos cumplen la condición, la ACL acabará y devolverá un valor "falso" al comando que la llamó. Además, siempre existe una condición "*deny any any"* implícito al final de cualquier ACL, de modo que los paquetes de datos que no cumplan ninguna de las condiciones de la ACL se descartan automáticamente. Es por tanto crítico el orden en que se aplican las líneas de la ACL, y merece especial atención en su diseño.

Por ejemplo, la ACL estática número 101 se podría definir con estos comandos:

```
Router(config)# access-list 101 remark Criterios para marcar precedencia 1
Router(config)# access-list 101 permit ip host 193.145.232.131 host 10.1.3.3
Router(config)# access-list 101 deny udp any 10.1.0.0 0.0.255.255 eq 80
Router(config)# access-list 101 permit ip host 193.145.232.132 host 10.1.2.2
```

La primera línea (*remark*) establece una descripción para la lista. La segunda línea define la primera condición; se devuelve "verdadero" para los paquetes IP que vienen desde el *host* 193.145.232.131 y van al 10.1.3.3. La tercera línea define una segunda condición: la lista devuelve "falso" para los paquetes UDP que vienen desde cualquier equipo (*any*) y van dirigidos a una dirección que empieza por "10.1." y al puerto 80. Con el lenguaje de IOS, en las listas de acceso no se especifican máscaras de red, como sería 255.255.0.0, sino un patrón como 0.0.255.255 que corresponde a la máscara de red invertida. La cuarta línea define otra condición más: devolver "verdadero" para los paquetes IP que van desde el *host* 193.145.232.132 al 10.1.2.2. Si no se cumple alguna de las tres condiciones, la lista devolverá "falso".

En general, las listas de acceso permiten establecer las condiciones no sólo por direcciones IP, sino también por puertos, protocolos, determinados bits de las cabeceras, tamaño de paquetes, valores de valores de QoS..., incluyendo también campos de otros protocolos diferentes al nivel de red.

Hay que considerar que los números utilizados para identificar las ACLs definen el espectro de actuación de la lista de este modo:

| Rango del identificador | Aplicación |
|---|---|
| 1 – 99 | Lista IP estándar |
| 100 – 199 | Lista IP extendida |
| 200 – 299 | Lista de acceso por campo "type-code" |
| 700 – 799 | Lista LAN con direcciones de 48-bit MAC |
| 1100 – 1199 | Lista LAN extendida con direcciones de 48-bit MAC |
| 1300 – 1999 | Lista IP estándar (rango expandido) |
| 2000 – 2699 | Lista IP extendida (rango expandido) |

En un router con IOS, se puede comprobar la configuración de ACLs ejecutando el comando "*show access-lists*", que devolverá un resultado como el siguiente, donde el valor "*matches*" indica el número de paquetes que han cumplido alguna condición de la lista:

```
Router# show access-lists
Extended IP access list 101 (201 matches)
   remark Lista con criterios para marcar con precedencia 1
   permit ip host 193.145.232.131 host 10.1.3.3
   permit ip host 193.145.232.131 host 10.1.3.3
   deny udp any 10.1.0.0 0.0.255.255 eq 80
   permit ip host 193.145.232.132 host 10.1.2.2
```

## 2.2. Traducción de direcciones con NAT y PAT

Dentro de las técnicas empleadas en el enrutamiento, una de las más útiles y que más se ha extendido con IPv4 es NAT (*Network Address Translation*), definida en la RFC 3022. Básicamente, NAT sirve para cambiar (o traducir) las direcciones de los paquetes del nivel de red de forma transparente a los niveles superiores, especialmente al de aplicación. Como se estudia a continuación, NAT también puede cambiar los puertos de transporte de TCP y UDP si es necesario. El objetivo principal de la traducción es permitir interconectar redes que usan rangos de direcciones incompatibles entre sí, como pueden ser las direcciones privadas y públicas de IPv4.

En su configuración más simple, NAT trabaja en un router que une dos redes, cada una de las cuales puede usar su propio esquema de direcciones IP, bien sean privadas o públicas. Una de las redes se designa como **interior** o ***inside*** y la otra como **exterior** u ***outside***. Típicamente la interior es una red privada y la exterior una red pública con acceso a Internet.

La aplicación más utilizada de NAT es que los equipos de una red privada, con direccionamiento privado, puedan acceder a un esquema de direccionamiento público de forma transparente. Como es posible asignar muchas direcciones privadas a un pequeño rango de direcciones públicas se obtiene una reducción de costes, al tener que solicitar menos direcciones IPv4 públicas. También hay que tener en cuenta que las direcciones IPv4 públicas son escasas, y es difícil adquirir subredes o rangos consecutivos amplios. Mientras que las direcciones IPv4 públicas son asignadas globalmente por NIC (*Network Information Center*) o localmente por los proveedores de acceso a internet, como direcciones privadas válidas se pueden coger de los siguientes rangos:

- 1 red de clase A: **10.0.0.0**.
- 16 redes de clase B: **172.16.0.0** a **172.31.0.0**.
- 256 redes de clase C: **192.168.0.0** a **192.168.255.0**.

En muchos casos se dispone de un número grande de direcciones IP internas privadas que deben ser traducidas a un pequeño número de direcciones externas públicas (una sola en el caso límite). Esto es posible gracias a una característica conocida como PAT (*Port Address Translation*), también denominada *overload*, y que es parte de la funcionalidad de NAT. Ésta se basa en utilizar distintos números de puerto cliente de TCP o UDP con la misma dirección externa para distinguir entre las traducciones de direcciones internas diferentes.

Además de la interconexión de redes privadas con públicas, NAT ofrece otras ventajas, entre las que destacan las siguientes: se puede simplificar el direccionamiento de una red privada usando direcciones de clases A o B, y se aumenta la seguridad por el uso de direcciones privadas inaccesibles desde el lado público.

Los principales inconvenientes de NAT derivan de la propia traducción. NAT requiere explorar las cabeceras de los paquetes IP de red o de niveles superiores, e incluso los datos, para cambiar las direcciones IP y los números de puerto de TCP o UDP. Ese proceso también implica recalcular las sumas de chequeo de errores. Por ello NAT repercute en el rendimiento de los routers además de dificultar el seguimiento o traza de los paquetes. También hay que tener en cuenta que la traducción no siempre es sencilla o posible, y de hecho no todos los protocolos de aplicación basados en TCP/IP admiten NAT. Cambiar las direcciones IP en una cabecera de un paquete es fácil, pero hay aplicaciones, como por ejemplo los protocolos de muchos juegos en red, que envían información sobre el direccionamiento IP dentro de los datos de algún paquete, e incluso codifican dicha información con valores ASCII en vez de numéricos. Esto implica que NAT no pueda funcionar correctamente cuando se utilizan mecanismos de seguridad con encriptación de datos. Aun así, NAT soporta muchos protocolos.

Hay dos tipos de traducciones posibles y aplicables a la vez: **dinámica y estática**. Con la traducción dinámica, el administrador puede configurar en el router un conjunto de direcciones de una red que deben ser traducidas a un conjunto de direcciones diferentes en la otra red, normalmente más reducido. Para cada paquete de red nuevo que llegue, el router decidirá dinámicamente que direcciones debe emplear para el cambio, siguiendo estrategias como *round-robin* para seleccionar la dirección nueva concreta. Este es el caso de utilizado para conectar una red privada con muchos equipos a Internet mediante un acceso público con

pocas direcciones IP. En cambio, las traducciones estáticas son fijadas explícitamente por el administrador de la red, y definen una sustitución concreta de una dirección IP externa a una interna, o viceversa. Por ejemplo, la asignación estática puede resultar útil cuando un equipo externo desea acceder a un servidor interno.

Las funciones básicas de NAT (y PAT) las realizan muchos routers sencillos (los típicos de accesos ADSL o cable-módem), y los S.O. modernos como MS. Windows 2000, XP, Vista o Linux mediante los paquetes de software apropiados. Los routers de gamas media y alta permiten configuraciones más complejas de NAT, algunas de las cuales se verá en esta práctica. En la red del laboratorio, el router Cisco2513 aplica NAT a los paquetes IP que pasan por sus interfaces Ethernet 1 o TokenRing 1.

Cabe mencionar que el número de traducciones NAT que puede mantener un router depende principalmente de memoria física del mismo, ya que para cada traducción se requiere mantener información en una tabla. Esta tabla contiene las traducciones de las conexiones en curso, además de las realizadas recientemente a modo de caché.

## Traducción de direcciones internas

En la **Figura 1** se describe un ejemplo del uso típico de NAT. Considérese la estructura de red mostrada, donde se interconecta una red privada (también denominada intranet, red interna o *inside*) con Intenet (red externa o *outside*) mediante un router con NAT habilitado. Aunque un router puede traducir las direcciones de la red interna, las de la red externa o ambas a la vez, lo más sencillo y habitual es utilizar únicamente traducción de direcciones internas. En este sentido, según el ejemplo, en la red privada se usan direcciones IP privadas de la red 10.1.0.0/16, mientras que en el lado externo el router tiene asignadas dos direcciones IP públicas de clase A: 80.1.2.3 y 80.1.2.4.

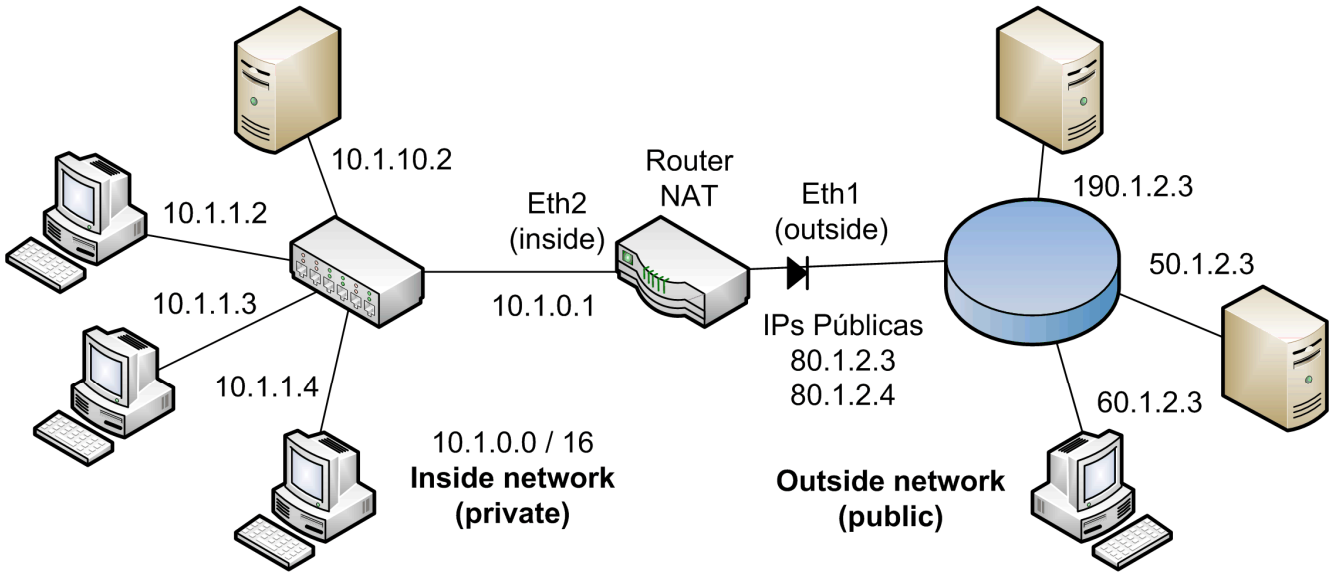


**Figura 1**. Ejemplo de aplicación de NAT.

Interesa que el router traduzca cualquier dirección 10.1.x.x interna a una dirección pública que permita acceder a los servicios de Internet cuando los paquetes salen a la red externa. Puesto que solo hay dos IP públicas, se requiere una traducción con PAT (*overload*). De esta forma, los equipos como el 10.1.1.2, el 10.1.1.3 o el 10.1.1.4 pueden comunicarse con servidores en el exterior mediante traducciones dinámicas, como por ejemplo:

| paquete en la red interior | paquete en la red exterior |
|---|---|
| origen: IP 10.1.1.2, puerto 1000<br>destino: IP 190.1.2.3, puerto 53 | origen: IP 80.1.2.3, puerto 1000<br>destino: IP 190.1.2.3, puerto 53 |
| origen: IP 10.1.1.3, puerto 2000<br>destino: IP 50.1.2.3, puerto 80 | origen: IP 80.1.2.4, puerto 2000<br>destino: IP 50.1.2.3, puerto 80 |
| origen: IP 10.1.1.4, puerto 1000<br>destino: IP 50.1.2.3, puerto 80 | origen: IP 80.1.2.3, puerto 1001<br>destino: IP 50.1.2.3, puerto 80 |

Hay que notar que NAT trata de mantener el número de puerto cliente si es posible. El router mantiene las traducciones en una tabla a modo de caché para que las direcciones destino de los paquetes de vuelta procedentes de los servidores sean traducidas a direcciones privadas siguiendo el proceso inverso. En este caso no interesa considerar traducciones diferentes para las direcciones públicas o externas. Esto es, el direccionamiento interno nunca se verá en el exterior, pero interesa que las direcciones externas si se vean como tales en la red interna.

Si se desease además disponer de servidores dentro de la red privada, por ejemplo un servidor Web (puerto 80) en el equipo 10.1.10.2, otro servidor Web (puerto 80) en el equipo 10.1.1.3 y un servidor FTP (puerto 21) en el equipo 10.1.1.4, asociados a la dirección pública 80.1.2.3, y que sean accesibles desde equipos externos cualquiera con dirección IP X.X.X.X también habría que configurar NAT para realizar estas traducciones internas y estáticas:

| paquete en la red exterior | paquete en la red interior |
|---|---|
| origen: IP X1.X1.X1.X1, puerto Y1<br>destino: IP 80.1.2.3, puerto 80 | origen: IP X1.X1.X1.X1, puerto Y1<br>destino: IP 10.1.10.2, puerto 80 |
| origen: IP X2.X2.X2.X2, puerto Y2<br>destino: IP 80.1.2.3, puerto 8080 | origen: IP X2.X2.X2.X2, puerto Y2<br>destino: IP 10.1.1.3, puerto 80 |
| origen: IP X3.X3.X3.X3, puerto Y3<br>destino: IP 80.1.2.3, puerto 21 | origen: IP X3.X3.X3.X3, puerto Y3<br>destino: IP 10.1.1.4, puerto 21 |

De este modo, incluso resulta posible configurar varios servidores para una misma aplicación, por ejemplo Web, que, que desde el punto de vista del lado exterior sean accesibles a través de distintos puertos. Como se observa, también es posible emplear puertos diferentes en la red interna y la red externa.

En un router que utiliza IOS se puede consultar el estado de la tabla de traducciones de NAT con el comando "*show ip nat address translations*". Si se consultarse el estado de la tabla de NAT de un router con la configuración anterior, considerando que aún permanecen las traducciones dinámicas además de las estáticas predefinidas, se tendría lo siguiente:

```
Inside global     Inside local      Outside local       Outside global
80.1.2.3:1000     10.1.1.2:1000     190.1.2.3:53        190.1.2.3:53
80.1.2.4:2000     10.1.1.3:2000     50.1.2.3:80         50.1.2.3:80
80.1.2.3:1001     10.1.1.4:1000     50.1.2.3:80         50.1.2.3:80
80.1.2.3:80       10.1.10.2:80           ---                 ---
80.1.2.3:8080     10.1.1.3:80            ---                 ---
80.1.2.3:21       10.1.1.4:21            ---                 ---
```

Los guiones significan "cualquier IP". Las distintas columnas de la tabla representan las siguientes direcciones:

- **Inside local**. Es la dirección asignada a un equipo de la red interna (privada) con la que se encamina en la red interna. Normalmente será una dirección privada no usable en Internet.
- **Inside global**. Es la dirección externa (pública) que aparenta tener un equipo de la red interna (privada) cuando se direcciona en la red externa. Es una dirección asignada al interfaz externo del router, y normalmente una dirección pública de Internet.
- **Outside local**. Es la dirección que un equipo externo (público) aparenta tener cuando se direcciona dentro de la red interna (privada).
- **Outside global**. Es la dirección asignada a un equipo de la red externa (pública) con la que se encamina en la red externa.

Como ejemplo, los comandos para configurar los casos anteriores en un router que utiliza IOS serían los siguientes:

```
interface Eth2
 ip address 10.1.0.1 255.255.0.0
 ip nat inside

interface Eth1
 ip address 80.1.2.3
 ip address 80.1.2.4 secondary
 ip nat outside

ip nat inside source interface Eth1 overload
ip nat inside source static tcp 10.1.10.2 80 interface Eth1 80
ip nat inside source static tcp 10.1.1.3 80 interface Eth1 8080
ip nat inside source static tcp 10.1.1.4 21 interface Eth1 21
```

Como se observa, primero se especifica que interfaces son externas y cuales internas. La primera línea “ip nat…” define la traducción dinámica interna como *overload* para aplicar PAT si es necesario, y las líneas posteriores las traducciones estáticas.

Los routers con IOS permiten especificar que NAT solo se debe aplicar a los paquetes IP con determinadas características. Por ejemplo, si se desea que NAT sólo se aplique a un grupo determinado de equipos de la red interna, se puede definir una ACL junto al comando “route-map” con la especificación de la traducción dinámica. El ejemplo siguiente hace que únicamente se aplique NAT a los equipos considerados en la definición del comando “route-map” identificado como “permitidos”. A su vez, los equipos que encajan en el “route-map” se definen con la lista de acceso 100, como los paquetes que parten de las subredes 10.1.0.0/16 y 10.2.0.0/16.

```
ip nat inside source route-map permitidos interface Eth1 overload

access-list 100 permit ip 10.2.0.0 0.0.255.255 any
access-list 100 permit ip 10.1.0.0 0.0.255.255 any

route-map permitidos permit 10
match ip address 100
```

Aunque usando el comando “route-map” se dispone de más flexibilidad para especificar a qué equipos se aplica NAT, se puede asociar un comando de traducción NAT directamente a una lista de acceso. Por ejemplo, los siguientes comandos, aplicados al router de los ejemplos anteriores, harían que los paquetes dirigidos a la red 172.25.30.0/24 y procedentes de

cualquier IP (any) de la red interna, se envíen por el interfaz externo sin que se les aplique NAT. Al resto de paquetes si se aplicaría NAT. Para ello es necesario acabar la lista 106 con un "*permit any any*", ya que si no se aplicaría la condición por defecto "*deny any any*".

```
ip nat inside source list 106 interface Eth1 overload

access-list 106 deny IP any 172.25.30.0 0.0.0.255
access-list 106 permit any any
```

La traducción de direcciones internas es soportada por la mayoría de routers, si bien los más sencillos (los típicos de accesos ADSL o cable-módem) no admiten listas de acceso para definir a que paquetes se debe aplicar NAT, ni especificaciones estáticas para cambiar números de puertos.

**Traducción de direcciones externas**

Una situación en la que se puede poner en marcha la traducción de direcciones externas para el ejemplo anterior (Figura 1) puede ser la siguiente: se desea que un equipo de Internet con dirección IP 190.1.2.3 sea direccionado en la red interna como si fuera el 10.10.10.5, esto es, como si fuera un equipo con dirección privada. Por ejemplo, el router realizaría esta traducción cuando un cliente Web (puerto 1010) en el equipo con la dirección 10.1.1.4 de la red privada acceda al servidor Web (puerto 80) de la dirección 10.10.10.5:

| paquete en la red interior | paquete en la red exterior |
|---|---|
| origen: IP 10.1.1.4, puerto 1010<br>destino: IP 10.10.10.5, puerto 80 | origen: IP 80.1.2.3, puerto 1010<br>destino: IP 190.1.2.3, puerto 80 |

En la tabla NAT de un router Cisco la traducción quedaría reflejada así:

```
Inside global     Inside local   Outside local   Outside global
80.1.2.3:1010     10.1.1.4:1010  10.10.10.5:80   190.1.2.3:80
```

Para que en general cualquier equipo de la red interna pudiese acceder a los servicios del equipo con dirección pública 190.1.2.3 como si éste fuera un servidor en la dirección privada 10.10.10.5 habría que añadir una entrada estática con el siguiente comando:

```
ip nat outside source static 190.1.2.3 10.10.10.5
```

La entrada estática anterior se reflejaría así en la tabla de NAT:

```
Inside global     Inside local   Outside local   Outside global
     ---               ---        10.10.10.5      190.1.2.3
```

Cabe destacar que para que una traducción como la anterior funcione correctamente, el router debe recibir los paquetes dirigidos a la dirección 10.10.10.5, por lo que hay que configurar los equipos para usen la dirección del router como puerta de enlace (específica o por defecto) para el destino 10.10.10.5/32.

También se puede configurar la traducción de direcciones externas para que se aplique automáticamente cuando un equipo público de la red externa (pública) acceda a un equipo privado de la red interna (privada). Es decir, cuando sea el equipo externo el que inicia la comunicación. Esto es especialmente útil cuando se quiere ocultar las direcciones originales de un grupo de equipos externos que tienen que acceder a servicios de equipos internos, o cuando las direcciones de los equipos externos coinciden con direcciones usadas para los equipos internos, como es el caso del ejemplo mostrado en la **Figura 2**. En este ejemplo, los equipos de la red LAN2, pueden acceder sin problemas a la LAN1, pero, en principio, los equipos de la LAN3 no pueden porque emplean el mismo direccionamiento, y las respuestas a sus paquetes acabarían en equipos de la LAN1. Para que los equipos de la LAN3 puedan

acceder a la LAN 1 sus direcciones (que son externas) deben ser traducidas por el NAT de Router 1.

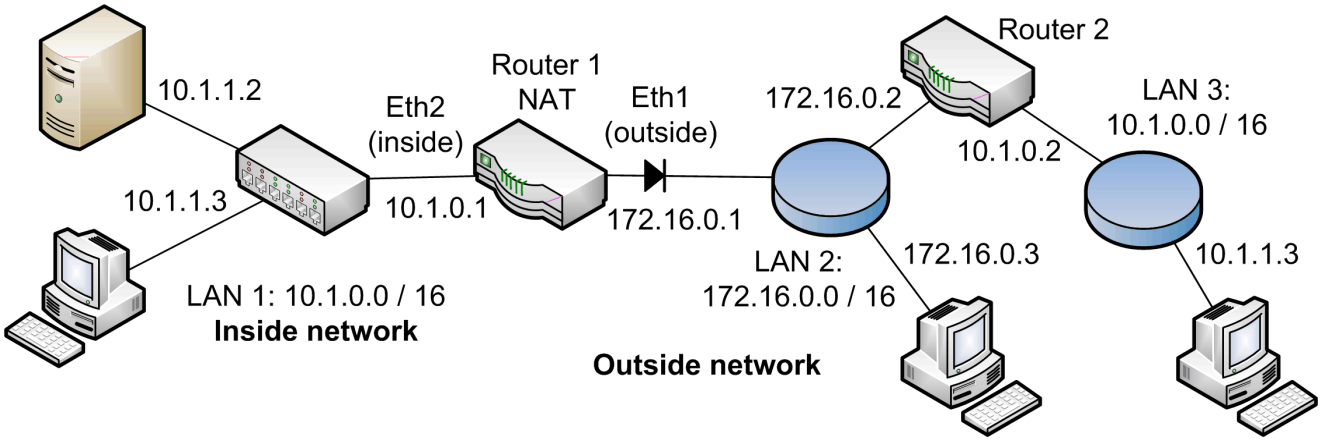


**Figura 2**. Ejemplo de aplicación de traducción de direcciones externas.

Para ello se requiere definir una lista de acceso con las direcciones externas que deben ser convertidas, y una lista de direcciones ("*nat pool*") con las posibles direcciones a utilizar dentro de la red interna. Por ejemplo, los siguientes comandos hacen que los paquetes que proceden de una dirección de la subred externa 10.1.0.0/16 (lista 1) lleguen a la parte interna con las direcciones privadas de la red 10.55.0.0/16 en el rango 10.55.0.1 a 10.55.255.254 ("nat pool ips-nuevas"):

```
ip nat pool ips-nuevas 10.55.0.1 10.55.255.254 netmask 255.255.0.0
access-list 1 permit 10.1.0.0 0.0.255.255
ip nat outside source list 1 pool ips-nuevas
```

Además de la configuración anterior de NAT *outside*, habría que realizar una configuración *inside* como las comentadas en el apartado anterior para que se traduzcan las direcciones de la LAN 1 por la dirección externa del router (172.16.0.1) para las LAN 2 y 3.

La mayoría de routers sencillos no permiten configurar una traducción de direcciones externa, y se requiere un router de gama media o alta, o un equipo MS. Windows o Linux con los paquetes de software adecuados.

## 2.3. Enrutamiento dinámico con RIP

El primer protocolo de encaminamiento dinámico estudiado en esta práctica será 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 v1 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 qué 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 v2 emplea los algoritmos básicos de RIP v1, añade 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.
- *Máscaras de subred*. Permite trabajar con rutas de subredes. El gran problema que tenía RIP v1 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 al destino, 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 o firma 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.
- *Multicast*. Los paquetes RIP v2 se envían a una dirección IP específica; la dirección de *multicast* 224.0.0.9. Solo los routers con RIP v2 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 sin necesidad de ARP. Por ejemplo, un paquete IP con destino 224.0.0.9 viajará en una trama de enlace Ethernet con una dirección MAC destino como 01:00:5E:00:00:09, donde 01:00:5E define un rango de direcciones especiales de MAC y 00:00:09 referencia la dirección de *multicast* de RIP v2.

Los mensajes RIP son transportados por datagramas UDP dirigidos al número de puerto 520. El formato del mensaje de RIP 2 se muestra en la **Figura 3**. 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).

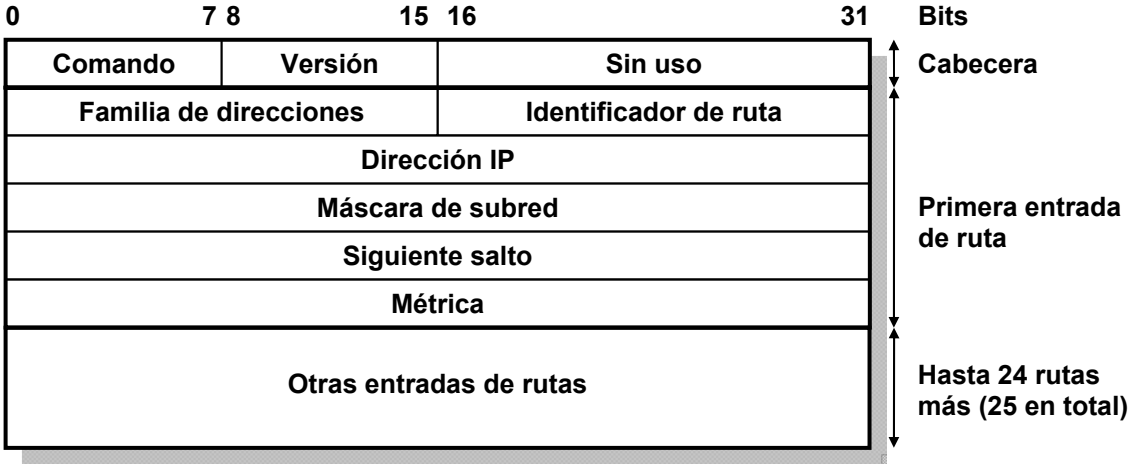


**Figura 3**. Estructura de un mensaje de RIP v2.

Los campos de un mensaje de RIP tienen los siguientes usos:

- **Versión**. Con RIP 2, este campo debe tener el 2.
- **Comando**. Indica la función del mensaje RIP. Tiene el valor 1 (RIP *request* o solicitud) ó 2 (RIP *response* o respuesta).
- **Familia de direcciones.** Para identificar el protocolo al que pertenecen los datos de una entrada de rutas se usa el campo. Con IP vale 2.
- **Identificador de ruta**. Permite separar los mensajes RIP referentes a la red donde trabaja RIP de los mensajes relativos a otros procedimientos de encaminamiento.

Cuando se utiliza la información sobre autentificación, esta se envía en campos adicionales que se incluyen antes y después de las entradas de rutas.

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 con 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 un router quiere actualizar su tabla de encaminamiento, 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 automáticamente a los routers adyacentes a través de la dirección *multicast* 224.0.0.9 (comando 2).

SI un router que acepta mensajes RIP 2 a la dirección de *multicast* recibe un mensaje, 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 modifica 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" si no es nula.

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 16 (infinito). La eliminación permanente se retrasa 60 s. más para asegurarse de que esta acción ha sido notificada al resto de la red con el tiempo suficiente.

### 2.4. EIGRP

EIGRP (*Enhanced Interior Gateway Routing Protocol*) es una evolución del protocolo IGRP desarrollado por Cisco en 1986 con la intención de subsanar las deficiencias de RIP. La primera versión de EIGRP aparece en 1990, con el objetivo de proporcionar mejor escalabilidad y tiempos de convergencia. EIGRP es un protocolo de vector de distancia con características de "estado de enlace", y trata de reunir lo mejor de cada tipo. El algoritmo

DUAL (*Diffusing Update Algorithm*) que se utiliza es el encargado de obtener convergencias libres de bucles y con tiempos muy reducidos. Mientras que RIP realiza actualizaciones cada medio minuto típicamente, los tiempos de actualizaciones de EIGRP son del orden de segundos. EIGRP, dispone de 4 componentes que se describen a continuación.

- **Módulos de protocolo**. EIGRP utiliza diferentes módulos que de forma independiente soportan los protocolos de red IP, IPX y AppleTalk.
- **Descubrimiento y Recuperación de Vecinos**. Un router con EIGRP mantiene información de sus vecinos (routers adyacentes) en una tabla para cada protocolo de red utilizado. Para mantener la tabla actualizada, se envía mensajes *Hello* cada 5 segundos, usando la dirección IP de *multicast* 224.0.0.10, y se espera las posibles respuestas. Si el router no recibe un mensaje *Hello* en 15 segundos (3 actualizaciones) de un vecino, elimina la dirección de este vecino de la tabla.
- **Protocolo de transporte de rutas fiable**. EIGRP emplea un protocolo fiable que utiliza confirmaciones y números de secuencia. De este modo se asegura la entrega ordenada de información como puede ser las actualizaciones de rutas. Este protocolo se apoya directamente sobre el protocolo de red IP, sin usar ni TCP ni UDP, y envía los mensajes a la dirección destino de *multicast* 224.0.0.10.
- **Algoritmo DUAL**. EIGRP implementa DUAL para seleccionar caminos. Está comprobado matemáticamente que este algoritmo garantiza que no ocurrirán bucles en el encaminamiento. Tampoco necesita incorporar mecanismos de actualizaciones periódicas, lo cual ralentizaría los tiempos de convergencia.

DUAL siempre selecciona para cada destino el mejor camino entre el router y ese destino. Para ello, dado el router donde se ejecuta DUAL, este determina el mejor sucesor (siguiente router) para ese camino, y una segunda alternativa, denominada "*feasible sucesor*". En caso de un fallo del sucesor en curso para un camino, automáticamente sería seleccionado el "*feasible sucesor*". El mejor camino se determina conforme a una métrica, que formalmente viene dada por la siguiente expresión:

$$métrica = \begin{cases} \left(K_1 \cdot B + \dfrac{K_2 \cdot B}{256 - Load} + K_3 \cdot Delay\right) \cdot \dfrac{K_5}{Reliability + K_4} & Si\ K_5 \neq 0 \\ K_1 \cdot B + \dfrac{K_2 \cdot B}{256 - Load} + K_3 \cdot Delay & Si\ K_5 = 0 \end{cases}$$

Donde las variables representan:

- *B*. Representa el ancho de banda del camino. Se determina de la siguiente manera, siendo valores $BW_i$ los anchos de banda de los interfaces del camino medidos en Kbps:

$$B = 256 \frac{10^7}{\min\limits_{\forall i} BW_i}$$

- *Delay*. Representa el retardo total del camino. Se calcula a partir de los valores $Delay_i$ que miden los retardos de los interfaces de **salida** (en µs) de los routers del camino.

$$Delay = 256 \sum_{\forall i} \frac{\mathrm{Delay_i}}{10}$$

- *Load*. Representa la carga de tráfico en el camino con un valor de 1 a 255. Un valor mayor representa que hay más carga.
- *Reliability*. Representa la fiabilidad del camino con un valor de 1 a 255. A mayor valor, más fiabilidad.
- $K_1$ a $K_5$. Parámetros para ponderar como afecta cada término a la métrica.

En la práctica, es habitual considerar $K_1$=1, $K_2$=0, $K_3$=1, $K_4$=0 y $K_5$=0, con lo que el cálculo de la métrica se simplifica a la siguiente expresión:

$$métrica = 256\left(\frac{10^7}{\min_{\forall i} BW_i} + \sum_{\forall i}\frac{\text{Delay}_i}{10}\right)$$

En cualquier caso, se observa como la métrica de EIGRP es más compleja que la métrica simple de RIP, basada esta última sólo en número de saltos. En los routers con IOS de Cisco, los valores $BW_i$ y $Delay_i$ se pueden obtener fácilmente consultando la configuración de los interfaces de los mismos usando el comando "*show interfaces*".

La figura **Figura 4** muestra la estructura de un mensaje EIGRP. Se puede observar los campos de numeración de mensaje, de confirmación y de suma de verificación que garantizan la entrega fiable y ordenada. El campo de código identifica el significado de cada mensaje en concreto. En función de los campos código y tipo, el campo de contenido tendrá un determinado tipo de información.

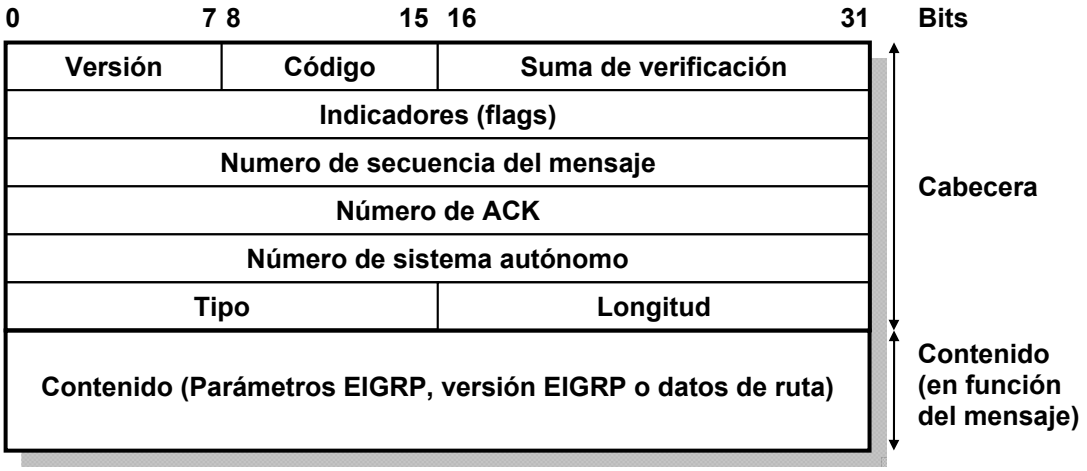


**Figura 4**. Estructura de un mensaje de EIGRP.

Los posibles mensajes que utiliza EIGRP son:

- **Update** (código 1). Es un mensaje de actualización cuyo contenido es información de rutas que han cambiado. Cuando se trabaja con encaminamiento IP, para cada ruta se indica su dirección destino, prefijo de máscara y opcionalmente la dirección del siguiente salto. También se indican otros valores como el MTU, el mínimo BW y la suma de *Delays* para esa ruta. Debe ser confirmado con un mensaje Ack.
- **Query** (código 3). EIGRP envía este tipo de mensajes para encontrar sucesores alcanzables (*feasible succesor*). Contiene información de rutas como *Update*.
- **Reply** (código 4). Estos mensajes se usan como respuesta a mensajes *Query* y también contienen información de rutas como Update.

- **Hello** (código 5). Mensaje usado para descubrimiento y recuperación de vecinos. En su contenido se indican los parámetros $K_i$ que usa router que envía el mensaje para el cálculo de la métrica, además de la versión del protocolo y de S.O.
- **Acknowledgement** o **Ack**. Es como un mensaje *Hello* (código 5) sin datos, y sirve para reconocer la recepción de un mensaje *Update*.

Aunque un router envía mensajes *Hello* cada 5 segundos para buscar vecinos, EIGRP únicamente actualiza las rutas cuando es necesario, y no existen temporizadores periódicos como en RIP en este caso. Por una parte, cuando un router modifica o incluye en su tabla de encaminamiento un destino, envía un mensaje *Update* a sus vecinos para informar sobre ello. Los otros routers considerarán el mensaje con el nuevo destino, y, en función de las métricas calculadas, actualizarán sus tablas. Además, contestarán al primer router con mensajes *Ack*.

Por otra parte, cuando un router deja de conocer como se accede a un destino, por ejemplo porque alguno de sus interfaces deja de funcionar, envía un mensaje *Query* a sus routers vecinos para solicitar sucesores alcanzables para ese destino. Este mensaje *Query* incluye la ruta del destino inaccesible y un valor de *delay* "infinito" (4294967295 o FFFFFFFFhex). Los routers vecinos responderán con mensajes *Reply* con posibles rutas al destino, o indicando que tampoco pueden acceder al destino (*delay* infinito), además de actualizar sus tablas de encaminamiento.

Aunque en esta práctica se introduce el funcionamiento de EIGRP, será en la siguiente práctica, al abordar las VPNs (*Virtual Private Networks*), cuando se compruebe lo efectivas que resultan las actualizaciones de este protocolo frente a las de RIP.

### 2.5. Routers redundantes con HSRP

En las instalaciones profesionales que demandan cierta robustez, no se puede confiar funciones de encaminamiento a un único router, ni tampoco a un router que tenga una única conexión a la red que pueda fallar. Lo adecuado es utilizar varios routers redundantes, de forma que si falla uno en un momento dado, o falla su conexión a la red, otro pueda asumir sus funciones. Además es muy importante que, durante el traslado de las funciones de un router a otro, los equipos de usuarios que necesitan esas funciones sigan trabajando sin necesidad de cambios en su configuración. Para que esta tarea se realice automáticamente, se puede utilizar protocolos como el HSRP (*Host Standby Routing Protocol*) de Cisco Systems, definido en la RFC 2281, o el VRRP (*Virtual* Router *Redundancy Protocol*), una versión del anterior definida en la RFC 2338. En esta práctica se estudiará el funcionamiento básico de HSRP.

Con HSRP, dos o más routers disponibles, y conectados a una misma red, se comunican entre sí para crear entre todos la ilusión de un único "**router virtual**", que es el router utilizado por los equipos de usuarios de esa red como puerta de enlace por defecto. Al router virtual se le asignan una dirección IP y una dirección MAC, que comparten todos los routers disponibles. Como dirección IP del router virtual se puede escoger una dirección no usada en la red. La MAC del router virtual siempre tiene la forma 00:00:0C:07:AC:xx.

El protocolo asegura que en un momento dado, un único router, el que tiene mayor prioridad de entre los que están funcionando, atiende las funciones del router virtual. A ese router se le llama "**router activo**". Y si el router activo falla, el protocolo se encarga de escoger otro router de entre los que están funcionando (denominados "**routers en espera**" o "*standby* routers") para que sea el nuevo router activo y realice las funciones del router virtual. Todo este proceso e realiza de forma transparente a los equipos de usuarios.

Para conseguir lo anterior, HSRP define tres tipos de mensajes: 0 o ***hello*** (saludo), 1 o ***coup*** (asalto) y 2 o ***resign*** (renuncia). Tanto el router activo como los que están en espera envían mensajes de *hello* cada cierto tiempo llamado "***hello time***" ("tiempo de saludo"), y en estos mensajes el router emisor informa de su estado (activo, en espera, enviando *hello* o recibiendo *hello*), su prioridad, su tiempo de saludo… Cuando un router en espera detecta que no recibe mensajes de *hello* del router activo tras pasar un tiempo llamado "***hold time***" ("tiempo de retención"), y además ese es el router que tiene más prioridad (lo cual sabe por los mensajes de *hello* recibidos antes), decide ser el nuevo router activo. Para informar de esto, envía un mensaje de tipo *coup*. Un router puede dejar de ser el router activo por un fallo, o por que lo solicite explícitamente enviando un mensaje tipo *resign*. Los valores por defecto para el *hello time* y el *hold time* son de 3 y 10 segundos respectivamente. Con estos valores pequeños las transiciones de un router activo a otro se hacen rápidamente, y las conexiones TCP de los equipos usuarios que usan el router virtual como puerta de enlace no se interrumpen.

Todos los mensajes de HSRP se colocan dentro de paquetes **UDP-IP** dirigidos al puerto **1985** y a la dirección IP de *multicast* **224.0.0.2**, siendo escuchados por otros routers con HSRP. Las direcciones origen de los datagramas IP son las direcciones real que tienen asignadas los routers, no la asignada al router virtual.

La **Figura 5** muestra un ejemplo de aplicación, en el que se dispone de una red LAN1 con equipos clientes que se conecta a través de enlaces WAN a otra red LAN2 donde están los equipos servidores. Por seguridad, la red LAN1 se conecta mediante dos routers, R1 y R2, con dos enlaces RDSI independientes al router R3 que da acceso a la LAN2, de forma que si un enlace deja de funcionar, o falla R1 o R2, aun queda otro camino. Para garantizar que la puerta de enlace por defecto para los equipos clientes es la adecuada (la del enlace que está funcionando), se activa HSRP en los routers R1 y R2, a través de la red 10.1.0.0/16, de forma que atiendan un "router virtual" con dirección IP 10.1.0.3. Esta será la puerta de enlace por defecto a configurar en los equipos de la red 10.1.0.0/16. En un momento dado, solo uno de los caminos funciona; el asociado al router activo, que, en el caso de que los routers funionen correctamente, será el que tenga configurada una mayor prioridad.

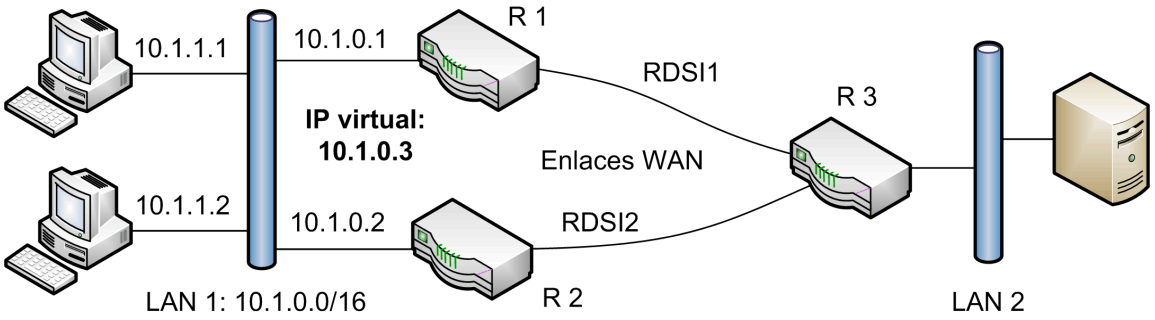


**Figura 5**. Configuración de dos routers redundantes usando HSRP.

Finalmente, cabe destacar otros dos aspectos de HSRP. En primer lugar, dentro de una misma red, se pueden configurar varios grupos de routers, atendiendo cada grupo un router virtual distinto. Un mismo router puede pertenecer a varios grupos. El número de grupo se coloca también dentro de todos los mensajes HSRP, y corresponde con el valor XX que se coloca en el último byte de la dirección MAC del equipo virtual (00:00:0C:07:AC:XX), En segundo lugar, todos los mensajes de HSRP llevan una cadena de autentificación de hasta 8 bytes o caracteres como medida de seguridad, de forma que los routers solo aceptan los mensajes que contienen la misma cadena que ellos tienen guardada en su configuración.

Para configurar HSRP en routers Cisco se emplea el comando "standby". Por ejemplo, la siguiente secuencia de comandos configura el interfaz de red "FastEthnernet 1" con HSRP versión 2, define el identificador HSRP 20, la dirección IP virtual 172.20.43.234, asigna al router una prioridad de 80, marca el router como activo, y define un "*hello time*" de 5 s y un "*hold time*" de 15 s:

```
interface Ethnernet 1
standby version 2
standby 20 ip 172.20.43.236
standby 20 priority 80
standby 20 preempt
standby 20 timers 5 15
```

El identificador HSRP permite distinguir diferentes configuraciones de HSRP sobre un mismo interface. Si se desea ver la configuración actual HSRP en un router Cisco hay que ejecutar el comando "*show standby*" que mostraría una información como la siguiente:

```
Ethernet1 - Group 126
  Local state is Active, priority 80, may preempt
  Hellotime 5 holdtime 15 configured hellotime 5 sec holdtime 15 sec
  Next hello sent in 00:00:03.466
  Hot standby IP address is 172.20.43.236 configured
  Active router is local
  Standby router is unknown expired
  Standby virtual mac address is 0000.0c07.ac7e
  2 state changes, last state change 00:01:49
```

# 3. Herramientas disponibles para realizar la práctica

## 3.1. Monitores de red Wireshark y tcpdump

En las prácticas se emplearán los monitores de red **Wireshark** y **tcpdump**. Ambos son unos programas muy potentes para captura de tramas y análisis de protocolos, con versiones para diferentes S.O. y de libre distribución bajo licencia GNU. Por ello su uso está muy extendido para administrar redes. Como otras muchas herramientas de red, se basan en unas librerías comunes conocidas como "pcap" o "winpcap", dependiendo de la plataforma utilizada, que también hay que instalar en el sistema.

Mientras que *Wireshark* ofrece una completa interfaz gráfica para acceder al contenido de los paquetes que circulan por la red, *tcpdump* es un programa de consola o línea de comando. Por eso, el primero es adecuado para capturar tramas en redes conectadas directamente al equipo donde se usa, mientras que el segundo es más adecuado para capturar tramas en redes remotas, accediendo a quipos remotos. La ventaja es que ambos usan el mismo formato de archivo para guardar las capturas, por lo que las capturas realizadas con *tcpdump* se pueden ver después gráficamente con *Wireshark*.

El programa *tcpdump* suele instalarse por defecto en los sistemas Linux, como una herramienta más de administración. Su versión equivalente para Windows se llama *windump*.

## 3.2. Acceso a otros equipos del laboratorio

Se puede acceder a los equipos Linux del laboratorio para ver sus tablas de encaminamiento, capturar tramas o ejecutar comandos como "ping". Para ello se pueden utilizar los servicios de ejecución remota y de terminal remoto, con el usuario "**alumnos**" y la contraseña indicada por el profesor de prácticas.

- Para la ejecución remota de comandos sencillos 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 cliente ***PuTTY*** con la opción Telnet o SSH. Telnet es un servicio que permite acceder remotamente a la consola de línea de comandos de un equipo para ejecutar comandos. SSH es también un servicio que permite acceder a la consola de línea de comandos, pero con encriptación de todos los datos intercambiados, por lo que cada vez se usa más. El programa *PuTTY* es libre y se puede descargar desde:

  http://www.chiark.greenend.org.uk/~sgtatham/putty/
- Con los programas *Telnet* o *PuTTY* se pude ejecutar aplicaciones interactivas como el monitor de red *tcpdump* disponible en los equipos Linux del laboratorio. En este caso concreto se debe ejecutar el siguiente comando en la ventana del programa terminal:

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

  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. Lo más cómodo es ejecutar el monitor de red para que guarde la captura en un archivo, en vez de mostrarla directamente en la pantalla de consola. Para ello se usa la siguiente sintaxis. La captura se finaliza con Control-C.

  ```
  sudo /usr/sbin/tcpdump –i eth0 –w miarchivo
  ```

  Se puede indicar un filtro para la captura. Por ejemplo, si se quiere capturar solo los paquetes que envía o recibe el equipo con dirección 10.3.7.0 se puede poner

  ```
  sudo /usr/sbin/tcpdump –i eth0 –w miarchivo host 10.3.7.0
  ```

  Si además se quiere limitar la captura a paquetes que envía o recibe un servidor Web (puerto 80) se puede poner:

  ```
  sudo /usr/sbin/tcpdump –i eth0 –w miarchivo host 10.3.7.0 and port 80
  ```
- Se puede usar un cliente FTP para recuperar el archivo con una captura de *tcpdump* realizada en otro equipo. En una consola de MS-DOS de Windows, se puede usar el comando "**ftp <dir_IP>**". Antes de ejecutar el programa, conviene cambiar al directorio local en donde se quiere guardar el archivo. Tras introducir el usuario y la clave, se puede pasar a modo binario con el comando "**bin**", y después recuperar el archivo con "**get <miarchivo>**". Para salir del programa FTP se usa el comando "bye". El archivo se puede abrir con el programa *Wireshark* para analizarlo con la interfaz gráfica.

### 3.3. Configuración de los routers Cisco del laboratorio

Es posible analizar la configuración de los tres routers del laboratorio ejecutando el comando ***stdprac*** en el equipo Linux 2 (ver apartado 3.1):

```
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. Ejecutando el comando "stdprac" sin parámetros se obtiene un listado completo de las opciones y parámetros del comando.
- **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, con el comando "nat" se puede especificar una dirección IP para ver solo entradas que tienen esa dirección.

De los posibles comandos, para la realización de esta práctica interesan los siguientes:

- **conf**. Muestra la configuración completa del router. Equivale a ejecutar "*show conf*".
- **hsrp**. Muestra el estado de HSRP. Equivale a ejecutar "*show standby*".
- **intf**. Muestra información sobre los interfaces. Equivale a ejecutar "show interfaces".
- **lst**. Muestra la configuración de la listas de acceso (ACL). Equivale a ejecutar "*show access list*".
- **nat**. Muestra la tabla de traducciones de NAT. Equivale a ejecutar "*show ip nat translations*".
- **rmap**. Muestra configuración de clasificación de tráfico "*route-map*". Equivale a ejecutar "show *route-map*".
- **rutas**. Muestra la tabla de encaminamiento. Equivale a ejecutar "*show ip route*".

### 3.4. Herramientas de red TCP/IP

Se puede hacer uso de las herramientas de línea de comando típicas de TCP/IP:

- ***ping***. Se puede usar tanto en el PC del alumno como en los Linux del laboratorio. La sintaxis cambia entre Linux y MS. Windows.
- ***netstat***. Para analizar las tablas de encaminamiento del PC del alumno (en la línea de comandos de MS. Windows), o las tablas de encaminamiento en los equipos Linux del laboratorio, accediendo remotamente según lo explicado en el apartado 3.1.
- ***route***. Permite ver y editar la tabla de rutas de los PCs de los alumnos con MS. Windows. La sintaxis del comando se puede obtener ejecutando "route" sin parámetros.
- ***ifconfig***. Para utilizar el comando *ifconfig* en los equipos Linux del laboratorio desde la cuenta "alumnos" (ver apartado 3.1) hay que ejecutarlo como "/sbin/ifconfig". También se puede ver el resultado de este comando dentro del archivo "**ifconfig.txt**" que hay en la cuenta "alumnos" de cada Linux. Esto se puede hacer accediendo remotamente al equipo Linux y ejecutando "**cat ifconfig.txt**".

## 4. Documentación complementaria

Para ampliar los conocimientos sobre los temas de esta práctica se pueden consultar las siguientes normativas, así como otros documentos, disponibles entre los materiales del Campus Virtual de "Sistemas de Transporte de Datos", en la carpeta "Documentos":

- RFC1721. Análisis de RIP 2.
- RFC2453. Descripción de RIP 2.
- RFC3022. Definición y aplicación de NAT.
- RFC 2281. Cisco Hot Standby Router Protocol (HSRP).

Se pueden consultar manuales de los monitores de red "Wireshark" y "tcpdump" en sus páginas Web:

- http://www.wireshark.org/
- http://www.tcpdump.org/

Además, en la carpeta de prácticas del Campus Virtual está disponible el documento "Tablas de encaminamiento" que resume los aspectos más importantes del encaminamiento estático de IPv4, y los comandos para configurar tablas de encaminamiento.

## 5. Estructura de la red del laboratorio

La **Figura 6** muestra la estructura de redes del laboratorio L24, sobre la cual se plantean las cuestiones a realizar en esta práctica. Se trata de la misma estructura que la usada en la asignatura de Redes, pero con nuevas configuraciones en los routers para permitir experimentar los temas tratados en Sistemas de Transporte de Datos. Esta estructura está compuesta de diferentes segmentos de red que utilizan diferentes niveles de enlace, y que están interconectados por varios equipos de interconexión: tres routers de la marca Cisco (modelos 2513, 1720 y 1601), cuatro PC funcionando con SO Linux (Linux 1 a Linux 4) funcionando también como routers, y finalmente el router propio del edificio de la Escuela (Router EPS). Además, existen varios conmutadores y hubs que interconectan los equipos de las redes Ethernet.

En la red del laboratorio coexisten diversos tipos de medios físicos y niveles de enlace: tres enlaces serie V.35 (entre los routers Cisco) o RS-232 (entre los routers 2513 y el Linux 1), los tres con protocolo de enlace PPP, dos redes locales Ethernet basadas en hubs y conmutadores, una red local en anillo Token Ring de 16Mbps (IEEE 802.5), y una red WiFi (802.11b/g). Para todas estas redes, se utiliza el protocolo de red IP como protocolo de interconexión, y los routers encaminan paquetes de este protocolo. Para ello, a cada segmento de la red con un nivel de enlace diferente se le ha asignado una subred IP. Sobre IP se usan el resto de protocolos de la arquitectura TCP/IP.

El esquema muestra para cada interfaz de red de cada equipo su dirección IP, y el nombre del interfaz que utiliza su SO. Además también se indican las direcciones de enlace (MAC) para los distintos routers de la red Ethernet 172.20.43.192, a la que se conectan los PC del laboratorio desde donde se realizarán los experimentos.

Por defecto, al iniciarse el PC del laboratorio que el alumno debe utilizar, este se configura para usar como puerta de enlace el Router EPS (172.20.43.195), con lo que el tráfico hacia otras redes es encaminado por ese router. Para realizar los experimentos de las

prácticas, el alumno cambiar primero la puerta de enlace por defecto del PC usado a la dirección 172.20.43.230, que se corresponde con el Router 1720. De esta forma el tráfico hacia el exterior se encamina por los equipos del laboratorio. Esto se puede hacer fácilmente ejecutando el archivo de comandos "C:\pracredes.bat" del PC.

Cuando los paquetes se encaminan por la red del laboratorio, el tráfico dirigido a subredes que no están presentes en la estructura de red local, se encamina hacia la red de la universidad y hacia Internet a través del router 2513, que está conectado a la red de la Escuela. Los demás routers del laboratorio encaminan por defecto los paquetes hacia redes que no conocen hacia el router 2513, a través de diferentes caminos.

Finalmente, cabe comentar que los equipos Linux2 y Linux3 actúan como servidores ofreciendo diferentes servicios de TCP/IP (Web, Telnet, FTP, SSH…) a otros equipos del laboratorio y también algunos servicios a equipos externos a través del router 2513.

# 6. Experimentos

La puerta de enlace por defecto para los PCs del laboratorio es 172.20.43.195, un router de la EPS (ver **Figura 6**). Antes de resolver las cuestiones siguientes, hay que ejecutar el script "C:/pracredes.bat" del PC, para cambiar la puerta de enlace a la dirección 172.20.43.230 (router Cisco 1720), de forma que se puedan alcanzar las diferentes redes del laboratorio.

## 6.1. Cuestiones sobre NAT

- Examina la configuración de NAT de los routers del laboratorio. ¿Qué routers tienen NAT activado? Desde el punto de vista cada router que tenga NAT activado, ¿Qué redes son internas y cuales externas?
- Examina la configuración de NAT del router Cisco 2513. ¿A qué paquetes se aplica una traducción de direcciones internas? ¿Qué entradas estáticas de traducción de direcciones internas tiene definidas ese router y a qué protocolos y servicios (puertos) se aplican? ¿Cuántas IP externas tiene asignadas el router Cisco2513? Esas direcciones externas, ¿son direcciones públicas de Internet o privadas?
- Utiliza un navegador Web para acceder a la dirección "http://www.aurova2.ua.es/std" y analiza a que equipos pertenecen las direcciones IP mostradas en la página Web. Después examina la tabla de traducciones NAT para buscar la entrada correspondiente a la traducción los paquetes intercambiados entre tu PC y el servidor. Compara las direcciones y puertos que ve el servidor Web con las direcciones y puertos en la red 172.20.43.192/26. El objetivo es ver la traducción interna realizada por NAT en el router Cisco 2513 en la salida a Internet.
- Accede a otros servidores externos, como por ejemplo al portal de Google ("http://www.google.es") y busca las traducciones correspondientes en la tabla de NAT para examinar la dirección y puerto del cliente que ve el servidor.
- Accede a la dirección Web "http://172.20.41.233" (servidor Web en Linux 3) y analiza a que equipos pertenecen las direcciones IP mostradas en la página Web. Después examina la tabla de traducciones NAT para buscar la entrada correspondiente a la traducción los paquetes intercambiados entre tu PC y el servidor.

- Accede de nuevo a la dirección "http://172.20.41.233", mientras ejecutas el monitor de red *tcpdump* remotamente en el equipo Linux 3 para capturar los paquetes del interfaz de la red Token Ring (tr0). Para la captura. Analiza la captura y busca los paquetes que has enviado y recibido del servidor web, teniendo en cuenta las IPs y puertos vistos en la tabla de NAT.
- Accede con el navegador Web a las URLs "http://193.145.233.8" y "http://172.25.32.98". Accede después a las URLs "http://10.8.1.1" y "http://10.8.1.2". ¿Qué páginas Web puedes ver? ¿Qué tipo de traducción se está aplicando? ¿Cuál es la verdadera dirección IP del servidor en cada caso? Examina la tabla NAT después de los accesos para analizar la situación, y determina cuál es la traducción dinámica asociada a la conexión de tu equipo con los servidores de "http://10.8.1.1" y "http://10.8.1.2".
- Cambia la puerta de enlace por defecto de tu PC del laboratorio para acceder a Internet a través del router de la EPS, usando los siguientes comandos en una consola de MSDOS de Windows:

```
route delete 0.0.0.0
route add 0.0.0.0 mask 0.0.0.0 172.20.43.195
```

  Accede después a la dirección "http://172.25.40.91:8080" (servidor Web en Cisco 2513). Observa las direcciones y puertos mostrados en la página. Examina también la tabla de traducciones NAT del router Cisco 2513 buscando la traducción realizada. ¿A qué servidor web estás accediendo? ¿Qué camino crees que siguen los paquetes intercambiados entre su equipo y el servidor Web?
- Prueba de nuevo a acceder a la dirección "http://172.25.40.91:8080" mientras usas *tcpdump* en el Linux 3 para capturar los paquetes que intercambia tu equipo con el servidor Web. Presta atención al escoger la interfaz adecuada para la captura con *tcpdump*.
- No olvides volver a ejecutar "C:/pracredes.bat" antes de continuar.

## 6.2. Cuestiones sobre encaminamiento dinámico

- Analiza la configuración de las tablas de encaminamiento de los distintos routers y equipos Linux para conocer que caminos siguen los paquetes dirigidos a las distintas redes del laboratorio.
- Realiza una captura (de al menos 30 segundos) con el monitor de red para localizar mensajes RIP 2 en la red 172.20.43.192/26. Averigua de quien proceden los mensajes RIP capturados e interpreta la información sobre rutas que transportan, examinando las direcciones IP, las máscaras y números de saltos de las rutas.
- Determina que routers utilizan la información de RIP para actualizar sus tablas.
- ¿Concuerda toda la información sobre rutas que transportan los mensajes RIP con la que hay en las tablas de encaminamiento de los routers?
- ¿Envía mensajes RIP el router Cisco 2513? Captura alguno de esos mensajes.
- Examina la expresión con la que EIGRP calcula la métrica de un camino o ruta. Cuando un router determina que la métrica de un camino A es menor que la métrica de otro camino B, ¿Cuál de los dos caminos es mejor?

- Averigua si está funcionando el protocolo EIGRP en la red. ¿Qué mensajes de EIGRP se pueden capturar? ¿Quién los envía?
- Busca los mensajes de EIGRP que informan de los parámetros $K_i$ que utilizan los routers para el cálculo de las métricas. ¿Qué clase de mensajes son? ¿Qué variables usan los routers Cisco 1701 y 1601 para calcular las métricas de EIGRP?
- ¿A qué direcciones IP y MAC van destinados los mensajes RIP e EIGRP?
- Determina los valores de Delay y BW de los interfaces de los routers Cisco del laboratorio, y calcula las métricas de los siguientes caminos: a) "172.20.43.230 - 172.20.43.231", b) "10.4.2.6 - 10.4.2.5 - 10.4.2.1", c) "10.4.2.6 - 10.4.2.5 - 172.20.41.233" ¿Qué caminos tienen la peor y la mejor métrica?

### 6.3. Cuestiones sobre HSRP

- Ejecuta el monitor de red para capturar mensajes HSRP en la red 172.20.43.192/26 y analiza esos mensajes. ¿Qué tipos de mensajes HSRP se pueden ver en esa red? ¿Qué direcciones origen y destino, MAC e IP tienen esos mensajes? ¿Qué routers los envían?
- Según el contenido de los mensajes HSRP, ¿Qué router del laboratorio es el activo? ¿Qué routers están en espera? ¿Qué tiempos de saludo y de retención tienen configurados cada router? ¿Qué prioridad tiene cada router? ¿Cuál es la dirección del IP router virtual?
- Cambia la puerta de enlace por defecto del PC que estás usando a la dirección IP del "router virtual". Puedes hacerlo fácilmente con los comandos "route detele 0.0.0.0" y "route add 0.0.0.0 mask 0.0.0.0 <Puerta_de_enlace>" ejecutados en la consola de comandos. Captura los paquetes que se generan cuando accedes a una página Web. ¿Cuál es la dirección MAC destino de los paquetes que envía tu equipo? ¿A quién pertenece esa dirección MAC?
- Manteniendo la puerta de enlace del ejerció anterior, si el enlace PPP 10.4.2.4/30 fallase, ¿Podría tu equipo acceder a Internet? ¿Por dónde? ¿Qué camino seguirían los paquetes de ida y de vuelta a un servidor web de Internet?

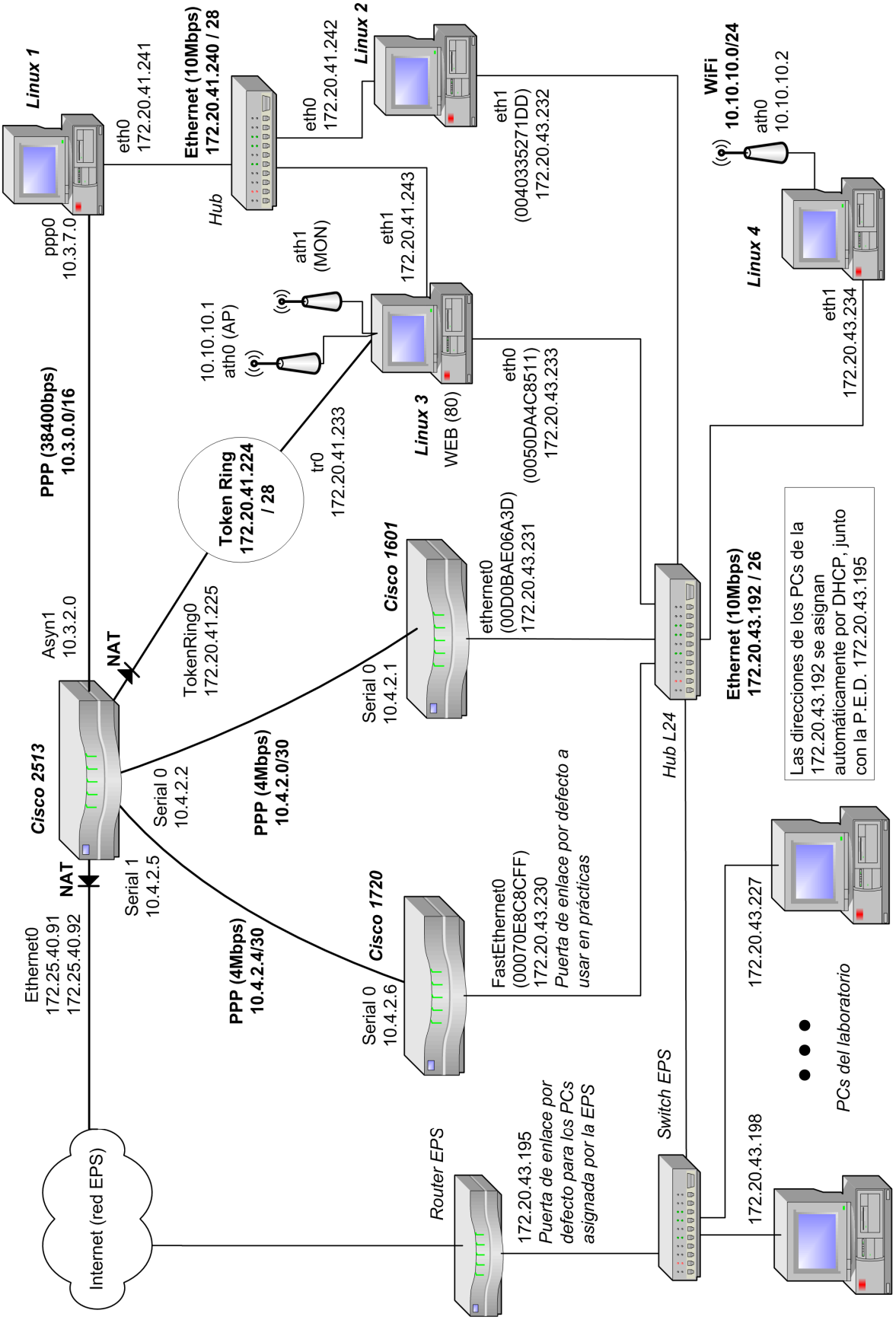


**Figura 6**. Estructura de la red del laboratorio.