Redes

Ingeniería Informática (9185)

Manual de la Práctica 4:

Direccionamiento y encaminamiento con IPv4

Francisco Andrés Candelas Herías

Jorge Pomares Baeza

Grupo de **I**nnovación **E**ducativa en **A**utomática

Universitat d'Alacant
Universidad de Alicante

1. Objetivos

- 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 asignar las direcciones IPv4 a los equipos de una red, y a configurar las entradas de las tablas de encaminamiento de los *routers*.

2. Conocimientos básicos de encaminamiento estático con IPv4

2.1. Encaminamiento en un equipo con el protocolo IP

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.

Un *router* 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. La Figura 1 resume estos pasos.

A. *¿La dirección IP destino pertenece a una interfaz de red de está 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 interfaz *loopback* interno a nivel IP. Un interfaz *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 está 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 otras interfaces en las redes conectadas directamente al equipo. Estas últimas direcciones IP son denominadas *gateways* o **puertas de enlace**, y permiten acceder a los destinos fuera de las redes conectadas directamente.

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

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

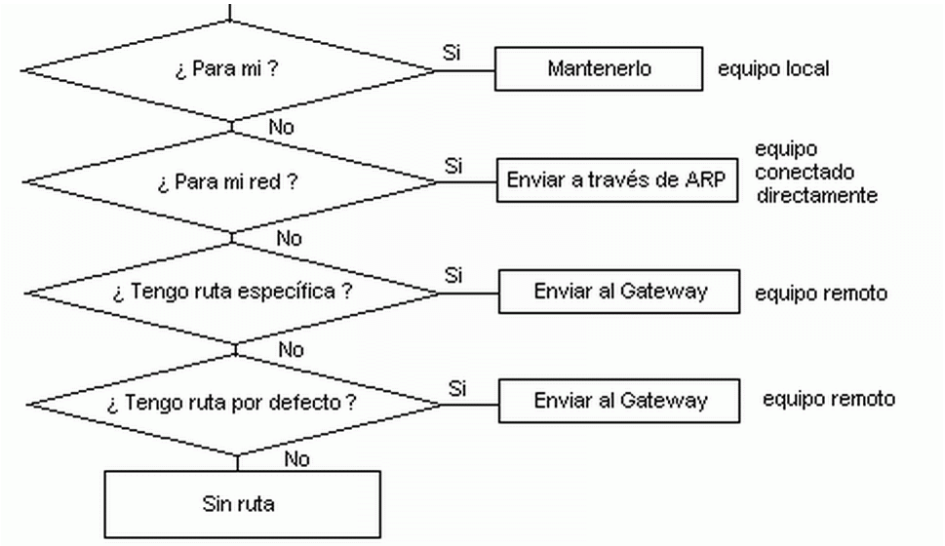

Figura 1

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 de la puerta de enlace por defecto al que se envían los paquetes que no van dirigidos a la propia red local.

También cabe destacar que no es obligatorio configurar la dirección IP de la puerta de enlace por defecto. Si no se configura esta entrada, el equipo sólo será capaz de reenviar paquetes IP destinados a redes conectadas directamente a él, u a otros destinos cuya puerta de enlace se haya definido explícitamente.

2.2. 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 destino_2 …	máscara_1 máscara_2 …	gateway_1 gateway_2 …

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
```

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.

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 el siguiente:

```
Kernel IP routing table
Destination   Gateway    Genmask         Flags   MSS Window  irtt Iface
10.6.7.1      10.6.7.0   255.255.255.255 UGH     296 0          0 ppp0
10.1.0.0      0.0.0.0    255.255.0.0     U      1500 0          0 eth0
10.6.0.0      0.0.0.0    255.255.0.0     U       296 0          0 ppp0
127.0.0.0     0.0.0.0    255.0.0.0       U      3584 0          0 lo
0.0.0.0       10.1.2.0   0.0.0.0         UG     1500 0          0 eth0
```

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 10.6.7.1. La búsqueda tendrá éxito en la primera entrada y el datagrama será enviado por la interfaz física local "ppp0" que tiene dirección 10.6.7.0. 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 10.1.0.0 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 10.6.0.0 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 10.1.2.0 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...) 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   172.20.43.228  1
    172.20.43.192  255.255.255.192     172.20.43.228   172.20.43.228  1
    172.20.43.228  255.255.255.255         127.0.0.1   127.0.0.1      1
    172.20.43.255  255.255.255.255     172.20.43.228   172.20.43.228  1
        224.0.0.0        224.0.0.0     172.20.43.228   172.20.43.228  1
  255.255.255.255  255.255.255.255     172.20.43.228   0.0.0.0        1
        127.0.0.0        255.0.0.0         127.0.0.1   127.0.0.1      1
```

En este caso la tabla muestra que el equipo tiene como puerta de enlace por defecto (destino 0.0.0.0) la dirección IP 172.20.43.230, y que está conectado directamente a la red 172.20.43.192/26 por su interfaz de red con IP 172.20.43.228. Además las tablas de MS. Windows indican otros destinos evidentes sin mayor relevancia que parecen complicar la tabla: los paquetes dirigidos a la IP propia (172.20.43.228) se deben enviar por el interfaz de *loopback*, la dirección de *broadcast* de su red (172.20.43.255) se alcanza por su propia interfaz 172.20.43.228, la direcciones de *multicast* y *broadcast* global también se alcanzar por su propia interfaz 172.20.43.228, y a la red de *loopbacks* se accede por su propia dirección de *loopback*. La metrica indica el número de redes a atravesar para llegar al destino.

Cabe destacar que, mientras en un equipo Linux-Unix las entradas correspondientes a destinos o redes conectados directamente se identifican con la puerta de enlace 0.0.0.0 (ya que no hace falta puerta de enlace), en los equipos MS. Windows estas entradas se identifican

porque tienen como puerta de enlace la dirección IP del interfaz de red de la propia máquina por donde deben salir los paquetes.

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

2.3. Información sobre los interfaces de red

En sistemas Unix, se puede utilizar para ver o modificar la configuración de cada interfaz el comando "ifconfig <nombre de la interfaz>". Para ello se necesitan privilegios de *root*. Si quisiéramos saber las características de la tarjeta de red Ethernet del equipo Linux de ejemplos los anteriores ejecutaríamos "ifconfig eth0", obteniendo una respuesta similar a esta:

```
eth0    Link encap:Ethernet  HWaddr 00:40:33:52:71:C8
        inet addr:10.1.7.0  Bcast:10.1.255.255  Mask:255.255.0.0
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:195116 errors:0 dropped:0 overruns:0 frame:0
        TX packets:38492 errors:0 dropped:0 overruns:0 carrier:0
        Collisions:2
        Interrupt:10 Base address:0x300
```

Como información interesante puede observarse que la interfaz se encuentra en servicio (UP), admite dirección de *broadcast*, su dirección IP correspondiente es 10.1.7.0 y existe una máscara que define una subred de 8 bits con una porción de máquina de 16 bits. Además, se indica el tamaño máximo de datos de la trama de enlace (MTU), cuentas sobre los datos enviados y recibidos, etc.

El comando "ifconfig" no sólo permite observar las configuraciones de un sistema Unix (o Linux) sino también cambiarlas. Además de la dirección IP y la máscara, es posible cambiar parámetros como la dirección de *broadcast* o el MTU del interfaz. Se puede consultar el manual del sistema para obtener información sobre el comando ("man ifconfig"). Por ejemplo, el siguiente comando cambia la dirección IP y la máscara de red del interfaz "eth0" a los valores 10.1.106.1 y 255.255.0.0 respectivamente:

```
ifconfig eth0 10.1.106.1 netmask 255.255.0.0 broadcast 10.1.255.255
```

También se pude usar "ifconfig" para activar nuevas interfaces de red. Por ejemplo, para crear la interfaz de *loopback* en una máquina que no la tiene:

```
ifconfig lo 127.0.0.1
```

En los sistemas MS. Windows se puede ver y modificar las características de los interfaces de red a través del Panel de Control, o con la opción Propiedades del menú que emerge al pulsar el botón derecho sobre el Icono de Red en el escritorio de Windows XP. También se puede ver el estado de las interfaces de red ejecutando el comando "ipconfig –all" en la consola de comandos. En MS. Windows los interfaces no tienen nombres específicos tipo "eth0", y se identifican por su IP o por un número de orden o índice. Además, todas interfaces quedan reflejadas en la tabla de encaminamiento como se muestra en el apartado anterior.

2.4. 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 es:

```
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 10.6.7.0 MASK 255.255.255.0 10.1.7.0" añade una entrada de ruta para poder alcanzar la red 10.6.7.0 a través de la puerta de enlace local 10.1.7.0.

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 10.1.2.1 se puede ejecutar:

```
route del default
route add default gw 10.1.2.1
```

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 192.168.10.0/24 a través de la puerta 10.1.2.0 (que debe ser alcanzable a partir de otras entradas existentes), habría que ejecutar:

```
route add -net 192.168.10.0 gw 10.1.2.0 netmask 255.255.255.0
```

3. Herramientas disponibles para realizar la práctica

3.1. Acceso a otros equipos del laboratorio

Se puede acceder a los equipos **Linux 1, Linux 2** y **Linux 3** del laboratorio (172.20.41.241, 172.20.43.232 y 172.20.43.233) 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**" con la contraseña "**alumnos**".

- 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", que permite acceder al servicio SSH (Secure Shell). 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. Con ambos programas se pude 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. 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 [filto]
  ```

  El programa "putty" es libre y se puede descargar desde:

  http://www.chiark.greenend.org.uk/~sgtatham/putty/

- Se puede usar un cliente FTP para recuperar el archivo con una captura de tcpdump realizada en otro equipo. En una ventana de MS-DOS, 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.

3.2. Configuración de los routers Cisco del laboratorio

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

```
redesprac <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*. El comando "**conf**" muestra la configuración completa.
- **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 el 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.

Ejecutando el comando "redesprac" sin parámetros se obtiene un listado completo de las opciones y parámetros del comando.

3.3. Herramientas de red TCP/IP

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

- **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 1, 2 y 3, 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.
- **ping**. Se puede usar tanto en el PC del alumno como en los Linux 1, 2 y 3. La sintaxis cambia entre Linux y MS. Windows.
- **ifconfig**. Para ver cual es la configuración de los interfaces en los equipos Linux 1, 2 y 3 se habrá de ejecutar el siguiente comando: "/sbin/ifconfig".
- **traceroute**. Se puede ejecutar el comando "**tracert –d <IP>**" en MS. Windows en el PC del alumno para obtener la lista de *routers* intermedios hasta alcanzar la dirección IP especificada. El parámetro –d indica que se muestren las direcciones de forma numérica. En los Linux 1 y 2 se puede ejecutar el comando equivalente como "**traceroute –n IP**"

3.4. Simulador de encaminamiento KivaNT

En la página Web "http://www.aurova.ua.es/kiva" hay disponible un simulador de encaminamiento IP sobre redes Ethernet y routers, que pude ser utilizado para ejercitar el diseño de tablas de encaminamiento. El simulador es una aplicación Java que se descarga y ejecuta localmente. Para ello se requiere tener instalado el JRE de Java. La aplicación permite dibujar esquemas de redes, con equipos, routers y diferentes tipos de redes (aunque solo se puede simular las redes Ethernet), configurar las tablas de encaminamiento y simular el envío de datos con ICMP-echo entre equipos. Con la simulación se muestra una traza de las tramas ARP y los paquetes IP que se han desencadenado en las redes.

4. Información complementaria

4.1. Introducción al nivel de enlace de una LAN Token-Ring

Se ha incluido ente las redes del laboratorio una LAN Token-Ring (testigo-anillo), en la que se pueden capturar tramas desde el Linux3. Este tipo de LAN, normalizada como o IEEE 802.5, define un método de control de acceso (MAC: *Media Access Control*) por paso de testigo en una red con topología en anillo, muy diferente al usado por Ethnernet. El "paso de testigo" se basa en una trama especial conocida como testigo, que da permiso de transmisión al equipo receptor. En estado de reposo, el testigo circula de un equipo al siguiente en la red cuya topología es en anillo, dando vueltas continuamente. Cuando un equipo desea enviar tramas de datos, debe esperar antes a recibir el testigo.

Una vez realizada la transmisión de la trama de datos, esta circula por el anillo de un equipo al siguiente, cada equipo del anillo retransmite la trama, hasta llegar al equipo destino, si existe, que lee los datos, y luego la trama continúa hasta que retorna a la estación emisora, que es la encargada de retirarla, y así evitar que esté permanentemente circulando por el anillo. Ese retorno de la trama de datos también se aprovecha para realizar una confirmación a nivel de enlace a la estación emisora.

4.2. Formato de trama MAC de Token-RIng

En esta normativa se definen dos formatos, uno para la trama asociada al testigo, y otro para la trama de transmisión de datos. Como se ha comentado, la primera habilita el permiso de transmisión al equipo que en ese momento lo tiene en posesión, mientras que la segunda permite enviar datos desde un equipo a otro.

En la Figura 2 se puede apreciar el formato de la trama de datos. Los campos delimitadores de comienzo y de final tienen la función de que la estación receptora pueda determinar los límites de la trama sin necesidad de un campo que indique su longitud. Por lo tanto, se añaden un total de 21 bytes de información de nivel MAC.

1 byte	1 byte	1 byte	2 o 6 bytes	2 o 6 bytes	hasta 5000 bytes de MTU	4 bytes	1 byte	1 byte
Delimitador Comienzo	Control de Acceso	Control de Trama	Dirección Destino	Dirección Origen	Información	FCS	Delimitador Final	Estado de Trama

Figura 2

Los bits del campo de Control de Acceso permiten indicar la prioridad de los. El campo de Control de Trama indica el tipo de trama (trama de gestión MAC o trama de información) y algunas funciones de control. Una trama de gestión MAC es interpretada por todas las tarjetas de la red, y es utilizada sólo por el nivel de enlace para funciones propias, mientras que una de información contiene datos de niveles superiores, y sólo la interpretan aquellas tarjetas a las que va destinada la información. Por último, el campo de Estado de Trama contiene dos bits que se utilizan para confirmar la recepción correcta de tramas.

Cabe destacar que, si se capturan tramas de Token Ring con un programa monitor como Wireshark o tcpdump, solo se verán los campos presentes entre los delimitadores, ya que los otros son tratados a bajo nivel. Además, al realizar una captura se observará como, además de las tramas de información generadas por niveles superiores, por ejemplo tras ejecutar un comando "ping", en la red circulan muchas otras tramas de gestión MAC. Un ejemplo puede

ser una trama de gestión MAC tipo SMP (Standby Monitor Present) que indica que un equipo se ha dado de alta en la red.

4.3. Nivel LLC en una LAN

El nivel LLC (Logical Link Control, control lógico del enlace) está definido en la norma IEEE 802.2 como un subnivel del nivel de enlace que completa al MAC. Es independiente del medio físico y de la topología de la red, y su misión principal es ofrecer unos servicios generales al nivel superior (red) con total independencia del MAC y de la topología empleados. También puede gestionar el control de flujo en la red con un protocolo de ventana deslizante de envío continuo derivado de HDLC, aunque no se suele usar en LAN. El LLC define un formato de trama propio, que incluye unos valores conocidos como SAP (Punto de Acceso de Servicio), que tienen una función similar a los puertos del protocolo TCP. La cabecera típica de LLC presenta un total de 8 bytes.

Al contrario que ocurre con las LANs Ethernet, en las que no se requiere utilizar el subnivel LLC para enviar datagramas IP, con las redes LAN Token Ring si que se necesita este subnivel. Así, en una red Token Ring, cuando se envía un datagrama IP, este se encapsula sobre una trama LLC, que a su vez se encapsula como en una trama MAC de información.

5. Cuestiones a realizar

5.1. Ejercicio sobre configuración de encaminamiento IP

– Para la estructura de red privada de la Figura 2, trata de definir las subredes IP necesarias, asigna las direcciones IP de los interfaces de red, determina las puertas de enlace por defecto de los PCs de usuario y configura las tablas de encaminamiento de los *routers*, de forma que se eviten los mensajes de redirección cuando se accede a Internet. Para las direcciones internas se ha escogido la dirección 193.162.130.0. Para las tablas de los *routers* se requiere configurar, para cada entrada, la IP destino, su máscara, su puerta de enlace y el número de saltos mínimo.

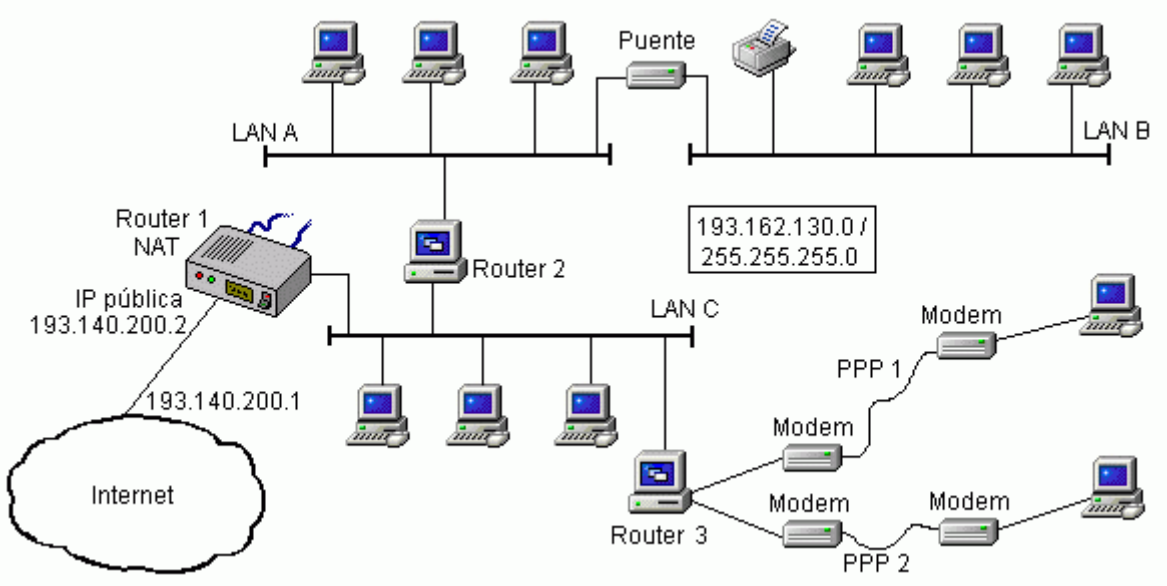

Figura 2

– Después, supón que se quita el puente para aislar los segmentos LAN A y LAN B, y se conecta la LAN B al Router 2 mediante una nueva interfaz de red situada en este último equipo. Trata de reasignar las direcciones de la red, evitando modificaciones fuera de las redes LAN A, LAN B y del Router 2.

5.2. Ejercicios sobre encaminamiento IP en el laboratorio

Antes de tratar de analizar la red del laboratorio, asegúrate de que has ejecutado el script "C:\pracredes.bat" de tu equipo en el laboratorio.

– Analiza la configuración de las tablas de encaminamiento de distintos equipos de la red (PC del alumno, Linux 1, Linux 2, Linux 3 y los tres *routers*) con las herramientas descritas en el apartado 3.

– Intenta dibujar la red del laboratorio a partir de la información de las tablas obtenida antes, y compara el resultado con el esquema de la red del laboratorio utilizado desde la práctica 1.

– ¿Qué equipo está conectado a la red 10.5.2.0/24? ¿Qué tipo de interfaz conecta el equipo a esa red?

– Si ejecutas el comando "ping 172.20.41.241" en tu equipo del laboratorio, ¿Qué camino siguen y cuantas redes atraviesan los paquetes de "echo request"? ¿Y los de "echo reply"?

– ¿Cómo puedes modificar la tabla de encaminamiento de tu equipo para hacer más corto el camino de los paquetes IP que parten de tu equipo hacia un destino situado en la red 172.20.41.240/28? Comprueba si la modificación tiene éxito o no usando el comando "tracert" **varias veces**.

– 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 10.4.2.1. Después ejecuta el comando "tracert –d 10.4.2.1" desde tu equipo y examina el resultado. Averigua también que camino siguen los paquetes de respuesta desde la IP 10.4.2.1 hacia tu equipo.

– Si ejecutas el comando "ping 10.10.10.2" en tu equipo del laboratorio. ¿Qué camino siguen y cuantas redes atraviesan los paquetes de "echo request"? ¿Y los de "echo reply"?

– Intenta modificar la tabla de encaminamiento de tu PC del laboratorio para alcanzar las direcciones de la red 10.3.0.0/16 pasando por el equipo Linux 2, la red 172.20.41.240/28 y por el Linux 1, en vez de hacerlo por los routers Cisco. Comprueba si la modificación tiene éxito o no usando el comando "tracert" varias veces, y determina el porqué.

– 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 puerta de enlace por defecto alternativa a la 172.20.43.230 en tu equipo: Linux 2, Linux 3 o Cisco 1720? ¿Qué comandos debes ejecutar en tu equipo para ello? No olvides restaurar la puerta de enlace por defecto a 172.20.43.230 al acabar esta cuestión.

– 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 apartado anterior?

- ¿Qué ocurre cuando se ejecuta en el PC del alumno con MS. Windows el comando "tracert –d" a una dirección IP de la red 10.3.0.0/16 que no sea la 10.3.2.0 ni la 10.3.7.0? ¿Qué camino sigue el paquete? Justifica la respuesta analizando como se realiza el encaminamiento a esas direcciones. ¿Qué entradas de encaminamiento de los routers del laboratorio sería conveniente eliminar para evitar ese encaminamiento?
- ¿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"?
- A través de Linux 3 y empleando los comandos adecuados trata de capturar tramas Token Ring. Analiza el formato de estas tramas.
- Determinar experimentalmente el retardo en la red Token Ring del laboratorio empleando el comando ping. Teniendo en cuenta la longitud de las cabeceras MAC y LLC, calcular la velocidad de transmisión y la cadencia eficaz para TCP y UDP en esa red.