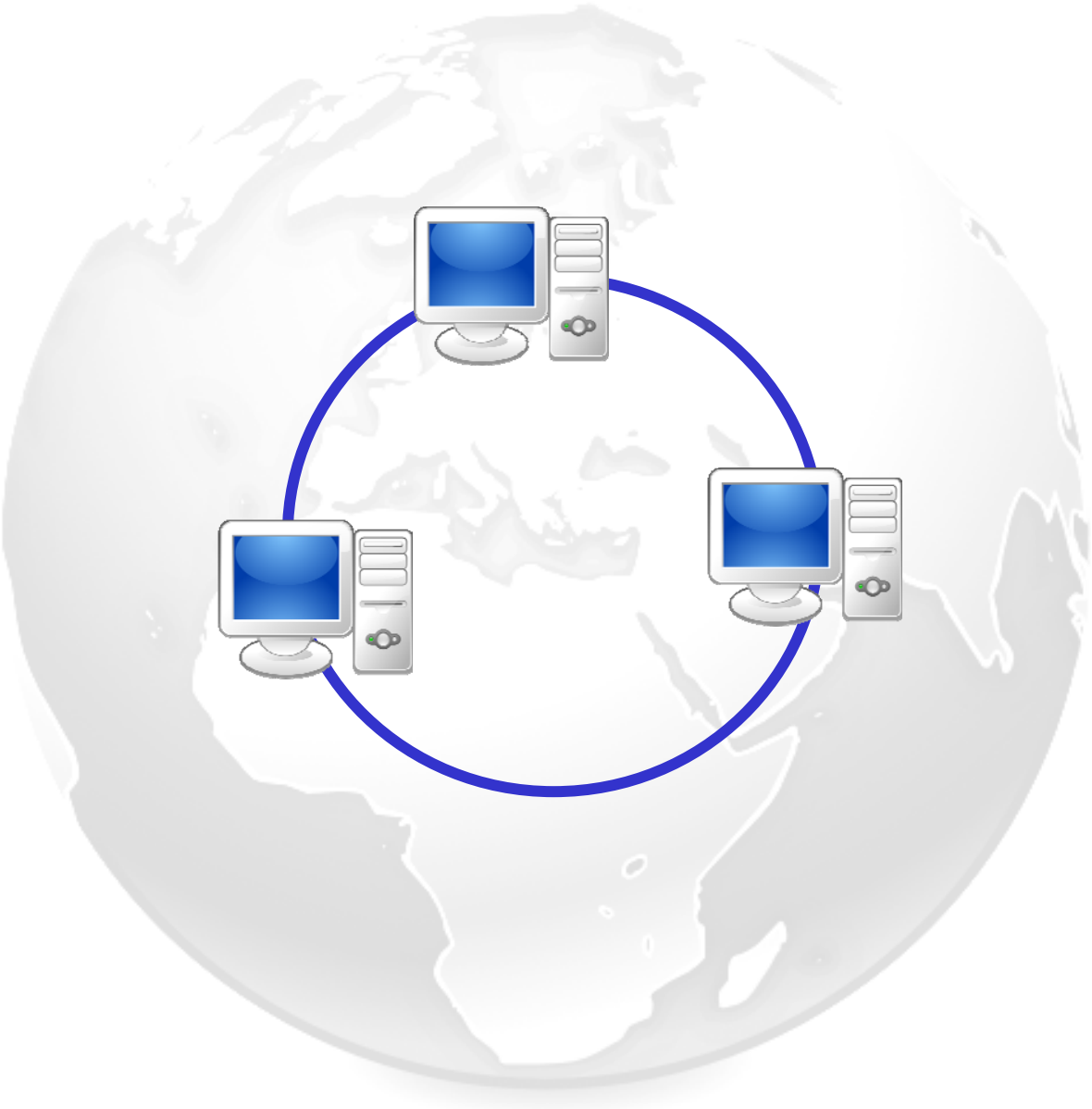


MANUAL DE PRÁCTICAS DE LABORATORIO

J. MUÑOZ

Departamento de Electrónica, Automática e Informática Industrial.
Escuela Universitaria de Ingeniería Técnica Industrial.
Ronda de Valencia, 3.
28012 Madrid.

ISBN-13: 978-84-691-4608-8

TABLA DE CONTENIDOS

1. INTRODUCCIÓN

1.1 Sobre este manual

Este manual contiene un conjunto de prácticas de laboratorio que sirven como guía para el estudio de los protocolos TCP/IP que se utilizan en Redes de Computadores como Internet. El manual está estructurado en cuatro prácticas. Cada práctica contiene una introducción teórica y un guión con ejercicios. De forma resumida, el contenido de cada práctica es el siguiente:

Práctica 1: Red de Área Local (LAN)

Esta práctica repasa conceptos fundamentales de TCP/IP y enseña cómo se configura en Linux la tarjeta de red para crear una red de área local (LAN). También se introducen algunos comandos básicos como ifconfig o ping, se analiza cuál es el papel del protocolo ARP en la resolución de direcciones y se muestra la utilidad de aplicaciones como SSH (Secure Shell) o FTP (File Transfer Protocol).

Práctica 2: Análisis de protocolos

En esta práctica se realizan ejercicios muy similares a los de la práctica anterior pero observando lo que ocurre desde un punto de vista diferente, ya que se captura y se analiza el tráfico de datos que circula por la red. Para ello, se aprende a manejar como usuario el analizador de protocolos de red denominado Wireshark. El análisis del tráfico capturado permite estudiar cómo funcionan los protocolos, cómo se encapsulan los datos transmitidos o cuáles son los problemas de seguridad más comunes de ciertas aplicaciones.

Práctica 3: Enrutamiento estático

En esta práctica se explican conceptos de enrutamiento IP y qué es y

para que sirve una tabla de rutas. Además, se realiza una introducción a los comandos del sistema operativo CISCO IOS, lo cuál servirá para configurar los routers y crear las tablas de rutas de forma manual.

Práctica 4: Enrutamiento dinámico

En práctica es análoga a la anterior, con la diferencia de que la tabla de rutas se configura utilizando enrutamiento dinámico. En particular, se analiza el funcionamiento del protocolo RIP (Router Information Protocol).

1.2 Requisitos hardware y software del Laboratorio

Las prácticas han sido diseñadas para un laboratorio compuesto por doce ordenadores, cuatro routers CISCO, tres switches Lynksys y cables de interconexión. Con estos equipos, el Laboratorio permite reproducir, en miniatura, desde una pequeña red de área local o LAN (Local Area Network) hasta una red de área amplia o WAN (Wide Area Network) como Internet, y simular diferentes escenarios de tráfico que están presentes en las redes reales.

El software necesario para los ordenadores del Laboratorio el Laboratorio se puede encontrar en cualquier distribución reciente de Linux, aunque aquí se utiliza la distribución Linux-Knoppix que se ejecuta directamente desde un CD y que contiene un conjunto de aplicaciones que son de utilidad en el Laboratorio, por ejemplo, el analizador de protocolos de red Wireshark. Los routers CISCO utilizan un sistema operativo propio denominado CISCO IOS que se ejecuta desde una línea de comandos similar a la de Linux. Las secciones siguientes describen más en detalle el hardware y el software utilizado en el Laboratorio.

1.3 Hardware del Laboratorio

Las prácticas están diseñadas para un Laboratorio compuesto por doce ordenadores con sistema operativo Linux-Knoppix, una maqueta formada por tres switches Linksys y cuatro routers CISCO 1601 R (Figura 1), y cables de interconexión.

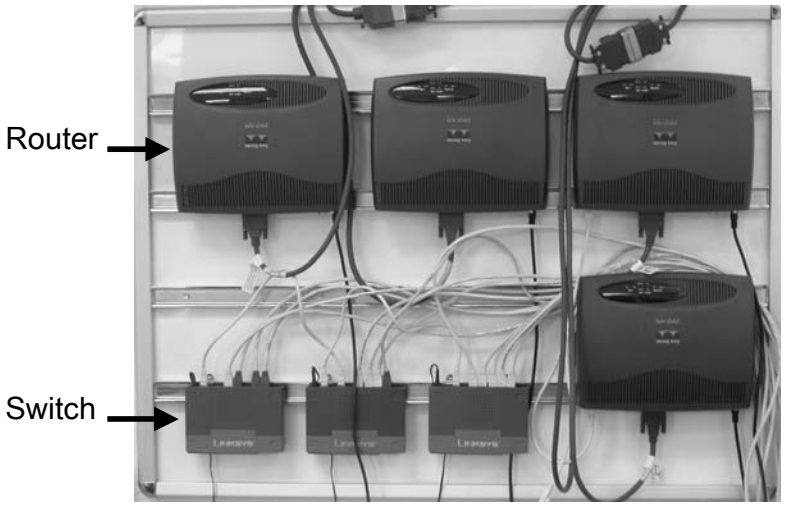


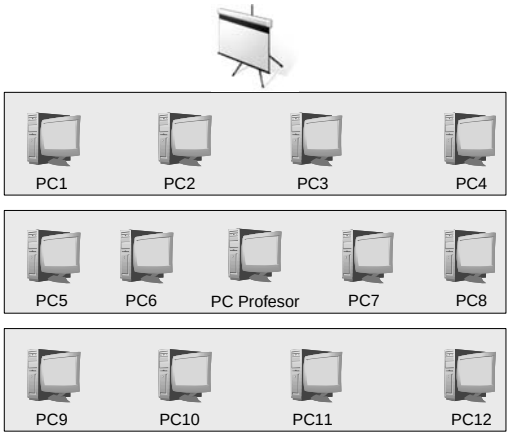
FIGURA 1. *Maqueta del laboratorio compuesta por tres switches y cuatro routers.*

1.3.1 Ordenadores

El Laboratorio dispone de doce ordenadores denominados PC1, PC2, …, PC12 distribuidos como se muestra en la Figura 2-a. Los ordenadores ejecutan el sistema operativo Linux-Knoppix y disponen de una tarjeta de red Ethernet 10/100 Mbps integrada en la placa base (Figura 2-b). Para guardar información durante las prácticas, cada ordenador dispone de una disquetera de 3 ½" y dos puertos USB.

En Linux, la interfaz Ethernet de la primera tarjeta de red se denomina *eth0*. Cada tarjeta de red está identificada, de forma única en el mundo, por una dirección de control de acceso al medio o MAC (Media Access Control Address) definida como un número hexadecimal de 48 bits escrito en hexadecimal. Por ejemplo, 00:0E:62:1D:AC:5B.

(a)



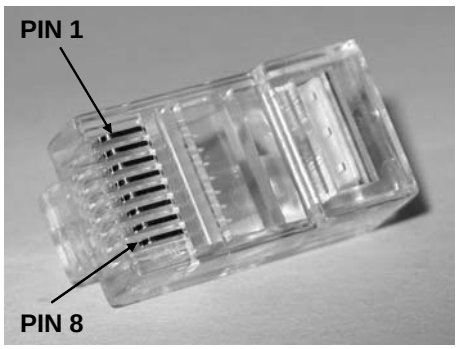
(b)

FIGURA 2. *(a) Distribución de los ordenadores en el laboratorio. (b) Tarjeta de red Ethernet integrada en la placa base.*

1.3.2 Cables de red

Las interfaces de red Ethernet se conectan entre sí con cables UTP (Unshielded Twisted Pair). Un cable UTP está formado por cuatro pares de cables trenzados no apantallados y terminado en cada extremo por un conector RJ-45 (Figura 3). A estos cables nos vamos a referir a partir de ahora como cables Ethernet.

(a)



(b)

FIGURA 3. *(a) Cable UTP. (b) Conector RJ-45.*

Los cables Ethernet pueden ser de dos tipos: cruzados o paralelos. La diferencia entre ambos tipos es la conexión entre los pines de los conectores RJ-45 de ambos extremos del cable. La Figura 4 muestra cómo se realizan las conexiones para cada tipo.

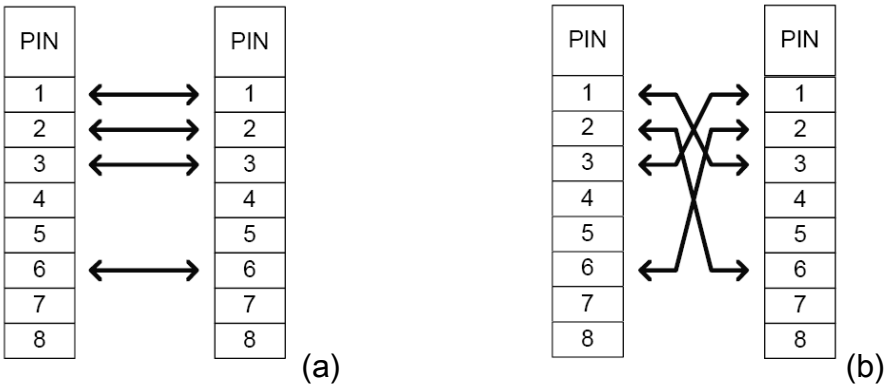


FIGURA 4. *Conexión entre los pines. (a) Cable paralelo. (b) Cable cruzado.*

En un cable paralelo, los pines 1, 2, 3 y 6 de un conector RJ-45 están conectados con los respectivos pines del conector RJ-45 del otro extremo del cable. En cambio, en un cable cruzado, los pines 1 y 3, y 2 y 6, están intercambiados en ambos extremos del cable. Es fácil confundir ambos tipos de cables porque externamente no hay ninguna diferencia. Una forma de distinguirlos consiste en poner los conectores RJ-45 uno al lado de otro y comparar los colores de los cables. Si los pines 1 de ambos cables son del mismo color, el cable es paralelo. En el laboratorio, para evitar confusiones, los cables cruzados están marcados con la letra C.

Los cables cruzados se utilizan, en general, para conectar directamente entre sí dos ordenadores, dos switches, o un ordenador con un router. Existe una excepción a esta regla en el caso de algunos switches, como los del Laboratorio, que tienen un puerto especial denominado “uplink”. Si se conecta el puerto “uplink” de un switch con un puerto normal de otro switch, se utiliza un cable paralelo.

Los cables paralelos se utilizan para conectar un ordenador o un router con un switch. La Figura 5 muestra algunas conexiones entre distintos equipo de la red y el tipo de cable correspondiente.

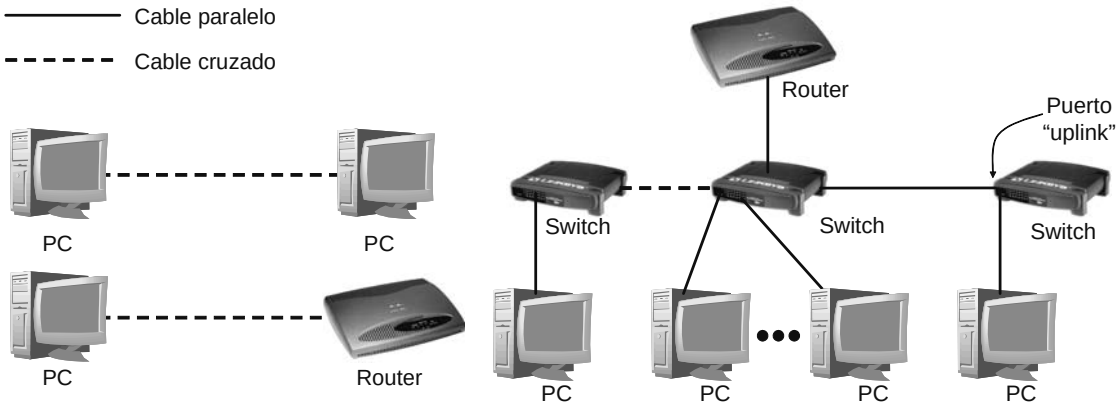


FIGURA 5. *Conexiones entre diferentes equipos de la red y tipos de cable utilizados.*

1.3.3 Switches

Un switch, o conmutador en castellano, es un dispositivo que permite interconectar varios equipos entre sí para crear una red. El Laboratorio dispone de tres switches CISCO Linksys 10/100 (Figura 6). Cada switch dispone de ocho puertos RJ-45. En cada puerto del switch se puede conectar un ordenador, un router u otro switch.

Para conectar dos switches entre sí, existe un puerto adicional denominado "uplink" que permite realizar esta conexión utilizando un cable paralelo en lugar de uno cruzado como se haría normalmente. El cable paralelo se conecta entre el puerto "uplink" de un switch y un puerto RJ-45 del otro (el uso del puerto "uplink" inhabilita automáticamente el puerto RJ-45 más cercano, de manera que el número de puertos útiles sigue siendo ocho).

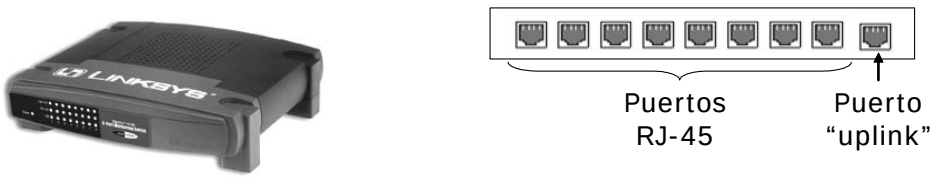


FIGURA 6. *Switch Cisco Linksys10/100 con 8-puertos RJ-45 más el puerto "uplink".*

Estos switches permiten una comunicación *full-dúplex*, es decir, se puede enviar y recibir información simultáneamente en todos sus puertos. En

otras palabras, cada equipo conectado al switch puede transmitir datos en cada instante a la máxima velocidad permitida. Por ejemplo, si hay cinco ordenadores conectados que tienen una tarjeta de red de 10 Mbps cada uno, la capacidad agregada de transmisión será de 50 Mbps.

Entre otras funciones, los switches pueden conocer y almacenar la dirección MAC de un equipo conectado en uno de sus puertos, por ejemplo, un ordenador. Esto permite, a diferencia de los *hubs*, o concentradores, que reenvian un paquete recibido por un puerto a todos los demás, que un paquete pueda ser enviado directamente desde el puerto de origen al de destino.

1.3.4 Routers

En una red de comunicación, los datos no se envían todos juntos, sino en grupos denominados paquetes lo que da lugar a un tipo de comunicación denominada “conmutación de paquetes”. En este tipo de comunicación cada paquete puede llegar a su destino por un camino diferente.

Un router, o encaminador en castellano, es un ordenador especializado que interconecta dos o más redes. Por tanto, al menos debe tener dos interfaces de red. El router se comporta básicamente como un repartidor, o conmutador, de paquetes: toma un paquete que le llega a través de una de sus interfaces de red y lo envía por una interfaz diferente.

FIGURA 7. *Router CISCO 1601 R.*

El Laboratorio dispone cuatro routers CISCO de la serie 1601 R (Figura 7) denominados en este manual como R1, R2, R3 y R4. Cada router tiene dos interfaces de red. La primera es una interfaz Ethernet con capa física 10BaseT

(velocidad de 10 Mbps) denominada ETHERNET0. La segunda es una interfaz serie de tipo WAN (Wide Area Network), denominada SERIAL0. La Figura 8 muestra el panel posterior de un router 1601 R en el que pueden verse ambas interfaces.

La interfaz ETHERNET0, situada a la izquierda, puede conectarse a través de conectores RJ-45 o AUI (Attachment Unit Interface) de 15 pines (Figura 9-a), aunque en el laboratorio sólo utilizaremos el primero para interconectar el router con los PCs del laboratorio a través de los switches con cables Ethernet de tipo paralelo (Figura 5, configuración de la derecha).

La interfaz WAN SERIAL0, situada a la derecha de la anterior, se conecta a través de un conector propio de CISCO de 60 pines (DB-60). Esta interfaz, que vamos a utilizar en el Laboratorio para conectar dos routers entre sí, es un puerto serie síncrono que permite operar en *full-dúplex* con velocidades de transmisión de hasta 2.048 Mbps. En lugar de Ethernet, el tráfico a través de la interfaz serie utiliza otros protocolos. Por ejemplo, SMDS (Switched Multi-megabit Data Services), X.21, o HDLC (High Level Data Link).

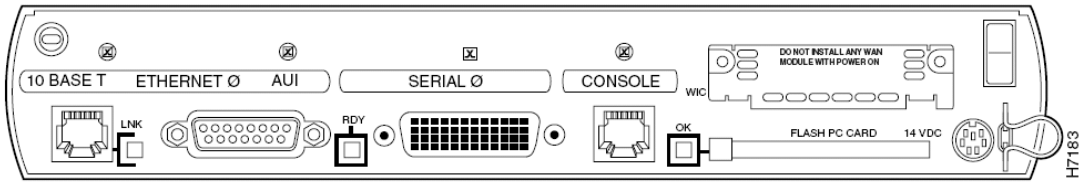


FIGURA 8. *Panel posterior de los routers CISCO 1601R*

El puerto denominado CONSOLE (consola), situado a la derecha del puerto serie) permite conectar el router con un ordenador dotado de un puerto serie RS-232 de 9 pines (DB-9) a través de un cable especial RJ-45 a DB-9 (Figura 9-b) que se suministra con los routers CISCO. El puerto de consola es un puerto serie asíncrono que permite enviar y recibir caracteres ASCII. A través de este puerto se puede configurar el router desde un ordenador ejecutando un programa de emulación de terminal, como *HyperTerminal* de Windows o *kermit* de Linux. El programa de emulación se encarga de enviar comandos al router y de mostrar la respuesta de éste en la pantalla del PC.

(a)

(b)

FIGURA 9. *(a) Conector AUI (DB-15). (b) Cable de consola (RJ-45 a DB-9.*

Las interfaces de red de los routers (direcciones IP, máscaras, etc.) del Laboratorio han sido configuradas desde un ordenador usando el puerto de consola. Sin embargo, en el Laboratorio no se va a utilizar este puerto para acceder a los routers, sino que se va a realizar la conexión a través de la red desde cualquier ordenador que tenga una dirección IP válida utilizando la aplicación Telnet (TELecommunication NETwork).

1.4 Software

1.4.1 Sistema operativo Linux-Knoppix

El sistema operativo que ejecutan los ordenadores del Laboratorio es Linux-Knoppix, una recopilación de software de GNU/Linux de libre distribución que se ejecuta directamente desde un CD (www.knoppix-es.org). Para aquéllos que no estén familiarizados con Linux o con Knoppix, este apartado proporciona una introducción básica a los comandos de consola más comunes así como al sistema de ventanas X-Window de Knoppix. X-Window es un protocolo que permite crear interfaces gráficas (ventanas) que se utilizan en la mayoría de los sistemas operativos basados en Linux, como Debian, KDE o Ubuntu. Cuando se arranca el sistema operativo, aparece un escritorio similar al que se muestra en la Figura 10. La consola de “root” (administrador) que aparece en el medio del escritorio puede abrirse seleccionándola en el Menú P (Programas y configuraciones específicas para Knoppix) que se despliega al pulsar sobre el icono del pingüino.

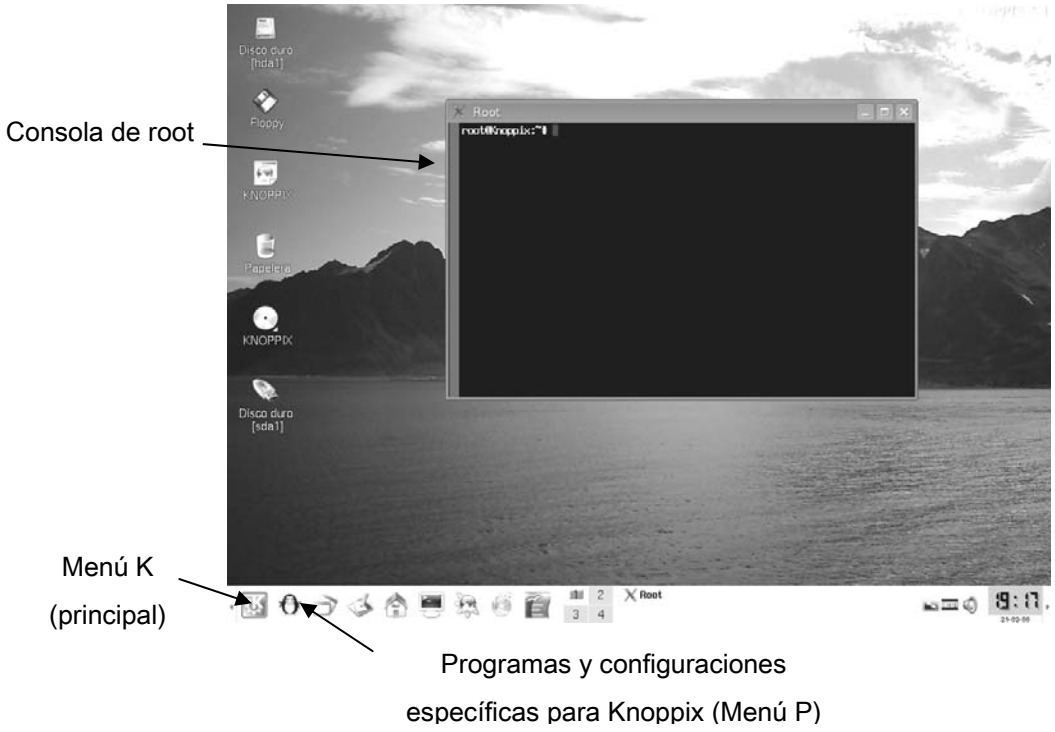


FIGURA 10. *Escritorio de Linux-Knoppix y consola de root.*

La consola de root concede al usuario privilegios de administrador, por ejemplo, para cambiar el nombre del equipo o configurar la tarjeta de red. La consola, también denominada shell, línea de comandos u órdenes, es un programa que interpreta y ejecuta comandos de Linux. El conjunto de caracteres que aparecen al comienzo de la línea de comandos se llama *prompt* e indica que se está a la espera de recibir comandos para ejecutarlos. Por ejemplo, en el caso de Linux-Knoppix, si no modificamos la configuración inicial del sistema operativo al abrir una consola de root aparece el siguiente *prompt*:

```
root@Knoppix:~#
```

El nombre que aparece antes de la arroba es el nombre del usuario (root) y el que aparece después es el nombre del equipo (Knoppix). En adelante, para facilitar la lectura, el *prompt* se ha omitido en la mayoría de los ejemplos.

1.4.2 Ejecución de comandos básicos en Linux

Cuando se teclea un comando en la línea de órdenes y se pulsa la tecla *Enter*, el programa interpreta el comando y, si es válido, lo ejecuta. Opcionalmente, el comando puede ir seguido de una lista de argumentos. Por ejemplo, el comando *help* proporciona ayuda sobre algunos comandos:

help help

Proporciona ayuda sobre el propio comando help

help cd

Proporciona ayuda sobre el comando cd

help –s cd

Lo mismo que el anterior, pero de forma abreviada

Otro comando útil para obtener información es *man*, que proporciona acceso al manual de Linux y muestra las páginas del comando deseado. Por ejemplo, si ejecutamos:

```
man ifconfig
```

Se abrirá una ventana con información sobre el comando *ifconfig* que sirve para configurar la interfaz de red (Figura 11).

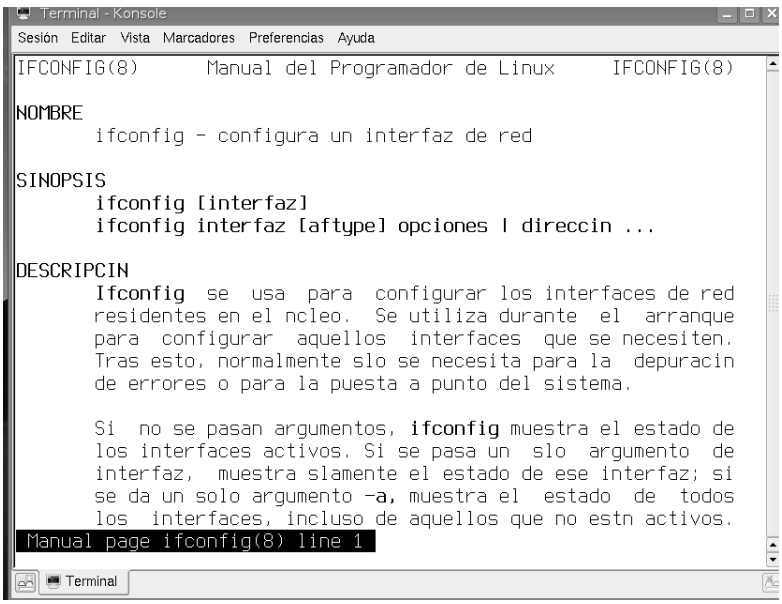


FIGURA 11. *Páginas del manual de Linux sobre el comando ifconfig*

El sistema operativo Linux, como la mayoría de sistemas operativos, dispone de un árbol jerárquico de de directorios. El directorio que ocupa el nivel superior de esta jerarquía se denomina directorio raíz y se indica con una barra (/). A continuación se muestran algunos comandos que permiten la navegación a través del árbol de directorios de Linux:

cd

Cambia de directorio.

Ejemplos:

cd ..	Cambia al directorio superior
cd datos	Cambia al directorio datos

ls

Muestra el contenido del directorio actual.

Ejemplos:

ls –l	Muestra información detallada
ls *.txt	Muestra archivos con extensión txt

pwd

Muestra la ruta del directorio actual.

En algunos ejercicios de las prácticas es necesario crear o modificar archivos de texto. Para este propósito, Linux dispone de varios editores de texto, como *vi* o *kwrite*. Normalmente, vamos a utilizar el segundo pero en algunas aplicaciones concretas, por ejemplo, la edición de un archivo en un ordenador remoto, utilizaremos *vi*. Por ejemplo, si queremos editar el archivo *hostname* ejecutaremos:

```
vi hostname
```

Una vez abierto el archivo, y ya dentro del editor, algunos comandos de edición que pueden utilizarse son los siguientes:

a	Insertar.
:q	Salir sin guardar.
:wq	Guardar y salir.
ESC	Anula el comando activo de edición

1.4.3 Configuración de las interfaces de red

En Linux, las interfaces de red para las tarjetas Ethernet se denominan *eth0* para la primera, *eth1* para la segunda y así sucesivamente. Además existe una interfaz virtual, denominada *loopback* o *lo*, que no está asociada a ninguna tarjeta de red y que permite al ordenador enviarse mensajes a sí mismo. Por convenio, la mayoría de los sistemas asignan a esta interfaz la dirección IP 127.0.0.1 y *localhost* como nombre al equipo.

Para configurar una interfaz de red en Linux desde línea de órdenes se utiliza el comando *ifconfig*. Por ejemplo, si queremos conocer información sobre la única tarjeta de red ethernet que dispone el ordenador ejecutaremos:

```
ifconfig eth0
```

Si a esta tarjeta queremos asignarle la dirección IP 192.168.1.1 y la máscara 255.255.255.0 tenemos que ejecutar la siguiente línea:

```
ifconfig eth0 192.168.1.1 netmask 255.255.255.0
```

Otros comandos útiles que suelen utilizarse para la configuración de la red son:

hostname

Muestra o establece el nombre del equipo.

Ejemplo:

hostname PC1 Establece el nombre del equipo en PC1

netstat

Proporciona diferente información de la configuración de la red, conexiones disponibles, estadísticas, etc.

La información de configuración de la red, así como los protocolos disponibles, puertos, etc., está disponible en los siguientes archivos de Linux:

/etc/hosts

Correspondencia entre direcciones IP y nombres de equipos.

/etc/protocols

Lista de protocolos disponibles.

/etc/services

Lista de servicios de red de internet y puertos.

1.4.4 El sistema de ventanas de Knoppix

Como ya se ha mencionado anteriormente, en la actualidad la mayoría de sistemas operativos Linux, en particular Knoppix, dispone de un sistema de ventanas basado en X-Window que facilita la realización de tareas por parte del usuario, en especial de los usuarios noveles.

La Figura 10 muestra el escritorio de Knoppix que aparece al arrancar el sistema operativo. Para abrir la consola de root que aparece en la misma figura hay que seleccionarla desplegando el Menú P. En la barra inferior también puede abrirse otra consola, denominada “Terminal-Konsole”, que permite ejecutar comandos de Linux pero en este caso sin privilegios de administrador.

Otras tareas que se pueden realizar en este entorno son las siguientes:

1. Navegar por la estructura de directorios usando la aplicación Konqueror (icono disponible en la barra inferior del escritorio). Por ejemplo, la Figura 12 muestra el árbol de directorios que cuelga del directorio raíz. Los medios para guardar información, como el disquete o la memoria USB, están dentro del directorio */media* y las carpetas de usuarios en el directorio */home*.

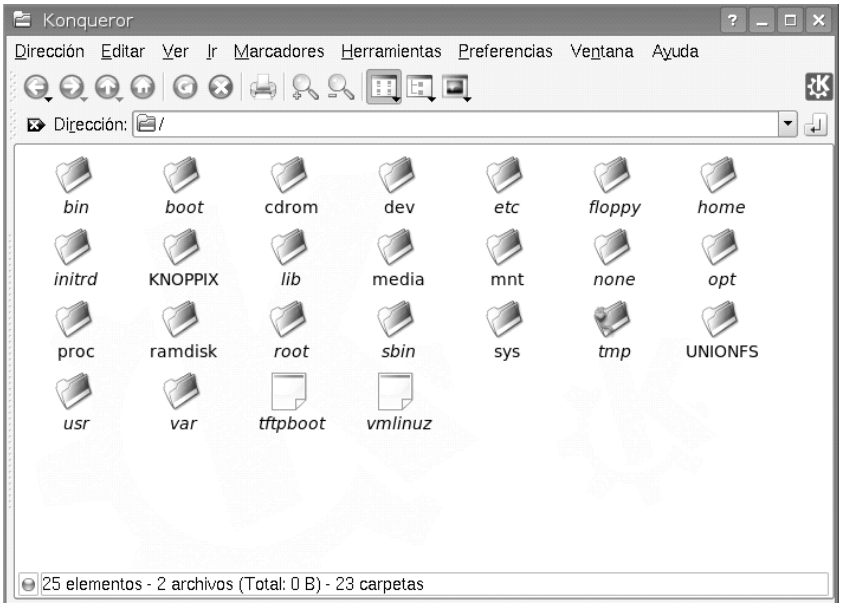


FIGURA 12. *Directorios que cuelgan del directorio raíz /.*

2. Ejecutar el editor Kwrite (Menú K→Editores→Kwrite) y abrir un documento de texto. Por ejemplo, */etc/services* (Figura 13).

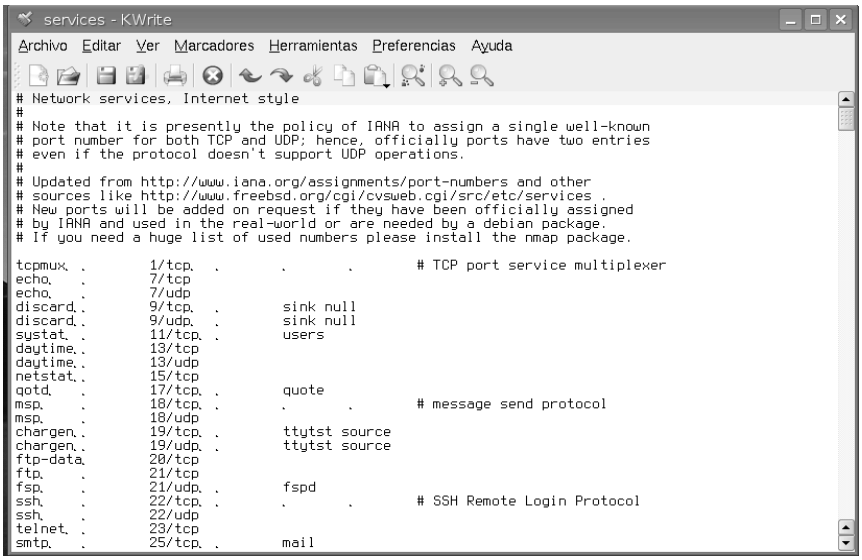


FIGURA 13. *Edición del archivo /etc/services con Kwrite.*

3. Configurar la tarjeta de red usando el asistente de Knoppix (Menú P→Red/Internet→Configuración de la tarjeta de red). En las prácticas, la configuración de la red (asignación de direcciones IP, máscaras, etc.) se realizará desde la línea de órdenes, utilizando *ifconfig*, o utilizando este asistente. Para utilizarlo debe responder No a la pregunta inicial ¿Utilizar broadcast DHCP? y seguir los pasos indicados por el asistente (el protocolo DHCP, Dynamic Host Configuration Protocol, sirve para asignar direcciones IP de forma automática).

1.4.5 Wireshark

Wireshark (www.wireshark.org) es un analizador de protocolos de red, o "packet sniffer", que captura y muestra el tráfico que pasa por una interfaz de red con un formato inteligible para el usuario.La versión anterior de este programa se conoce como Ethereal, pero el creador del mismo cambió de empresa y por cuestiones de registro de marcas le cambió el nombre.

La Figura 14 muestra la ventana principal del programa Wireshark. La zona inferior muestra el contenido en bruto de un paquete de datos. La zona intermedia muestra los protocolos encapsulados en dicho paquete y la zona

superior muestra todos los paquetes capturados. En la práctica 3 se describen con más detalle las funciones de este programa.

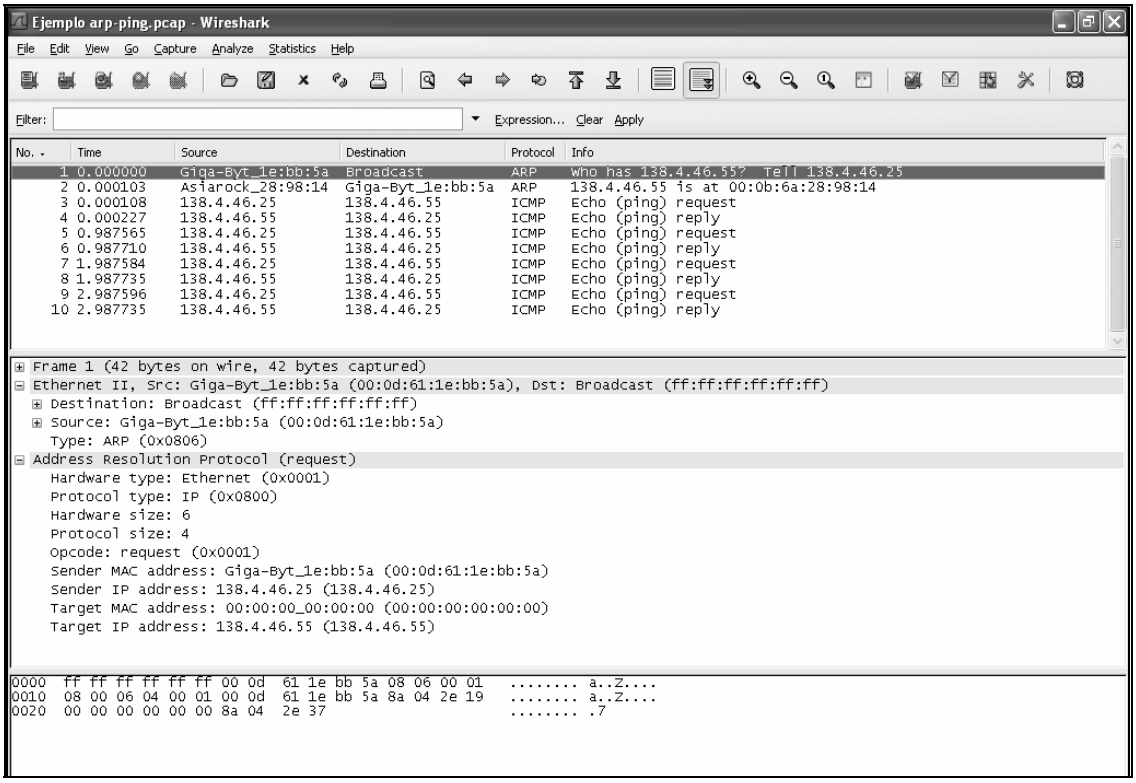


FIGURA 14. *Ventana principal de Wireshark.*

1.4.6 Sistema operativo CISCO IOS

Los routers del laboratorio son ordenadores especializados que ejecutan un sistema operativo propio denominado CISCO IOS, que está almacenado en una memoria flash PCMCIA (insertada en la parte inferior derecha del panel posterior. Ver la Figura 8) que se suministra con los routers.

Al arrancar el router, el sistema operativo se carga en una memoria DRAM (Dynamic Random Access Memory) desde donde se ejecuta. El sistema operativo CISCO IOS tiene, al igual que Linux, de una línea de comandos. Por ejemplo, la Figura 15 muestra un ejemplo de ejecución del comando *show*. En negrita se ha señalado, por ejemplo, las interfaces presentes en el router o el tamaño de las memorias flash y SDRAM.

```
R1> show version
Cisco Internetwork Operating System Software
IOS (tm) 1600 Software (C1600-BNSY-M), Version 12.0
Copyright (c) 1986-1997 by cisco Systems, Inc.
Compiled Mon 11-Aug-97 14:10 by cisco
Image text-base: 0x02005000, data-base: 0x02477BD0
ROM: System Bootstrap, Version 11.1(12)AA,DEPLOYMENT RELEASE SOFTWARE (f)
ROM: 1600 Software (C1600-RBOOT-R), Version 11.1(12)AA, EARLY DEPLOYMENT RELEASE
Router uptime is 12 minutes
System restarted by power-on
System image file is "flash:c1600-bnsy-mz", booted via flash
cisco 1605 (68360) processor (revision C) with 7680K/512K bytes of memory.
Processor board ID 06027889, with hardware revision 00000000
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIP compliant.
1 Ethernet/IEEE 802.3 interface(s)
1 Serial network interface(s)
System/IO memory with parity disabled
8192K bytes of DRAM onboard
System running from RAM
8K bytes of non-volatile configuration memory.
4096K bytes of processor board PCMCIA flash (Read/Write)
Configuration register is 0x2102
```

FIGURA 15. *Línea de comandos del sistema operativo CISCO IOS.*

En las prácticas, para acceder a un router desde un PC y ejecutar el sistema operativo CISCO IOS utilizaremos la aplicación *telnet*, un programa de emulación de terminal que ejecuta comandos en el router y que permite ver sus respuestas en una ventana de terminal, como la de la Figura 15, en la pantalla del PC (esta forma de acceso al router es posible porque su interfaz de red Ethernet, a través de la cuál se realiza la conexión, ha sido previamente configurada desde un PC usando el puerto de consola). En la práctica 4 se describe más en detalle este sistema operativo.

2. RED DE ÁREA LOCAL (LAN)

2.1 Introducción

En esta práctica se va a configurar una red de área local (LAN) formada por cuatro ordenadores que se interconectan entre sí a través de un switch, tal y como se representa en la Figura 16. Como en el Laboratorio hay doce ordenadores, realmente se van a configurar tres redes independientes como la de la Figura 16, cada una formada por los ordenadores PC1 a PC4, PC5 a PC8, y PC9 a PC12.

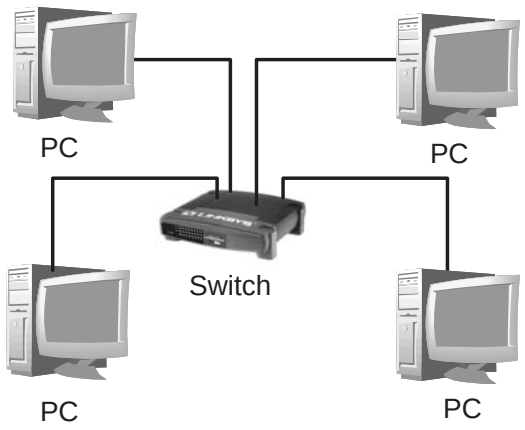


FIGURA 16. *Red de cuatro ordenadores interconectados a través de un switch.*

Una vez configuradas las direcciones IP de los ordenadores de cada red, se comprobará que ésta funciona correctamente ejecutando una serie de aplicaciones. Por ejemplo: el comando *ping*, que sirve para comprobar si una dirección IP está accesible en la red, el comando *arp* que gestiona la tabla ARP (Address Resolution Protocol), o la aplicación *ssh* (Secure Shell) que se utiliza para realizar una conexión remota segura con otro ordenador y ejecutar

comandos en él. A continuación se repasan algunos conceptos fundamentales de redes de computadores que serán de utilidad no sólo en esta práctica sino también en las restantes prácticas del Laboratorio.

2.2 TCP/IP

TCP/IP es un conjunto de protocolos de comunicación que permite a ordenadores, routers, etc., de diferentes fabricantes y con distintos sistemas operativos comunicarse entre sí. El nombre del conjunto está formado por los nombres de los dos protocolos más importantes del mismo: TCP (Transmission Control Protocol) e IP (Internet Protocol), aunque hay muchos más, por ejemplo, ARP (Address Resolution Protocol), ICMP (Internet Control Message Protocol), IGMP (Internet Group Management Protocol) o UDP (User Datagram Protocol).

Los protocolos TCP/IP están organizados en una estructura de cuatro capas denominadas de enlace, de red, de transporte y de aplicación[1], dispuestas en la estructura jerárquica que se muestra en la Figura 17. Cada capa es responsable de un aspecto de la comunicación.

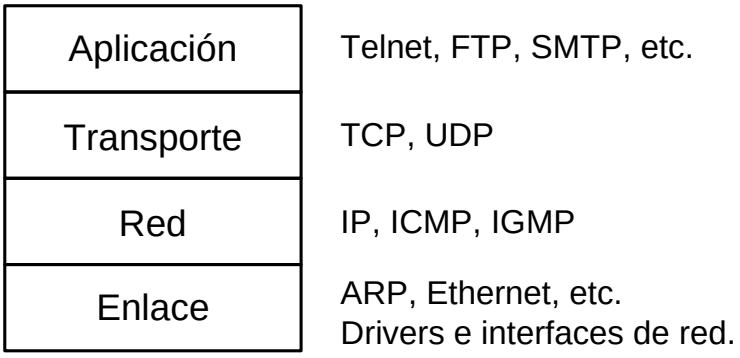


FIGURA 17. *Capas del conjunto de protocolos TCP/IP.*

[1] A veces se añade una capa adicional, denominada capa física, situada bajo la capa de enlace, que aquí se ha considerado incluida dentro de ésta.

La capa de enlace de datos incluye protocolos como Ethernet o ARP, pero también los drivers de los dispositivos, la tarjeta de red o cualquier otro medio que se utilice para la comunicación.

La capa de red, formada por los protocolos IP, ICMP e IGMP, se encarga del movimiento de los datos a través de la red.

La capa de transporte, con los protocolos TCP y UDP, se encarga del transporte de mensajes que da soporte a la capa de aplicación. Por ejemplo, TCP proporciona a las aplicaciones un servicio “orientado a conexión”, el cuál, por ejemplo, controla la velocidad de transmisión de los datos y garantiza que llegan a su destino.

Finalmente, la capa de aplicación se encarga de las aplicaciones de la red. Algunas de las más conocidas son Telnet, para hacer una conexión remota, FTP (File Transfer Protocol) para transferir archivos, o SMTP (Simple Mail Transfer Protocol) para correo electrónico.

2.3 Direcciones IP y DNS

Una dirección IP es un número de 32 bits que identifica de manera única a una interfaz de red dentro de Internet. Cada dirección IP tiene que ser única y para ello existe una organización llamada Internet Network Information Center (http://www.internic.net), que se encarga de asignar las direcciones. Una dirección IP normalmente se representa, para hacerla más inteligible, por los valores decimales de cada uno de sus cuatro bytes separados por puntos. Por ejemplo, la dirección IP 11000000 10101000 00000001 00000001 se escribiría como 192.168.1.1.

Hay tres tipos de direcciones IP: unicast (para un equipo individual), broadcast (para los equipos de la misma red), y multicast (para los equipos que del mismo grupo multicast o de multidifusión). Asimismo, las direcciones IP se clasifican en cinco clases, denominadas A, B, C, D, y E cuyos rangos se indican en la Figura 18.

La clase A dispone de 7 bits dentro del primer byte para direcciones de red, lo que hace un total de 2^7=128 redes, menos dos que no se pueden utilizar (la 0.0.0.0 y la 127.0.0.0 que se reserva para la función *loopback*). Cada una de

estas 126 redes dispone de 2^{24}=16.777.216 direcciones que se pueden asignar a equipos (hosts) menos dos que no se pueden utilizar. La primera es la que tiene todos los bits a 0 e identifica a la red. La segunda es la que tiene todos los bits a 1 y se utiliza como dirección de broadcast de esa red. Es decir, en una red clase A hay 16.777.214 direcciones IP disponibles para equipos.

La clase B dispone de 16.384 redes, cada una con 65.534 direcciones que se pueden asignar a equipos. Y la clase C, 2.097.152 redes de 254 equipos cada una.

Por ejemplo, la dirección IP 192.168.1.1 pertenece a una red de clase C cuya dirección es la 192.168.1.0 y su dirección de broadcast es 192.168.1.255. Esta red dispone de 254 direcciones para hosts (de la 192.168.1.1 a la 192.168.1.254), de las cuáles la primera (192.168.1.1) suele reservarse para la puerta de enlace, normalmente un router.

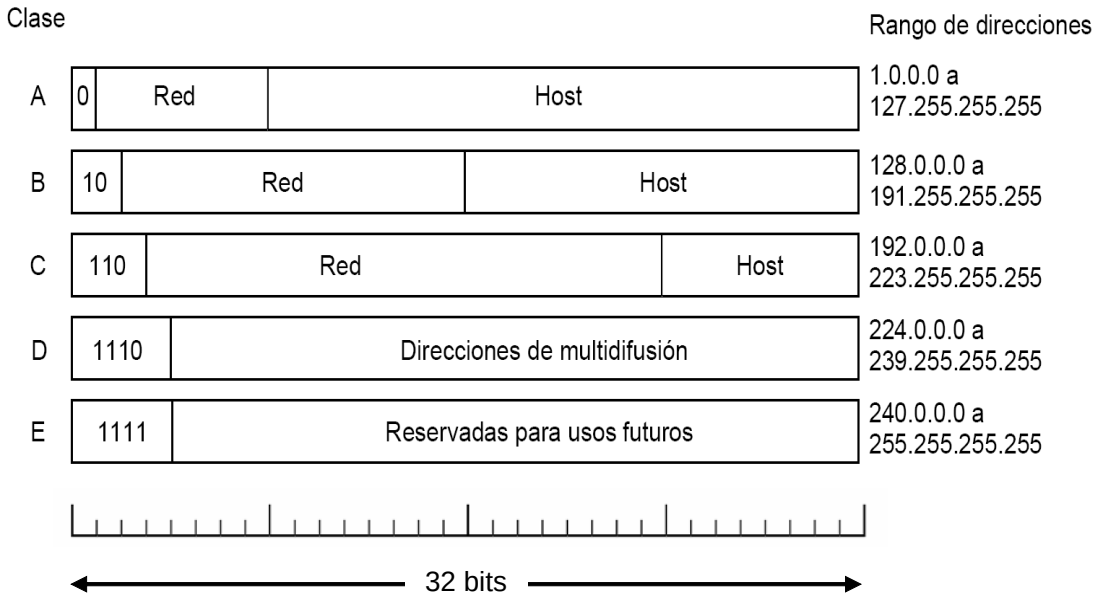


FIGURA 18. *Clases de direcciones IP.*

La primera parte de una dirección IP indica la red que alberga un conjunto de equipos y la segunda identifica a un equipo determinado dentro de esa red. Para indicar qué parte de la dirección corresponde a la red, lo que suele denominarse como prefijo de red, y qué parte corresponde al equipo se

utiliza la máscara de red. Esta máscara es un número de 32 bits cuyos primeros bits, tantos como tenga el prefijo de red, valen 1 siendo el resto igual a 0. La Figura 19 muestra las máscaras de las tres clases anteriores:

Clase	Máscara
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

FIGURA 19. *Máscaras de las clases de redes A, B y C.*

Las máscaras también suelen escribirse con una barra, /, seguida del número de bits que valen 1. Por ejemplo, las máscaras anteriores se escribirían, respectivamente, como /8, /16 y /24.

Merece la pena mencionar, de pasada, que la parte de la dirección IP correspondiente a hosts se puede dividir a su vez en dos partes, una de subred y otra de hosts, lo cuál permite dividir una red más amplia en pequeños fragmentos o subredes. Por ejemplo, la red que puede albergar un menor número de hosts es la de clase C con 254, un número de ordenadores que puede ser excesivo para conectarlos todos juntos en la misma red, sin mencionar los 16.777.214 permitidos en una red de clase A.

Una dirección IP identifica a una interfaz en una red y al equipo que la contiene. Sin embargo, para una persona es más cómodo referirse al equipo por su nombre que utilizar su dirección IP. Para poder utilizar nombres en lugar de direcciones IP, existe una base de datos distribuida denominada DNS (Domain Name System) que proporciona las correspondencias entre direcciones IP y nombres de equipos. Por ejemplo, los dominios de Internet como .com, .es, .gov, .org, .net, .edu, etc., forman parte del DNS y, al igual que las direcciones IP, son gestionados por la organización Internic. Cuando una aplicación necesita saber el nombre de host correspondiente a una IP, o viceversa, simplemente invoca una función del sistema operativo (en Linux, *gethostbyname* y *gethostbyaddr*, respectivamente) que contacta con un servidor DNS para obtenerlo. El laboratorio no dispone de servidor DNS, aunque se va a implementar un DNS rudimentario editando el archivo *hosts*.

2.4 Encapsulado y demultiplexado de protocolos. Puertos.

Cuando una aplicación envía datos usando TCP/IP, éstos pasan por todas las capas representadas en la Figura 17 antes de salir, en forma de bits, por la tarjeta de red. En cada capa se añade una cabecera propia a los datos provenientes de la capa anterior y, a veces, más información.

La Figura 20 muestra un ejemplo de encapsulado de un conjunto de datos enviados por una aplicación usando TCP en la capa de transporte y Ethernet en la capa de enlace. En primer lugar, la capa de aplicación añade una cabecera para indicar el tipo de aplicación (FTP, SMTP, etc.) a los datos del usuario. A continuación, la capa de transporte añade otra cabecera indicando que se utiliza TCP, y así sucesivamente hasta la última capa.

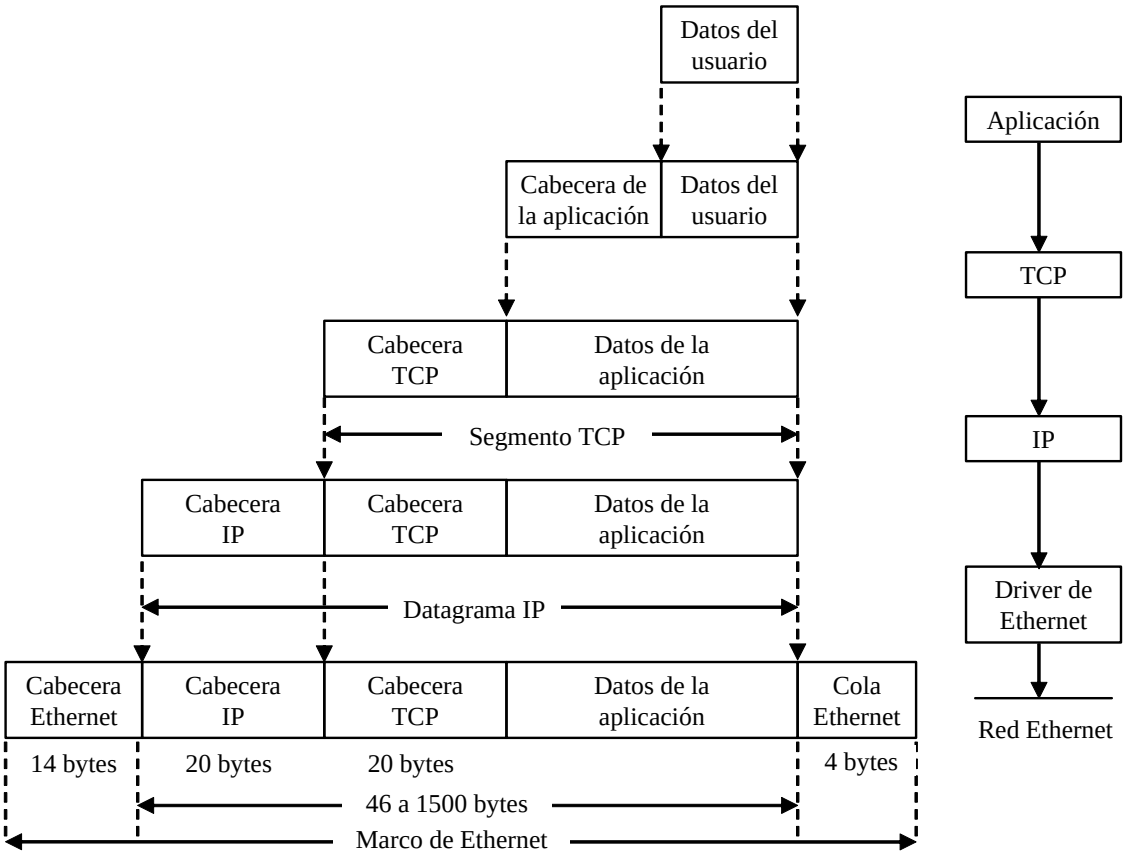


FIGURA 20. *Ejemplo de encapsulado de datos de una aplicación usando TCP y Ethernet.*

Las unidades de datos que se envían de una capa a la siguiente se denominan habitualmente y de arriba abajo: segmento, datagrama y marco o traza. Cuando un marco es recibido por el equipo destinatario se realiza el proceso inverso, es decir, se van quitando las cabeceras en cada capa, empezando por la de enlace, y los datos restantes se envían a la capa superior. A este proceso se le denomina demultiplexación.

Para identificar a las aplicaciones que van a recibir los datos, los protocolos de transporte, como TCP, utilizan un número de 16 bits denominado puerto. En Linux, la lista de puertos bien conocidos[2] está disponible en el archivo *etc/services* (Figura 13, página 19). Por ejemplo, FTP tiene asignado el puerto 21, SSH el 22, Telnet el 23 y SMTP el 25.

2.5 Protocolos

2.5.1 Ethernet

Las redes Ethernet son la tecnología dominante en las redes de área local que utilizan TCP/IP. Las primeras generaciones de redes Ethernet utilizaban una topología de bus, en la que el canal de transmisión era un cable coaxial al que estaban conectadas todas las interfaces de la red. En la topología anterior se comparte el canal, de manera que es importante que solamente una interfaz de red transmita datos al mismo tiempo. En caso contrario, si dos o más equipos transmiten a la vez, los datos se corrompen y se produce lo que se denomina “colisión”. Para evitar las colisiones, en Ethernet se utiliza el protocolo CSMA/CD (Carrier Sense Multiple Access with Collision Detections), que está implementado en el hardware de la tarjeta de red y que se encarga de gestionar el acceso al canal. En la red del Laboratorio, los equipos están interconectados a través de switches que permiten una comunicación full-dúplex, de manera que cualquier equipo conectado en la red puede transmitir datos en cualquier momento sin que ocurran colisiones.

[2] Traducción literal del inglés en el que se denominan “well-know ports”. Son puertos que están asociados a una única, y bien conocida, aplicación.

La Figura 21 muestra el formato más común de un marco de Ethernet II. La cabecera Ethernet tiene un tamaño de 14 bytes. Los dos primeros campos son las direcciones MAC del receptor y del emisor. El siguiente campo, indica el tipo de protocolo de los datos que vienen a continuación (denominados parte útil o "payload"). Por ejemplo, si la parte útil del marco de Ethernet es un datagrama IP, este campo toma el valor 0x8000. Como puede verse, la carga tiene una longitud entre 46 y 1500 bytes (si el datagrama tiene menos de 46 bytes se añaden ceros hasta completar esta longitud mínima). El último campo CRC (Cyclic Redundancy Check) se utiliza para detectar errores de transmisión[3] y tiene una longitud de 4 bytes.

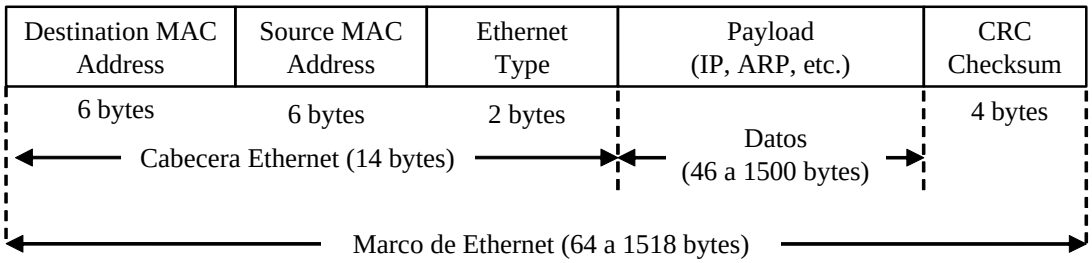


FIGURA 21. *Formato más común de una traza de Ethernet II.*

2.5.2 Address Resolution Protocol (ARP)

Como ya se ha mencionado anteriormente, cuando se transmite un datagrama IP en Ethernet se encapsula en un marco de Ethernet cuya cabecera debe incluir la dirección MAC del destinatario, la cuál puede no ser conocida por el remitente. Y aquí es donde el protocolo ARP entra en juego.

La tarea más común de ARP es encontrar la dirección MAC asociada a una dirección IP. Para ello, envía un mensaje de petición a la dirección MAC de

[3] El campo checksum, o suma de verificación, es igual a la suma de los bytes de todo el marco. Para comprobar la integridad de los datos, cuando se recibe el paquete se vuelven a sumar los bytes y se compara el resultado con el valor almacenado en checksum. Si ambos valores coinciden, es probable que no haya habido errores en la transmisión.

broadcast de la red (ff:ff:ff:ff:ff:ff) que es recibido por todos los equipos conectados a ella. Si un equipo comprueba que la dirección IP por la que se pregunta coincide con la suya, envía al peticionario su dirección MAC (el resto de los equipos ignora la petición). Cuando el equipo peticionario recibe la respuesta, almacena en una tabla, denominada caché ARP, la pareja dirección IP-dirección MAC. La misión de esta tabla es reducir el número de paquetes ARP que se envían. De esta forma, si un equipo necesita la dirección MAC asociada a una determinada dirección IP, antes de enviar un mensaje de broadcast primero comprueba si la tiene almacenada en la caché ARP.

La memoria caché ARP de un equipo no es estática, sino que se actualiza cada pocos minutos. De esta forma puede adaptarse a los posibles cambios de direcciones IP o MAC que ocurran en la red. Cuando un equipo realiza una petición ARP, incluye en el mensaje sus propias direcciones IP y MAC, de manera que al enviarlo a la dirección de broadcast el resto de los equipos de la red actualizarán su caché ARP con la pareja IP-MAC del peticionario. La Figura 22 muestra el formato de un mensaje ARP, cuyos campos tienen el siguiente significado:

Hardware type (2 bytes)

Especifica el tipo de hardware (0x0001 para una tarjeta Ethernet).

Protocol type (2 bytes)

Especifica el tipo de protocolo (0x8000 cuando ARP resuelve direcciones IP)

Hardware size (1 bytes)

Especifica la longitud, en bytes, de la dirección hardware (0x0006 para MAC)

Protocol size (1 bytes)

Especifica la longitud, en bytes, de la dirección del protocolo (0x0004 para IP).

Operation code (2 bytes)

Especifica si se trata de una petición (0x0001) o de una respuesta (0x0002) ARP.

Sender/target hardware address (n bytes)

Contiene las direcciones físicas del hardware.

Source/target protocol address (m bytes)

Contiene las direcciones del protocolo. En TCP/IP son 32 bits.

Hardware type	
Protocol type	
Hardware size (n)	Protocol size (m)
Operation code	
Sender hardware address	
Sender protocol address	
Target hardware address	
Target protocol address	

FIGURA 22. *Formato de una paquete ARP.*

La longitud de un paquete ARP está determinado por el tamaño de las direcciones del hardware y del tipo de protocolo. Con direcciones MAC de 48 bits y direcciones IP de 32 bits, el tamaño de un paquete de petición, o de respuesta, ARP es de 28 bytes. Los mensajes ARP no tienen cabecera IP y se encapsulan directamente en marcos de Ethernet.

2.5.3 Internet Protocol (IP)

El protocolo IP se encarga de transportar los datos (datagramas IP) desde el origen hasta el destino a través de la red. En el equipo remitente, IP recibe un segmento de la capa de transporte, TCP o UDP, y lo encapsula en un datagrama IP. A continuación, IP demanda el servicio del protocolo de la capa de enlace (normalmente Ethernet) y encapsula el paquete en un marco que es enviado al equipo destinatario (si está en la misma red) o al router (si el equipo destinatario pertenece a una red distinta).

Cuando un router recibe un marco, demultiplexa el datagrama IP del mismo, comprueba la IP del destinatario y lo encapsula de nuevo en una traza con la dirección MAC del siguiente equipo al que tiene que ser enviado (el destinatario final u otro router). Y así sucesivamente. Cuando el marco llega finalmente a su destino, en la capa de enlace se demultiplexa el marco para obtener el datagrama IP, y en la capa de red se demultiplexa el datagrama IP para obtenet el segmento TCP o UDP, el cuál es enviado a la capa de transporte. Finalmente, los datos son enviados a la aplicación correspondiente.

En este proceso, el único protocolo que se encarga del transporte es IP. Cualquier envío de datos de los protocolos TCP, UDP, ICMP o IGMP es siempre transmitido como un datagrama IP. Este "monopolio" de IP tiene la ventaja de que cualquier equipo, router, etc. que utilice IP puede comunicarse con cualquier otro de la red. Pero el hecho de que no haya alternativa a IP tiene la desventaja de que cualquier aplicación, sean cuáles sean sus necesidades, sólo recibe el nivel de servicio que puede proporcionar IP, el cuál no es precisamente fiable. Por ejemplo, IP no garantiza que un paquete llegue a su destino o que los paquetes lleguen en la secuencia en la que fueron enviados.

La versión actual de IP es la 4 (IPv4), aunque existe una nueva versión (IPv6) en proceso de implantación motivada por el rápido crecimiento de internet y la consecuente disminución de direcciones IP disponibles. La Figura 23 muestra el formato de un datagrama IPv4.

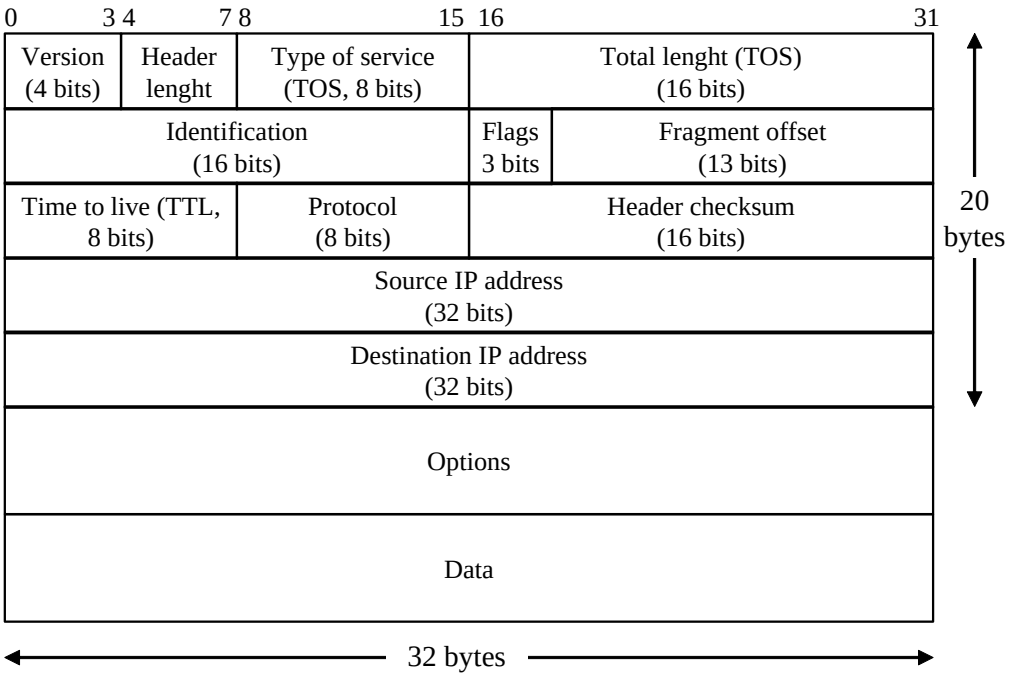


FIGURA 23. *Formato de un datagrama IPv4.*

En la primera fila, el primer campo (*version*), indica el número de la versión, por ejemplo, 4 para IPv4. El segundo campo (*header lenght*) indica la longitud de la cabecera en múltiplos de cuatro bytes, lo cuál permite conocer dónde empiezan los datos (campo *data*). Como este campo ocupa 4 bits,

puede tomar 15 como valor máximo y, por tanto, la cabecera tendrá una longitud máxima de 60 bytes (4x15bytes). La longitud mínima de la cabecera es 20 bytes, lo cuál ocurre cuando el campo *options* está vacío.

El tercer campo, TOS (*Type-of-Service*), indica las preferencias sobre el servicio que se desea que proporcione IP, pero sin ninguna garantía de que IP lo consiga. Como ya se ha mencionado, IP no garantiza que los paquetes se pierdan o lleguen ordenados, ni tampoco la velocidad de transmisión o cuánto van a tardar en llegar a su destino. El cuarto campo (*total lenght*), indica el número total de bytes del datagrama IP, incluyendo la cabecera y los datos.

En la segunda fila, todos los campos (*identification, flags y fragment offset*) están asociados a la fragmentación de los datagramas IP. En principio, el tamaño máximo de un datagrama IP es de 65.535 bytes. Sin embargo, debido a las restricciones impuestas por el protocolo Ethernet, los datagramas IP no pueden superar los 1500 bytes (carga o “payload” máxima permitida. Ver Figura 21, página 30). Este límite, denominado denominado MTU (Maximum Transmission Unit), obliga a realizar un proceso de segmentación relativamente complejo que se especifica por medio de los tres campos mencionados.

Ya en la tercera fila, el campo TTL(*Time-To-Live*) indica la vida útil de un datagrama IP, lo cuál es útil si el datagrama queda atrapado en un bucle de la red. Cada vez que un router procesa el datagrama decrementa en 1 el valor de este campo y si llega a cero lo elimina. Es obvio que el campo TTL tiene que tener un valor inicial superior al número de routers que se pueden encontrar en la ruta más larga a través de la red, ya que en caso contrario puede que el paquete no llegue a su destino. El valor inicial de TTL suele ser mayor o igual que 64.

El campo *protocol* identifica el protocolo al que pertenecen los datos y que se necesita para la demultiplexación. La figura siguiente especifica el valor de este campo para los protocolos ICMP; TCP y UDP.

Campo *protocol*	Protocolo
1	ICMP
6	TCP
17	UDP

FIGURA 24. *Identificación de protocolos de datos contenidos en un datagrama IP.*

El campo *checksum*, o suma de verificación, tiene el significado mencionado anteriormente. En el caso del datagrama IP, sólo se computan los bytes de la cabecera IP. Cuando IP detecta un error en este campo, descarta el datagrama.

Los campos que siguen a *checksum* son las direcciones IP del remitente y del destinatario. El campo *options* que completa la cabacera del datagrama IP no es obligatorio y sirve, aunque se utiliza en raras ocasiones, para indicar algunas opciones especiales. Por ejemplo, para determinar el MTU de una ruta. Finalmente, el campo *data* contiene la parte útil, o "payload", encapsulada en el datagrama IP. Por ejemplo, un mensaje ICMP de la propia capa de red o un segmento TCP o UDP de la capa de transporte.

2.5.4 Internet Control Message Protocol (ICMP)

El protocolo ICMP se utiliza como soporte al protocolo IP para enviar mensajes de error. Por ejemplo, si un router descarta un datagrama IP porque el campo TTL es nulo envía al equipo un remitente un mensaje ICMP avisando de esta circunstancia y explicando el motivo. ICMP también proporciona la posibilidad de diagnosticar el estado de la red, por ejemplo, enviando mensajes de petición de eco usando el comando *ping* del que hablaremos más adelante. Un mensaje ICMP se encapsula dentro de un datagrama IP, tal y como se muestra en la Figura 25. Como puede verse, al mensaje ICMP también se le añade la cabecera IP.

Cabecera IP	Mensaje ICMP

FIGURA 25. *Encapsulado de un mensaje ICMP en un datagrama IP.*

El formato de un mensaje ICMP está representado en la Figura 26. Su longitud mínima es 8 bytes, de los cuáles 4 bytes corresponden a los campos

type, *code* y *checksum* y, si no hay información adicional, se completan los 4 bytes restantes con ceros.

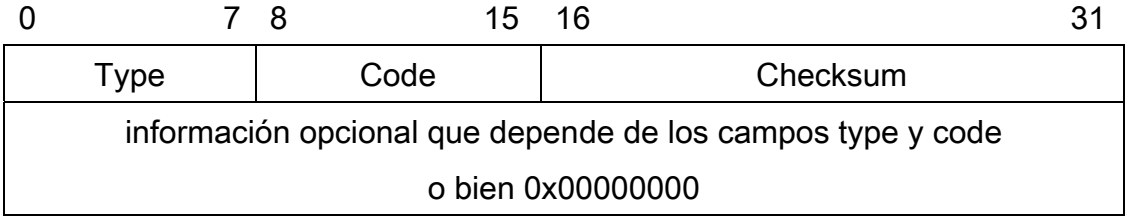


FIGURA 26. *Formato de un mensaje ICMP.*

Los tipos de mensajes ICMP se identifican con los campos *type* y *code*. Los mensajes ICMP pueden clasificarse en dos grandes categorías, mensajes de consulta y mensajes de error. En total hay 33 tipos de mensajes ICMP, algunos de los cuáles se indican en la Figura 27.

type	code	Mensaje ICMP	Tipo
0	0	Echo reply (petición de eco)	Consulta
0	0	Network unreachable (red inalcanzable)	Error
0	1	Host unreachable (equipo inalcanzable)	Error
0	2	Protocol unreachable (protocolo inalcanzable)	Error
0	3	Port unreachable (puerto inalcanzable)	Error
8	0	Echo request (respuesta de eco)	Consulta

FIGURA 27. *Algunos tipos de mensajes ICMP.*

Un mensaje de consulta consiste en un par de mensajes ICMP, uno de petición y uno de respuesta, tal y como se representa en la Figura 28. En esta figura se ha supuesto que la consulta es una petición/respuesta de eco que se utiliza para comprobar si una dirección IP es accesible en la red. Primero se envía el mensaje de petición de eco (*echo request*) a una dirección IP y a continuación ésta responde con un mensaje de respuesta de eco (*echo reply*). El formato de ambos de los mensajes de petición y respuesta de eco, que analizaremos en el Laboratorio, se muestra en la Figura 29.

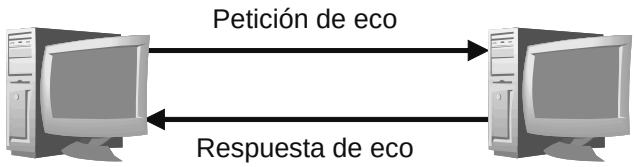


FIGURA 28. *Mensajes de petición y respuesta de eco ICMP.*

0 u 8	0	Checksum
Identifier		Sequence number
Información opcional		

FIGURA 29. *Formato de paquetes ICMP de petición y respuesta de eco.*

Un mensaje de error informa de que ha ocurrido un error en el envío de un datagrama IP, por ejemplo, cuando un router lo descarta. El formato de un mensaje ICMP de error puede verse en la Figura 30. La cabecera del mensaje ICMP está formada por los campos *type*, *code* y *checksum* seguidos de cuatro bytes a cero (0x00000000). La cabecera IP y los 8 bytes de carga útil que vienen a continuación también forman parte del mensaje ICMP y pertenecen al datagrama IP que originó el error.

Cabecera IP	Cabecera ICMP	Cabecera IP	8 bytes de carga útil

FIGURA 30. *Formato de un mensaje ICMP de error.*

Por ejemplo, el mensaje *host unreachable* indica que el router de una red no recibe una respuesta ARP de la dirección IP del destinatario. Aunque los mensajes también pueden indicar algo que no tiene que ver con la configuración de la red. Por ejemplo, el mensaje *port unreachable* indica que capa de transporte no ha podido entregar los datos a la aplicación correspondiente. Esto puedo ocurrir cuando se utiliza el protocolo UDP y un programa ejecutado desde un cliente intenta conectar con un servidor que no existe, por ejemplo, cuando se se usa TFTP (Trivial File Transfer Protocol). Con TCP esto no ocurre porque la conexión se cierra inmediatamente.

2.6 Comandos

2.6.1 ifconfig

El comando *ifconfig* se utiliza para configurar las interfaces de red en Linux, por ejemplo, para habilitarlas o para asignarles una dirección IP. A continuación se muestran algunos ejemplos de uso de este comando:

ifconfig

Muestra el estado de las interfaces activas.

ifconfig –a

Muestra el estado de todas las interfaces, estén o no activas.

ifconfig eth0

Muestra el estado de la interfaz eth0.

ifconfig eth0 up

Habilita la interfaz eth0 (si se asigna una dirección a la interfaz, la habilitación se produce de forma automática)

ifconfig eth0 down

Deshabilita la interfaz eth0.

ifconfig eth0 192.168.1.1 netmask 255.255.255.0

Asigna a la interfaz eth0 la dirección IP 192.168.1.1 y la máscara 255.255.255.

2.6.2 ping

El comando *ping* es una herramienta simple pero muy útil que sirve para determinar si una dirección IP es accesible en una red por medio de los paquetes de petición de eco y de respuesta de eco definidos en el protocolo ICMP. El comando *ping* envia un paquete de petición de eco (ICMP Echo Request) a una dirección IP y espera que ésta conteste con un paquete de respuesta de eco (ICMP Echo Reply).

Cuando se ejecuta el comando *ping*, Linux mide y muestra el tiempo que pasa entre el envío de un paquete de petición de eco y la recepción del paquete de respuesta. Por ejemplo, si queremos comprobar si la dirección IP es accesible en la red ejecutaremos:

```
ping 192.168.1.1
```

Si la dirección está accesible, en la consola de Linux aparecerán continuamente líneas parecidas a las siguientes:

```
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.024 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.019 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.020 ms
```

A continuación se muestran algunas opciones del comando:

ping IP

Comprueba si la dirección IP es accesible (la ejecución se detiene pulsando Ctrl+Z).

Ejemplo:

```
ping 192.168.1.20
```

ping –c n IP

La ejecución se detiene cuando se han enviado n paquetes de petición de eco a la dirección IP y se han recibido desde ella otros n paquetes de respuesta de eco.

Ejemplo: `ping –c 1 192.168.1.20`

ping –v IP

Informa al usuario de lo que ocurre de manera extendida.

2.6.3 arp

El comando *arp* gestiona la memoria caché ARP del sistema que contiene la tabla de correspondencias entre direcciones IP y direcciones MAC. Por ejemplo, con este comando puede borrarse toda la tabla o eliminar una de sus entradas. A continuación se muestran algunas opciones de este comando:

arp

Muestra el contenido de la tabla ARP

arp –a 192.168.1.1

Muestra la entrada de la dirección IP 192.168.1.1 (si se omite la dirección IP se muestran todas las entradas).

arp –d IP

Borra la entrada para la dirección IP. Ejemplo: arp –d 192.168.1.25

Las entradas de la memoria caché ARP no son permanentes sino que se eliminan después de cierto tiempo (a menos que se renueven). En algunas implementaciones de ARP, puede observarse que un equipo envía a veces por su cuenta peticiones ARP a una dirección IP cuya entrada está aún en la caché ARP. El motivo de esta petición es comprobar si esa dirección IP está accesible antes de borrar su entrada de la tabla.

2.6.4 ssh

El comando *ssh* (Secure Shell) permite a un equipo (cliente ssh) conectarse a un equipo remoto (servidor ssh), mediante una comunicación encriptada y segura, y ejecutar comandos en él. Por ejemplo, para que el usuario knoppix conecte con el servidor remoto 192.168.1.10 ejecutaremos desde la línea de comandos la siguiente orden:

```
ssh knoppix@192.168.1.10
```

Para que la conexión sea posible, el servidor ssh debe estar activado en el equipo remoto. Para hacer esto en Linux-Knoppix, seleccione en el Menú P: Servidores y servicios→ Arrancar servidor ssh.

2.6.5 ftp

El comando *ftp* permite iniciar una sesión en un servidor FTP (File Transfer Protocol). Por ejemplo, la siguiente línea:

```
ftp 192.168.1.25
```

Inicia una sesión con el servidor FTP cuya dirección IP es 192.168.1.25. Una vez iniciada la sesión con éxito, después de haber introducido el nombre de usuario y la contraseña, el *prompt* que ve el usuario cambia a:

```
ftp>
```

Desde el *prompt* FTP se pueden ejecutar unos pocos comandos que permiten navegar por los directorios y descargar ficheros desde el servidor (equipo remoto) o subirlos desde el cliente (nuestro equipo). Algunos de estos comandos son los siguientes:

cd

Cambia de directorio en el servidor.

Ejemplo:

cd ramdisk Cambia al directorio ramdisk0

get

Descarga un fichero del servidor.

Ejemplo: get archivo1.txt

help

Proporciona la lista de comandos disponibles.

lcd

Muestra o cambia de directorio en el cliente.

Ejemplo:

lcd home Cambia al directorio home

ls

Muestra el contenido del directorio actual en el servidor.

put

Sube un archivo al servidor.

Ejemplo: put archivo2.txt

pwd

Ver el directorio remoto en el que estamos.

quit

Finaliza la conexión remota.

2.7 Descripción de la práctica

2.7.1 Configuración de la red

1. Establezca como nombre de su ordenador PCX, donde X es el número de su puesto en el Laboratorio. Por ejemplo, para el puesto 1:

```
hostname PC1
```

2. Use el comando *ifconfig* para descubrir la dirección MAC de la tarjeta Ethernet de su ordenador y anótela a continuación:

   Puesto:

   Dirección MAC:

3. Utilizando *ifconfig*, configure en su equipo la interfaz *eth0* con la dirección IP y la máscara (/M) siguientes:

Puesto	Dirección IP /M	Puesto	Dirección IP /M	Puesto	Dirección IP /M
1	192.168.1.2 /24	5	192.168.3.2 /24	9	192.168.5.2 /24
2	192.168.1.3 /24	6	192.168.3.3 /24	10	192.168.5.3 /24
3	192.168.1.4 /24	7	192.168.3.4 /24	11	192.168.5.4 /24
4	192.168.1.5 /24	8	192.168.3.5 /24	12	192.168.5.5 /24

Cada grupo de cuatro ordenadores pertenece a una misma red de clase C en la que se ha reservado la primera dirección disponible, como se hace habitualmente, para la puerta de enlace. En las prácticas 4 y 5 asignaremos esta dirección al router.

La tabla siguiente resume la composición y las direcciones IP de cada una de las tres redes.

Puestos	Red	Broadcast	Puerta de enlace
1 a 4	192.168.1.0	192.168.1.255	192.168.1.1
5 a 8	192.168.3.0	192.168.3.255	192.168.3.1
9 a 12	192.168.5.0	192.168.5.255	192.168.5.1

2.7.2 Diagnóstico del estado de la red y direcciones MAC

1. Compruebe, mediante el comando ping, la conectividad de los otros ordenadores conectados en la misma red.
2. Comprueba la tabla ARP de su ordenador y rellene la siguiente tabla con las direcciones MAC de los ordenadores de su red incluyendo el suyo:

Puesto	Dirección IP	Dirección MAC

4. Compruebe mediante el comando ping la conectividad con la máquina 192.168.2.1. ¿Cuál es el resultado? ¿Por qué?
5. Repita el proceso de configuración de la interfaz de red utilizando el asistente de Knoppix (Menú P→Red/Internet→Configuración de la tarjeta de red) y asigne a la puerta de enlace la primera dirección IP disponible en la red.
6. Compruebe mediante el comando ping la conectividad de la puerta de enlace. ¿Cuál es el resultado? ¿Por qué?

2.7.3 Sesión ssh

1. Active el servidor SSH en su ordenador y establezca redes como contraseña del usuario knoppix. Esto permitará que otros ordenadores de la red puedan realizar una conexión remota a su ordenador.
2. Realice una conexión remota al ordenador del puesto más cercano mediante el comando *ssh*. Por ejemplo:

```
ssh knoppix@192.168.1.25
```

3. Compruebe que está conectado y que puede ejecutar comandos de Linux en el directorio remoto. ¿En qué directorio remoto está?
4. Edite con *vi* un archivo de texto, escriba en él una frase y guárdelo en el equipo remoto. Por ejemplo:

```
vi archivo1.txt
```

Algunos comandos de edición de *vi* son los siguientes:

```
a       Insertar.
:q      Salir sin guardar.
:wq     Guardar y salir.
ESC     Anula el comando activo de edición
```

5. Finalice la conexión remota.

2.7.4 Sesión ftp

1. Active el servidor FTP en su ordenador siguiendo los pasos siguientes:
2. Ejecute en una consola de root la siguiente línea:

```
in.ftpd -D
```

3. Ejecute, desde una consola de root, el editor *Kwrite* y edite el archivo:

```
/etc/hosts.allow
```

4. Escriba en el archivo anterior, antes de la última línea, la siguiente:

```
ftp in.ftpd : ALL@ALL : ALLOW
```

5. Guarde el archivo.
6. Asigne la contraseña redes al usuario knoppix ejecutando desde la consola de root la siguiente orden:

```
passwd  knoppix
```

7. Una vez activado el servidor en su ordenador, realice una conexión FTP al ordenador del puesto más cercano mediante el comando *ftp*. Por ejemplo:

```
ftp 192.168.1.25
```

8. Compruebe que está conectado y que puede ejecutar comandos FTP en el servidor. ¿En qué directorio remoto está? ¿En qué directorio local está?
9. Descargue en su ordenador el archivo creado en el apartado anterior. Edítelo y comprueba que se ha recibido sin errores.
10. Finalice la sesión FTP.

2.7.5 DNS rudimentario

Aunque el Laboratorio no dispone de un servidor DNS, se puede crear un servicio DNS rudimentario editando el fichero *etc/hosts* y escribiendo en cada línea una pareja dirección IP-nombre del equipo. Para ello, siga los pasos siguientes:

1. Desde de una consola de root, para tener privilegios de administrador, ejecute *kwrite* y abra desde el editor el fichero *etc/hosts*.
2. Escriba tres líneas en el fichero, cada una formada por la dirección IP y el nombre de un ordenador de su red.
3. Guarde el fichero.
4. Ejecute un *ping* al resto de ordenadores de la red pero utilizando el nombre en lugar de la dirección IP. ¿Cuál es el resultado?.

3. ANÁLISIS DE PROTOCOLOS

3.1 Introducción

En esta práctica se va a trabajar sobre la misma configuración de red utilizada en la práctica anterior (Figura 31) y se van a repetir los mismos ejercicios, pero en este caso observando y analizando el tráfico de paquetes que circula por la red. Para ello, conviene repasar todos los conceptos teóricos introducidos en la práctica anterior, en especial, el encapsulado y la demultiplexación de los protocolos.

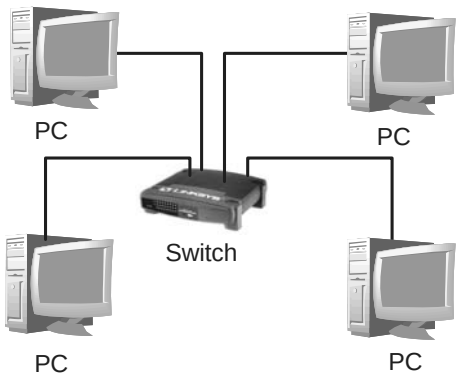


FIGURA 31. *Red de cuatro ordenadores interconectados a través de un switch.*

Para observar y analizar el tráfico en una red se utilizan herramientas que monitorizan y presentan el tráfico binario de la red en un forma inteligible para las personas. Estas herramientas se denominan analizadores de protocolos de red[4].

[4] En inglés se denominan Network Protocol Analizers o “Packet Sniffers” (“olfateadores de paquetes”).

En el laboratorio vamos a utilizar el analizador de redes Wireshark[5] que está incluido entre las aplicaciones que incorpora Knoppix.Un analizador de protocolos de red configura la interfaz de red en un modo denominado “modo promiscuo” que puede capturar todo el tráfico que circula por la red[6]. La Figura 32 muestra la arquitectura software de un analizador de protocolos de red en Linux con una tarjeta de red Ethernet. Un analizador como Wireshark se comunica con un elemento del kernel (componente central del sistema operativo) denominado “filtro socket” que puede configurar el driver de la tarjeta de Ethernet para obtener una copia de las trazas transmitidas y recibidas por ella.

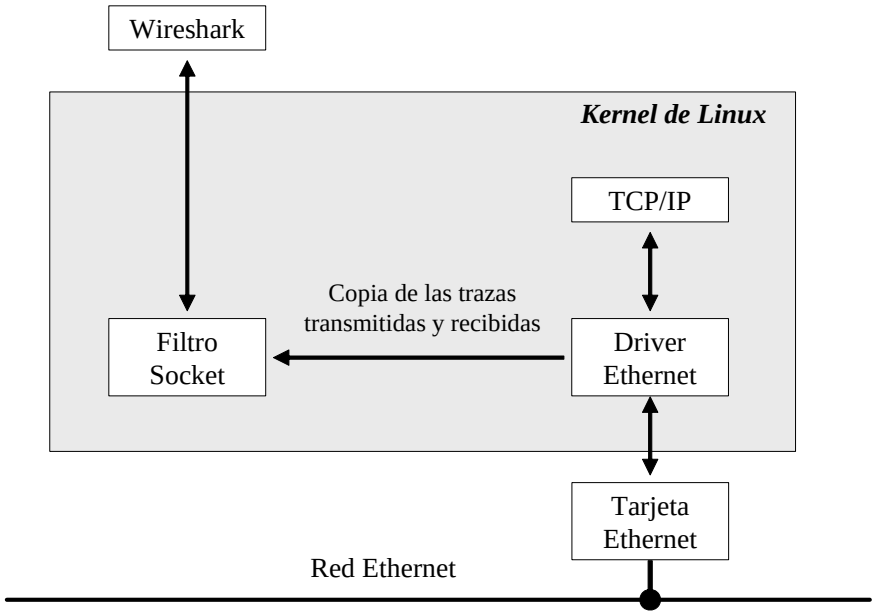


FIGURA 32. *Arquitectura software de un analizador de protocolos de red en Linux.*

[5] Puede descargarse de http://www.wireshark.org/ no sólo para Linux, sino también para otros sistemas operativos como Windows, MAC OS o Solarix.

[6] En las redes reales, por cuestiones de seguridad, no se permite a los usuarios capturar ni analizar el tráfico de una red, lo cuál suele estar restringido al administrador.

3.2 Wireshark

En este apartado se describen algunas características básicas de Wireshark que serán de utilidad para la realización de esta práctica. Cuando se ejecuta Wireshark (*Menú K → Internet → Wireshark (as root)*) y se realiza una captura de tráfico, más adelante veremos cómo hacerlo, aparece una ventana como la que se muestra en la Figura 33. La ventana está dividida en tres zonas en la que se muestra el tráfico capturado en diferentes formatos.

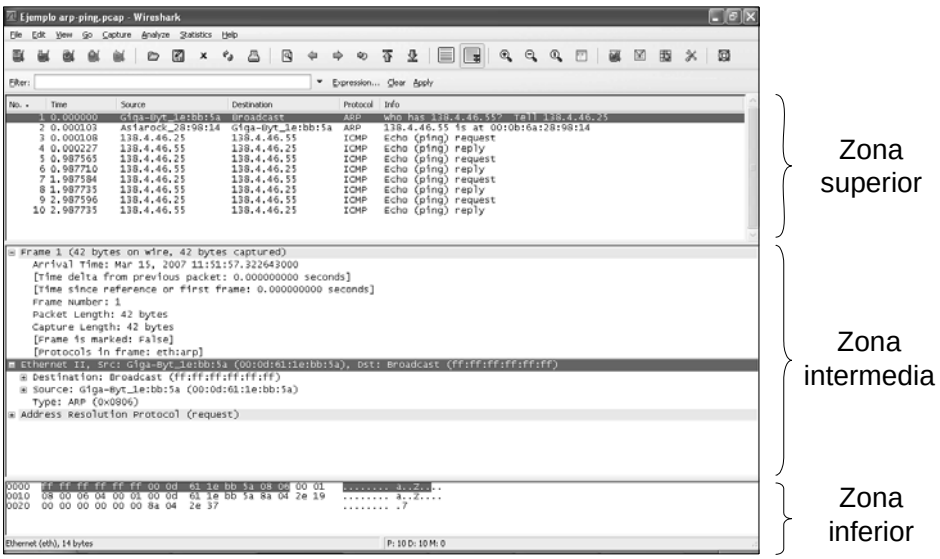


FIGURA 33. *Ventana de Wireshark.*

La zona superior muestra todos los paquetes capturados, uno por línea. Cada línea contiene el orden y el tiempo de captura, el origen y el destino del paquete, el protocolo encapsulado e información adicional. Al seleccionar un paquete, su contenido se muestra en las dos zonas siguientes.

La zona intermedia muestra los protocolos, uno por línea, del paquete seleccionado. Cada protocolo puede desplegarse pulsando sobre la pestaña de la izquierda para mostrar más información o contraerse, para ocupar una sola línea, pulsando sobre la misma pestaña.

La zona inferior muestra el contenido binario de cada traza en hexadecimal (a la izquierda) y en ASCII (a la derecha).

3.2.1 Captura de tráfico

Antes de iniciar una captura de tráfico hay que seleccionar la interfaz de red que se va a utilizar. Para ello, seleccione en el menú “Capture” que aparece la barra de superior el submenú “Options”, tal y como se representa en la Figura 34. Al hacerlo, aparecerá una ventana de opciones de captura como la de la Figura 35. Para seleccionar la interfaz, despliegue la pestaña (▼) que aparece en la primera línea (“Interface”) y elija la tarjeta Ethernet. Si lo ha hecho correctamente, en la línea siguiente (“IP address”) aparecerá la dirección IP de su ordenador.

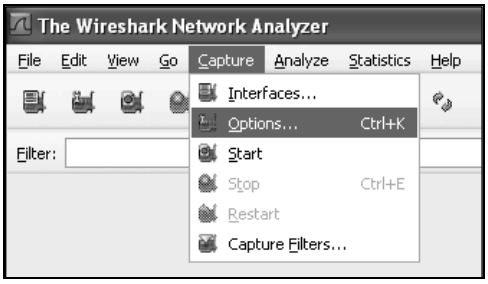


FIGURA 34. *Selección de opciones de captura.*

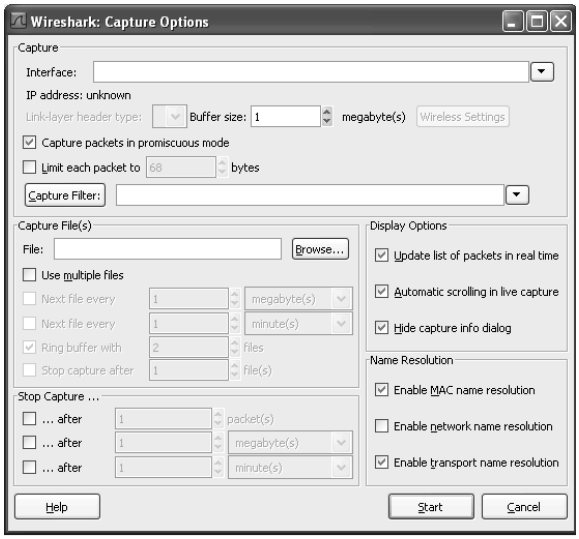


FIGURA 35. *Ventana de opciones de captura.*

Para iniciar una captura de tráfico puede seleccionar la opción “Start” del menú “Capture” (Figura 34) o de la ventana de opciones (Figura 35). Para capturar datos en el “modo promiscuo” compruebe que la opción “Capture packets in promiscuous mode” está seleccionada en la ventana de opciones. El “modo promiscuo” de funcionamiento de la tarjeta de red permite visualizar todo el tráfico que circula por la red local y no sólo aquel que va dirigido desde o hacia la interfaz Ethernet de su propio ordenador.

3.2.2 Filtros de captura

Los filtros permiten capturar sólo aquellos paquetes que tengan ciertas características, por ejemplo, los que pertenecen a una determinada aplicación. Para especificar un filtro de captura debe escribirlo en la línea en blanco que hay a la derecha del botón “Capture Filter” situado en la ventana de opciones (Figura 35). Por ejemplo, si queremos capturar el tráfico desde o hacia la dirección IP 198.168.1.25 escribiremos:

```
host 192.168.1.25
```

Pulsando sobre el botón “Capture Filter” se abrirá una ventana como la de la Figura 36 en la que pueden seleccionarse algunos filtros predefinidos en el programa o crear y guardar nuevos filtros.

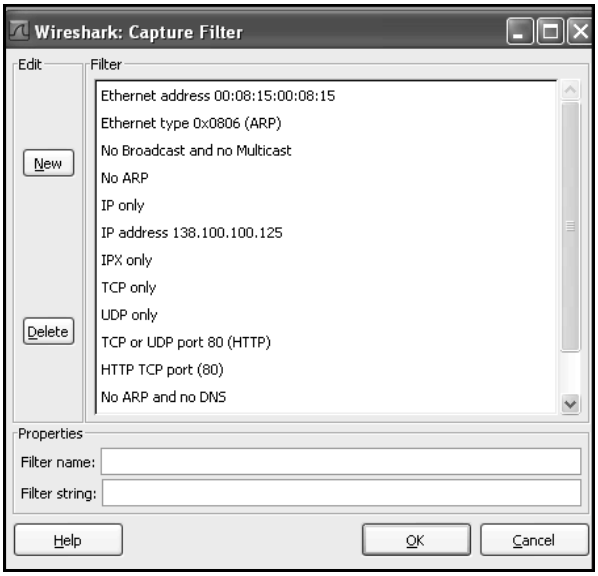


FIGURA 36. *Ventana de filtros de captura.*

Un filtro de captura está formado por una o varias expresiones unidas por las conjunciones and/or y opcionalmente precedidas por not:

```
[not] expresión [and | or [not] expresión ...]
```

La Figura 37 muestra algunas expresiones que pueden utilizarse en los filtros de captura y la Figura 38 presenta algunos ejemplos de aplicación.

Expresión	Descripción
[src|dst] host <host>	Filtrar el tráfico desde o hacia el host especificado por <host>. Opcionalmente, la expresión host puede ir precedida de src o dst, para indicar, respectivamente, que sólo se están interesado en el tráfico desde el host (source) o hacia el host (destination)
ether [src|dst] host <ehost>	Filtra el tráfico desde o hacia una dirección Ethernet. La opción src|dst tienen el significado contado anteriormente.
[tcp|udp] [src|dst] port <port>	Filtra el tráfico en el puerto (port) especificado. El archivo **/etc/services** contiene la lista los puertos que corresponde a cada aplicación). Por ejemplo, los puertos 20, 21, 22 y 23 corresponden, respectivamente a ftp-data, ftp, ssh y telnet. La opción tcp|udp permite elegir el tráfico TCP o UDP respectivamente (si se omite, se seleccionarán todos los paquetes de ambos protocolos). La opción src|dst tiene el significado contado anteriormente.
ip|ether proto <protocol>	Filtra el protocolo especificado (IP o Ethernet)

FIGURA 37. *Expresiones para los filtros de captura.*

Filtro	Descripción
host 192.168.1.10	Captura tráfico desde y hacia el host 192.168.1.10
dst host 172.18.5.4	Captura tráfico sólo hacia el host 172.18.5.4
port 21	Captura tráfico FTP
arp	Captura tráfico ARP
port 22 and host 10.0.0.5	Captura tráfico ssh desde o hacia el host 10.0.0.5

FIGURA 38. *Ejemplos de filtros de captura.*

3.2.3 Guardar una captura

Si desea guardar una captura de tráfico seleccione en el menú “File” la opción “Save as” (Figura 39) y elija el directorio de destino en el disquete o en la memoria USB. El fichero de captura se guarda con las extensiones *.pcap o *.cap de Wireshark que utilizan la mayoría de los analizadores de red. Las capturas pueden abrirse en cualquier otro ordenador que tenga instalado el programa Wireshark (hay disponible una versión para Windows).

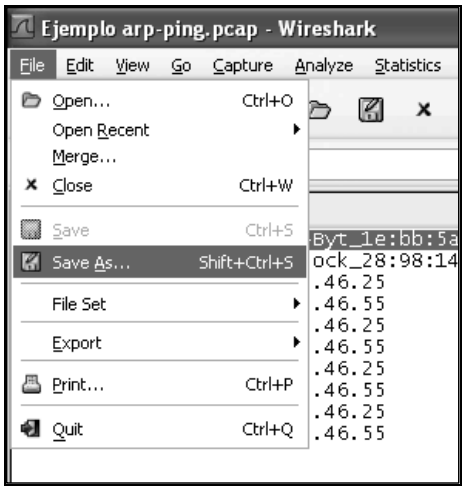


FIGURA 39. *Guardar una captura de tráfico.*

3.3 Descripción de la práctica

3.3.1 Configuración de la red

Configure en su equipo la interfaz *eth0* con la dirección IP y la máscara (/M) siguientes:

Puesto	Dirección IP /M	Puesto	Dirección IP /M	Puesto	Dirección IP /M
1	192.168.1.2 /24	5	192.168.3.2 /24	9	192.168.5.2 /24
2	192.168.1.3 /24	6	192.168.3.3 /24	10	192.168.5.3 /24
3	192.168.1.4 /24	7	192.168.3.4 /24	11	192.168.5.4 /24
4	192.168.1.5 /24	8	192.168.3.5 /24	12	192.168.5.5 /24

La tabla siguiente resume la composición y las direcciones IP de cada una de las tres redes.

Puestos	Red	Broadcast	Puerta de enlace
1 a 4	192.168.1.0	192.168.1.255	192.168.1.1
5 a 8	192.168.3.0	192.168.3.255	192.168.3.1
9 a 12	192.168.5.0	192.168.5.255	192.168.5.1

3.3.2 Modo promiscuo

1. Inicie una captura de datos asegurándose de que está habilitada la opción “Capture packets in promiscuous mode” en la ventana de opciones de captura.
2. Sin detener la captura, realice un ping a la dirección IP del ordenador situado en el puesto más cercano al suyo.
3. Detenga el ping y la captura de datos.
4. ¿Cuántas trazas ha capturado? ¿Quiénes son los remitentes y los destinatarios de esos paquetes? ¿Qué protocolos aparecen en esas trazas?.

5. Si desea conservar la captura, guárdela ahora.
6. Repita las operaciones anteriores pero deshabilitando el modo promiscuo, ¿cuál es la diferencia?. Habilite de nuevo el modo promiscuo.
7. Si desea conservar la captura, guárdela ahora.

3.3.3 Protocolo ARP

1. Examine la tabla ARP de su ordenador. Si contiene la entrada de la dirección IP a la que ha realizado el ping en el apartado anterior, bórrela:

```
arp –d 192.168.X.X
```

2. Especifique un filtro para capturar sólo las trazas con origen y destino en su propia máquina e inicie una captura de datos.
3. Sin detener la captura, ejecute la siguiente orden completando los dos últimos bytes con los de la dirección IP del ordenador contiguo al suyo:

```
ping –c1 192.168.X.X
```

4. Detenga la captura y asegúrese de que ha capturado al menos cuatro trazas, dos del protocolo ARP y dos del protocolo ICMP. Si no ha sido así, repita los pasos 1 a 3.
5. Analice la primera traza. ¿Cuál es su tamaño total en bytes? ¿Cuál es el tamaño de la cabecera de Ethernet II? ¿Cuál es la dirección MAC del destinatario? ¿Y la del remitente? ¿Qué protocolo hay encapsulado en la traza?
6. Analice el mensaje ARP encapsulado en la primera traza y rellene la siguiente tabla con los campos correspondientes:

<table>
<tr><td colspan="2">Hardware type</td><td colspan="2"></td></tr>
<tr><td colspan="2">Protocol type</td><td colspan="2"></td></tr>
<tr><td>Hardware size</td><td>Protocol size</td><td></td><td></td></tr>
<tr><td colspan="2">Operation code</td><td colspan="2"></td></tr>
<tr><td colspan="2">Sender hardware address</td><td colspan="2"></td></tr>
<tr><td colspan="2">Sender protocol address</td><td colspan="2"></td></tr>
<tr><td colspan="2">Target hardware address</td><td colspan="2"></td></tr>
<tr><td colspan="2">Target protocol address</td><td colspan="2"></td></tr>
</table>

7. ¿Cuál es el tamaño del mensaje ARP del apartado anterior en bytes? ¿Se trata de un mensaje de petición o de una respuesta ARP? ¿En qué campo del mensaje se especifica el tipo de mensaje?
8. Analice el mensaje ARP encapsulado en la segunda traza capturada. ¿Se trata de una petición o de una respuesta ARP? ¿Quién es el remitente del paquete? ¿Y el destinatario? ¿Qué información contiene?
9. ¿Por qué los mensajes ARP no tienen cabecera IP?

3.3.4 Protocolo ICMP

1. Analice la tercera traza de la captura realizada en el apartado 3.3.3.
2. ¿Cuál es la versión del protocolo IP? ¿Cuál es el tamaño total de la traza en bytes? ¿Cuál es el tamaño de la cabecera IP en bytes? ¿Y del datagrama IP completo?
3. ¿ A qué protocolo pertenece el mensaje encapsulado en el datagrama IP? ¿Qué tipo de mensaje es? ¿Quién es el remitente? ¿Cuántos bytes ocupa?. Rellene la tabla con los campos indicados:

Type	
Code	

4. Analice la cuarta traza de la captura realizada en el apartado 3.3.3.
5. ¿A qué protocolo pertenece el mensaje encapsulado en la traza? ¿Qué tipo de mensaje es? ¿Quién es el remitente? Rellene la tabla con los campos indicados:

Type	
Code	

6. Si desea conservar la captura, guárdela ahora.

3.3.5 Sesión ssh

1. Active el servidor SSH en su ordenador y establezca redes como contraseña del usuario knoppix.
2. ¿Cuál es el puerto del protocolo SSH?
3. Inicie una captura de datos usando un filtro que capture únicamente tráfico SSH desde o hacia su ordenador. Sin detener la captura, inicie una conexión remota al ordenador contiguo al suyo . Por ejemplo:

```
ssh knoppix@192.168.1.2
```

4. Detenga la captura de datos y finalice la sesión remota.
5. Examine las trazas enviadas desde su ordenador.
6. ¿Encuentra la clave que ha introducido para iniciar la sesión remota? ¿Por qué?
7. Si desea conservar la captura, guárdela ahora.

3.3.6 Sesión ftp

1. Active el servidor FTP en su ordenador siguiendo los pasos siguientes:
2. Ejecute en una consola de root la siguiente línea:

```
in.ftpd -D
```

3. Ejecute, desde una consola de root, el editor *Kwrite* y edite el archivo:

```
/etc/hosts.allow
```

4. Escriba en el archivo anterior, antes de la última línea, la siguiente:

```
ftp in.ftpd : ALL@ALL : ALLOW
```

5. Guarde el archivo.
6. Asigne la contraseña redes al usuario knoppix ejecutando desde la consola de root la siguiente orden:

```
passwd knoppix
```

7. Edite un archivo de texto, escriba en él una frase cualquiera y guárdelo en el directorio:

```
/ramdisk/home/knoppix
```

con el nombre mensajeX.txt, donde X es su número de puesto en el laboratorio.

8. ¿Cuál es el puerto del protocolo FTP?
9. Inicie una nueva captura de datos usando un filtro que capture únicamente paquetes FTP desde o hacia su ordenador. Realice una conexión FTP al ordenador del puesto contiguo al suyo. Por ejemplo:

```
ftp 192.168.1.2
```

10. Detenga la captura de datos pero no finalice la conexión FTP.
11. Analice las trazas capturadas que han sido enviadas desde su ordenador para establecer la conexión. ¿Encuentra el nombre de usuario y la clave que ha introducido para iniciar la conexión FTP? ¿Por qué?
12. Si desea conservar la captura, guárdela ahora.
13. ¿Cuál es el puerto del protocolo FTP-DATA?
14. Inicie una nueva captura de datos usando un filtro que capture únicamente paquetes FTP-DATA desde el servidor FTP hacia su ordenador.
15. Descargue el archivo mensajeX.txt que encontrará en el directorio remoto del servidor ejecutando la siguiente orden:

```
get mensajeX.txt
```

16. Finalice la sesión FTP y luego detenga la captura de datos.
17. Edite el archivo mensajeX.txt descargado en su ordenador y compruebe su contenido.
18. Observe si entre las trazas capturadas existe alguna que contenga los datos del archivo descargado. ¿Por qué puede ver el contenido del archivo? ¿Qué puertos utiliza el protocolo TCP para el servidor y el cliente de FTP-DATA?.
19. Si desea conservar la captura, guárdela ahora.

4. ENRUTAMIENTO ESTÁTICO

4.1 Introducción

Esta práctica se va a trabajar con la topología de red representada en la Figura 40. La red está dividida en cinco redes: las tres redes Ethernet LAN utilizadas en las prácticas anteriores (192.168.1.0, 192.168.3.0 y 192.168.5.0) y dos redes WAN (192.168.2.0 y 192.168.4.0) que interconectan las tres primeras a través de las interfaces serie de los routers R1, R2, R3 y R4.

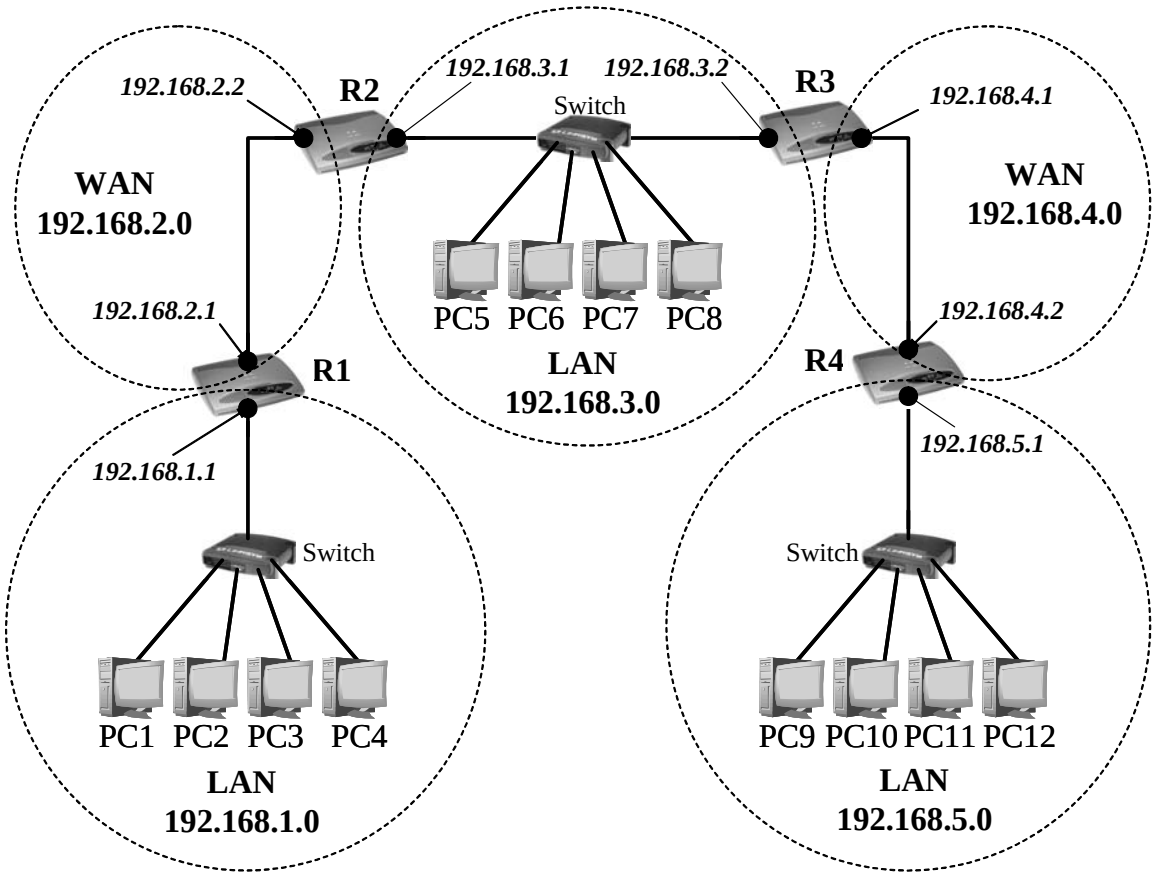


FIGURA 40. *Topología de la red del laboratorio.*

La composición de cada una de las cinco redes anteriores (clase C /24) es la siguiente:

- La red 192.168.1.0 está formada por los ordenadores de los puestos 1 al 4 del laboratorio, un switch, y el router R1 conectado a través de su interfaz Ethernet.
- La red 192.168.2.0 está formada por los routers R1 y R2 conectados a través de sus interfaces serie.
- La red 192.168.3.0 está formada por los ordenadores de los puestos 5 a 8 del laboratorio, un switch, y los routers R2 y R3 conectados a través de sus interfaces Ethernet.
- La red 192.168.4.0 está formada por los routers R3 y R4 conectados a través de su interfaces serie.
- La red 192.168.5.0 está formada por los ordenadores de los puestos 9 a 12 del laboratorio, un switch, y el router R4 conectado a través de su interfaz Ethernet.

En los apartados siguientes se repasan algunos conceptos básicos de enrutamiento IP y realiza una pequeña introducción al sistema operativo CISCO IOS en la que se describen los modos de configuración y comandos más comunes que se utilizarán a lo largo de esta práctica y de la siguiente.

4.2 Enrutamiento IP

El enrutamiento IP es un concepto relativamente simple. Cuando un equipo tiene que envíar una traza a otro, primero comprueba si la dirección IP del destinatario pertenece a su propia red y, si es el caso, le envía la traza directamente (así es como se han transmitido las trazas en las prácticas anteriores). Sin embargo, si la dirección IP de destino pertenece a una red distinta, el equipo se limita simplemente a enviar la traza a su puerta de enlace, que en nuestro caso es un router que dispone de dos interfaces de red (un router debe tener al menos dos interfaces para interconectar dos redes, aunque puede tener más). Para poder enviarle la traza, el equipo remitente debe

conocer la dirección MAC del router, una misión de la que se encarga, como ya es sabido, el protocolo ARP.

Una vez que el router recibe la traza, la demultiplexa y extrae la dirección IP de la red de destino. A continuación, el router examina su tabla de rutas para decidir dónde tiene que reenviar los datos. Cada ruta de esta tabla está compuesta por las direcciones IP de una red de destino y de próximo salto. La dirección de próximo salto es la dirección de otro equipo conectado en la misma red a través del cuál se puede acceder a esa red. Por ejemplo, con la topología de red de la Figura 40, el router R2 tendría la siguiente tabla de rutas:

Red de destino	Próximo salto
192.168.1.0 /24	R1
192.168.2.0 /24	Directo
192.168.3.0 /24	Directo
192.168.4.0 /24	R3
192.168.5.0 /24	R3

FIGURA 41. *Tabla de rutas del router R2.*

Si al buscar en la tabla el router encuentra una ruta con la red del destinatario pueden ocurrir dos casos. Primero, que esa red esté conectada al router, en cuyo caso no hay próximo salto (próximo salto indicado con la palabra “Directo” en la tabla de la Figura 41) y el router envía directamente los datos al equipo destinatario. Segundo, que el router no pertenezca a la red de destino, en cuyo caso reenviará el paquete a la dirección de próximo salto, normalmente a otro router. Y así, salto a salto, hasta que los datos llegan a un router que pertenece a la red de destino y que puede enviar directamente los datos al equipo destinatario.

En la red de la Figura 40 es fácil determinar cuál es el número de saltos que tiene que dar un paquete desde el origen hasta el destino. Por ejemplo, desde el PC1 hasta el PC12 daría 5 saltos (PC1 a R1, R1 a R2, R2 a R3, R3 a R4 y R4 a PC12)[7]. En cada salto, el router correspondiente demultiplexa el

[7] Normalmente, el número de saltos hace referencia al número de routers por los que

paquete, comprueba la dirección IP y lo encapsula de nuevo en una traza que contiene la dirección MAC del próximo salto. En general, en una red más compleja como Internet existen varios caminos para llegar al mismo destino y se desconoce cuál es el número de saltos que dará un paquete.

La tabla de rutas puede crearse utilizando, básicamente, dos mecanismos: enrutamiento estático o dinámico. El primer mecanismo es el que vamos a utilizar en esta práctica y consiste en crear la tabla de rutas de forma manual, para lo cuál es necesario que la topología de la red sea conocida previamente. Este tipo de enrutamiento suele utilizarse en sistemas pequeños y que cambian lentamente. En cambio, en el enrutamiento dinámico las rutas se crean de forma automática mediante el intercambio de información entre los routers mediante un protocolo de comunicación, por ejemplo, el protocolo RIP (Router Information Protocol). Este segundo tipo de enrutamiento será el objeto de la práctica siguiente.

Para que la red de la Figura 40 funcione correctamente, es necesario que cada router tenga completa su correspondiente tabla de rutas. El contenido de las tablas de rutas de los routers R1, R3 y R4 está indicado en la Figura 42.

Router R1		Router R3		Router R4	
Red de destino	Próximo salto	Red de destino	Próximo salto	Red de destino	Próximo salto
192.168.1.0 /24	Directo	192.168.1.0 /24	R2	192.168.1.0 /24	R3
192.168.2.0 /24	Directo	192.168.2.0 /24	R2	192.168.2.0 /24	R3
192.168.3.0 /24	R2	192.168.3.0 /24	Directo	192.168.3.0 /24	R3
192.168.4.0 /24	R2	192.168.4.0 /24	Directo	192.168.4.0 /24	Directo
192.168.5.0 /24	R2	192.168.5.0 /24	R4	192.168.5.0 /24	Directo

FIGURA 42. *Tablas de rutas de los routers R1, R3 y R4.*

pasan los datos hasta alcanzar su destino. Siguiendo con el ejemplo, utilizando este convenio se diría que el número de saltos es 4 y no 5.

4.3 Sistema operativo CISCO IOS

Un router CISCO es un ordenador especializado que ejecuta su propio sistema operativo denominado CISCO Internet Operating System (CISCO IOS). Este sistema operativo, propiedad de la empresa CISCO, está almacenado en una memoria flash PCMCIA insertada en el panel posterior del router (el router no tiene disco duro). Al arrancar el router, el sistema operativo se carga en una memoria DRAM (Dynamic Random Access Memory) desde donde se ejecuta.

Para acceder al router por primera vez, hay que hacerlo a través del puerto de consola, que es un puerto serie asíncrono que permite enviar y recibir caracteres ASCII. A este puerto se puede conectar un ordenador (usando un cable RJ-45 a DB-9) que disponga de un puerto serie RS-232 y de un programa de emulación de terminal, como *HyperTerminal* de Windows o *kermit* de Linux, que se encarga de enviar comandos al router y de mostrar la respuesta de éste en la pantalla del ordenador. Este método de acceso se ha utilizado para configurar las interfaces Ethernet de los routers con las direcciones indicadas en la tabla de la Figura 43. A cada router se le ha asignado, como es habitual, la primera dirección disponible de la red Ethernet a la que está conectado (192.168.X.1), salvo al router R3, que pertenece a la misma red que R2 (la 192.168.3.0) y al que se la ha asignado la siguiente (192.168.3.2).

Router	Dirección IP /máscara
R1	192.168.1.1 /24
R2	192.168.3.1 /24
R3	192.168.3.2 /24
R4	192.168.5.1 /24

FIGURA 43. *Direcciones IP asignadas a las interfaces Ethernet de los routers.*

Una vez configuradas estas direcciones IP, también se puede acceder a los routers, y así es como lo vamos a hacer en el Laboratorio, a través de la aplicación telnet. Por ejemplo, para acceder al router R1 desde el PC1 habría que ejecutar desde la consola de Knoppix la siguiente línea de comandos:

```
telnet 192.168.1.1
```

Una vez establecida la conexión, para lo cuál hay que introducir una contraseña (**redes3**), aparecerá una línea de comandos de CISCO IOS con el siguiente prompt:

```
R1>
```

El símbolo **>** que aparece después del nombre del router indica que se pueden ejecutar comandos en el *Modo de usuario*. A diferencia de Linux, la línea de comandos de CISCO IOS tiene varios modos de ejecución en los que sólo se pueden utilizar sólo determinados comandos. En total, hay cientos de comandos y muchos de ellos tienen numerosas opciones. Sin embargo, para los propósitos del Laboratorio sólo es necesario conocer algunos de ellos. Hay dos modos de ejecución básicos denominados *Modo de usuario* y *Modo de administrador*. Además, desde este último modo se puede acceder a otros tres modos denominados *Modo de configuración global*, *Modo de configuración de interfaz* y *Modo de configuración de router*. Cada uno de los modos se puede identificar porque el prompt de cada uno de ellos es distinto (Figura 44). En cada uno de los modos puede obtenerse una lista de los comandos disponibles tecleando el signo de interrogación (?). Por ejemplo, para el *Modo de usuario*:

```
R1>?
```

Modo de operación	Prompt de la línea de comandos
Usuario	R1>
Administrador	R1#
Configuración global	R1(config)#
Configuración de interfaz	R1(config-if)#
Configuración de router	R1(config-router)#

FIGURA 44. *Prompt de los diferentes modos de ejecución de CISCO IOS suponiendo que el nombre del router es R1.*

La Figura 45 resume las transiciones entre los cinco modos de ejecución de CISCO IOS. A continuación se detallan las funciones cada uno de estos modos y algunos de los comandos disponibles, en particular, los que se utilizan para realizar la transición de un modo a otro.

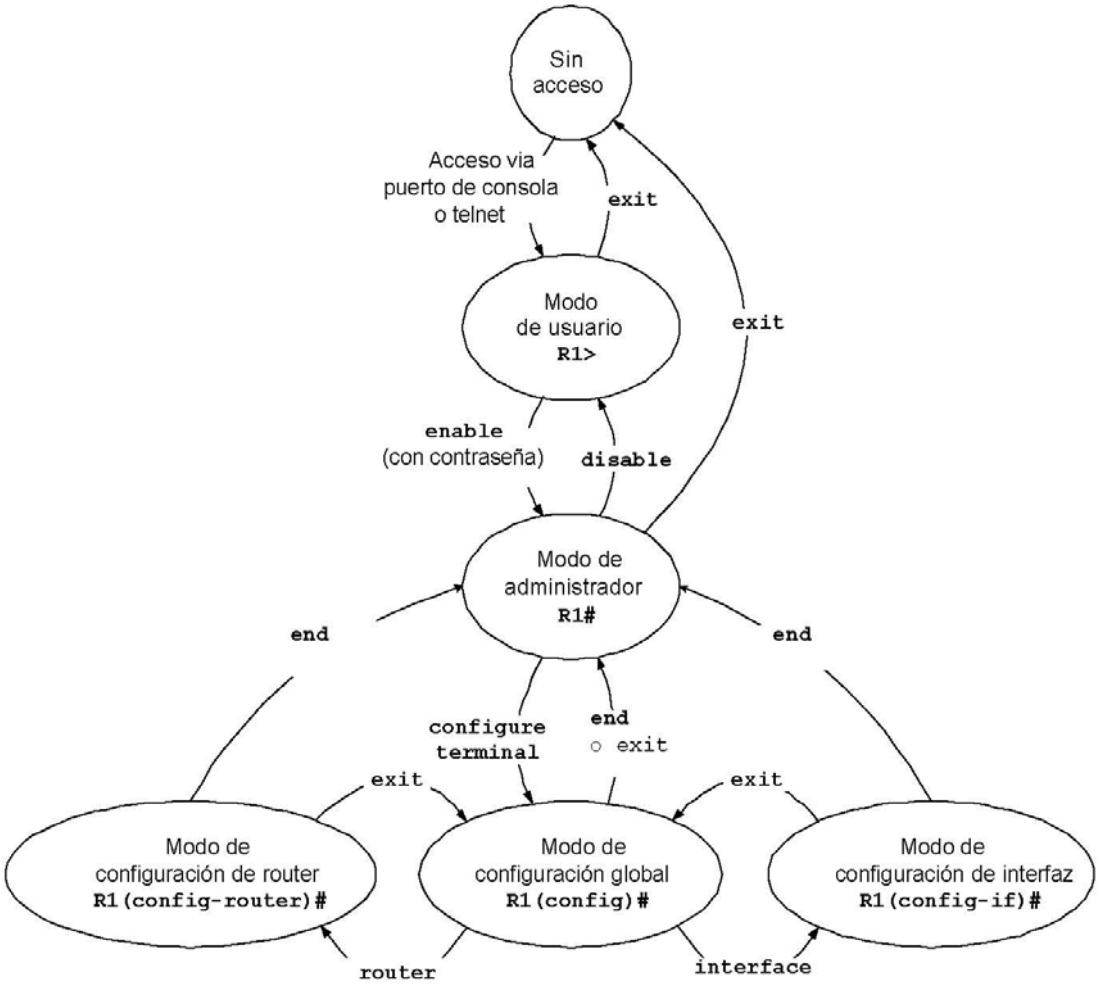


FIGURA 45. *Modos de ejecución de comandos en CISCO IOS*[8].

4.3.1 Modo usuario (EXEC)

En el *Modo de usuario* se pueden ejecutar una serie limitada de comandos (*ping*, *traceroute*, etc.) pero no se puede modificar la configuración del router, por ejemplo, para asignarle una dirección IP. A este modo se accede directamente cuando se realiza una conexión al router a través del puerto de consola o usando la aplicación telnet (en este último caso, siempre es necesario introducir una contraseña). Algunos de los comandos disponibles en el *Modo de usuario* son los siguientes:

[8] Adaptado del libro "Mastering Networks: An Internet Lab Manual". J. Liebeherr, M. El Zarki. Addison-Wesley. 2004

enable

Acceso al Modo de administrador.

exit

Finaliza la conexión con el router.

ping

Envía mensajes de petición de eco.

show

Muestra información del sistema.

Ejemplo:

show version Información no privilegiada de hardware y software

traceroute

Traza una ruta hasta un destino (número de saltos).

Ejemplo:

traceroute 192.168.1.4

Para obtener la lista completa de comandos, hay que escribir el signo de interrogación ? en la línea de comandos. Por ejemplo:

```
R1>?
Exec commands:
 <1-99>          Session number to resume
access-enable    Create a temporary Access-List entry
access-profile   Apply user-profile to interface
clear            Reset functions
connect          Open a terminal connection
...
```

Para obtener información adicional sobre las opciones de un comando en cualquiera de los modos se teclea el nombre del comando seguido del signo ?. Por ejemplo:

```
R1>show ?
backup           Backup status
clock            Display the system clock
...
```

4.3.2 Modo de administrador

El *Modo de administrador* permite ver o cambiar la configuración del router. Para acceder a este modo desde el *Modo de usuario* hay que ejecutar el comando *enable* e introducir una contraseña (**redes1**):

```
R1>enable
Password: redes1
R1#
```

Algunos de los comandos disponibles en el *Modo de administrador* son los siguientes:

```
configure
   Opciones de configuración.
      Ejemplo:
         configure terminal        Accede al Modo de configuración global
clear ip route *
   Borra la tabla de rutas.
disable
   Retorna al Modo de usuario.
exit
   Finaliza la conexión con el router.
ping
   Envía mensajes de petición de eco.
reload
   Reinicia el sistema.
show
   Muestra información privilegiada del sistema.
      Ejemplos:
         show interfaces        Información de las interfaces
         show ip arp            Muestra la tabla ARP
         show ip route          Muestra la tabla de rutas
         show protocols         Información IP y enrutamiento
         show running-config    Configuración actual del sistema
         show startup-config    Configuración de arranque del sistema
```

Los archivos *running-config* y *startup-config* contienen información sobre las configuraciones actual e inicial del sistema, respectivamente. El archivo *startup-config* contiene la secuencia de comandos de CISCO IOS que se ejecutan al arrancar o reiniciar el sistema.

Cuando el router arranca, la información del archivo *startup-config* se copia en el archivo *running-config*, en el cuál se irán reflejando los cambios que se vayan realizando en la configuración. Si se desea que estos cambios no desaparezcan al reiniciar el sistema operativo, habría que guardar el contenido actual del archivo *running-config* en el archivo *startup-config*.

4.3.3 Modo de configuración global

El *Modo de configuración global* permite cambiar parámetros de configuración del router y sirve de puerta de acceso a los modos de configuración de las interfaces y de los protocolos de enrutamiento que se describen en los dos apartados siguientes. Para acceder a este modo desde el *Modo de administrador* hay que ejecutar el siguiente comando:

```
R1#configure terminal
R1(config)#
```

La opción *terminal* del comando *configure* indica al router que la configuración se va a realizar desde la consola. Existen otras alternativas para configurar el router, por ejemplo, cargando un archivo de configuración o transfiriéndolo desde un equipo remoto.

Algunos de los comandos disponibles en este modo son los siguientes:

end

Regresa al Modo de administrador.

exit

Regresa al Modo de administrador.

interface

Accede al Modo de configuración de la interfaz seleccionada.

```
      Ejemplos:
         interface Ethernet 0
         interface Serial 0
ip
   Configuración IP.
      Ejemplos:
         ip route          Establece una ruta estática
         ip routing        Habilita el enrutamiento IP
no
   Niega un comando.
      Ejemplo:
         no ip routing     Deshabilita el enrutamiento IP
router
   Selecciona un protocolo de enrutamiento para configurarlo.
      Ejemplo:
         router rip        Selecciona el protocolo RIP
```

Por ejemplo, para habilitar el enrutamiento IP en el router R3 y añadir a la tabla de rutas la red de destino 192.168.5.0 /24 con dirección de próximo salto 192.168.4.2 (que es la dirección IP de la interfaz serie del router R4) ejecutaríamos la siguiente secuencia de comandos partiendo del *Modo de usuario*:

```
R3>enable
Password: redes1
R3#configure terminal
R3(config)#ip routing
R3(config)#ip route 192.168.5.0  255.255.255.0  192.168.4.2
```

Si ahora regresamos al *Modo de administrador* y observamos el contenido de la tabla de rutas aparerá una entrada con la ruta estática que se acaba de añadir marcada con el código S (Static):

```
R3(config)#exit
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o – ODR

S    192.168.5.0/24 [120/1] via 192.168.4.2, 00:00:10, Ethernet0
C    192.168.3.0/24 is directly connected, Ethernet0
C    192.168.4.0/24 is directly connected, Serial0
```

Además de la ruta estática aparecen otras dos rutas con el código C (Connected) que son las dos redes a las que el router R3 está conectado a través de sus interfaces Ethernet0 y Serial0, las cuáles se añaden a la tabla de forma automática.

4.3.4 Modo de configuración de interfaz

El *Modo de configuración de interfaz* se utiliza para configurar una interfaz del router, por ejemplo, para asignarle una dirección IP. Para acceder a este modo desde el *Modo de configuración global* hay que ejecutar el comando *interface* seguido del nombre de la interfaz que se desea configurar, por ejemplo:

```
R1(config)#interface Serial 0
R1(config-if)#
```

Algunos de los comandos disponibles para configurar las interfaces de red son los siguientes:

clock

Configura el reloj de la interfaz serie, en bits por segundo.

Ejemplo:

clock rate 4800

encapsulation

Tipo de encapsulado para la interfaz serie.

Ejemplo:

encapsulation hdlc Encapsulado hdlc (High Level Data Link)

ip

Comandos de configuración de IP.

Ejemplo:

ip address dirección_IP máscara Asignación de dirección IP

no

Niega un comando (ejecuta lo contrario al comando).

Ejemplo:

no shutdown Habilita la interfaz seleccionada

shutdown

Deshabilita la interfaz seleccionada.

Por ejemplo para asignar la dirección IP 192.168.2.1/24 a la interfaz serie del router R1 ejecutaríamos la siguiente secuencia de comandos partiendo del *Modo de usuario* y regresando, después de configurar la interfaz, al *Modo de administrador*:

```
R1>enable
Password: redes1
R1#configure terminal
R1(config)#interface serial 0
R1(config-if)#ip address 192.168.2.1 255.255.255.0
R1(config-if)#encapsulation hdlc
R1(config-if)#clock rate 4800
R1(config-if)#no shutdown
R1(config-if)#end
R1#
```

4.3.5 Modo de configuración de router

El *Modo de configuración de router* se utiliza para establecer o modificar los parámetros de un determinado protocolo de enrutamiento. Para poder acceder a este modo, primero hay que habilitar el enrutamiento IP en el router desde el *Modo de configuración global*:

```
R1(config)#ip routing
```

Y seleccionar luego el protocolo deseado. Por ejemplo, si se selecciona el protocolo RIP (Router Information Protocol):

```
R1(config)#router rip
R1(config-router)#
```

Algunos de los comandos que se pueden ejecutar en este modo con el protocolo RIP son los siguientes:

exit

Sale del modo de configuración del router.

network

Habilita el protocolo RIP en una red IP.

Ejemplo:

network 192.168.4.0

no

Niega un comando.

Ejemplo:

no network 192.168.4.0

version

Cambia la versión del protocolo RIP.

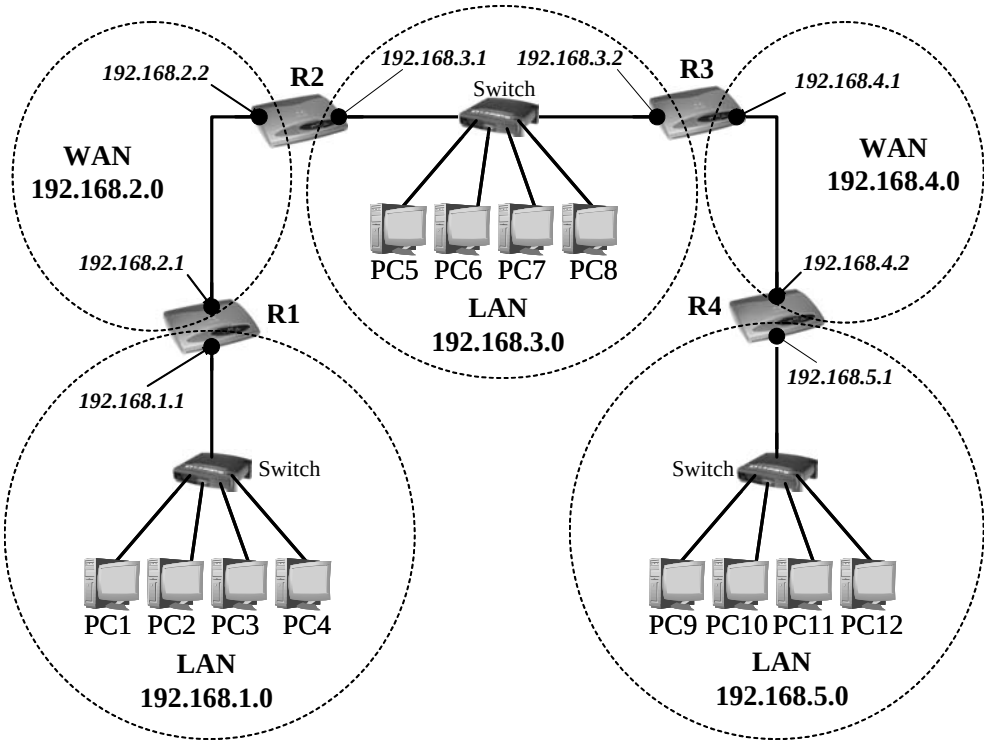
Ejemplo:

version 2 Cambia a RIPv2

4.4 Descripción de la práctica

4.4.1 Configuración de la red

La topología de red que se va a utilizar es la que se ha descrito en la introducción de esta práctica y se presenta de nuevo en la Figura 46 junto a las cuatro tablas de rutas.



Red de destino	Próximo salto
192.168.1.0/24	Directo
192.168.2.0/24	Directo
192.168.3.0/24	R2
192.168.4.0/24	R2
192.168.5.0/24	R2

Tabla de rutas de R1

Red de destino	Próximo salto
192.168.1.0/24	R1
192.168.2.0/24	Directo
192.168.3.0/24	Directo
192.168.4.0/24	R3
192.168.5.0/24	R3

Tabla de rutas de R2

Red de destino	Próximo salto
192.168.1.0/24	R2
192.168.2.0/24	R2
192.168.3.0/24	Directo
192.168.4.0/24	Directo
192.168.5.0/24	R4

Tabla de rutas de R3

Red de destino	Próximo salto
192.168.1.0/24	R3
192.168.2.0/24	R3
192.168.3.0/24	R3
192.168.4.0/24	Directo
192.168.5.0/24	Directo

Tabla de rutas de R4

FIGURA 46. *Topología de la red del laboratorio y tablas de rutas.*

En primer lugar, configure la interfaz Ethernet de su equipo con la dirección IP y la máscara indicadas en la tabla siguiente (ATENCIÓN: las direcciones IP de la red 192.168.3.0 empiezan en la 192.168.3.3):

Puesto	Dirección IP /M	Puesto	Dirección IP /M	Puesto	Dirección IP /M
1	192.168.1.2 /24	5	192.168.3.3 /24	9	192.168.5.2 /24
2	192.168.1.3 /24	6	192.168.3.4 /24	10	192.168.5.3 /24
3	192.168.1.4 /24	7	192.168.3.5 /24	11	192.168.5.4 /24
4	192.168.1.5 /24	8	192.168.3.6 /24	12	192.168.5.5 /24

FIGURA 47. *Direcciones IP de la interfaz Ethernet0 de los ordenadores.*

Cada grupo de cuatro ordenadores pertenece a una misma red en la que se ha reservado la primera dirección disponible de la red para el router, excepto en la red 192.168.3.0 en la que se han reservado las dos primeras para los routers R2 y R3.

Una vez configurada la IP de su ordenador, compruebe la conectividad de todos los ordenadores y routers de su propia red. La tabla siguiente indica las direcciones IP de las interfaces de cada router.

Router	Interfaz Ethernet 0	Interfaz Serial 0
R1	192.168.1.1 /24	192.168.2.1 /24
R2	192.168.3.1 /24	192.168.2.2 /24
R3	192.168.3.2 /24	192.168.4.1 /24
R4	192.168.5.1 /24	192.168.4.2 /24

FIGURA 48. *Direcciones IP de las interfaces Ethernet0 y Serial0 de los routers.*

4.4.2 Configuración de los routers en CISCO IOS

1. Acceda a su router vía telnet. Por ejemplo:

```
telnet 192.168.1.1
Password: redes3
R1>
```

IMPORTANTE: En el caso de la red 192.168.3.0, los puestos 5 y 6 accederán al router R2, y los puestos 7 y 8 al router R3.

2. Examine los comandos disponibles en el Modo de usuario. Liste las opciones disponibles para el comando *show*.
3. Examine la versión del hardware y software del router. ¿Cuál es la versión de CISCO IOS? ¿Cuántos interfaces tiene el router?
4. ¿Cuánta memoria DRAM tiene el router? ¿Cuál es el tamaño de la tarjeta flash PCMCIA?
5. Acceda al modo administrador:

```
R1>enable
Password: redes1
R1#
```

6. Examine los comandos disponibles en el Modo de administrador.
7. Liste las opciones disponibles para el comando *show* (aunque el nombre del comando es el mismo, las opciones son distintas a las disponibles en el Modo de usuario).
8. Examine el contenido del archivo *running-config* usando el comando show. ¿Cuál es el nombre de las interfaces disponibles en el router? ¿Cuál es la dirección IP y la máscara de subred de la interfaz Ethernet0?
9. Si se está realizando una modificación en la configuración del router y debido a una pérdida del suministro eléctrico se apaga el equipo. ¿Qué configuración se carga después de reiniciarlo? ¿Por qué?
10. Examine las interfaces del router utilizando el comando show.

11. ¿ Cuál es el MTU (Maximum Transmission Unit) de las interfaces? ¿Qué tipo de encapsulado utiliza la interfaz serie?
12. Liste las opciones del comando *configure* y acceda al modo de configuración global:

```
R1#configure terminal
R1(config)#
```

13. Liste los comandos disponibles en este modo.
14. Examine las opciones del comando *ip* y habilite el enrutamiento ip.
15. Examine las opciones del comando *interface* y acceda al Modo de configuración de la interfaz serie.
16. Configure la interfaz serie del router con la dirección IP indicada en la tabla de la Figura 48. Para ello, siga los pasos indicados en el último ejemplo del apartado 4.3.4 particularizándolo para su propio router.
17. Regrese al Modo de administrador y examine el estado de la interfaz serie. Compruebe que la dirección IP está bien configurada y que la interfaz está habilitada (“up”).
18. Finalice la sesión con el router y desde su ordenador compruebe la conectividad del resto de ordenadores del laboratorio, ¿cuáles responden?.
19. ¿Cuál es la dirección MAC de la interfaz Ethernet de su router? ¿Cómo la ha descubierto?

4.4.3 Enrutamiento estático

1. Conéctese de nuevo a su router vía telnet usando la aplicación “Terminal Console”.
2. Examine la tabla de rutas utilizando el comando show en el Modo de administrador. ¿Qué rutas aparecen? ¿De qué tipo son?
3. Examine la tabla de rutas que debería tener su router (Figura 46, página 73).
4. ¿Cuántas rutas faltan en su router? ¿En total, cuántas tiene que haber en cada router para que la red de la Figura 46 esté completamente operativa?
5. Complete las direcciones IP de próximo salto de todas las rutas de la tabla siguiente (las dos redes de destino que están directamente conectadas a cada uno de los routers se han omitido):

Router	Red	Dirección IP del próximo salto
R1	192.168.3.0 /24 192.168.4.0 /24 192.168.5.0 /24	
R2	192.168.1.0 /24 192.168.4.0 /24 192.168.5.0 /24	
R3	192.168.1.0 /24 192.168.2.0 /24 192.168.5.0 /24	
R4	192.168.1.0 /24 192.168.2.0 /24 192.168.3.0 /24	

6. Acceda al Modo de configuración global y añada manualmente a su router las rutas de la tabla anterior, una por una, utilizando el comando ip.
7. Regrese al Modo de administrador y examine de nuevo la tabla de rutas. ¿Aparecen las rutas que faltaban? ¿De qué tipo son?

8. Si la tabla está completa, guarde su contenido en un archivo de texto para elaborar la memoria de la práctica.
9. Termine la sesión con el router y compruebe desde su ordenador la conectividad de todos los routers y de todos los ordenadores del laboratorio.
10. Examine en la tabla ARP de su ordenador las direcciones MAC asociadas a las direcciones IP pertenecientes a otras redes. ¿A qué equipo pertenece esa MAC? ¿Por qué?
11. Examine la topología de la red de la Figura 46 (página 73) ¿Cuál es el máximo número de saltos desde un ordenador del laboratorio hasta otro?
12. ¿Y desde su ordenador, cuál es número máximo de saltos que dará un paquete? Compruébelo trazando una ruta desde su ordenador hasta uno de los ordenadores de la red más lejana. Para ello, utilize el comando traceroute (disponible tanto en CISCO IOS como en Linux) seguido de la dirección IP de destino. Por ejemplo:

```
traceroute 192.168.1.4
```

13. Guarde la ruta trazada en un archivo de texto para elaborar la memoria de la práctica.
14. ¿Qué ventajas o desventajas cree que tiene el enrutamiento estático?

5. ENRUTAMIENTO DINÁMICO

5.1 Introducción

En la práctica anterior se han repasado algunos conceptos básicos del enrutamiento IP y se ha configurado la tabla de rutas utilizando enrutamiento estático. Este mecanismo permite al administrador de la red crear y modificar la tabla de rutas de forma manual ejecutando, en el caso de sistema operativo CISCO IOS, el comando *ip route* desde el *Modo de configuración global*. La Figura 49 muestra la topología de la red que se va utilizar en esta práctica y que es idéntica a la de la práctica anterior.

La Figura 50 muestra las tablas de rutas de los cuatro routers de la red anterior. Cada tabla dispone de cinco rutas, una por cada una de las cinco redes existentes. Cada ruta de la tabla está compuesta por la dirección IP de la red de destino seguida de la dirección IP del próximo salto, que pertenece a la interfaz de un router vecino conectado en la misma red del router al que pertenece la tabla. Cuando un router recibe un paquete, examina la dirección IP de la red destino y busca en su tabla de rutas la dirección IP de próximo salto a la cuál hay que enviar el paquete.

En el caso de que la red destino esté directamente conectada a una de las interfaces del router, no hay próximo salto y el router envía el paquete al equipo destinatario. De las cinco rutas que contiene la tabla, las dos rutas de las redes de destino que están directamente conectadas al router se añaden de forma automática y no tienen dirección de próximo salto (rutas en las que figura la palabra “directo” como dirección IP de próximo salto). Por tanto, para completar la tabla sólo hay que añadir las tres rutas restantes, tal y como se ha hecho en la práctica anterior.

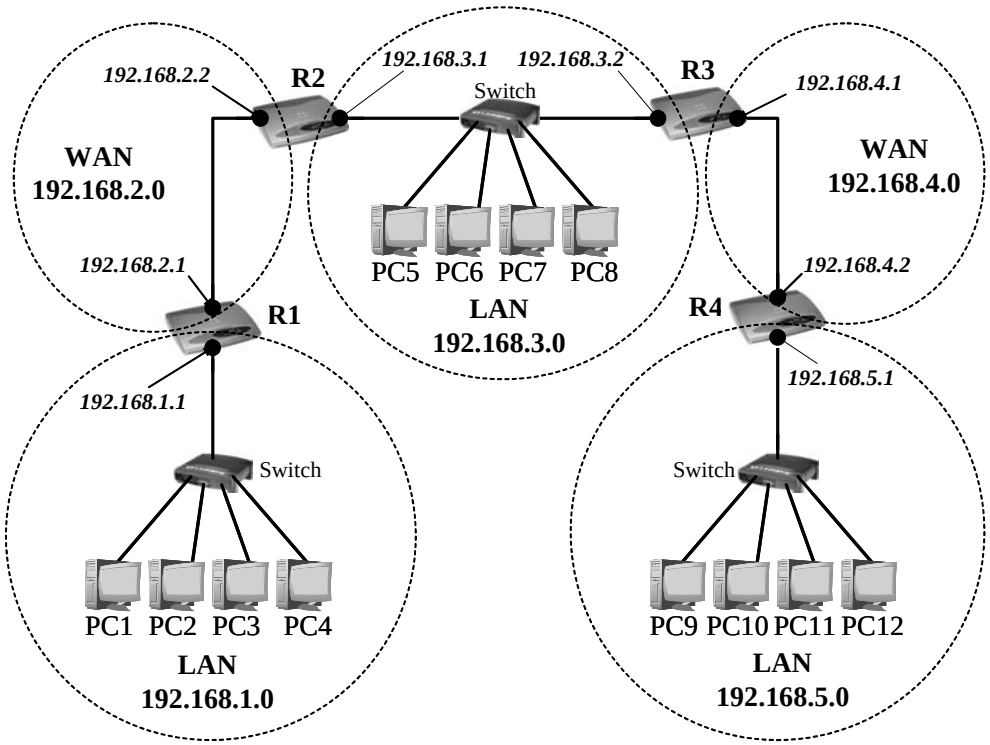


FIGURA 49. *Topología de la red del laboratorio.*

Red de destino	Dirección IP de próximo salto
192.168.1.0 /24	Directo
192.168.2.0 /24	Directo
192.168.3.0 /24	192.168.2.2
192.168.4.0 /24	192.168.2.2
192.168.5.0 /24	192.168.2.2

Tabla de rutas de R1

Red de destino	Dirección IP de próximo salto
192.168.1.0 /24	192.168.2.1
192.168.2.0 /24	Directo
192.168.3.0 /24	Directo
192.168.4.0 /24	192.168.3.2
192.168.5.0 /24	192.168.3.2

Tabla de rutas de R2

Red de destino	Dirección IP de próximo salto
192.168.1.0 /24	192.168.3.1
192.168.2.0 /24	192.168.3.1
192.168.3.0 /24	Directo
192.168.4.0 /24	Directo
192.168.5.0 /24	192.168.4.2

Tabla de rutas de R3

Red de destino	Dirección IP de próximo salto
192.168.1.0 /24	192.168.4.1
192.168.2.0 /24	192.168.4.1
192.168.3.0 /24	192.168.4.1
192.168.4.0 /24	Directo
192.168.5.0 /24	Directo

Tabla de rutas de R4

FIGURA 50. *Tablas de rutas.*

Para utilizar el enrutamiento estático, el administrador tiene que conocer la topología de la red y modificar la tabla de rutas en función de los cambios que vayan ocurriendo en la misma, lo cuál sólo es factible en redes relativamente pequeñas y que cambian lentamente. Sin embargo, en redes grandes y que cambian muy deprisa, como es el caso de Internet, este mecanismo de enrutamiento es inviable y hay que recurrir a algún tipo de procedimiento automático que se encargue de crear y modificar las tablas de

rutas a partir del intercambio de información entre los routers. Este procedimiento automático se denomina enrutamiento dinámico y es el objeto de esta práctica.

5.2 Protocolos de enrutamiento dinámico. El protocolo RIP.

Internet está formada por un conjunto de sistemas autónomos, cada uno de los cuáles suele estar gestionado por un único administrador que es el que elige el protocolo de comunicación que utilizan los routers en ese sistema autónomo. Este protocolo de comunicación se denomina genéricamente IGP (Interior Gateway Protocol) y puede seleccionarse entre varios de los disponibles, por ejemplo, Interior Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF) o Router Information Protocol (RIP).

Los routers que pertenecen a sistemas autónomos diferentes se comunican entre sí a través de protocolos de enrutamiento que se denominan genéricamente EGPs (Exterior Gateway Protocols) o Interdomain Routing Protocols. Entre ellos podemos encontrar a EGP (que utiliza el nombre genérico de este conjunto de protocolos) o BGP (Border Gateway Protocol).

En esta práctica nos vamos a centrar en los protocolos IGP, y de ellos se ha elegido el protocolo RIP porque su funcionamiento es relativamente sencillo, es muy popular, y está implementado en la mayoría de los sistemas TCP/IP. A continuación se describen algunas características de este protocolo que serán de utilidad a lo largo de la práctica.

Los mensajes RIP se encapsulan en datagramas UDP (Figura 51-a). La cabecera UDP (Figura 51-b) tiene un tamaño de 8 bytes y contiene cuatro campos. Los dos primeros son los puertos del remitente (*Source port number*) y del destinatario (*Destination port number*), cuyo valor es 520 en el caso del protocolo RIP. El siguiente campo (*UDP lenght*) indica la longitud del datagrama UDP, aunque que esta información es redundante, ya que la cabecera IP contiene la longitud total del datagrama IP y podría obtenerse la longitud del datagrama UDP sin más que restarle la longitud de la cabecera IP. El último campo (*UDP checksum*) es una suma de verificación para comprobar la integridad de los datos transmitidos.

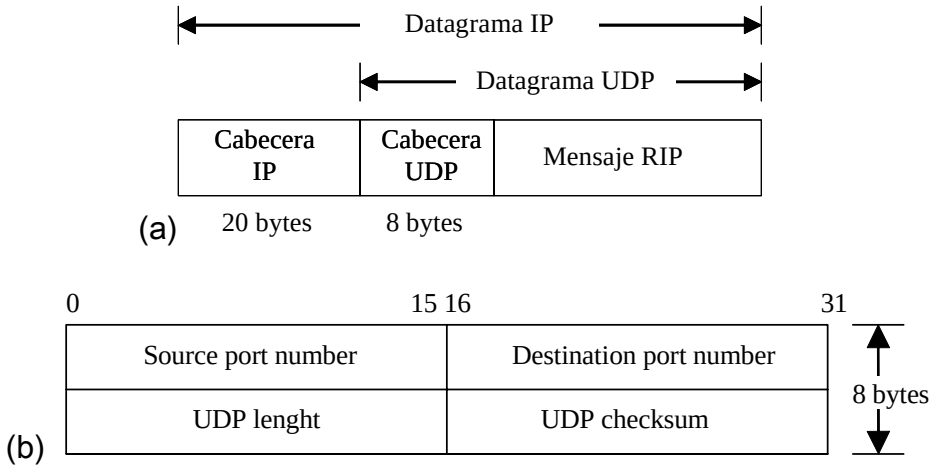


FIGURA 51. *(a) Encapsulado de un mensaje RIP en un datagrama UDP. (b) Cabecera UDP.*

Existen dos versiones de RIP, RIPv1 y RIPv2, cuyos mensajes tienen el formato indicado en la Figura 52 y en la Figura 53, respectivamente, cuando se usan con direcciones IP. Los routers del laboratorio utilizan por defecto la versión RIPv1 pero pueden configurarse, aunque no lo vamos a hacer, para que utilicen RIPv2. Los campos del formato del mensaje RIPv2 tienen el significado que se describe a continuación. Los campos del mensaje RIPv1 tienen el mismo significado con la diferencia de que algunos campos de RIPv2 no existen en RIPv1 (campos indicados con “debe ser cero” en la Figura 52).

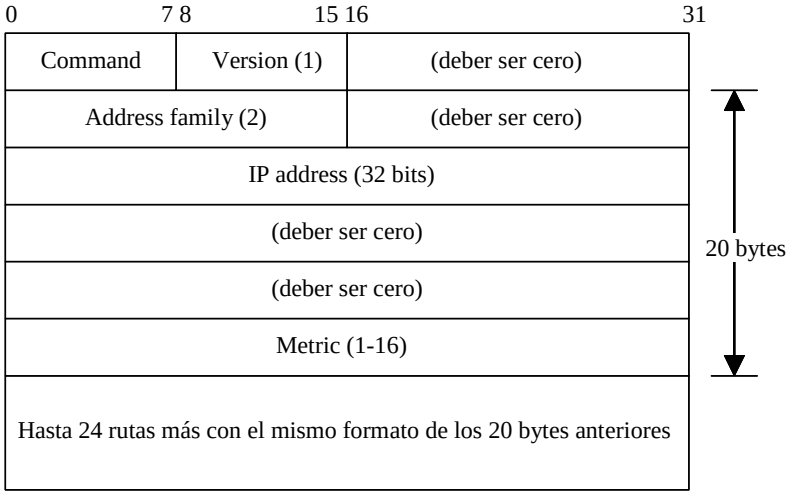


FIGURA 52. *Formato de un mensaje RIP versión 1 cuando se usa con direcciones IP.*

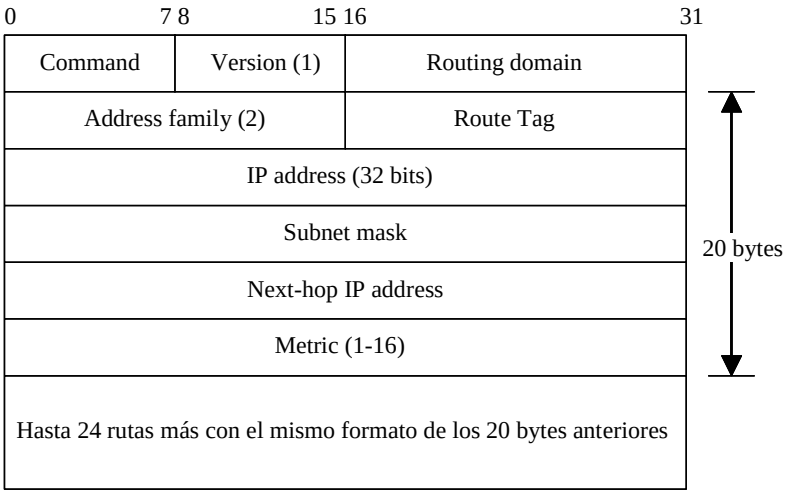


FIGURA 53. *Formato de un mensaje RIP versión 2 cuando se usa con direcciones IP.*

En la primera fila, el campo *command* indica el tipo de mensaje RIP, por ejemplo un 1 si se trata de una petición o un 2 si es una respuesta. El campo *version* indica la versión del protocolo RIP (1 ó 2). El campo *routing domain* identifica el proceso que se está ejecutando en el router al cuál pertenece el mensaje RIP. En los siguientes 20 bytes, los cuatro primeros están ocupados por los campos *Address family*, que indica el tipo de dirección (un 2 en el caso de direcciones IP), y *Route tag*, que identifica al sistema autónomo de forma única con un número cuando se utilizan protocolos EGPs. En los restantes dieciséis bytes, está la dirección IP de la red de destino con su correspondiente máscara, la dirección IP del siguiente salto y la métrica, o número de saltos, que puede tomar un valor entre 1 y 16. Este último es un valor especial llamado "infinito" que se utiliza para indicar que no existe una ruta hasta ese destino. Con RIP, el número máximo de saltos está limitado a 15, lo cuál restringe el tamaño de la red en la que puede utilizarse este protocolo. En total, en cada mensaje RIP se pueden anunciar hasta 25 rutas con el formato indicado para los 20 bytes anteriores.

El funcionamiento básico del protocolo RIPv1 es el siguiente. Inicialmente, el router envía un mensaje de petición por cada una de sus interfaces. Por ejemplo, a la dirección de broadcast de la red en una red Ethernet. En este mensaje, se pide a otros routers que le envíen su tabla completa de rutas. En el formato de este mensaje especial de petición, el campo comando vale 1, la familia de direcciones es 0 y la métrica vale 16.

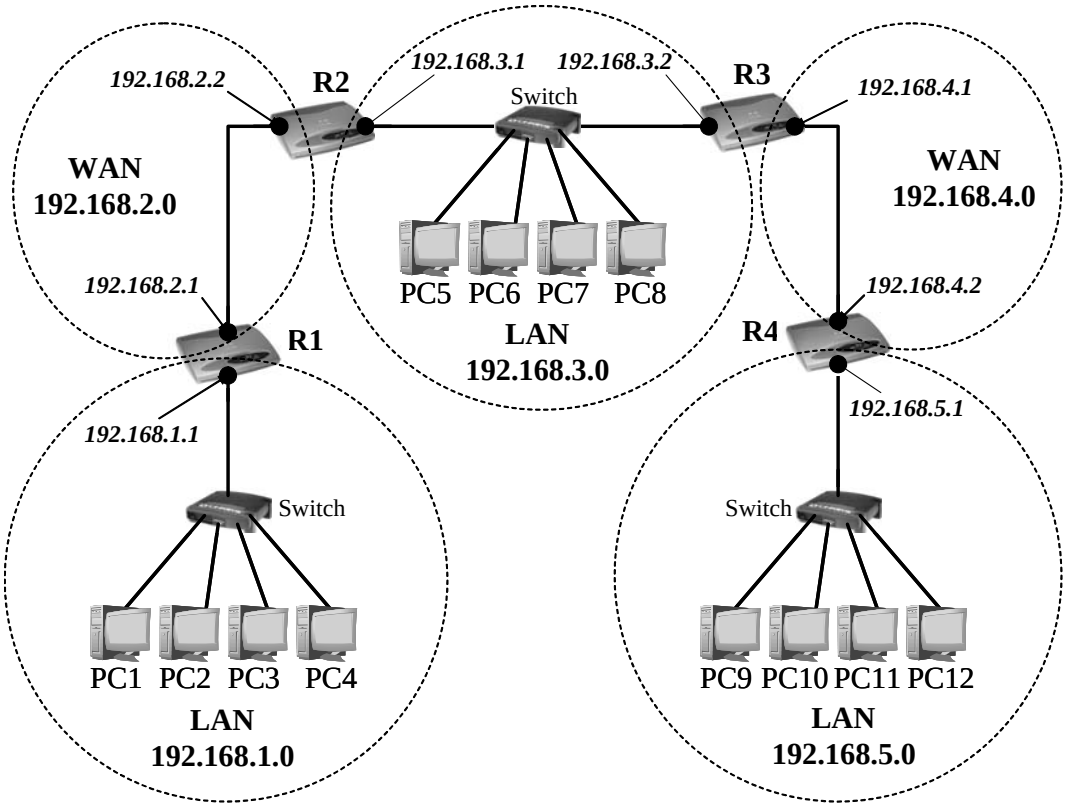
Posteriormente, y de forma periódica cada 30 segundos, el router difunde mensajes de respuesta a sus routers vecinos indicando cuáles son las redes accesibles a través de él y la distancia a la que están en número de saltos. Si la red de destino está conectada directamente al router que difunde el mensaje, la métrica de esa ruta vale 1.

Cuando un router recibe uno de estos mensajes actualiza su tabla de rutas (con redes de destino que tienen como próximo salto el router que difunde el mensaje), incrementa en uno el número de saltos, y difunde la información entre sus routers vecinos. La actualización de la tabla puede consistir en añadir una ruta (si no existe), modificarla (si su métrica ha cambiado), reemplazarla (si existe una ruta alternativa con menor número de saltos) o borrarla. Esto último ocurre cuando el router no recibe información de esa ruta durante un periodo de 3 minutos. Pasado ese tiempo, el router cambia la métrica de la ruta a infinito (16) y espera 60 segundos antes de borrarla de su tabla (no la borra inmediatamente para asegurarse de difundir esta invalidación entre sus routers vecinos).

5.3 Descripción de la práctica

5.3.1 Configuración de la red

La topología de red que se va a utilizar en esta práctica es la misma que la de la práctica anterior y se presenta de nuevo en la Figura 54 junto a las tablas de rutas de los cuatro routers.



Red de destino	Dirección IP de próximo salto
192.168.1.0 /24	Directo
192.168.2.0 /24	Directo
192.168.3.0 /24	192.168.2.2
192.168.4.0 /24	192.168.2.2
192.168.5.0 /24	192.168.2.2

Tabla de rutas de R1

Red de destino	Dirección IP de próximo salto
192.168.1.0 /24	192.168.2.1
192.168.2.0 /24	Directo
192.168.3.0 /24	Directo
192.168.4.0 /24	192.168.3.2
192.168.5.0 /24	192.168.3.2

Tabla de rutas de R2

Red de destino	Dirección IP de próximo salto
192.168.1.0 /24	192.168.3.1
192.168.2.0 /24	192.168.3.1
192.168.3.0 /24	Directo
192.168.4.0 /24	Directo
192.168.5.0 /24	192.168.4.2

Tabla de rutas de R3

Red de destino	Dirección IP de próximo salto
192.168.1.0 /24	192.168.4.1
192.168.2.0 /24	192.168.4.1
192.168.3.0 /24	192.168.4.1
192.168.4.0 /24	Directo
192.168.5.0 /24	Directo

Tabla de rutas de R4

FIGURA 54. *Topología de la red del laboratorio y tablas de rutas.*

Configure la interfaz Ethernet de su equipo con la dirección IP y la máscara indicadas en la tabla siguiente (ATENCIÓN: las direcciones IP de la red 192.168.3.0 empiezan en la 192.168.3.3, ya que las dos primeras han sido reservadas para los routers R2 y R3).

Puesto	Dirección IP	Puesto	Dirección IP	Puesto	Dirección IP
1	192.168.1.2 /24	5	192.168.3.3 /24	9	192.168.5.2 /24
2	192.168.1.3 /24	6	192.168.3.4 /24	10	192.168.5.3 /24
3	192.168.1.4 /24	7	192.168.3.5 /24	11	192.168.5.4 /24
4	192.168.1.5 /24	8	192.168.3.6 /24	12	192.168.5.5 /24

FIGURA 55. *Direcciones IP de la interfaz Ethernet0 de los ordenadores.*

La tabla siguiente indica las direcciones IP de las interfaces de cada router. La dirección IP de la interfaz Ethernet es la de la puerta de enlace para los ordenadores. En el caso de la red 192.168.3.0 hay dos posibles puertas de enlace y, aunque puede elegirse cualquiera de ellas, los puestos 5 y 6 eligirán el router R2 (192.168.3.1) y los puestos 7 y 8 el router R3 (192.168.3.2).

Router	Interfaz Ethernet 0	Interfaz Serial 0
R1	192.168.1.1 /24	192.168.2.1 /24
R2	192.168.3.1 /24	192.168.2.2 /24
R3	192.168.3.2 /24	192.168.4.1 /24
R4	192.168.5.1 /24	192.168.4.2 /24

FIGURA 56. *Direcciones IP de las interfaces Ethernet0 y Serial0 de los routers.*

Cada grupo de cuatro ordenadores pertenece a una misma red en la que se ha reservado la primera dirección disponible de la red para la puerta de enlace (el router) excepto en la red 192.168.3.0 en la que se han reservado, como se ha mencionado anteriormente, las dos primeras para los routers R2 y R3.

5.3.2 Enrutamiento dinámico con RIP

1. Acceda a su puerta de enlace vía telnet utilizando la aplicación “Terminal Console”. Por ejemplo:

```
telnet 192.168.1.1
Password: redes3
R1>
```

IMPORTANTE: En el caso de la red 192.168.3.0, los puestos 5 y 6 accederán al router R2, y los puestos 7 y 8 al router R3.

2. Acceda al Modo de administrador y luego al Modo de configuración global. Por ejemplo:

```
R1>enable
Password: redes1
R1#configure terminal
R1(config)#
```

3. Habilite el enrutamiento IP:

```
R1(config)#ip routing
```

4. Regrese al modo de administrador y examine la tabla de rutas:

```
R1#show ip route
```

5. ¿Qué rutas aparecen? ¿Por qué?.
6. Guarde el contenido de la tabla de rutas.
7. Acceda de nuevo al Modo de configuración global.
8. En este modo, el comando *router* permite habilitar un protocolo de enrutamiento dinámico. Liste las opciones de este comando. ¿Qué tipos de protocolos (acrónimos entre paréntesis) se pueden habilitar?.
9. Habilite el protocolo RIP y accederá al Modo de configuración de router para este protocolo. Por ejemplo:

```
R1(config)#router rip
R1(config-router)#
```

10. Examine los comandos disponibles y muestre las opciones del comando *network* ¿Para qué sirve este comando?.
11. Habilite el enrutamiento RIP en las dos redes IP conectadas directamente a las interfaces del router. Por ejemplo, para el router R1:

```
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.2.0
```

12. Regrese al Modo de administrador y examine de nuevo la tabla de rutas. Si tabla no está completa, espere unos momentos hasta que lo esté. ¿De qué tipo (indicado por la primera letra de cada ruta) son las nuevas rutas que han aparecido?.
13. Compruebe que las rutas de la tabla coinciden con las indicadas en la Figura 54. Guarde el contenido de la tabla de rutas.
14. Compruebe que existe conectividad con el resto de equipos del laboratorio.
15. Ejecute la aplicación Wireshark (as root) e inicie una captura de paquetes con un filtro que capture únicamente el tráfico de la interfaz Ethernet de su puerta de enlace. Por ejemplo, para el router R1:

```
host 192.168.1.1
```

16. Tras un par de minutos, detenga la captura, guárdela si quiere conservarla, y analice los paquetes del protocolo RIP capturados.
17. ¿Con cuánta frecuencia envía mensajes RIP el router? ¿A qué dirección los envía? ¿Recibiría en su ordenador estos mensajes? ¿Por qué?.
18. ¿Cuál es la versión del protocolo RIP que utiliza el router: RIPv1 o RIPv2? ¿Qué tipo de mensajes RIP ha capturado?.
19. ¿Cuántas cabeceras lleva un mensaje RIP? ¿A qué protocolo pertenecen? ¿Cuál es el tamaño de cada cabecera?.
20. ¿Cuál es el tamaño del datagrama UDP (cabecera UDP más mensaje RIP? ¿Cómo lo ha determinado?.

21. Indique los campos del mensaje RIP encapsulado en el último paquete capturado:

Command	
Version	
Address family	

22. El protocolo RIP encapsula los mensajes en datagramas UDP que utilizan un puerto dedicado para ellos, ¿cuál es?.

23. ¿Cuántas rutas contiene el mensaje RIP analizado? Compruebe que las distancias a los destinos (métrica o número de saltos) contenidas en él son correctas comparándolas con la red de la Figura 54.

24. ¿Cuál es el máximo número de saltos desde su ordenador a otro del laboratorio? Compruébelo trazando una ruta desde su ordenador utilizando el comando *traceroute*.

25. Realice un ping desde su ordenador a un ordenador que pertenezca a su misma red. Examine la tabla ARP de su máquina ¿Aparece la dirección MAC de la máquina a la cuál ha realizado el ping?.

26. ¿Cuál es la dirección MAC de su puerta de enlace?.

27. Realice un ping desde su ordenador a otro ordenador que pertenezca a una red distinta de la suya. Muestre la tabla ARP de su máquina ¿Aparece la dirección MAC del ordenador al cuál ha realizado el ping? ¿Por qué?.

6. BIBLIOGRAFÍA

Título: TCP/IP Illustrated, Volume 1: The Protocols

Autor: W. Richard Stevens

Editor: Addison Wesley Professional. 1993.

Título: Mastering Networks: An Internet Lab Manual

Autor: Jorg Liebeherr, Magda El Zarki

Editor: Addison-Wesley. 2004.

Título: Redes de Computadores

Autor: Andrew S. Tanenbaum

Editor: Prentice Hall. 2003.

Título: Redes de Computadores. Un enfoque descendente basado en Internet

Autor: James F. Kurose, Keith W. Ross

Editor: Addison Wesley. 2000.

7. ENLACES

Sistema operativo Linux-Knoppix

www.knoppix-es.org

Analizador de protocolos de red Wireshark

http://www.wireshark.org/

TCP/IP Tutorial and Technical Overview. IBM Redbooks, 2006.

http://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf

Documentación de CISCO

http://www.cisco.com/univercd/home/home.htm