



PRÁCTICAS DE TELEMÁTICA

2004 - 2005

TCP/IP: niveles de enlace, red y transporte

18 de abril de 2005

- **Profesores:**
 - Francisco Merino Caminero
 - Federico Simmross Wattenberg

1. Objetivos

- Conocer algunas de las características de la red Internet, observando cómo los conceptos aprendidos en la asignatura se aplican en realidad.
- Tomar contacto con las utilidades software que se van a emplear en el laboratorio.
- Recordar las principales funcionalidades de las capas definidas en el modelo de referencia OSI, y compararlas con la familia de protocolos de Internet.
- Profundizar en el conocimiento de los niveles de “Enlace”, “Red” y “Transporte” de la familia de protocolos de TCP/IP. En concreto, se estudiarán los protocolos ARP, IP, ICMP, TCP y UDP.

2. Consideraciones previas

- Las prácticas se van a llevar a cabo utilizando el sistema operativo Linux (Knoppix), que tiene la particularidad de que puede funcionar directamente desde un CD-ROM y no es necesario instalarlo en el ordenador. Esto, además, permitirá a los alumnos disponer en casa de un entorno de trabajo lo más parecido posible al del laboratorio. A estos efectos, se puede bajar la imagen del CD en <http://ulises.tel.uva.es/mendiknoppix>. Si no has tenido experiencias previas con el mencionado sistema operativo, además de comentárselo a los profesores, puedes leer el capítulo de “Introducción a UNIX” de [Dimitriadis98].
- Aunque nos vamos a restringir al S.O. Linux, es vital tener en cuenta que los conceptos aprendidos en esta práctica son aplicables a implementaciones de TCP/IP en otros entornos operativos (DOS, MS-Windows, UNIX y sus derivados, etc.)
- En cuanto detectes alguna anomalía en lo referente al funcionamiento del entorno de trabajo, notifícaselo a los profesores.

- Se hace notar a los alumnos que el mal uso de los recursos propuestos puede llevar a la inutilización de la red de la EUP. Si detectas alguna forma de “atentar” contra la seguridad de la red, siempre será más ventajoso, desde el punto de vista académico, notificarlo a los profesores. La utilización “inadecuada” de los recursos del laboratorio implicará la aplicación de las medidas correctivas pertinentes.

3. Herramientas para la realización de la práctica

A continuación se describen las herramientas software que se van a tener que utilizar para realizar la práctica. Aunque al principio no se acabe de entender bien su propósito, éste quedará claro a medida que se avance en la realización de los diferentes ejercicios, pruebas, etc.

Parte de las herramientas son de dominio público y han sido obtenidas a través de la propia Internet. [Stevens95] explica todas ellas con detalle, si bien al primer sitio al que hay que acudir para saber cómo funciona un comando de cualquier variante de UNIX es el llamado “manual en línea”, al que se accede mediante el comando `man`. Abre una terminal y teclea, por ejemplo, `man tcpdump`.

- `tcpdump` es un programa desarrollado por *Van Jacobson*, *Craig Leres* y *Steven McCanne* (de la Universidad de California en Berkeley) que permite “capturar” todo el tráfico que circula por una red (en nuestro caso, siempre interfaces Ethernet). El apéndice A de [Stevens95] explica detalladamente las características del programa. Además, existe también una página del manual en línea en la que se pueden encontrar todas las opciones y el modo de utilización. Mediante `tcpdump` se va a poder ver en funcionamiento los protocolos de TCP/IP.
- `ping` (Packet Internet Groper) es una herramienta de diagnóstico enormemente utilizada para llevar a cabo pruebas de conectividad IP. El capítulo 7 de [Stevens95], el 9 de [Comer00] y la correspondiente página del manual en línea analizan la aplicación con detalle.
- `traceroute` (también creado por *Van Jacobson*) es una herramienta que permite averiguar la ruta que sigue un datagrama IP hasta su destino. Se basa en la utilización del protocolo ICMP (Internet Control Message Protocol o Protocolo de Mensajes de Control de Internet), que será abordado posteriormente, y en el campo TTL (Time-to-Live) de los datagramas IP. El capítulo 8 de [Stevens95] explica con profundidad las características de esta aplicación (también existe la correspondiente página del manual en línea) y propone algunos ejemplos de utilización.
- `sock` es un programa que permite generar y recibir datagramas UDP y segmentos TCP. El apéndice C de [Stevens95] detalla su funcionamiento y sus opciones.

También tendrán que emplearse ciertas utilidades que incorporan los sistemas operativos de las estaciones de trabajo donde se van a llevar a cabo las prácticas (se puede encontrar información sobre ellas en las correspondientes páginas del manual en línea):

- `netstat` es un potente comando que permite obtener información acerca de la red a la que está conectada una máquina: qué conexiones están activas, estadísticas de utilización, tablas de encaminamiento, etc.
- `ifconfig` es el comando que permite averiguar la configuración de las interfaces de red de un host (al administrador, o superusuario, le permite además cambiar dicha configuración). Ejecuta

```
ifconfig -a
```

en alguna de las máquinas y analiza el resultado obtenido.

- `nslookup` es una utilidad que permite al usuario interactuar con el sistema de nombres de dominio DNS (Domain Name System). Aunque su funcionamiento no se va a estudiar en este laboratorio, baste decir aquí que el DNS es el sistema que permite hacer la correspondencia entre direcciones IP (ej. `157.88.64.200`) y nombres de dominio (*docencia1.tscit.eup.uva.es*). En esta práctica se utilizará principalmente para obtener la dirección IP a partir de los nombres de dominio y viceversa. Para utilizarlo, basta con ejecutar `nslookup` y, en el *prompt* que se obtiene, introducir el nombre de la máquina cuya dirección IP se quiere obtener o la dirección IP del nombre de dominio que se desea averiguar.

4. Desarrollo de la práctica

Para la realización de la práctica, deberá entregarse un trabajo escrito en el que se ponga de manifiesto que se han entendido los conceptos que se tratan en la asignatura. Para ello, será necesario aplicar los conocimientos adquiridos en las clases de teoría y los que se irán viendo en las sesiones de laboratorio. Las principales fuentes de información externa, serán el ya mencionado comando `man`, y los documentos que describen cada uno de los protocolos que se van a estudiar, los RFCs que se detallan a continuación, o si lo prefieres, el libro de Stevens [Stevens95]:

- RFC 826: El protocolo ARP (Address Resolution Protocol).
- RFC 791: El protocolo IP (Internet Protocol).
- RFC 792: El protocolo ICMP (Internet Control Message Protocol).
- RFC 793: El protocolo TCP (Transmission Control Protocol).
- RFC 768: El protocolo UDP (User Datagram Protocol).

Estos documentos se pueden encontrar en multitud de sitios de Internet, pero uno de ellos es el FTP de la red de universidades española, la Red IRIS: `ftp://ftp.rediris.es/pub/docs/rfc/`. Además de todos los RFCs numerados, se puede encontrar un documento llamado `“rfc-index.txt”` que contiene el índice de todos los demás.

Recuerda que el objetivo de esta práctica es obtener un conocimiento general acerca del funcionamiento de los protocolos de internet. Así pues, NO es necesario ni deseable estudiar a fondo los mencionados RFCs sino, simplemente, leer y comprender los apartados que sean necesarios para la redacción del trabajo.

El trabajo, que debe constar como máximo de 10 páginas, debe intentar responder lo mejor posible a las cuestiones que se plantean en las secciones siguientes. Estructúralo en secciones y trata cada protocolo por separado, de forma semejante a este enunciado.

5. Configuración de la tarjeta de red

Una vez arrancado el sistema operativo, y antes de nada, es necesario configurar la tarjeta de red. Para ello, selecciona el menú “Knoppix - Red/Internet - Configuración de la tarjeta de red”.

La dirección IP debe ser ÚNICA en el mundo, dado que las máquinas del laboratorio están permanentemente presentes en Internet. Consulta el apéndice A para averiguar la que corresponde a tu máquina.

El resto de los parámetros solicitados DEBEN ser los siguientes:

- Máscara de subred: `255.255.255.0`
La máscara de subred indica qué bits de la dirección IP corresponden a la red (bits a 1) y qué bits numeran la máquina dentro de dicha red (bits a 0).
- Dirección de broadcast: `157.88.64.255`
Dirección IP especial que se usa para enviar paquetes a todas las máquinas de la subred a la vez.

- Servidor de nombres: 157.88.18.189
Máquina que contiene una lista de equivalencias entre nombres de Internet (ej: `docencia1.tscit.eup.uva.es`) y direcciones IP (ej: 157.88.64.200).
- Puerta de enlace: 157.88.64.186
También llamado *gateway*, es el primero de los “nodos intermedios” que nos permiten comunicarnos con el resto de Internet. Todos los paquetes IP que no sean para nuestra subred deben pasar a través de él.

6. IP (Internet Protocol)

IP [RFC791] es el protocolo central de Internet. Todo lo que se envía por la red está encapsulado en forma de paquetes IP, que a su vez se encapsulan en tramas del correspondiente protocolo de nivel 2 (Ethernet en el caso del laboratorio).

- Todos los paquetes IP incluyen en su cabecera una dirección destino y una dirección origen. Abre dos ventanas y ejecuta `tcpdump` en una y `ping` en otra. Observa cómo `tcpdump` normalmente muestra mucho más tráfico del que originamos activamente. A la vista de los parámetros que has introducido al configurar la tarjeta de red, ¿cuál puede ser la causa de este tráfico extra?
- Observa los demás campos de la cabecera de un paquete IP. ¿Hay alguno que sea innecesario desde el punto de vista del estándar OSI?
- El RFC791 especifica que la longitud máxima de un paquete IP es de 64Kbytes, pero advierte que esta longitud es poco práctica en la mayoría de las redes. ¿Estás de acuerdo con esta afirmación?

7. ARP: Address Resolution Protocol

ARP (Address Resolution Protocol) [RFC826] es el protocolo que permite averiguar direcciones de interfaces de red a partir de direcciones IP en redes multipunto como la Ethernet del laboratorio. Cada tarjeta Ethernet que existe en el mundo tiene asignado un número de 48 bits que la identifica de forma única. Dado que el hardware de red implementa solamente los protocolos de nivel físico y de enlace, es necesario un mecanismo que permita traducir direcciones IP a direcciones MAC. Éste es el propósito del protocolo ARP.

- Utiliza `arp -a` para ver las tablas “caché” de ARP de las estaciones de trabajo. Observa cómo cambian cuando realizas conexiones con otras máquinas.
- Utiliza `tcpdump arp` para ver a ARP en acción. Explica los resultados obtenidos.

8. ICMP: Internet Control Message Protocol

ICMP es uno de los protocolos que acompañan a IP en el nivel de red. Su propósito es, como su nombre indica, intercambiar mensajes de control entre varias máquinas. Uno de los mensajes ICMP más útiles (consulta [RFC792]) es el llamado “Echo Request”, que solicita a una máquina remota un paquete ICMP de tipo “Echo Reply”. Mediante el comando `ping` se pueden enviar y recibir este tipo de mensajes.

- Haz pruebas con `ping` (utilizando generalmente la opción `-v`) usando direcciones de máquina locales y remotas. Interpreta los resultados (trata, como siempre, de utilizar al mismo tiempo `tcpdump`).

- Toda máquina que implementa la pila de protocolos TCP/IP incluye una interfaz de red virtual que sirve para conectar con la propia máquina. Su nombre es *loopback*, y su dirección 127.0.0.1. Compruébalo mediante el comando `ifconfig`. ¿Es posible acceder al interfaz *loopback* de otra máquina?
- Haz un ping a algunos sitios cercanos y distantes. ¿Cómo varían los valores `icmp_seq` y `TTL`?
- Utiliza el comando `traceroute` para rastrear el camino que siguen los paquetes hasta algún sitio lejano (por ejemplo, `www.yahoo.com`), y a algún otro sitio de la Universidad (`www.uva.es` u otras máquinas del laboratorio). Haz más de una prueba con cada sitio, y utiliza simultáneamente `tcpdump`. ¿Puedes deducir el método que emplea `traceroute` para rastrear el camino seguido por los paquetes IP?
- Utilizando las herramientas disponibles y los conceptos repasados hasta este momento, ¿serías capaz de dar una idea general de la topología de la red Internet?. Justifica todas las afirmaciones que hagas.

9. TCP: Transmission Control Protocol

TCP [RFC793] (Protocolo de Control de la Transmisión) es el protocolo que utilizan la mayoría de las aplicaciones de Internet. Para ellas, lo único importante es la dirección del *host* destino (es decir, la dirección de nivel 3 de la máquina destinataria) y la dirección del proceso destino *dentro* de la máquina destino (es decir, la dirección de nivel 4 del proceso destinatario). Si las direcciones de nivel 3 se llaman “direcciones IP”, cabría pensar que las de nivel 4 se llaman “direcciones TCP”, pero en realidad se llaman “puertos TCP”. Puedes consultar una lista reducida con los números de puerto asignados a los servicios más importantes en el fichero `/etc/services` (utiliza el comando `less` para leerla).

Nota: Antes de realizar las pruebas propuestas en este apartado y el siguiente, necesitas habilitar algunos servicios de red. Para ello, selecciona el menú “Knoppix - Consola de root”, y teclea:

```
/etc/init.d/inetd start
/etc/init.d/smail start
```

En todo momento puedes ver qué servicios están activos mediante el comando `netstat -a`.

- Utiliza el comando `sock` para conectar “a mano” con tu propia máquina (o alguna otra del laboratorio, siempre que tenga habilitados los servicios mencionados) en estos puertos: `echo`, `chargen`, `daytime`, `telnet`, `ftp`, `smtp` (Pulsa `^C` para salir). Como siempre, analiza el tráfico generado con `tcpdump`. Observa que por defecto, `tcpdump` no captura el tráfico que va destinado a la propia máquina de origen. ¿Se puede capturar este tráfico de alguna manera?
- Prueba e intenta averiguar para qué sirven los mencionados servicios.
- ¿Qué ocurre cuando tratas de conectar con un servicio que no está disponible en la máquina destino? Intenta responder desde los puntos de vista de los distintos niveles de la pila de protocolos.
- Observa la diferencia entre conectar al servicio `ftp` de tu propia máquina mediante la dirección IP de la tarjeta de red (`157.88.64.x`) y la de la interfaz *loopback* (`127.0.0.1`).
- Observa también que algunos servicios responden a comandos tecleados en texto legible. Conecta con alguno de los servicios mencionados y teclea `help`. ¿A qué crees que se debe?

10. UDP: User Datagram Protocol

El protocolo UDP [RFC768] (Protocolo de Datagramas de Usuario) es muy similar en funcionamiento a IP, en cuanto a que no está orientado a conexión, y a que no es fiable, pero dispone de su propia cabecera y se encapsula en paquetes de nivel 3 igual que los segmentos de TCP. La lista de puertos UDP se encuentra también en el fichero `/etc/services`.

Nota: Recuerda que debes activar algunos servicios de red antes de proseguir. Consulta el apartado 9.

- Si UDP es tan parecido en funcionalidad a IP, ¿Cuál puede ser la razón de su existencia?
- Utiliza el comando `sock` para conectar con los servicios antes mencionados (apartado 9), pero ahora mediante el protocolo UDP (consulta la opción `-u`). ¿Estás conectando exactamente a los mismos sitios que anteriormente, o hay alguna diferencia?
- Observa la diferencia en el funcionamiento de los servicios `chargen` y `daytime` al conectar mediante TCP y UDP. ¿Sabrías decir cuál es el motivo?

11. Para finalizar

Describe, con todos los detalles que puedas (si quieres puedes mostrar los formatos de tramas y paquetes con sus contenidos relevantes), todo lo que ocurre (incluso a nivel Ethernet) cuando ejecutas `ping www.tel.uva.es`. No lo hagas de forma teórica, sino indicando direcciones reales, números de protocolo, etc. Además, indica qué herramientas utilizas (y cómo las utilizas) para averiguar toda la información que necesites.

12. Cuestiones administrativas

- Fecha de entrega del enunciado: 18 de abril de 2005.
- Fecha de entrega del trabajo para la convocatoria de junio: 14 de junio de 2005.
- Fecha de entrega del trabajo para la convocatoria de septiembre: 1 de septiembre de 2005.

A. Direcciones IP del laboratorio del departamento de TSCIT

<code>alfa.tscit.eup.uva.es.</code>	157.88.64.1
<code>it1.tscit.eup.uva.es.</code>	157.88.64.2
<code>tsc1.tscit.eup.uva.es.</code>	157.88.64.3
<code>delta.tscit.eup.uva.es.</code>	157.88.64.4
<code>docencia1.tscit.eup.uva.es.</code>	157.88.64.200
<code>docencia2.tscit.eup.uva.es.</code>	157.88.64.201
<code>docencia3.tscit.eup.uva.es.</code>	157.88.64.202
<code>docencia4.tscit.eup.uva.es.</code>	157.88.64.203
<code>docencia5.tscit.eup.uva.es.</code>	157.88.64.204
<code>docencia6.tscit.eup.uva.es.</code>	157.88.64.205
<code>docencia7.tscit.eup.uva.es.</code>	157.88.64.206
<code>docencia8.tscit.eup.uva.es.</code>	157.88.64.207
<code>docencia9.tscit.eup.uva.es.</code>	157.88.64.208
<code>docencia10.tscit.eup.uva.es.</code>	157.88.64.209
<code>docencia11.tscit.eup.uva.es.</code>	157.88.64.210
<code>docencia12.tscit.eup.uva.es.</code>	157.88.64.211

docencia13.tscit.eup.uva.es. 157.88.64.212
docencia14.tscit.eup.uva.es. 157.88.64.213
docencia15.tscit.eup.uva.es. 157.88.64.214
docencia16.tscit.eup.uva.es. 157.88.64.215
docencia17.tscit.eup.uva.es. 157.88.64.216
docencia18.tscit.eup.uva.es. 157.88.64.217
proyectos1.tscit.eup.uva.es. 157.88.64.218
proyectos2.tscit.eup.uva.es. 157.88.64.219
proyectos3.tscit.eup.uva.es. 157.88.64.220
proyectos4.tscit.eup.uva.es. 157.88.64.221
proyectos5.tscit.eup.uva.es. 157.88.64.222
proyectos6.tscit.eup.uva.es. 157.88.64.223
proyectos7.tscit.eup.uva.es. 157.88.64.224

Referencias

- [Comer00] DOUGLAS E. COMER. *“Internetworking with TCP/IP. I, Principles, protocols, and architecture”*. Prentice - Hall International, London, 4th edition, 2000.
- [Dimitriadis98] I. A. DIMITRIADIS AND F. J. D’IAZ PERNAS (ED.). *“Introducci’on pr’actica a la administraci’on de sistemas en Internet”*. Servicio de publicaciones de la Universidad de Valladolid (to be published), Valladolid (Spain), 1998.
- [RFC768] J. POSTEL. *“User Datagram Protocol”*. Request for Comments 768 (STD 6). ISI, August 1980.
- [RFC791] J. POSTEL. *“Internet Protocol (STD 5)”*. Request for Comments 791. ISI, September 1981.
- [RFC792] J. POSTEL. *“Internet Control Message Protocol”*. Request for Comments 792. ISI, September 1981.
- [RFC793] J. POSTEL. *“Transmission Control Protocol”*. Request for Comments 793 (STD 5). University of Southern California, September 1981.
- [RFC826] DAVID C. PLUMMER. *“An Ethernet Address Resolution Protocol”*. Request for Comments 826, November 1982.
- [Stevens95] W. RICHARD STEVENS. *“TCP/IP illustrated. 1, The protocols”*. Addison - Wesley, Reading, Massachusetts, 5th printing edition, 1995.