Práctica 6: Configuración de TCP/IP en Windows XP y Linux

1. Introducción

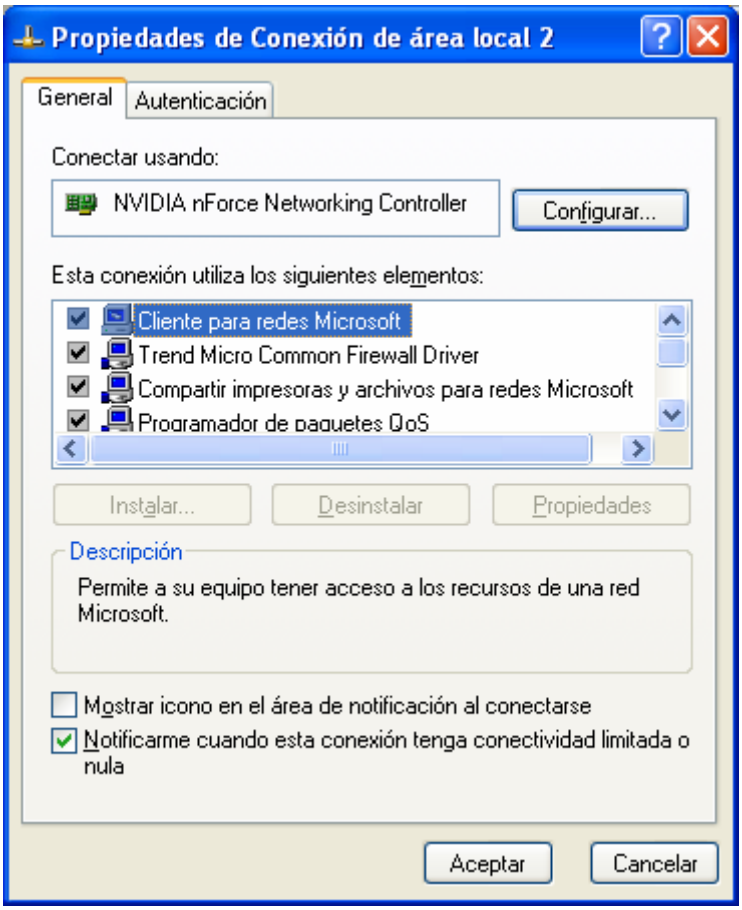
Esta práctica está dedicada a revisar el procedimiento básico de instalación y configuración de los protocolos TCP/IP en Windows XP y Linux. Se muestra el uso de algunas herramientas útiles a la hora de resolver problemas con estos protocolos: configurar el software de red, verificar su funcionamiento y ajustar los parámetros relacionados con TCP/IP. Algunos de los conceptos que se manejan en esta práctica aún no se han estudiado en las clases de teoría. Por eso, en el desarrollo de esta práctica se introducen las herramientas desde un punto de vista funcional: qué aplicaciones se utilizan, qué parámetros requieren y cuál es la función principal de las mismas. No se presentan los detalles de implementación que requerirían un conocimiento más profundo de los protocolos.

Sin duda, los procedimientos que vamos a revisar constituyen un material que será de gran utilidad en el desarrollo posterior de la asignatura. Cuando los conceptos teóricos asociados hayan sido expuestos en las clases de teoría, será un buen momento para volver sobre el contenido de la práctica y repetir algunos pasos con un mejor aprovechamiento. Por otra parte, la práctica adquirida facilitará la asimilación posterior de la teoría asociada.

2. Configuración de TCP/IP en Windows XP

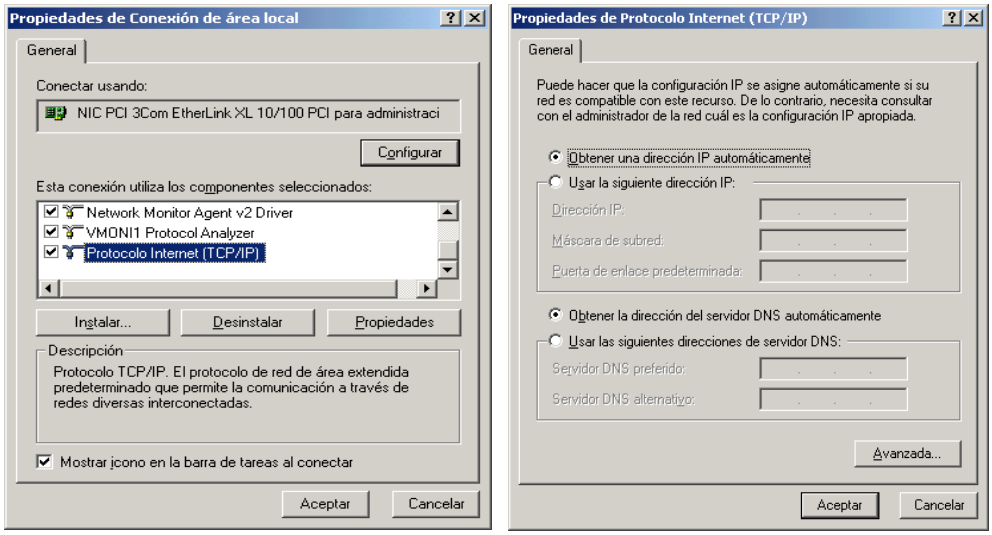
Para utilizar los protocolos TCP/IP desde una máquina Windows XP conectada a una red de área local (Ethernet en nuestro caso) es necesario tener instalada una tarjeta adaptadora o NIC (*Network Interface Adapter*). En nuestros computadores esta tarjeta ya está instalada y configurada. Para ver la configuración de la tarjeta adaptadora Ethernet:

1. Pulsa el botón **Inicio**, y después **Panel de control**.
2. Haz doble-clic sobre el icono **Conexiones de red**.
3. Selecciona el icono de **Conexión de área local 2** y con el botón de la derecha del ratón selecciona la opción **Propiedades**. Aparece la ventana **Propiedades de Conexión de área local 2**.



4. Presionando sobre el botón **Configurar** aparece la ventana que se muestra a continuación en la que puedes acceder a algunas características de este adaptador.

Además del adaptador de red, para poder utilizar aplicaciones Internet es necesario que estén instalados los protocolos TCP/IP. De nuevo, estos protocolos ya están instalados en nuestras máquinas. Para comprobarlo podrías seguir los pasos siguientes (**si tuvieras los permisos necesarios**):



5. Desde la ventana **Propiedades de Conexión de área local** que se muestra arriba a la izquierda, selecciona el item **Protocolo Internet (TCP/IP)** y pulsando sobre el botón **Propiedades**, aparece la ventana de **Propiedades de Protocolo Internet (TCP/IP)** (arriba derecha), donde se indican algunos datos relativos al funcionamiento de estos protocolos.

Por motivos de seguridad el botón de Propiedades está desactivado. No es demasiado importante ya que la información que normalmente obtendremos es la que aparece en la figura (arriba derecha). Como podemos observar, la configuración más habitual consiste en que la mayoría de los parámetros necesarios para el funcionamiento de TCP/IP (¡incluyendo la propia dirección IP!) no se configuran manualmente, sino que se obtienen automáticamente durante el proceso de inicialización de la máquina.

Esto es posible gracias a un protocolo llamado DHCP (*Dynamic Host Configuration Protocol*). Este protocolo permite que un servidor de servicio DHCP instalado en nuestra red de área local detecte la presencia de nuevas máquinas en la red y les asigne una dirección IP de una lista de direcciones IP disponibles. Además de la dirección IP, el servidor DHCP proporciona información adicional necesaria para el funcionamiento de los protocolos TCP/IP (dirección IP del servidor DNS, dirección IP del router, etc.)

2.1 La orden ipconfig

Una vez que los protocolos TCP/IP están instalados, la orden **ipconfig** (se ejecuta desde una ventana de DOS -Símbolo del sistema-) proporciona información sobre la configuración de la red en nuestra máquina (para cada uno de los adaptadores de red instalados).

El formato de la orden es el siguiente:

```
C:\>ipconfig /?

USO: ipconfig [/? | /all | /release [adapter] | /renew [adaptador]
            | /flushdns | /registerdns
            | /showclassid adaptador
            | /setclassid adaptador [classidtoset] ]
adaptador    Nombre completo o modelo con '*' y '?'
Opciones
/?           Muestra este mensaje de ayuda.
/all         Muestra toda la información de configuración.
/release     Libera la dirección IP para el adaptador especificado.
/renew       Renueva la dirección IP para el adaptador especificado.
/flushdns    Purga la caché de resolución de DNS.
/registerdns Actualiza todas las concesiones DHCP y vuelve a
             registrar los nombres DNS
/displaydns  Muestra el contenido de la caché de resolución de DNS.
/showclassid Muestra todos los Id. de clase DHCP permitidos para el
             adaptador.
/setclassid  Modifica el Id. de clase DHCP.
```

Tecleando simplemente **ipconfig** obtenemos información sobre:

- **Dirección IP**: dirección IP asignada a nuestra máquina, bien de forma permanente, o bien de forma dinámica mediante el protocolo DHCP.
- **Máscara de subred**: indica qué parte de la dirección IP identifica la red, y qué parte identifica al computador (a un adaptador de red). Aunque la red de la UPV tiene una dirección de clase B (158.42.0.0), la máscara de subred (255.255.254.0) indica que los 23 bits más significativos de cada dirección IP (bits a 1 en la máscara) deben considerarse dirección de red, y los 9 últimos (bits a 0 en la máscara) dirección de *host*. Esto se debe a que se han definido subredes dentro de la red de la UPV.
- **Puerta de enlace predeterminada**: dirección IP del router que conecta nuestra subred con el resto de la red de la UPV y con el exterior (Internet).

Si ejecutamos la orden **ipconfig /all** obtenemos información adicional, entre la cual destaca:

- **Dirección física**: es la dirección física que corresponde a la tarjeta adaptadora de red (Ethernet en nuestro caso) que está instalada en nuestro computador y nos permite el acceso a la red.
- **Servidores DNS**: la dirección IP de la(s) máquina(s) que realiza(n) las traducciones de nombres a direcciones IP (servidor de nombres).
- **Servidor DHCP**: dirección IP de la máquina que nos ha asignado la dirección IP y la mayoría de parámetros que aparecen en esta ventana.
- **Concesión obtenida (concesión caduca):** fecha en la que fue obtenida (caducará) la dirección IP actual. Aplicable únicamente en el caso de información obtenida por DHCP.

Las órdenes **ipconfig /release** e **ipconfig /renew** permiten liberar y renovar la dirección IP obtenida mediante DHCP.

Según la información obtenida, los servidores DNS y DHCP, ¿están en la misma subred que el computador de prácticas? ¿Por qué?

Ejercicio 1:

Ejecuta la orden **ipconfig** y completa la información siguiente:

Dirección física del adaptador Ethernet	
Dirección IP	
Máscara de subred	
Dirección IP del router (puerta de enlace)	
Servidor DNS	
Servidor DHCP	

2.2 La orden ping

Mediante la orden **ping** (que se ejecuta desde una ventana DOS) se obtiene una estimación del tiempo de ida y vuelta de un paquete, desde la estación origen a una estación destino que se especifica. Para ello se almacena el instante de tiempo en el que se envía el paquete y cuando llega la respuesta al valor almacenado se le resta del tiempo actual. El

funcionamiento de la orden **ping** se basa en el uso de mensajes ICMP de tipo 0 (*Echo reply*) y 8 (*Echo request*).

Otras utilidades de la orden **ping** son:

- Averiguar si un destino está operativo, conectado a la red y sus protocolos TCP/IP en funcionamiento.
- Conocer la fiabilidad de la ruta entre origen y destino (calculando el porcentaje de paquetes que obtienen respuesta).

Ejemplo:

```
C:\>ping www.upc.es
Haciendo ping a inopia.upc.es [147.83.20.85] con 32 bytes de
datos:
Respuesta desde 147.83.20.85: bytes=32 tiempo=23ms TDV=248
Respuesta desde 147.83.20.85: bytes=32 tiempo=20ms TDV=248
Respuesta desde 147.83.20.85: bytes=32 tiempo=31ms TDV=248
Respuesta desde 147.83.20.85: bytes=32 tiempo=24ms TDV=248
Estadísticas de ping para 147.83.20.85:
Paquetes: enviados = 4, Recibidos = 4, perdidos = 0 (0% loss),
Tiempos aproximados de recorrido redondo en milisegundos:
    mínimo = 20ms, máximo =  31ms, promedio =  24ms
```

La orden **ping** admite un serie de opciones, algunas de las más útiles se muestran a continuación:

```
ping [-t] [-a] [-n cantidad] [-l tamaño] [-f] [-i TTL] [-v TOS]
    [-r cantidad] [-w Tiempo de espera agotado] lista de destinos
  Opciones:
    -t            Solicita eco al host hasta ser interrumpido.
                  Para ver estadísticas y continuar: Ctrl-Inter.
                  Para interrumpir: presione Ctrl-C.
    -a            Resuelve direcciones a nombres de host.
    -n cantidad   Cantidad de solicitudes de eco a enviar.
    -l tamaño     Tamaño del búfer de envíos.
    -f            No fragmentar el paquete.
    -i TTL        Tiempo de vida.
    -v TOS        Tipo de servicio.
    -w tiempo     Tiempo de espera agotado de respuesta en miliseg.
```

Ejercicio 2:

Haz un ping a las direcciones siguientes: zoltar.redes.upv.es (servidor dentro del Laboratorio de Redes), www.upv.es (servidor web de la UPV), www.uv.es (servidor web de la Universidad de Valencia), www.elpais.es (servidor web comercial), www.berkeley.edu (servidor web de la Universidad de California en Berkeley). Anota los resultados en la tabla siguiente:

	Paquetes			**Tiempo de ida y vuelta (ms)**		
	Enviados	**Recibidos**	**Perdidos**	**Mínimo**	**Máximo**	**Medio**
zoltar.redes.upv.es						
www.upv.es						
ftp.rediris.es						
www.elpais.es						
www.berkeley.edu						

Los resultados que se obtienen mediante la orden **ping** son, a veces, difíciles de interpretar. El usuario obtiene poca información de por qué el tiempo de ida y vuelta es mayor en unos destinos que en otros. Incluso cuando no hay respuesta al ping, no es posible conocer cuál es el problema: la máquina referenciada está fuera de servicio, no existe una ruta desde el origen al destino o la saturación de la red es tan alta que no se obtiene respuesta del destino en un tiempo razonable. También, en ocasiones por motivos de seguridad y para evitar dar información sobre los ordenadores conectados a la red, los administradores de las redes filtran los mensajes de ping en los cortafuegos o desactivan el servicio en los propios ordenadores. A pesar de lo dicho, es una de las herramientas que más utilizan los administradores y usuarios de equipos conectados en red.

A través de las opciones de la orden ping podemos modificar las características del paquete (datagrama IP) que se enviará a través de la red para sondear al destino. En este punto vamos a modificar uno de esos parámetros. La cantidad máxima de información que puede transportar una trama Ethernet (su MTU) es de 1500 bytes. Si queremos enviar un bloque de información mayor, deberá fragmentarse en varias tramas. Cuando en la orden ping especificamos la opción –f estamos solicitando que el bloque de

datos asociado al paquete de "ping" no se fragmente en su recorrido desde la estación origen a la estación destino.

Ejercicio 3:

Ejecuta la secuencia de órdenes siguiente:

```
ping -l 1000 -f zoltar.redes.upv.es
ping -l 1500 -f zoltar.redes.upv.es
ping -l 2000 -f zoltar.redes.upv.es
```

Habrás comprobado que no se pueden enviar los bloques de datos de 1500 y 2000 bytes sin fragmentación. Averigua por tanteo el tamaño máximo (en bytes) del bloque de datos que puede enviarse dentro de un solo paquete. Intenta justificar este tamaño máximo.

2.3 La orden tracert

La orden **tracert** (se ejecuta desde una ventana DOS) permite conocer el camino (secuencia de routers) que debe atravesar un paquete para llegar desde la estación origen a la estación destino. El funcionamiento se basa en gestionar adecuadamente un parámetro de la cabecera de los datagramas IP (el campo TTL: tiempo de vida) y en la información que aportan los mensajes ICMP que generan los routers cuando les llega un datagrama cuyo tiempo de vida se ha agotado. Por cada nuevo router atravesado por el datagrama se dice que hay un *salto* en la ruta. Podemos decir, que el programa **tracert** calcula y describe el número de saltos de una ruta.

Como se ha dicho, **tracert** utiliza ICMP y el campo tiempo de vida (TTL) de la cabecera IP. El campo TTL tiene 8 bits que el emisor inicializa a algún valor. El valor recomendado actualmente en el RFC de números asignados (RFC 1700) es de 64. Cada router que atraviesa el datagrama debe reducir el TTL en una unidad. Cuando un router recibe un datagrama IP con TTL igual a uno y decrementa este valor obtiene un cero. Consecuentemente, el router descarta el datagrama y envía un mensaje ICMP de tipo 11 (*tiempo excedido)* a la máquina origen. La clave para el funcionamiento del programa **tracert** es que este mensaje ICMP contiene la dirección IP del router.

El funcionamiento de **tracert** es el siguiente: Se envía un datagrama IP a la máquina destino con TTL igual a 1. El primer router con el que se encuentre este datagrama decrementará el TTL y al obtener un cero lo

descartará, enviando un mensaje ICMP de "tiempo excedido" al origen. Así se identifica el primer router en el camino. A continuación se envía un datagrama con TTL igual a 2 para encontrar la dirección del segundo router, y así sucesivamente.

Cuando el datagrama tenga un valor de TTL suficiente para llegar a su destino necesitamos que también la máquina destino genere un mensaje alertando de esta circunstancia. Para ello tracert utiliza dos posibilidades distintas: enviar mensajes ICMP de eco (es la que usa Windows) o mensajes UDP a un puerto arbitrariamente grande y muy probablemente cerrado (es la opción que se usa en Linux). Si el mensaje enviado fue de eco, una respuesta de eco es señal de que el mensaje llegó a su destino final. Si lo que enviado fue un datagrama UDP, al estar el puerto cerrado en el destino, el sistema responderá con un mensaje ICMP de puerto inalcanzable.

El programa de DOS **tracert** realiza la siguiente función: para averiguar cada nuevo salto envía tres datagramas y para cada uno de ellos calcula el valor del tiempo de ida y vuelta. Si en un tiempo máximo (configurable) no hay respuesta se indica en la salida mediante un asterisco.

Algunas puntualizaciones:

- No hay ninguna garantía de que la ruta que se ha utilizado una vez vaya a ser utilizada la siguiente (cuando estudiemos el protocolo IP veremos por qué).
- No hay ninguna garantía de que el camino seguido por el paquete de vuelta sea el mismo que ha seguido el paquete de ida. Esto implica que a partir del tiempo de ida y vuelta que ofrece **tracert** puede no ser directo estimar el tiempo de ida o de vuelta por separado (si el tiempo que tarda el paquete en ir desde el origen hasta el *router* es de 1 segundo y el tiempo que tarda el paquete de vuelta es de 3 segundos, el valor que nos proporcionará **tracert** será de 4 segundos)
- La dirección IP que se devuelve en el mensaje ICMP es la dirección de la interfaz entrante del router.

Ejercicio 4:

Ejecuta la orden **tracert** para los siguientes destinos y anota el número de saltos.

	Saltos
herodes.redes.upv.es	
www.upv.es	
www.ua.es	
www.net.berkeley.edu	

Observa que para alcanzar una máquina que está dentro de la red de la UPV (por ejemplo, www.upv.es) se atraviesan, en algunos casos, varios routers.

Analiza cuáles pueden ser las causas de la respuesta obtenida a la orden **tracert www.ua.es**.

Ejercicio 5:

Desde el navegador accede a la página **http://www.traceroute.org/#USA**. En esta página puedes seleccionar diversos sitios web desde los que puedes lanzar un traceroute a una máquina destino cualquiera. Selecciona el sitio de la University of California, Berkeley y solicita un traceroute a tu máquina de prácticas. Compara el resultado con el del ejercicio anterior. ¿Se sigue el mismo recorrido desde la UPV a Berkeley y viceversa? Observarás que algunos routers tienen nombres similares en los dos casos pero con direcciones IP distintas, ¿a qué crees que es debido?

2.4 La orden netstat

La orden **netstat** (desde **Símbolo del sistema**) ofrece diversa información sobre el estado y estadísticas de los protocolos de red. Se pueden obtener datos sobre los principales sucesos Ethernet, IP, ICMP, UDP y TCP. El formato de la orden es el que se muestra a continuación:

```
netstat [-a] [-e] [-n] [-s] [-p proto] [-r] [intervalo]
```

```
-a      Muestra todas las conexiones y puertos escucha.
-e      Muestra estadísticas Ethernet. Se puede combinar con -s.
```

```
-n      Muestra números de puertos y direcciones en formato numérico.

-p proto   Muestra conexiones del protocolo especificado por proto;
que puede ser tcp o udp. Si se usa con la opción -s para mostrar
estadísticas por protocolo, proto puede ser TCP, UDP o IP.

-r      Muestra el contenido de la tabla de rutas.

-s      Muestra estadísticas por protocolo. En forma predeterminada,
se muestran para TCP, UDP e IP; se puede utilizar la opción -p
para especificar un subconjunto de lo predeterminado.

Intervalo  Vuelve a mostrar las estadísticas seleccionadas, haciendo
pausas en el intervalo de segundos especificado entre cada muestra.
```

Mediante la orden **netstat –r** obtenemos información sobre la tabla de encaminamiento (produce la misma salida que la orden **route print**).

Para averiguar la ruta se sigue el proceso siguiente. Cuando hay que encaminar un datagrama:

1. Para cada línea de la tabla de encaminamiento, se realiza un AND lógico entre la **dirección IP destino** del datagrama y la **máscara de red**. IP compara el resultado con la **Red destino** y marca todas las rutas en las que se produce coincidencia.
2. De la lista de rutas coincidentes IP selecciona la ruta que tiene más bits en la máscara. Esta es la ruta más específica y se conoce como la ruta de máxima coincidencia.
3. Si hay varias rutas de máxima coincidencia, se usa la ruta con menor **métrica**. Si hay varias con la misma métrica se usa una cualquiera de entre ellas.

Ejercicio 6:

Visualiza la tabla de encaminamiento del ordenador en el que estás trabajando.

Ejercicio 7:

La orden **netstat –e** proporciona estadísticas sobre el número de bytes y tramas enviadas y recibidas por el adaptador Ethernet. Se detalla el número de tramas unicast (un solo destino), no unicast (múltiples destinos y difusiones), paquetes erróneos y descartados.

Ejecuta esta orden y anota los resultados en la tabla siguiente:

	Recibidos	**Enviados**
Bytes		
Paquetes unicast		
Paquetes no unicast		
Descartados		
Errores		

Ejercicio 8:

La orden **netstat –sp IP** produce estadísticas sobre el tráfico IP. Ejecuta esta orden y anota los resultados en la tabla siguiente:

	Cantidad
Paquetes recibidos	
Errores de encabezado recibidos	
Errores de dirección recibidos	
Datagramas reenviados	
Protocolos desconocidos recibidos	
Paquetes recibidos descartados	
Paquetes recibidos procesados	
Solicitudes de salida	
Descartes de ruta	
Paquetes de salida descartados	
Paquetes de salida sin ruta	
Reensambles requeridos	
Reensambles correctos	
Reensambles fallidos	
Datagramas correctamente fragmentados	
Datagramas mal fragmentados	
Fragmentos creados	

Ejercicio 9:

Análogamente la orden **netstat –sp TCP** produce estadísticas sobre el tráfico TCP (también se pueden solicitar estadísticas sobre los protocolos ICMP y UDP). Ejecuta esta orden y anota los resultados en la tabla siguiente:

	Cantidad
Activos abiertos	
Pasivos abiertos	
Intentos de conexión erróneos	
Conexiones restablecidas	
Conexiones actuales	
Segmentos recibidos	
Segmentos enviados	
Segmentos retransmitidos	

La orden **netstat** sin argumentos ofrece información sobre las conexiones activas en nuestra máquina. Si se utiliza con la opción **–a**, además de la información anterior se indica también la relación de puertos TCP y UDP en los que hay alguna aplicación escuchando (dispuesta a aceptar conexiones TCP o datagramas UDP).

2.5 La orden arp

El computador que estamos utilizando en esta práctica está conectado a una red de área local Ethernet que, a su vez, se conecta a Internet a través de un router (cuya dirección IP habréis averiguado en las secciones anteriores). Cuando nuestras aplicaciones en red (Netscape, por ejemplo) generan peticiones para otros computadores de Internet, crean paquetes (también llamados datagramas) que contienen la dirección IP de la máquina destino. El uso de direcciones IP (y de los protocolos TCP/IP) crea la ilusión de que todas la máquinas que se comunican pertenecen a una única (e inmensa) red común: Internet. Si la dirección IP destino corresponde a una máquina de nuestra propia red (tiene el mismo identificador de red), el paquete puede ser entregado directamente a su destino sin más intermediarios. Sin embargo, cuando la dirección IP corresponde a una red externa, la entrega de la información debe realizarse a través del router. En primer lugar, habrá que entregar la información al router de nuestra red y éste será el encargado de encaminar el paquete para hacerlo llegar e la red destino donde se

encuentra el computador referenciado. Como vemos, en cualquiera de los dos casos, en una primera instancia se realiza una transmisión de información a través de la red de área local.

Desafortunadamente, las direcciones IP no son, por sí mismas, válidas para transmitir una trama a través de la red de área local. Las tarjetas adaptadoras de red que conectan las estaciones con el medio no entienden las direcciones IP, sólo entienden direcciones físicas. Por tanto, para que un datagrama IP viaje por la red de área local, este debe encapsularse dentro de un trama (Ethernet en nuestro caso). Esa trama Ethernet contiene la dirección física del siguiente destino que, como hemos visto, puede tratarse del computador final al que van dirigidos los paquetes (origen y destino en la misma red local) o del router que encaminará el paquete hacia el exterior (origen y destino distintas redes).

En TCP/IP se utiliza un protocolo para la obtención de direcciones físicas a partir de direcciones IP dentro de una red de área local. Este protocolo se conoce con el nombre ARP (*Address Resolution Protocol*). Los detalles del funcionamiento de este protocolo se estudiarán en las clases de teoría de esta asignatura. De momento, nos puede bastar con saber que podemos conocer información sobre este protocolo a través de la orden **arp** de DOS. Esta orden nos permite ver (y modificar) la caché ARP de nuestro computador. La caché ARP es una tabla que almacena temporalmente las relaciones entre direcciones IP y direcciones físicas, que ha conseguido averiguar nuestro computador utilizando el protocolo ARP. Es importante destacar, que la mayoría de estas entradas se generaran automáticamente (y de forma transparente al usuario) cuando se ejecuta una aplicación Internet (ping, cliente web, cliente ftp, etc.). Por tanto, muy rara vez (fuera de esta práctica) requiere el usuario modificar manualmente esta tabla.

Más concretamente, la orden **arp** de DOS permite:

- Ver la caché local de ARP (**arp –a**)
- Eliminar entradas manualmente de la caché (**arp –d <dir_IP>** o **arp –d ***), si el usuario dispone del permiso para ello (no es nuestro caso).

Añadir entradas manualmente a la caché (**arp –s <dir_IP> <dir_Eth>**), si el usuario dispone del permiso para ello (no es nuestro caso).

Ejercicio 10:

Desde una ventana DOS ejecuta la orden **arp –a** para comprobar el contenido de la caché. A continuación ejecuta la orden **ping 158.42.180.62** (es la dirección de la máquina zoltar.redes.upv.es) y examina de nuevo la caché ARP. Anota las direcciones de zoltar en la tabla siguiente:

Dirección IP	Dirección Física

Ejecuta la orden **ping www.uji.es** y comprueba si ha aparecido en la caché la dirección IP del servidor www.uji.es. Consulta la información ofrecida por la orden **ipconfig** para averiguar a quién pertenece la otra dirección que aparece.

Como sabes, antes de la ejecución de la orden ping, se ha realizado una consulta al servidor DNS para resolver el nombre **www.uji.es**. ¿Por qué no aparece la dirección de este servidor en la caché ARP?

3. Configuración de TCP/IP en Linux

En Linux encontramos las mismas órdenes que acabamos de estudiar dentro del entorno Windows XP, en particular:

- Orden **traceroute**, equivale a la orden **tracert** de Windows
- Orden **arp**, equivale a la orden de Windows del mismo nombre.
- Orden **netstat**, equivalente a la que hemos estudiado para Windows.

Por ello, aquí sólo revisaremos algunas diferencias significativas entre los dos sistemas operativos.

3.1 La orden ifconfig

La orden **ifconfig** permite configurar y obtener información sobre la configuración de red. Utilizando esta orden con las opciones adecuadas podemos configurar todo el software de TCP/IP. En nuestro caso el software ya está instalado y, además, no tenemos permisos de administración para modificar los parámetros. Así que nos limitaremos a inspeccionar la información mediante **ifconfig**.

Si ejecutamos **ifconfig** seguido del nombre de un interfaz (**eth0** en nuestro caso) obtendremos información sobre la configuración de esta interfaz. Si se ejecuta sin parámetros, presenta las características de todas las interfaces que se hayan configurado. A modo de ejemplo, la consulta de la configuración de la interfaz Ethernet **eth0** sería:

```
#/sbin/ifconfig eth0
eth0      Link encap:Ethernet  Hwaddr 00:04:75:C8:F0:86
inet addr:158.42.180.60 Bcast:158.42.181.255
     Mask:255.255.254.0
inet6 addr: fe80::204:75ff:fec8:f086/10 Scope:Link
UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:4316000 errors:3 dropped:0 overruns:1 frame:3
TX packets:31299 errors:0 dropped:0 overruns:0 carrier:0
collisions:34 txqueuelen:100
RX bytes:3313701041 (3160.1 Mb)  TX bytes:11503484 (10.9 Mb)
Interrupt:5 Base address:0xa800
```

Los campos **MTU** y **Metric** informan sobre los valores actuales de la MTU (Unidad Máxima de Transferencia) y de la métrica para una interfaz dada. Algunos sistemas operativos usan el valor **Metric** para calcular el coste de una ruta. Linux no usa este valor por el momento, pero lo define por razones de compatibilidad.

Las líneas **RX packets** y **TX packets** dan información sobre de los paquetes recibidos o transmitidos sin errores, del número de errores ocurridos, de cuántos paquetes han sido descartados, seguramente por memoria insuficiente, y cuántos se han perdido por desbordamiento, condición que ocurre cuando la recepción de paquetes es demasiado rápida y el sistema operativo es incapaz de dar servicio al paquete anterior antes de la llegada del nuevo paquete. Los nombres de los campos que genera **ifconfig** coinciden más o menos con los parámetros con los que se puede ejecutar esta orden.

A continuación tenemos una lista de algunos parámetros reconocidos por **ifconfig** (puedes visualizar todas las opciones disponibles mediante la orden **man ifconfig**). Las opciones que simplemente activan alguna característica pueden usarse para desactivarla precediéndolas de un guión (-).

La utilización de estos parámetros nos permitiría cambiar la configuración del interfaz (si tuviésemos los privilegios necesarios).

- **up:** marca la interface como "up" o activa, es decir, disponible para que sea usada por el nivel IP. (Esta opción corresponde a los indicadores UP RUNNING).
- **down:** marca la interface como "down" o inactiva, es decir, inaccesible al nivel IP.
- **netmask máscara:** asigna una máscara de subred a una interfaz.
- **broadcast dirección:** la dirección de difusión se obtiene, generalmente, usando la parte de red de la dirección y activando todos los bits de la parte correspondiente a la máquina (**ifconfig** confirma el establecimiento de una dirección de difusión incluyendo el indicador BROADCAST).
- **metric número:** puede ser usada para asignar un valor de métrica a la tabla de encaminamiento creada para la interfaz.
- **mtu bytes:** fija la unidad máxima de transferencia, o lo que es lo mismo, el máximo número de octetos que la interfaz es capaz de manejar en una única transacción. Para Ethernet, la MTU toma el valor 1500 por defecto.
- **arp:** esta opción es específica de redes de difusión como Ethernet. Permite el uso de ARP, el Protocolo de Resolución de Direcciones, para detectar la dirección física de las máquinas conectadas a la red. Para redes de difusión, esta opción es habilitada por defecto. **ifconfig** avisa que ARP ha sido inhabilitado mediante el indicador NOARP. **-arp** inhabilita el uso de ARP para esta interfaz.
- **promisc:** pone la interfaz en modo promiscuo. En una red de difusión, esto hace que la interfaz reciba todos los paquetes, independientemente de si están dirigidos a ella o no. Esto permite el análisis del tráfico de red mediante utilidades como filtros de paquetes. Se trata de una buena técnica para localizar problemas de red que de otra forma resultan difíciles. Por otro lado, esto también posibilita ataques, permitiendo al atacante analizar el tráfico de la red en busca de claves u otras cosas peligrosas. (Esta opción corresponde al indicador PROMISC). **-promisc** desactiva el modo promiscuo.

Ejercicio 11:

Ejecuta la orden **ifconfig eth0** y, basándote en la descripción anterior, analiza la información obtenida.

3.2 El directorio /proc/net

El sistema de ficheros **proc** es una interface que permite el acceso a la información del sistema operativo en funcionamiento a través de un sistema de ficheros. Dentro del directorio **/proc** se pueden listar los ficheros y ver su contenido como en cualquier otro sistema de ficheros. Normalmente aparecen ficheros como **loadavg**, que contiene la carga media del sistema, o **meminfo**, que contiene información sobre la memoria física y virtual. Para ver información relacionada con la red descenderemos al subdirectorio **net** (**/proc/net**). Este directorio contiene una serie de ficheros con información sobre las tablas ARP del núcleo, el estado de las conexiones TCP, las tablas de encaminamiento, etc. La mayoría de las herramientas de administración de redes utilizan estos ficheros para acceder a la información que precisan. Puedes visualizar el contenido del fichero **arp** y compararlo con el que has visto en Windows.

3.3 La orden netstat

La orden **netstat** tiene un funcionamiento muy similar al descrito para Windows XP. A continuación describiremos únicamente la opción de esta orden que permite consultar la tabla de encaminamiento, ya que esta parte no ha sido tratada en la versión anterior.

Si ejecuta **netstat** usando el indicador **-nr**, puede ver la información de la tabla de encaminamiento del núcleo (produce una salida muy similar a la orden **route**). Por ejemplo:

```
# netstat -nr
Kernel IP routing table
Destination   Gateway  Genmask     Flags    MSS  Window  irtt  Iface
158.42.0.0    0.0.0.0  255.255.0.0    U      1500   0     0  eth0
127.0.0.0     0.0.0.0  255.0.0.0      U      3584   0     0  lo
0.0.0.0   158.42.1.10  0.0.0.0        UG     1500   0     0  eth0
```

La segunda columna de la salida producida por **netstat** informa sobre los routers a los que apunta la información de encaminamiento. Si una ruta no usa router, el programa indica la dirección 0.0.0.0. La tercera columna muestra el nivel de generalización de una ruta. Dada una dirección IP, el núcleo recorre la tabla registro a registro haciendo un AND lógico de la dirección IP y la mascara de nivel de generalización (**Genmask**) antes de compararla con el destino que muestra dicho registro (**Destination**). La ruta por defecto tiene máscara 0.0.0.0.

La cuarta columna muestra varios indicadores que describen la ruta:

G La ruta utiliza un router.

U La interfaz está activa.

H Esta interfaz permite el acceso a una sola máquina.

Las columnas **MSS**, **Window** y **irtt** indican los valores iniciales de algunos parámetros que se utilizan en las conexiones TCP que se establecen a través de esta ruta. La columna **Iface** indica a través de qué interfaz se realizan estas rutas. En nuestro caso solo estamos interesados en las rutas que se establecen a través de la interfaz Ethernet (**eth0**).

Ejercicio 12:

Utiliza la orden **netstat –nr** y rellena la tabla para las rutas relacionadas con la interfaz **eth0**:

Destino	Router (Gateway)	Máscara de red