

## **Práctica 1**

### **Generalidades de TCP/IP**

#### **Objetivos**

1. Conocer las direcciones físicas y lógicas de una red IP y la traducción de una a otra.
2. Comprender el direccionamiento por dominios.
3. Familiarizarse con el manejo de los comandos relacionados con el TCP/IP.

#### **Materiales**

- Ordenadores del Laboratorio de Redes de Computadores (E14), con sistema operativo
- Sistema Operativo Windows o Linux.
- Conexión a Internet de la UCA.

## **Estudio Teórico**

### **Direcciones Físicas**

Para establecer comunicación en una red de ordenadores se necesita un sistema de direccionamiento de manera que en todo momento se pueda hacer referencia a una máquina de manera unívoca.

En una red física dos máquinas se pueden comunicar sólo si cada una de ellas conoce la dirección física de la otra.

Cada tecnología de red posee un formato distinto para la dirección física.

Si nos centramos en Ethernet, que es la más utilizada, se puede observar que la **dirección física** está formada por un número de 48 bits (al que también se le llama dirección Ethernet o MAC).

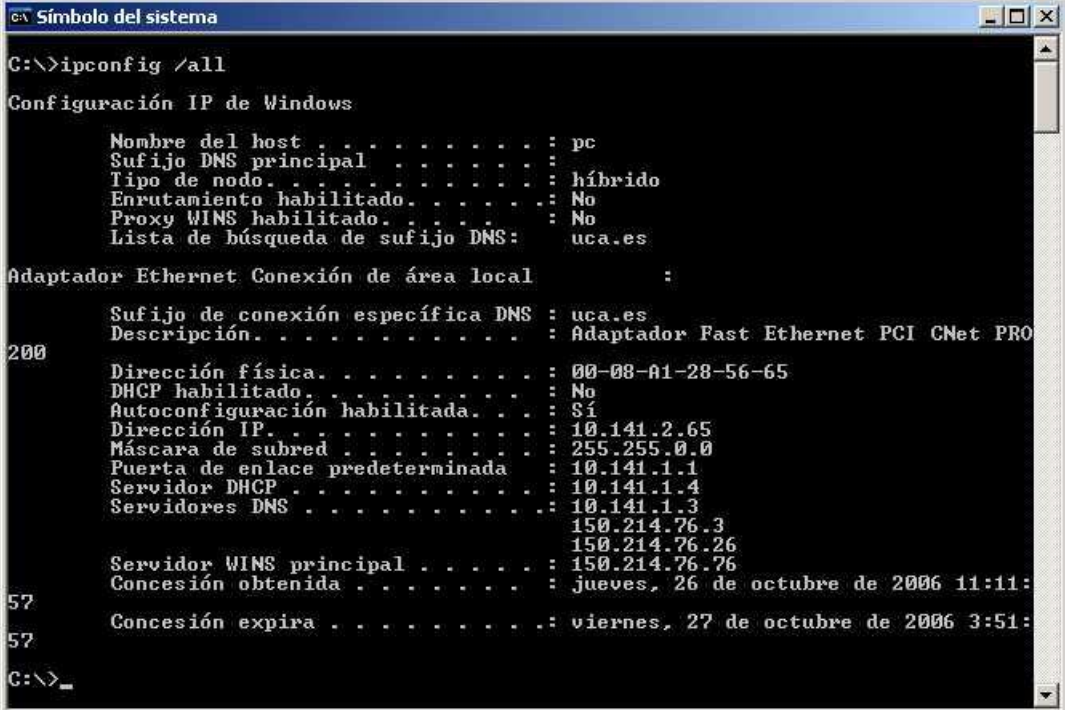
Estas direcciones son asignadas al hardware de red por los fabricantes. El IEEE maneja el espacio de direcciones Ethernet y las suministra a los fabricantes en bloques para que se las asignen a al hardware de red, de forma que dos dispositivos de red nunca tendrán la misma dirección física.

La dirección Ethernet habitualmente se muestra por seis números hexadecimales de dos cifras cada uno.

Para verla en tu ordenador, si empleas Windows, utiliza uno de estos dos métodos:

1. Ejecuta el Símbolo del Sistema (*cmd*), también conocido como Terminal o *Shell*, en modo administrador (botón derecho y "Ejecutar como Administrador"). Una vez abierto el terminal, emplea el siguiente comando: ***ipconfig*** o ***ipconfig/all*** y observa el apartado Dirección física (si lo empleas con la opción

all, se mostrará información de todas las interfaces de red disponibles en el PC):



```
C:\>ipconfig /all

Configuración IP de Windows

    Nombre del host . . . . . : pc
    Sufijo DNS principal . . . . . :
    Tipo de nodo . . . . . : híbrido
    Enrutamiento habilitado. . . . . : No
    Proxy WINS habilitado. . . . . : No
    Lista de búsqueda de sufijo DNS: uca.es

Adaptador Ethernet Conexión de área local :

    Sufijo de conexión específica DNS : uca.es
    Descripción. . . . . : Adaptador Fast Ethernet PCI CNet PRO
200
    Dirección física. . . . . : 00-08-A1-28-56-65
    DHCP habilitado. . . . . : No
    Autoconfiguración habilitada. . . . . : Sí
    Dirección IP. . . . . : 10.141.2.65
    Máscara de subred . . . . . : 255.255.0.0
    Puerta de enlace predeterminada : 10.141.1.1
    Servidor DHCP . . . . . : 10.141.1.4
    Servidores DNS . . . . . : 10.141.1.3
                             150.214.76.3
                             150.214.76.26
    Servidor WINS principal . . . . . : 150.214.76.76
57   Concesión obtenida . . . . . : jueves, 26 de octubre de 2006 11:11:
57   Concesión expira . . . . . : viernes, 27 de octubre de 2006 3:51:
C:\>_
```

2. En el Panel de Control haz clic en Centro de Redes y Recursos Compartidos. Una vez abierto, en el menú de la izquierda, selecciona la opción Cambiar configuración del adaptador. Selecciona una conexión, y haciendo clic con el botón derecho del ratón, selecciona Estado. Aparece entonces el cuadro de diálogo del estado de la conexión seleccionada. Por último, haz clic en el botón Detalles y observa entonces el apartado dirección física.

Si estás empleando Linux, tienes, de igual manera, dos opciones:

1. Abre un terminal y ejecuta el comando **ifconfig**. Se mostrará la información de la interfaz de red en la que podrás encontrar la dirección física.
2. En el menú superior, selecciona el icono de red y haz clic en "Información". Se abrirá un menú con la información de la interfaz de red.

## **Direcciones IP**

Las redes físicas se interconectan con otras redes físicas por medio de *routers* (éstas incluso pueden ser de distintas tecnologías), pero con el direccionamiento físico no se puede acceder a máquinas de redes externas.

Los protocolos que están ejecutándose en las máquinas de las redes implementan las normas para la correcta comunicación de estas.

El conjunto de protocolos TCP/IP es el más comúnmente usado y una de sus principales características es el establecer conexiones entre máquinas de distintas redes con independencia de la tecnología usada en cada una de ellas.

Con TCP/IP se pueden establecer redes lógicas sin las limitaciones de las redes físicas. Para ello se hace uso del direccionamiento IP.

Cada máquina TCP/IP tiene asociado una dirección IP formada por un número binario de 32 bits que está dividido en dos partes:

1. La parte que identifica a la red (*NETID*): esta parte tiene un número de bits que depende del tamaño y tipo de la red (puede ser 8,16 o 24).
2. La parte que identifica a la máquina dentro de la red (*HOSTID*): su número de bits es 32 menos los ocupados por el *NETID*. Las direcciones de los *host* son asignadas por el administrador de la red (un *host* o anfitrión no es más que un ordenador que está conectado a internet y que por tanto tiene una dirección IP).

Las redes se clasifican por clases o tipos dependiendo del número de *hosts* que la formen. Cada tipo o clase tiene un tamaño de *NETID* y *HOSTID* distinto.

Existen 5 tipos principales:

- **Tipo A:** la parte que identifica a la red (*NETID*) es el primer byte donde el primer bit es siempre '0'. Con los siete restantes se identifica a la red pudiendo direccionar  $2^7$  redes (128) con direcciones que van de la 0 a la 127 (en realidad a la 126 pues la 127 está reservada). El número de *host* que puede tener esta red es de  $2^{24}$  (16.777.216).
- **Tipo B:** la parte que identifica a la red son los dos primeros bytes donde los dos primeros bits son siempre '10' y con los catorce restantes se pueden direccionar a  $2^{14}$  redes (16.384). Por tanto el primer byte en las direcciones de tipo B va del 128 al 191 y estas redes pueden tener hasta  $2^{16}$  *host* (65536).
- **Tipo C:** la parte que identifica a la red son los tres primeros bytes donde los tres primeros bits son siempre '110' y con los 21 restantes se pueden direccionar a  $2^{21}$  redes (2.097.152). Por tanto el primer byte en las direcciones de tipo C va del 192 al 223 y estas redes pueden tener hasta  $2^8$  *host* (256).
- **Tipo D:** multidifusión.
- **Tipo E:** reservadas.

	0	1	2	3	4	8	16	24	31	
Class A	0	netid				hostid				
Class B	1	0	netid					hostid		
Class C	1	1	0	netid					hostid	
Class D	1	1	1	0						
Class E	1	1	1	1	0					

Es habitual encontrar una red IP dividida en **subredes**. Un caso práctico se da en la Universidad de Cádiz que tiene establecida una subred para cada Escuela o Facultad.

En estos casos se hace necesario identificar de algún modo cada una de las subredes, lo cual se lleva a cabo con la **Máscara de Subred**.

A cada dirección IP se le asocia ahora una máscara que también es de 32 bits.

La máscara se utiliza para dividir la parte destinada la *host* (*HOSTID*) en dos partes, la primera de estas identifica a la subred y la segunda al *host* dentro de la subred:

<i>NETID</i>	<i>HOSTID</i>	
<i>NETID</i>	<i>SUBNETID</i>	<i>HOSTID</i>

En la máscara los bits a '1' significan que los bits correspondientes en el *HOSTID* de la dirección IP serán tratados como dirección de la subred y los bits a '0' de la máscara indican que los bits correspondientes en el *HOSTID* de la dirección IP identifican al *host*.

Un ejemplo: sea la dirección IP 128.0.**137**.75 y sea la máscara de subred 255.255.**255**.0. 128 en binario comienza por 10 lo que indica que es de tipo B, por tanto 128.0 identifica la red. Si observamos en la parte destinada al *HOSTID* en la máscara, los '1' y los hacemos corresponder con la IP obtendremos la dirección de la subred que en este caso es 137 y si observamos en la máscara los '0' y los hacemos corresponder con la dirección IP obtendremos la identificación del *host* dentro de la subred que en este caso es 75.

MS: 11111111.11111111.**11111111**.00000000

IP: 10000000.00000000.**10001001**.01001011

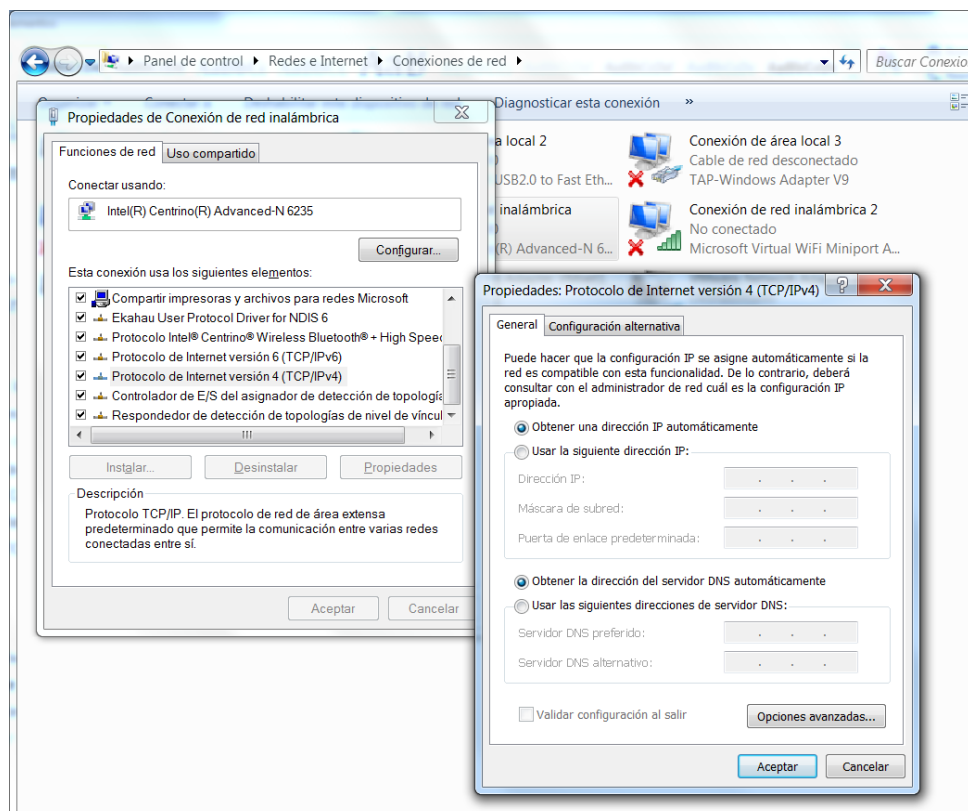
ID de RED

ID de SUBRED

ID de HOST

Cuando las redes no poseen subredes se utilizan máscaras que tienen 0 como valor del *HOSTID*: 255.**0.0.0** para redes tipo A, 255.255.**0.0** para redes tipo B y 255.255.255.**0** para redes tipo C.

En Windows, puedes configurar tanto la dirección IP como la máscara de subred de tu ordenador siguiendo los siguientes pasos: Panel de Control -> Centro de Redes y Recursos Compartidos -> Cambiar Configurator del Adaptador. Selecciona la conexión que quieras configurar y en el menú de opciones selecciona Cambiar la configuración de esta conexión. Aparece un cuadro de diálogo en el que debes seleccionar Protocolo Internet versión 4 (TCP/IPv4) y hacer clic en Propiedades:



En Linux, tienes dos opciones:

1. En el menú superior general, selecciona el icono de red, selecciona la conexión que quieras editar (en caso de tener varias) y haz clic en Editar.
2. Desde el terminal, abre el fichero ***/etc/network/interfaces*** con tu editor de texto preferido (gedit, nano, vim, etc.) y edítalo de la siguiente manera:
  - a. Dinámico:

```
auto eth0
iface eth0 inet dhcp
```
  - b. Estático:

```
auto eth0
iface eth0 inet static
address ...
gateway ...
[netmask ...]
[network ...]
[broadcast ...]
```

Tras guardar y cerrar el fichero, tendrás que restaurar las conexiones de red para que surta efecto mediante el siguiente comando ***sudo /etc/init.d/networking restart***.

El organismo encargado de asignar las direcciones IP a nivel mundial es la **Autoridad para Asignación de Números de Internet** ([www.iana.com](http://www.iana.com)), este delega sus funciones de asignación de IP en Europa a **Ripe** ([www.ripe.net](http://www.ripe.net)). En esta web, podréis ver vuestra IP actual (arriba a la derecha).

Estos organismos poseen unas bases de datos públicas donde se pueden hacer consultas para obtener información variada sobre cada una de las redes que forman Internet, por ejemplo: nombre de la



entidad que gestiona la red, personas de contacto, rangos de IP que posee la red, etc... A este tipo de servicio se le llama **Whois**.

Windows no posee ningún comando que implemente un cliente *Whois*, por ello la forma más sencilla de acceder a este servicio es a través de la web ([www.ripe.net](http://www.ripe.net) o [www.dominios.es/dominios](http://www.dominios.es/dominios)) aunque también se podría hacer por medio de una aplicación comercial.

Linux sí que incluye por defecto el comando *whois* que se puede ejecutar desde el terminal.

## **Direcciones IP Especiales**

Existen direcciones IP que se utilizan para referirse a toda una red, estas son las que poseen ceros en el campo *Hostid*. Se le llama **dirección de red**.

La dirección que direcciona a un *host* dentro de una red tiene el *netid* a 0 y el en el *hostid* la dirección del *host*.

Existen una IP con la que se puede direccionar a todos los *host* de una red a la vez, esta es la que tiene todos los bits del *hostid* a 1 y se le llama **dirección de difusión dirigida**.

Está también la **dirección de Loopback**, que empieza por 127 y con cualquier combinación en el resto de bits. Se utiliza para realizar pruebas y procesos dentro de una misma máquina. Cuando se realiza una comunicación con esta dirección como destino, en realidad no se envía nada a la red, aunque se comporta como si se hubiera enviado. En una red nunca habrá un paquete con dirección 127.

La dirección IP que tiene todos los bits a 1 se utiliza para direccionar a todos los *host* de la red. Se le llama **dirección de difusión limitada**.

La IP con todos los bits a 0 direcciona al propio *host*.

## **Traducción de Direcciones IP a Físicas: ARP (Windows/Linux)**

Como se comentó anteriormente, para que dos equipos de una red se comuniquen ambos deben conocer la dirección física del equipo remoto, para ello se necesita un mecanismo para obtenerla a través de la dirección IP, es lo que se conoce como **Protocolo de Asociación de Direcciones** (ARP).

La forma de trabajar de ARP es la siguiente: cuando un *host* (*host A*) desea saber la dirección física de otro (*host B*) a partir de la IP, el primero envía por difusión un paquete especial que pide al *host* que tiene dicha IP que le responda con su dirección física. Todos los *host* de la red recibirán este paquete pero sólo el *host B* reconocerá su propia IP y enviará al *host A* su dirección física. Posteriormente el *host A* usará esa dirección física para comunicarse con B.

Con objeto de no enviar constantemente paquetes de multidifusión, y por tanto reducir los costos de la comunicación, las máquinas que usan ARP normalmente guardan en una tabla las asignaciones [dirección IP – dirección física] más recientemente realizadas.. De esta manera siempre que se desee realizar una comunicación se mirará antes en este fichero por si contiene la dirección física del *host* de destino, y si así fuera no sería necesario enviar el paquete de difusión a la red.

Para observar o modificar la tabla ARP de tu equipo puedes usar el comando *ARP* desde el terminal tanto en Windows como en Linux.

En la ayuda, *arp /?* (Windows) o *info arp* (Linux) encontrarás cuales son las opciones más interesantes.

## **Sistemas de Nombre Por Dominio**

Además de la dirección IP existe otro método para nombrar a un *host* dentro de internet, es lo que se llama Sistema de Nombres por Dominios (**DNS**).

Este sistema es más intuitivo, suele ser fácil de memorizar y simplemente con mirar la dirección se puede localizar geográficamente al *host*, saber su pertenencia o el propósito de este.

Con el DNS cada máquina recibe un nombre de dominio que habitualmente consta de varias partes separadas por puntos llamadas **subdominios** (lo habitual es que sean tres):

**nombre\_***host*. **dominioN**. **dominioN-1**. ... **dominio1**

El de más a la derecha tiene mayor nivel y puede ser de dos tipos:

1. Dominios de organizaciones: son del tipo .com, .edu, .gov, .mil, tv, etc.
2. Dominios geográficos: usados en todo el mundo menos EEUU. Son del tipo .es, .fr, .uk, .de, etc.

El central suele hacer referencia a la organización a la que pertenece el *host* y el de la izquierda suele ser el nombre del *host*.

A veces se hace necesario identificar a un/a usuario/a con el dominio, para ello ponemos delante el nombre del usuario/a seguido del carácter arroba (@):

**usuario@nombre host.subdominio.dominio principal**

Para saber el nombre por dominios de una máquina a partir de la IP o para acceder a la abundante información de la que disponen los servidores DNS, puedes utilizar el comando **nslookup** tanto en Windows como en Linux desde el terminal de comandos.

Este comando (*nslookup*) tiene dos modos de ejecución:

1. Estático: se ejecuta el comando seguido de la dirección IP que se quiere traducir, i.e., **nslookup www.google.es**
2. Interactivo: se ejecuta el comando sin ningún argumento (**nslookup**) y accedemos a una sesión en la que podemos ejecutar una serie de comandos que permitan extraer información, modificar el servidor DNS al que conectarnos, etc. Algunos de estos comandos son: help, exit, ls, lserver, root, server, set, set all, set cl[ass], set [no]deb[ug], set [no]d2, set [no]def[name], set do[main], set [no]ig[nore], set po[rt], set q[querytype], set [no]rec[urse], set ret[ry], set ro[ot], set [no]sea[rch], set srchl[ist], set ti[meout], set ty[pe], set [no]v[c] y view.

Sin embargo, lo habitual es que las listas de información que proporcionan el comando **ls** no estén accesible por motivos de seguridad.

El organismo que asigna a nivel mundial los nombres por dominios es **IANA** ([www.iana.com](http://www.iana.com)). En España esta función es delegada a la **Red Técnica Española de TV** ([www.red.es](http://www.red.es)) y dentro de ella el **Registro**

**Delegado de Internet** ([www.dominios.es/dominios](http://www.dominios.es/dominios)). Estas entidades también mantienen servidores **Whois** (accesible desde la opción "Busca y registra tu dominio"). En ellos no aparecen los rangos IP de las redes, pero si otro tipo de información como puede ser los servidores DNS que gestionan los dominios de cada entidad, además de los datos de estas y de personas de contactos, entre otros.

### **Comando *hostname* (Windows/Linux)**

Comando que se utiliza para saber el nombre del *host* en el que se está trabajando.

En Windows, este nombre y el dominio al que pertenece el *host* se configuran accediendo a Panel de Control -> Sistema -> Configuración avanzada del Sistema -> (Pestaña) Nombre de Equipo.

En Linux, se puede modificar el *hostname* mediante el comando: ***hostname "nuevo\_host"*** (se debe ser *root*) o siguiendo los siguientes pasos:

1. Editando el fichero */etc/hostname* con el nuevo nombre
2. Editando el fichero */etc/hosts* modificando la segunda línea con el nuevo nombre escogido.

Para modificar el grupo de trabajo, debes editar el fichero ***/etc/samba/smb.conf*** y en concreto, la línea donde dice "WORKGROUP=" incluyendo el nuevo nombre.

### **Comando *ping* (Windows/Linux)**

Este comando, disponible tanto bajo Windows como bajo Linux, se utiliza para comprobar el estado de la conexión con uno o varios *host*.

Simplemente lo que hace es enviar una serie de paquetes de solicitud de eco (echo request) a los *hosts* especificados. Estos, si funcionan

correctamente, enviarán automáticamente tantos paquetes de respuesta de eco (echo reply) como de solicitud hayan recibido.

El comando ping utiliza el protocolo ICMP (Protocolo de mensajes de control de Internet) que establece las normas de creación de los paquetes echo request y reply.

### **Comando Netstat (Windows/Linux)**

Con este comando se puede comprobar el estado de las conexiones que mantiene el PC (puertos abiertos), también puede mostrar una serie de estadísticas relacionadas con el protocolo TCP/IP.

### **Trazar rutas: comando tracert (Windows) o traceroute (Linux)**

El nombre de este comando proviene de Trace Route o trazador de rutas. Consiste en una herramienta de diagnóstico que determina el camino más probable que se tomara al establecer la comunicación con un *host*.

Esto lo hace enviando paquetes de echo *request* ICMP con valores variables de Período de Vida (TTL) para el destino.

Cada *router* de la ruta de acceso debe decrementar el período de vida de un paquete al menos en 1 antes de ponerlos en ruta. Cuando el Período de vida de un paquete llegue a 0, se supondrá que el *router* debe devolver al sistema de origen un mensaje de tiempo excedido (protocolo ICMP).

Para determinar la ruta, *tracert* o *traceroute* envía el primer paquete con un período de vida de 1 y lo incrementa en una unidad en cada transmisión posterior hasta que el destino responda o se alcance el período de vida máximo.

La ruta se determina examinando los mensajes de tiempo excedido ICMP enviados de vuelta por los *routers* intermedios. Sin embargo, algunos *routers* no devuelven los paquetes con valores de período de vida caducados, por lo que son invisibles para *tracert/traceroute* quedando la traza incompleta.

Para los usuarios de Linux, existe la posibilidad de usar el paquete *tracpath* que ofrece una información similar.

(En caso de no tener instalado ninguno de ellos, ejecuta *sudo apt-get install tracerout* para la instalación del paquete).

### **Comando finger (Windows/Linux)**

Este comando muestra información sobre un usuario de un sistema especificado que ejecuta el servicio *Finger*. La información de salida varía en función del sistema remoto.

Se puede ejecutar en modo local para comprobar toda la información de los usuarios que usan el equipo o en modo remoto. Habitualmente, de modo remoto suele estar desactivado su acceso puesto que es mucha la información a la que se tiene acceso con su ejecución.

### **Comando pathping (Windows)/mtr (Linux)**

Este comando es una herramienta de traza de rutas que combina características de los comandos *ping* y *tracert/traceroute* con información adicional que ninguna de esas herramientas proporciona. El comando *pathping/mtr* envía paquetes a cada *router* de la ruta hasta el destino final durante un período de tiempo y, a continuación, calcula los resultados en función de los paquetes devueltos en cada salto. Puesto que el comando muestra el nivel de pérdidas de



paquetes en un vínculo o *router* específicos, es sencillo determinar qué *routers* o vínculos podrían estar causando problemas en la red

## Desarrollo

**Obtén los siguientes datos de tu equipo y explica cómo se consiguen**

- Dirección física
- Dirección IP
- Tipo de Red
- *Hostid*
- *Netid*
- Mascara de la subred
- ¿Existen subredes?, ¿por qué?
- Nombre del *Host*
- Dominio

**Realiza los siguientes ejercicios y describe los pasos seguidos**

1. Visualiza la tabla ARP, comenta que entradas aparecen y  justifica su aparición ¿Has utilizado alguna opción?
2. Haz un ping al PC de algún compañero que no esté en la tabla. ¿Qué debería ocurrir? ¿Qué camino crees que siguen los paquetes?
3. Visualiza de nuevo la tabla ARP, ¿qué observas? Justifica lo que haya ocurrido.
4. Añade ahora la dirección de ese/a mismo/a compañero/a a la tabla ARP como una entrada estática. Explica cómo lo has hecho y, si no ha sido posible, contesta a las tres siguientes cuestiones con lo que crees que ocurre.
5. Visualiza la tabla ARP, ¿qué diferencia hay?
6. Borra la entrada estática de la tabla ARP.
7. Vuelve a visualizar la tabla, ¿qué observas?
8. Con **nslookup** averigua el servidor DNS principal al que accede tu PC. Anota la dirección IP. ¿Tiene sentido?
9. Con **nslookup** localiza las IP de los siguientes servidores Web:
  - a. [www.uca.es](http://www.uca.es)
  - b. [www.google.com](http://www.google.com)
  - c. [www.ubuntu.com](http://www.ubuntu.com)
  - d. [www.microsoft.com](http://www.microsoft.com)
10. Haz un ping a la dirección 127.2.3.4, ¿a dónde estoy  enviando los paquetes Echo ICMP?
11. Averigua por qué *host* pasan los paquetes hasta llegar a:
  - a. [merlin.uca.es](http://merlin.uca.es)
  - b. [www.ieee.org](http://www.ieee.org)



En caso de no conseguir alcanzar los *hosts* especificados, considera otros para conseguirlo.

¿Qué comando estás empleando? ¿Alguna opción?

Escribe los saltos y una breve reseña sobre el resultado obtenido.

12. Abre tres terminales y, de forma que puedas ver las tres ventanas al mismo tiempo junto con el navegador, sigue los siguientes pasos:

a. En un terminal ejecuta un comando del TCP/IP que te permita ver las conexiones que realiza tu *host* cada 2 segundos.

b. En otro haz un ftp al siguiente servidor de pruebas: [speedtest.tele2.net/](http://speedtest.tele2.net/) (usuario: *anonymous*, *sin contraseña*). Puedes emplear cualquier otro servidor ftp que conozcas.

-Para hacer ftp, desde el terminal escribir:

***ftp "nombre\_servidor"***

- *quit* es el comando para salir de la sesión de ftp

c. En otro terminal, haz un telnet a la siguiente dirección: *towel.blinkenlights.nl 23*.

-Para hacer ftp, desde el terminal escribir:

***telnet "nombre\_servidor"***

d. Desde el navegador, abre una web.

¿Qué observas en la primera ventana? Escribe una reseña de lo que ha ocurrido y lo que estás viendo.

13. Averigua algunos de los rangos de direcciones IP que tiene la red de la empresa ONO. Detalla cómo lo has hecho. ¿Lo podrías hacer desde tu equipo?

14. Averigua los servidores DNS de la red de la empresa ONO. Detalla cómo lo has hecho. ¿Lo podrías hacer desde tu equipo?

15. ¿Cuál es el nombre descriptivo de la red a la que pertenece el *host* en el que estás trabajando?