

Práctica 4

Configuración de red

Objetivos

- Conocer la disposición física de las interfaces y puertos de red disponibles en un equipo.
- Saber configura el protocolo TCP/IP correspondiente a una conexión de red.
- Conocer las herramientas básicas de diagnóstico de la red, así como su utilización para diagnosticar problemas de configuración de la red.
- Comprender la relación entre el nombre de un equipo y la configuración del DNS de la organización.
- Comprobar el funcionamiento de un equipo conectado a más de una red.
- Aprender a configurar una conexión de red directa entre dos equipos.

1 Introducción

En el estudio de las comunicaciones entre ordenadores son especialmente relevantes los conceptos de 1) *protocolo* y 2) *arquitectura de protocolos*. Un *protocolo* puede definirse como un conjunto de reglas que gobiernan el intercambio de datos entre dos entidades (entendiéndose por entidad, una aplicación o un sistema informático). Sin embargo, definir todas las tareas necesarias para comunicar entidades en un único protocolo resultaría demasiado inflexible. Debido a ello, resulta mucho más adecuado dividir dichas tareas entre múltiples protocolos que gobiernen el proceso global de las comunicaciones apoyándose unos en otros. Habitualmente los protocolos se organizan en capas o niveles, de modo que cada capa o nivel tiene asignado un conjunto definido de tareas dentro del proceso global de la comunicación. La organización en capas o niveles del software de comunicaciones es lo que se conoce como *arquitectura de protocolos*.

En las plataformas Windows modernas la gestión de las comunicaciones entre ordenadores se realiza mediante la arquitectura de protocolos TCP/IP. Esta arquitectura puede representarse mediante el modelo de capas mostrado en la figura 1. Este modelo organiza en 4 niveles o capas los diferentes protocolos requeridos para llevar a cabo comunicaciones entre ordenadores. La capa de aplicación define los protocolos usados por las aplicaciones que utilizan la red. Ejemplos de protocolos en la capa de aplicación son el SMTP para gestionar el correo electrónico y el HTTP para proporcionar acceso a la Web. La capa de transporte proporciona las funciones de comunicación necesarias

para establecer canales de comunicación entre aplicaciones situadas en sistemas diferentes¹. Para ello define los protocolos TCP y UDP. La capa de Internet gestiona el enrutamiento de datos, determinando la red a la que debe ser enviado cada paquete de datos a comunicar. Para esto, la capa de Internet define el protocolo IP. Y la capa de acceso a red gestiona las interfaces físicas de comunicación ubicadas en los computadores. Estas interfaces reciben habitualmente la denominación de NIC (*Network Interface Card*). La tecnología de NICs utilizada actualmente de forma estándar es Ethernet, que usa el protocolo de comunicación CSMA/CD.



Figura 1: Arquitectura de protocolos TCP/IP

En la figura 2 se muestran dos plataformas Windows en proceso de comunicación, así como la organización en capas del software de comunicaciones TCP/IP en dichas plataformas. La figura representa un navegador de Internet accediendo a un servidor web.

En relación con la organización del software de comunicaciones TCP/IP, en la figura 2 se observa cómo la capa de aplicación se implementa en programas de aplicación y en programas de sistema. Así por ejemplo, según se muestra en la figura, el programa de aplicación *navegador de Internet* y el programa de sistema *servidor web* implementan el protocolo HTTP, que es un protocolo estándar perteneciente al nivel de aplicación. Ambos programas, navegador y servidor web, se comunican utilizando dicho protocolo. El software correspondiente a las capas de transporte (TCP/UDP) e Internet (IP) se implementa en un *driver*, que recibe el nombre de *driver de protocolos*. Como todo *driver*, el *driver* de protocolos se integra en el núcleo de la plataforma Windows. El software de la capa de acceso a red (que contiene el protocolo CSMA/CD) se implementa en el *driver* de cada NIC integrada en el sistema. Como se muestra en la figura, un sistema puede integrar varias NICs, con objeto de conectar el sistema a varias redes. El sistema utilizará una u otra NIC en función de la red por la que desee comunicar.

¹ La capa de transporte también permite comunicar aplicaciones que se encuentran en el mismo sistema.

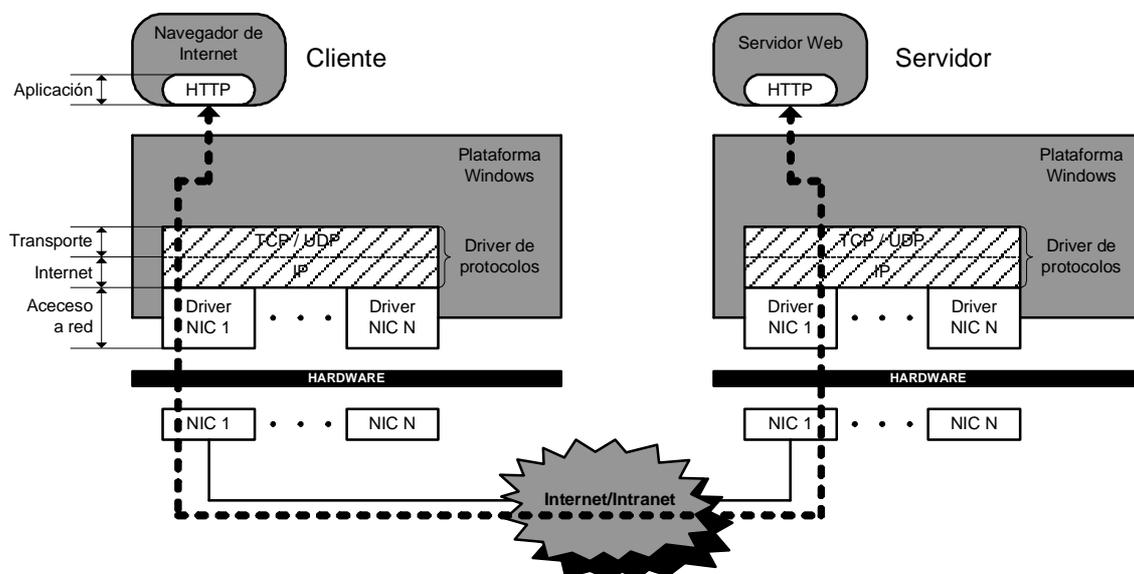


Figura 2: Organización del software de comunicaciones TCP/IP en la plataforma Windows

Desarrollo de la práctica

2 La dirección IP

La dirección IP es un valor de 32 bits (4 bytes) que identifica singularmente a cada dispositivo conectado a una red TCP/IP, como por ejemplo, Internet. Las direcciones IP se escriben habitualmente utilizando cuatro números decimales separados por puntos. Cada número decimal representa un byte de los cuatro existentes en la dirección, y cada uno de los cuatro números debe estar en el rango [0, 255], que es el rango de números naturales representables con un byte de información. Un ejemplo de dirección IP es la 150.20.247.35.

La dirección IP se estructura en dos partes: la parte de red y la parte de *host*. No obstante, el reparto de bits entre la parte de red y la parte de *host* es configurable mediante otro valor de 32 bits conocido como máscara de subred. Esta máscara funciona de la siguiente forma: si un *bit* en la máscara se encuentra a '1', el *bit* correspondiente en la dirección pertenece a la parte de red; si un *bit* en la máscara se encuentra a '0', el *bit* correspondiente en la dirección pertenece a la parte de *host*.

Imaginemos por ejemplo que a la dirección 150.20.247.35 se le aplica la máscara de subred 255.255.255.0. Esta máscara indica que los 24 bits más significativos de la dirección son la parte de red y los 8 bits menos significativos, la parte de *host*. Por lo tanto, en este caso, la parte de red de la dirección está formada por los 24 bits correspondientes a los valores 150.20.247, y la parte de *host*, por los 8 bits correspondientes al valor 35.

Una dirección IP cuya parte de *host* está todo a '0' se utiliza para expresar la subred completa. Así en el caso de la dirección anterior (IP = 150.20.247.35; máscara = 255.255.255.0), la forma de indicar la subred a la que pertenece la dirección es mediante la dirección especial 150.20.247.0.

Teniendo en cuenta toda la información anterior, la forma habitual de expresar el significado de la dirección 150.20.247.35 con máscara 255.255.255.0 sería: *host* 35 en la subred 150.20.247.0.

Vamos a ver otro ejemplo un poco más complicado. Supongamos que a la dirección anterior (150.20.247.35) se le aplica la máscara de subred 255.255.240.0. En este caso la separación de las partes de red y de *host* no es tan inmediata. Esto es debido a que en el byte de la máscara de valor 240, parte de sus bits están a '1' y otra parte a '0'. Nos resultará más fácil interpretar la dirección si descomponemos en binario el byte de la máscara de valor 240 así como el byte correspondiente en la dirección IP, y los contrastamos, tal y como se muestra a continuación:

	Parte de red	Parte de host
Máscara de subred: 255.255.240.0	-> 255.255.1111	0000.0
Dirección IP: 150.20.247.35	-> 150.20.1111	0111.35
Dirección subred:	-> 150.20.1111	0000.0
	-> 150.20.240.0	

El análisis anterior nos indica que la forma habitual de expresar el significado de la dirección 150.20.247.35 con máscara 255.255.240.0 sería: *host* 1827 en la subred 150.20.240.0. El número de *host* se calcula traduciendo a decimal el número binario correspondiente a la parte de *host* de la dirección.

H Teniendo en cuenta la explicación anterior determina el *host* y la dirección de la subred correspondientes a la dirección IP 125.18.143.14; máscara 255.255.128.0. Contesta a continuación.

–Pregunta 1–

Host:
Subred:

El mecanismo utilizado para expresar las direcciones IP mediante la dirección y la máscara de subred resulta un tanto engorroso. Debido a ello, suele utilizarse una notación alternativa más concisa, que se explica a continuación.

La máscara siempre está formada por un conjunto de unos en su parte izquierda y un conjunto de ceros en su parte derecha. Así por ejemplo, la máscara 255.255.255.0 tiene 24 unos a la izquierda y 8 ceros a la derecha. Para indicar que una dirección IP utiliza la máscara 255.255.255.0 se usa la notación /24 justo a continuación de la dirección IP. El indicador /24 significa que la máscara de subred tiene 24 unos. Así la dirección 150.20.247.35/24 significa dirección IP 150.20.247.35 con máscara de subred 255.255.255.0.

H Indica a continuación la máscara de subred utilizada en la dirección 150.20.7.35/18.

–Pregunta 2–

--

3 La interfaz de red

Empezaremos por identificar los puertos de red disponibles en los equipos del laboratorio.

H Desenchufa los cables traseros del ordenador Windows Server 2003 de tu mesa de trabajo. Entonces dale la vuelta al ordenador de forma que puedas observar su parte trasera.

En la figura 4 se muestran el conjunto de conectores del computador conocidos como conectores del panel posterior. Se trata de conectores integrados en la placa base que se hacen accesibles mediante agujeros mecanizados en el panel posterior de la caja del computador. El conector de red está marcado con un círculo. La disponibilidad de un conector de red entre los conectores del panel posterior significa que una interfaz de red viene integrada en el hardware de la placa base del sistema.



Figura 4: Conectores del panel posterior

Debajo de los conectores del panel posterior está el área correspondiente a las tarjetas de expansión. Estas tarjetas se pinchan en las ranuras de expansión de la placa base, y proporcionan conectores para periféricos externos que se hacen accesibles a través de ranuras abiertas en la parte posterior de la caja.

H Pon tu atención en el área de tarjetas de expansión. En ella debes observar tres elementos. Yendo de arriba hacia abajo, el primer elemento es la interfaz de vídeo. A continuación, se observa un *bracket* SATA (que permite conectar discos duros SATA externos), y finalmente una tarjeta de red, en la que se observa el conector de red correspondiente.

Ahora vas a buscar información sobre la tarjeta de red instalada en el computador. El fabricante de esta tarjeta es TP-LINK y el modelo, el TG-3269.

H Busca la web del fabricante y entra en ella. En el enlace de *Productos*, busca la categoría *Gigabit network adaptares* y entra en ella. A continuación busca información sobre el modelo TG-3269. Contesta las siguientes preguntas relativas a esta interfaz de red.

-Pregunta 3-

Velocidades posibles de transmisión de datos:

Tipo de bus (bus del computador en el que se conecta):

Si observas la parte posterior de la tarjeta podrás ver cuatro indicadores led. Uno de ellos está marcado como FXD. ¿Qué señala este indicador?

H Antes de continuar, vuelve a enchufar todos los cables al ordenador Windows Server 2003 con objeto de dejarlo listo para su utilización. Recuerda que el puerto de red que utilizamos habitualmente para conectar los equipos es el correspondiente al panel posterior.

Configuración de las interfaces

H Inicia sesión como *administrador* en el ordenador Windows Server 2003 de tu mesa de trabajo.

H La configuración de las interfaces de red es accesible a través de *Panel de control* -> *Conexiones de red*. Esta opción muestra un menú en el que se observan las conexiones de red disponibles en el sistema. No obstante, en vez de acceder a las conexiones de esta forma, si pulsas con el botón derecho del ratón sobre la entrada del menú *Conexiones de red* y eliges *Abrir*, se abre una ventana con las conexiones disponibles. Hazlo de esta manera, abre la ventana *Conexiones de red*.

En la ventana *Conexiones de red* debes observar tantas conexiones como interfaces de red estén disponibles en el equipo. Cuando se instala el sistema operativo, éste detecta todas las interfaces de red disponibles y genera una conexión de red para cada interfaz. De forma estándar, a la primera conexión se le da el nombre *Conexión de área local*, a la segunda conexión, *Conexión de área local 2* y así sucesivamente. Después, podremos cambiar estos nombres por otros más apropiados según el objetivo de la conexión. Por ejemplo, en nuestro caso, una conexión corresponde al conector de red del panel posterior, y la otra, al conector de la tarjeta PCI integrada en el sistema. Vamos a cambiar entonces los nombres de estas conexiones para que reflejen de una forma más precisa los conectores de red a los que hacen referencia.

H La conexión denominada *Conexión de área local* se corresponde con el conector de red del panel posterior. Podemos llamarla entonces *Conexión panel posterior*. Haz clic sobre ella y dale este nombre. La conexión denominada *Conexión de área local 2* se corresponde con el conector de la tarjeta de red PCI. Cámbiale el nombre por *Conexión tarjeta PCI*. De las dos conexiones, solamente *Conexión panel posterior* debe encontrarse en funcionamiento, ya que es la que está conectada a la infraestructura de comunicaciones del laboratorio. *Conexión tarjeta PCI* se encontrará marcada con un aspa roja, que indica que esta conexión de red está desconectada (no hay cable) en este momento.

H Haz doble clic sobre *Conexión panel posterior*. Como esta conexión está en funcionamiento, se abre la ventana *Estado de Conexión panel posterior*. En la pestaña *General* se muestra información sobre el estado de funcionamiento de la conexión. Se indica el tiempo que lleva en funcionamiento, la velocidad de funcionamiento (100Mbps) y el número de paquetes de datos enviados y recibidos. Pulsa sobre la pestaña *SopORTE* para ver información de la configuración IP de la interfaz.

H Ahora analizaremos algunos detalles relativos a la configuración de esta conexión (*Conexión panel posterior*). Para ello vuelve a la pestaña *General*. Entonces para configurar la conexión pulsa en el botón *Propiedades*. Se abre entonces la ventana *Propiedades de Conexión panel posterior*. En la ficha *General* se pueden configurar diversos aspectos de funcionamiento de la conexión. Pulsa en el botón *Configurar* para gestionar la interfaz de red asociada a esta conexión. Se abre entonces la ventana *Propiedades de Realtek RTL8168/8111 PCI-E Gigabit Ethernet NIC*. El título de esta ventana indica el nombre exacto de la interfaz de red. En el cuadro titulado *Estado del dispositivo* se indica si la interfaz está funcionando correctamente, o si por el contrario presenta algún problema. En la ficha *Controlador* se proporciona información sobre el controlador de dispositivo

(*driver*), que está integrado en el núcleo de Windows para controlar esta interfaz. Indica a continuación quién es el proveedor de este controlador.

-Pregunta 4-

H Cierra la ventana *Propiedades de Realtek RTL8168/8111 PCI-E Gigabit Ethernet NIC*, lo que te lleva de nuevo a la ventana *Estado de Conexión panel posterior*. Pulsa en *Propiedades* para volver a *Propiedades de Conexión panel posterior*.

En el recuadro titulado *Esta conexión utiliza los siguientes elementos* se indican el conjunto de clientes, servicios y protocolos que están disponibles para esta conexión. El elemento *Cliente para redes Microsoft* es un cliente, los elementos *Equilibrio de carga de red* y *Compartir impresoras y archivos para redes Microsoft* son servicios y el elemento *Protocolo de Internet TCP/IP* es un protocolo. Dejaremos los clientes y los servicios para otras prácticas y nos centraremos ahora en los protocolos. Como acabas de observar el protocolo de red instalado de forma estándar en la plataforma Windows para gestionar las comunicaciones es el TCP/IP. Veamos que otros protocolos están disponibles.

H Pulsa el botón *Instalar*. Se abre la ventana *Seleccionar tipo de componente de red*. En esta ventana puedes elegir entre *Cliente*, *Servicio* y *Protocolo*. Elige *Protocolo* y pulsa *Agregar*. Se abre la venta *Seleccionar el protocolo de red*. En esta ventana el *Protocolo de Internet (TCP/IP)* no está disponible, debido a que ya se encuentra instalado². No vas a instalar ninguno de estos protocolos, ya que las aplicaciones y servicios que se ejecutan de forma estándar en las plataformas Windows actuales se basan en el *Protocolo de Internet (TCP/IP)* ya instalado en el sistema.

H Uno de los protocolos disponibles para instalar es el *Apple Talk*. Busca en la Wikipedia información sobre este protocolo y contesta las siguientes preguntas.

-Pregunta 5-

¿Para qué tipo de sistemas fue desarrollado?

Actualmente se trata de un protocolo obsoleto. ¿Por qué otro protocolo ha sido sustituido en dichos sistemas?

Con relación a los protocolos, la conclusión es que la plataforma Windows proporciona un conjunto de protocolos alternativos a TCP/IP, siendo su objetivo permitir la conectividad de la plataforma Windows 2003 a otros sistemas (más bien obsoletos), que no soportan comunicaciones basadas en TCP/IP.

H Cierra todas las ventanas que tengas abiertas relativas a las conexiones de red.

² El *Protocolo de Internet TCP/IP* que se encuentra instalado en el sistema es el protocolo TCP/IP versión 4, que trabaja con direcciones de 32 bits. El protocolo *Microsoft TCP/IP versión 6* que observas en la venta *Seleccionar el protocolo de red* es el nuevo protocolo propuesto para gestionar Internet, basado en direcciones de 64 bits. No obstante, actualmente este protocolo cuenta con una difusión extremadamente limitada en las comunicaciones actuales.

Configuración básica del protocolo TCP/IP

Debido a que de forma estándar las comunicaciones en la plataforma Windows se hacen mediante el protocolo TCP/IP, una parte esencial de la configuración de red es la configuración de este protocolo.

La primera idea fundamental respecto a la configuración de este protocolo es que la configuración no es global para todo el sistema, sino que se realiza para cada interfaz de red instalada en el sistema. Como en nuestro sistema hay dos interfaces, cada una de ellas tendrá asignada una determinada configuración. Vamos a analizar esto.

H En el *Panel de control* abre la ventana *Conexiones de red*. En ella observa *Conexión panel posterior* y *Conexión tarjeta PCI*, correspondientes a las dos interfaces de red instaladas en el sistema. En primer lugar vas a comprobar que cada una de ellas tiene su propia configuración. Abre *Conexión panel posterior*, pulsa en *Propiedades*, entonces selecciona *Protocolo de Internet (TCP/IP)*. Pulsa en *Propiedades*. Se abre la ventana de configuración del protocolo. Anota a continuación la dirección IP asignada a esta conexión.

–Pregunta 6–

H Cierra todas las ventanas relativas a *Conexión panel posterior*. Entonces abre *Conexión tarjeta PCI*. A continuación abre las propiedades del protocolo TCP/IP y anota la dirección IP asignada a esta conexión.

–Pregunta 7–

H Cierra todas las ventanas relativas a *Conexión tarjeta PCI*.

Has comprobado que cada conexión de red está configurada con una dirección IP diferente.

¿Qué objetivo se persigue con tener varias conexiones (interfaces) de red en un ordenador? El propósito es que el ordenador pueda conectarse a varias redes diferentes, una por cada conexión, y cada red tendrá su propia configuración IP.

Ahora vamos a entrar en la configuración de cada una de estas interfaces red más detalladamente. Empezaremos por *Conexión panel posterior*.

H Mueve ligeramente el computador para observar el panel posterior y comprueba que el puerto de red correspondiente a esta conexión es el utilizado para conectar el computador a las bocas de red del laboratorio. Esto significa que esta conexión conecta el computador a la infraestructura de red de la Universidad y, a través de ella, a Internet. Analicemos entonces la configuración TCP/IP de esta conexión.

H Abre las propiedades del *Protocolo de Internet (TCP/IP)* correspondientes a *Conexión panel posterior*. Empezaremos analizando la *Dirección IP* y la *Máscara de red* de esta conexión. Observarás que la dirección IP es del tipo 156.35.151.XXX (correspondiendo las XXX al número del nombre del ordenador), y la máscara de subred es 255.255.255.0. Teniendo en cuenta estos valores y según lo visto en el apartado 2 de esta práctica, ¿en que subred TCP/IP se encuentra esta conexión? Debes contestar con un valor de 32 bits en notación decimal. Si tienes dudas pregúntale a tu profesor.

-Pregunta 8-

Todos los ordenadores del laboratorio se encuentran en la misma subred TCP/IP.

Pasaremos a analizar ahora el significado del campo *Puerta de enlace predeterminada*.

Los ordenadores que se encuentran en una misma subred TCP/IP pueden encontrarse y establecer comunicaciones entre ellos sin necesidad de utilizar ningún dispositivo intermediario. Sin embargo, cuando un ordenador A necesita establecer una comunicación con otro ordenador B que se encuentra en una subred TCP/IP diferente, el software TCP/IP de A necesita encontrar una ruta válida para alcanzar el ordenador B. Estas rutas son proporcionadas por unos dispositivos conocidos como *routers*. El *router* que da servicio a una determinada subred tendrá asignada una de las direcciones IP de esa subred. Pues bien, la dirección IP del *router* que sirve a una determinada subred es el valor que debe indicarse en el campo *Puerta de enlace predeterminada* de los ordenadores que se encuentran en dicha subred.

H Indica a continuación la dirección IP del *router* que da servicio a los PCs del laboratorio.

-Pregunta 9-

Una vez conocido el concepto de *puerta de enlace predeterminada*, las comunicaciones TCP/IP realizadas por un ordenador se pueden explicar de una forma muy sencilla. Si el ordenador necesita comunicar con otro ordenador que se encuentra en su misma subred, la comunicación se establece directamente entre ambos ordenadores. Sin embargo, si el ordenador necesita comunicar con otro ordenador que se encuentra en una subred diferente, entonces la comunicación se realizará a través del *router* o *puerta de enlace predeterminada* correspondiente.

En el recuadro inferior de la ventana *Propiedades de Protocolo de Internet (TCP/IP)* se configura el acceso del sistema al servidor DNS. El objetivo de este servidor es traducir nombres DNS en direcciones IP. La idea es que a un usuario le resulta mucho más cómodo acceder a un servidor utilizando su nombre DNS en vez de su dirección IP, ya que los nombres DNS son mucho más fáciles de recordar. Un ejemplo de nombre DNS es www.uniovi.es, que corresponde al servidor web de la Universidad. La dirección IP asignada a este servidor es 156.35.33.99. Obviamente, es mucho más amigable acceder a esta web utilizando el nombre DNS www.uniovi.es que su correspondiente dirección IP.

H Abre el navegador. Introduce en el campo dirección del navegador la siguiente dirección:

<http://156.35.33.99>

Comprueba que accedes a la web de la Universidad.

En este caso le hemos indicamos directamente al navegador la dirección IP (156.35.33.99) del servidor al que queremos acceder. Sin embargo, esta forma de proceder no es habitual. Lo corriente es indicarle al navegador el nombre DNS del servidor al que se desea acceder. En nuestro caso, www.uniovi.es.

H Cierra el navegador y vuelve a abrirlo. Introduce en el campo dirección del navegador la dirección <http://www.uniovi.es>. Comprueba que obtienes el mismo resultado que en el caso anterior.

En este segundo caso, le estamos indicando al navegador que acceda al servidor cuyo nombre DNS es www.uniovi.es. Pero el navegador lo que necesita es la dirección IP del servidor. Entonces el ordenador consulta a su servidor DNS asociado la dirección IP correspondiente al nombre DNS www.uniovi.es. El servidor DNS le indica que dicha dirección es 156.35.33.99, y a partir de aquí se continúa el proceso como en el primer caso.

El servidor DNS utilizado por el software TCP/IP de un ordenador es aquel cuya dirección IP se indica en el campo *Servidor DNS preferido* de la ventana *Propiedades de protocolo de Internet TCP/IP*. Si este servidor se encontrara fuera de conexión, se utilizaría como DNS el servidor cuya dirección se proporciona en el campo *Servidor DNS alternativo*.

H Vuelve a la ventana *Propiedades de protocolo de Internet TCP/IP* y toma nota de las direcciones de los servidores DNS de la Universidad.

–Pregunta 10–

Servidor DNS preferido:

Servidor DNS alternativo:

Vamos a hacer el experimento de eliminar los servidores DNS de la configuración TCP/IP.

H Haz que el campo *Servidor DNS preferido* quede en blanco. De la misma forma, haz que también quede en blanco el campo *Servidor DNS alternativo*. Pulsa en *Aceptar* para cerrar la ventana *Propiedades de protocolo de Internet TCP/IP*. Pulsa de nuevo en *Aceptar* para cerrar la ventana *Propiedades de Conexión panel posterior*. Pulsa en *Cerrar* para cerrar la ventana *Estado de conexión panel posterior*. Una vez que se han cerrado de esta forma todas estas ventanas se habrá aplicado la nueva configuración.

En este momento no hay servidor DNS configurado, por lo que debería quedar inhabilitada la utilización de nombres DNS.

H Abre el navegador e intenta acceder a www.uniovi.es. Según lo que se acaba de comentar, el navegador no debería acceder a esta dirección, ni a ninguna otra a través de un nombre DNS. Sin embargo, observarás que sí accede. Esto es debido a que el servicio del sistema que gestiona el acceso al servidor DNS mantiene un buffer con las direcciones DNS recientemente resueltas. Para eliminar este efecto hay que reiniciar el ordenador.

H Reinicia el ordenador. Inicia una nueva sesión. Abre el navegador. Debes comprobar que se muestra una página de error al intentar acceder a www.google.es, que es la dirección de la página de inicio configurada en el navegador. Ahora intenta acceder a www.uniovi.es y comprueba que también obtienes un error. El navegador no puede resolver los nombres DNS que le estamos indicando.

H Abre de nuevo la ventana de configuración del protocolo TCP/IP correspondiente a *Conexión panel posterior*. Configura *Servidor DNS preferido* y *Servidor DNS alternativo* usando las direcciones que anotaste en la pregunta 10. Cierra aceptando

todas las ventanas de configuración. Abre de nuevo el navegador y comprueba que ya puedes acceder a www.google.es y a www.uniovi.es.

4 Diagnóstico de la red

El software de la plataforma Windows proporciona un conjunto de herramientas que permiten obtener información de la red, así como diagnosticar su correcto funcionamiento. A continuación se presentan algunas de estas herramientas, que además, serán utilizadas en diversos experimentos de configuración de la red.

Ping

Esta es la herramienta principalmente utilizada para chequear el correcto funcionamiento de una conexión de red, ya que nos permite probar si un determinado ordenador es alcanzable. Esta herramienta se ejecuta desde una consola CMD. Al comando *Ping* se le pasa como parámetro la dirección IP o el nombre DNS del nodo que deseamos alcanzar. *Ping* opera enviando un paquete de datos de 32 bytes al nodo cuya dirección se le pasa como parámetro y esperando la respuesta. Si la respuesta se recibe en un tiempo satisfactorio, *Ping* indica mediante un mensaje que se ha recibido la respuesta. En el caso contrario, *Ping* muestra un mensaje indicando que se ha agotado el tiempo de espera para la solicitud. Este proceso se repite cuatro veces, es decir, *Ping* envía 4 paquetes de datos.

Para probar el funcionamiento de *Ping* vas a utilizar el ordenador XP de tu puesto de trabajo. Hasta ahora en la máquina XP has trabajado siempre como un usuario normal. Sin embargo, en esta práctica necesitarás utilizar un usuario con privilegios de administración. Para ello se ha habilitado en esta máquina el usuario *AlumnoAdmin*, clave *practicas*. Aunque para usar *Ping* no es necesario tener privilegios de administración, vas a utilizar el usuario *AlumnoAdmin* para todas las operaciones realizadas desde la máquina XP de tu mesa.

H Inicia una sesión en el ordenador XP de tu puesto de trabajo utilizando el usuario *AlumnoAdmin*. Abre una consola CMD. Ahora para probar la conectividad con el Windows Server, ejecuta el comando *Ping* seguido de la dirección IP del servidor, según el esquema que se indica a continuación:

```
ping 156.35.151.XXX
```

Ping debe indicar que hay conectividad con el servidor, mostrando que hay respuesta desde éste a los paquetes de datos enviados.

H Ahora vas a chequear la conectividad con una máquina que sabemos de antemano que no está disponible. Por ejemplo la IP 156.35.151.180 es una dirección que no está asignada a ninguna máquina. Haz *Ping* a esta dirección comprobando que no hay respuesta.

H Ahora vas a ubicarte de nuevo en la máquina Windows Server y vas a hacer diversos experimentos de conexión desde ella. Primero prueba que puedes hacer *Ping* desde ella a la máquina XP de tu mesa de trabajo. Ahora vas a hacer *Ping* utilizando el nombre DNS de la máquina destino. Por ejemplo, una máquina que sabemos que siempre está activa es el servidor de la EPSIG en el que se encuentran las carpetas de la asignatura, cuyo nombre DNS es *pin.epsig.uniovi.es*. Ejecuta entonces el comando

ping pin.epsig.uniovi.es

En este caso *Ping* preguntará primero al servidor DNS cuál es la dirección IP correspondiente al nombre DNS *pin.epsig.uniovi.es*. Después utilizará dicha dirección para enviar los paquetes de datos. En los mensajes generados por *Ping* se indicará la dirección IP del servidor. Escríbela a continuación:

–Pregunta 11–

--

H Recordarás que para acceder a la carpeta de la asignatura introduces en el campo *Abrir* de la ventana *Ejecutar* el nombre `\\pin.epsig.uniovi.es`. Ahora sabes que a este nombre DNS le corresponde la dirección IP que acabas de contestar en la pregunta interior. Entonces comprueba que puedes abrir la carpeta de la asignatura utilizando la dirección IP en vez del nombre DNS. Después cierra esta carpeta.

Aprovechando que ahora conoces la herramienta *Ping* para probar la conectividad entre sistemas, vas a realizar un experimento que te ayudará a comprender mejor el significado de la puerta de enlace predeterminada. Lo que vas a hacer es dejar en blanco el campo *Puerta de enlace predeterminada* de la configuración del protocolo TCP/IP del servidor de tu mesa de trabajo. Entonces vas a analizar cómo afecta este cambio de configuración a la conectividad del servidor con otros sistemas.

H En el Windows Server abre la ventana de configuración del protocolo de Internet (TCP/IP) correspondiente a la conexión del panel posterior. Deja en blanco del campo *Puerta de enlace predeterminada*. Cierra, aceptando, todas las ventanas de configuración para que se aplique la nueva configuración. Ahora haz *Ping* a la máquina XP de tu puesto de trabajo comprobando que hay conectividad. Después haz *Ping* a la dirección IP del servidor *pin.epsig.uniovi.es*. Para ello usa la dirección que contestaste en la pregunta 11. Entonces contesta las siguientes preguntas:

–Pregunta 12–

¿Hay conectividad con el servidor <i>pin.epsig.uniovi.es</i> ?
¿Qué mensaje muestra el comando <i>Ping</i> ?

Vamos a analizar los resultados de este experimento. Has eliminado la puerta de enlace en el servidor de tu mesa. Tras esto, observas que el servidor puede seguir accediendo al cliente de tu mesa de trabajo pero ya no puede acceder al servidor *pin.epsig.uniovi.es*. ¿Por qué el servidor puede seguir accediendo a un equipo y no a otro? La respuesta está en las subredes IP en las que se encuentran los equipos destino. El ordenador cliente de tu mesa de trabajo se encuentra en la misma subred IP que el ordenador servidor. Dicha subred es la 156.35.151.0. Por el hecho de estar ambos ordenadores en la misma subred, el servidor no necesita hacer uso de su puerta de enlace para alcanzar al cliente. Sin embargo, el servidor *pin.epsig.uniovi.es* se encuentra en una subred diferente. En concreto en la 156.35.141.0. Debido a esto, la única forma que tiene el servidor de tu mesa de trabajo de alcanzar al servidor de la EPSIG es a través de su puerta de enlace, pero como la has quitado de la configuración, no tiene acceso a ella y, consecuentemente, a ningún ordenador que esté fuera de la subred 156.35.151.0. De aquí viene el mensaje *Host de destino inalcanzable* devuelto por *Ping*, que significa que no hay una ruta posible hacia ese sistema.

H En el ordenador Windows Server de tu mesa de trabajo vuelve a dejar el campo *Puerta de enlace predeterminada* con el valor que tenía anteriormente. Si no

recuerdas el valor, puedes mirarlo en la configuración del equipo cliente, ya que todos los ordenadores del laboratorio utilizan la misma puerta de enlace.

H Una vez realizado el cambio anterior, utilizando el comando *Ping* comprueba que vuelves a tener acceso al servidor de la EPSIG.

Nslookup

Esta herramienta permite establecer una conexión con un servidor DNS e interrogar a dicho servidor sobre su contenido. Básicamente nos permitirá comprobar si un determinado nombre DNS se encuentra registrado y cuál es la dirección IP que tiene asignada. La herramienta *Nslookup* se ejecuta desde una consola CMD y, por defecto, establece conexión con el servidor DNS preferido establecido en la configuración del protocolo TCP/IP.

H En el Windows Server abre una consola CMD y ejecuta *Nslookup*. El comando indica que se establece una conexión con el servidor (DNS) predeterminado, que es *enol.si.uniovi.es* (ip = 156.35.14.2). Este servidor es el DNS principal de nuestra universidad.

Una vez que hemos entrado en *Nslookup*, éste se queda a la espera de las preguntas a realizar por el usuario. El símbolo '>' indica que se puede introducir una pregunta o comando. Las preguntas serán básicamente nombres DNS.

H Empezarás preguntando por un nombre no registrado para ver el comportamiento de *Nslookup* ante esta situación. Introduce *pin.epsig.uniovi.com*. *Nslookup* indica que no se puede encontrar este nombre. Ahora introduce *pin.epsig.uniovi.es*. Comprueba que *Nslookup* contesta con la dirección IP correspondiente a este nombre, lo que significa que el nombre se encuentra registrado en el servidor DNS. Finalmente, introduce el comando *Exit* para abandonar *Nslookup*.

Nslookup es una herramienta muy útil que nos permite comprobar si el servidor DNS de nuestra organización se encuentra correctamente configurado.

En este punto, antes de continuar con la práctica, vas a dejar las conexiones de red con los nombres que tenían originalmente en el equipo Windows Server.

H En el panel de control abre *Conexiones de red*. Cambia el nombre *Conexión panel posterior* por *Conexión de área local*. Después cambia el nombre *Conexión tarjeta PCI* por *Conexión de área local 2*.

5 Conexión de un equipo a varias redes

Los equipos del laboratorio cuentan con dos interfaces de red. Esto permitirá conectar cualquiera de estos equipos a dos redes diferentes. Puede haber diversas razones por las que sea necesario o útil conectar un equipo a varias redes. La razón más común es que el equipo actúe como *router* entre dos o más redes. En esta práctica trabajaremos con un escenario más sencillo. Configuraremos una red simple con los dos equipos de tu mesa de trabajo. El equipo Windows Server estará conectado a Internet mediante *Conexión de área local* (que corresponde al puerto de red del panel posterior). El equipo XP no estará conectado a Internet. Imagina que es un equipo que contiene información sensible y, por seguridad, queremos tenerlo desconectado de Internet. Sin embargo, deseamos que ambos equipos, el Windows Server y el XP, se encuentren interconectados. Para

ello estableceremos un enlace privado entre ambos equipos, usando *Conexión de área local 2* (que corresponde a la tarjeta de red instalada en el sistema). Resumiendo, el equipo Windows Server estará conectado a dos redes: Internet y la red privada que forma con el equipo XP. El equipo XP solamente estará conectado al equipo Window Server.

H Comenzaremos por desconectar el equipo XP. Tienes que tener abierta una sesión en este equipo con el usuario *AlumnoAdmin*. No es necesario desconectar físicamente el cable. Se puede inhabilitar la conexión desde el sistema operativo. Para ello, en *Panel de control* abre *Conexiones de red*. Pulsa con el botón derecho del ratón sobre *Conexión de área local* y elige *Desactivar*. El icono de la conexión se pone en color gris suave. Abre el navegador, comprobando que no hay acceso a Internet. Al desactivar la conexión es como si hubiésemos desenchufado el cable.

Ahora vamos a preparar *Conexión de área local 2* en ambos equipos antes de enchufar el cable que los interconecte. Para ello tendremos que configurar el protocolo TCP/IP en las conexiones de ambos equipos. Tendremos que asignar una dirección IP a cada equipo, de modo que ambas direcciones se encuentren en la misma subred. Cuando se establecen conexiones privadas entre equipos, es decir, que no conectan los equipos a Internet, se utilizan rangos de direcciones IP que están expresamente reservados para este uso. Por ejemplo, todas las direcciones correspondientes a la subred 192.168.0.0/16 están reservadas para configurar redes privadas. No obstante, esta subred es demasiado grande, así que podemos elegir una subred más pequeña dentro de ella para configurar nuestros equipos. Por ejemplo, podemos utilizar la subred 192.168.0.0/24.

H Indica a continuación la máscara de subred que corresponde a la subred 192.168.0.0/24. Si tienes dudas, pregúntale a tu profesor.

–Pregunta 13–

H En el ordenador Windows Server, abre la configuración del protocolo TCP/IP de *Conexión de área local 2*. Configura el campo *Dirección IP* con la dirección 192.168.0.XXX (*host XXX* en la subred 192.168.0.0/24). Configura el campo *Máscara de subred* con el valor contestado en la pregunta anterior. Ahora piensa en lo siguiente. ¿Es necesario configurar el campo *Puerta de enlace predeterminada*? ¿Por qué? Contesta a continuación:

–Pregunta 14–

Las direcciones de los servidores DNS tampoco hay que configurarlas, ya que no va a haber ningún servidor DNS en la red privada. Finaliza salvando la configuración.

H En el ordenador XP, siguiendo los mismos pasos que en el ordenador Windows Server, configura el protocolo TCP/IP de *Conexión de área local 2*.

H Activa *Conexión de área local 2* en ambos equipos, XP y Windows Server.

H Utilizando el cable de red proporcionado por tu profesor, conecta las tarjetas de red de ambos equipos.

NOTA:

Hay dos tipos de cables de red: directos y cruzados. Cuando un equipo se conecta a hardware de comunicaciones, se debe utilizar un cable directo. Sin embargo, cuando un equipo se conecta a otro equipo, debe utilizarse un cable cruzado. Los cables que conectan los equipos del laboratorio a las tomas de red ubicadas en la pared son directos, ya que mediante estas tomas, los equipos se conectan al hardware de comunicaciones del laboratorio. El cable que estás utilizando ahora para conectar los dos equipos de tu mesa de trabajo es cruzado.

No obstante, los *switches* de comunicaciones y las interfaces de red modernas permiten realizar conexiones con cables de red cruzados y directos, indistintamente.

H Ahora vas a probar la conectividad de la nueva conexión que acabas de establecer. En el Windows Server, haz *Ping* al equipo XP utilizando la IP privada que le acabas de asignar. Observa que tienes conexión. En el equipo Windows Server, prueba que sigues teniendo conexión a Internet, utilizando el navegador. Esta conexión se establecerá a través del puerto de red de su panel posterior. En el ordenador XP crea una carpeta en el escritorio y compártela. Accede a ella desde el ordenador Windows Server utilizando la dirección privada del ordenador XP.

Si las pruebas anteriores son satisfactorias, habrás comprobado cómo conectar directamente dos ordenadores a través de una conexión de red. También habrás observado cómo un ordenador puede funcionar conectado a varias redes.

6 Servicio de enrutamiento y acceso remoto

En este momento el ordenador XP se encuentra en una red privada, formada por él mismo y por el equipo Windows Server, y sin conexión a Internet. Sin embargo, el equipo Windows Server sí tiene conexión a Internet mediante *Conexión de área local*. Lo que vamos a hacer ahora es configurar el Windows Server como enrutador, con objeto de conectar el equipo XP a la red general de la universidad y, consecuentemente, a Internet. En nuestro caso el tipo de enrutamiento requerido se conoce como NAT (*Network Address Translation*), ya que el equipo XP se encuentra configurado con direcciones IP de tipo privado (192.168.XXX.XXX), que no son permitidas en Internet³.

Las capacidades de enrutamiento y acceso remoto son proporcionadas por el servicio *Enrutamiento y acceso remoto*, que se encuentra deshabilitado por defecto.

H Abre la consola *Servicios* y busca el servicio *Enrutamiento y acceso remoto*. Lee la descripción del servicio, comprobando que entre sus cometidos se encuentra el enrutamiento NAT. Comprueba también que se encuentra deshabilitado.

³ El enrutamiento NAT es el que se utiliza habitualmente en las redes domésticas para compartir la conexión a Internet del hogar entre varios ordenadores. No obstante, en dichas redes, el servicio NAT suele ser proporcionado por un router que se conecta al modem de cable o ADSL y que suele también proporcionar canales Wifi.

Ahora vas a habilitar este servicio y configurarlo para que proporcione la funcionalidad de router NAT.

H En *Herramientas administrativas* abre *Enrutamiento y acceso remoto*, lo que muestra la consola que te permite configurar este servicio. Esta consola te mostrará el equipo local como posible servidor de acceso remoto. Pulsa con el botón secundario del ratón sobre dicho equipo y selecciona *Configurar y habilitar enrutamiento y acceso remoto*. Esto abrirá el asistente para la instalación y configuración de este servicio. Pulsa *Siguiente* en la pantalla de bienvenida, lo que te lleva a la pantalla en el que se elige el tipo de servicio de enrutamiento deseado. Elige *Configuración personalizada* y en la siguiente pantalla, selecciona *NAT y Servidor de seguridad básico*. Entonces finaliza el asistente. El sistema indica que se ha instalado el servicio y pregunta si se desea iniciar. Contesta **SÍ**.

H Abre la consola *Servicios* y comprueba que ahora el servicio *Enrutamiento y acceso remoto* se encuentra iniciado.

Se pasará a continuación a configurar el servicio NAT, lo que es imprescindible para que funcione correctamente. Hay un aspecto esencial en la configuración de este servicio, que es la especificación del conjunto de interfaces de red utilizadas por él. Este servicio usará como mínimo dos interfaces: la interfaz que conecta el equipo a Internet, y que se conoce como *interfaz pública*, y la que conecta el equipo a la red privada, que se conoce como *interfaz privada*.

H Abre la herramienta *Enrutamiento y acceso remoto*. Abre la ayuda disponible en esta herramienta. Busca el tema de ayuda *Configurar el servidor de seguridad básico NAT*. En este tema encontrarás información sobre cómo agregar una interfaz a la traducción de direcciones y configurarla. Después de leer la ayuda correspondiente, deberás realizar las operaciones necesarias para agregar las interfaces pública y privada al sistema de traducción de direcciones. Cuando configures la interfaz pública NO es necesario que habilites la funcionalidad de *Servidor de seguridad básico*. Indica a continuación las conexiones de red que has elegido para las interfaces pública y privada:

–Pregunta 15–

Conexión para interfaz pública:

Conexión para interfaz privada:

H Para que el equipo XP de la red privada utilice el router NAT como su puerta de comunicación con Internet, habrá que configurar un parámetro de su protocolo TCP/IP (visto anteriormente en esta práctica) con el valor apropiado. ¿Cuál es dicho parámetro y con qué valor debe configurarse? Si tienes dudas, pregúntale a tu profesor.

–Pregunta 16–

H Realiza la configuración correspondiente a la pregunta anterior.

Si las operaciones anteriores han sido realizadas correctamente, el equipo XP debe tener acceso a la red general de la Universidad a través del servidor NAT. Vamos entonces a verificar la conectividad.

H Utilizando el comando *ping*, verifica la conectividad del equipo XP con la máquina *pin.epsig.uniovi.es* (cuya IP es 156.35.141.2). Utiliza la IP para llevar a cabo la verificación. Utilizando también la IP, verifica que puedes acceder a la carpeta de la asignatura.

Si la prueba anterior ha sido satisfactoria, el servidor NAT estará funcionando correctamente.

Analicemos ahora la conectividad utilizando nombres DNS.

H Repite las pruebas anteriores (*ping*, y acceso a la carpeta de la asignatura) utilizando el nombre DNS de la máquina *pin*. Observarás que no puedes conectar. Debes darte cuenta que el protocolo TCP/IP de la máquina XP no tiene configurado el servidor DNS, por lo que este servicio no está disponible.

El servidor NAT puede hacer de pasarela para las consultas DNS realizadas por los clientes de su red privada. La idea es simple: los clientes de la red privada envían sus consultas DNS al servidor NAT, y éste las reenvía al servidor DNS especificado en su interfaz pública. Para que esto funcione, habrá que llevar a cabo dos operaciones: 1) En los clientes de la red privada, especificar el servidor NAT como servidor DNS, y 2) habilitar la capacidad de resolución de nombres DNS en el servidor NAT.

H Configura el servidor DNS del equipo XP con la dirección privada del servidor NAT.

H Busca en la ayuda de la herramienta *Enrutamiento y acceso remoto* el tema *Habilitar la resolución de nombres para la traducción de direcciones de red*. Siguiendo las indicaciones de la ayuda, habilita esta capacidad en el servidor NAT.

H Verifica que puedes hacer *ping* a la máquina *pin.epsig.uniovi.es*, así como acceder a la carpeta de la asignatura, utilizando en ambos casos el nombre DNS de dicha máquina.

H Finalmente, dejaremos los ordenadores como estaban antes de realizar los apartados 5 y 6.

En el ordena XP:

- 1) Elimina la carpeta compartida que creaste en el escritorio en el apartado 5.
- 2) En *Conexión de área local 2* borra la configuración de *Puerta de enlace predeterminada* y *Servidor DNS*. Después desactiva esta conexión.
- 3) Activa *Conexión de área local*.
- 4) Comprueba que el ordenador tiene conexión a Internet. Para ello, utiliza el navegador.

En el ordenador Windows Server:

- 5) Deshabilitar el servicio *Enrutamiento y acceso remoto*. Para ello, abre la herramienta *Enrutamiento y acceso remoto*, pulsa con el botón derecho del ratón sobre el nombre del servidor [*ATCXXX(local)*] y selecciona *Deshabilitar enrutamiento y acceso remoto*.

- 6) Desconecta el cable cruzado de red y proporcióñaselo a tu profesor.

7 Ejercicios adicionales: el nombre de red

Durante el proceso de instalación de un equipo, hay que proporcionar un nombre, que será utilizado para identificar el equipo en la red en la que se encuentre integrado.

H Vas a ver el nombre de red del equipo Windows Server de tu mesa de trabajo. Para ello, pulsa con el botón derecho del ratón sobre *Mi PC* para abrir su menú contextual y elige la opción *Propiedades*. Se abre la ventana *Propiedades del sistema*. Selecciona la pestaña *Nombre de equipo*. Para ver cómo se organiza el nombre del equipo, pulsa el botón *Cambiar*. Observarás los campos *Nombre de equipo* y *Nombre completo de equipo*. Indica a continuación lo que hay en cada un de ellos:

–Pregunta 17–

Nombre de quipo:

Nombre completo de equipo:

Vamos a analizar más en detalle el significado de estos nombres. La forma de nombrar equipos en redes TCP/IP es mediante el convenio de nombres DNS. Este convenio organiza los nombres de los equipos en dominios. Entonces el nombre de un equipo queda organizado en dos partes: 1) un identificador del equipo dentro del dominio, y 2) un identificador del dominio al que pertenece el equipo. Con relación a la pregunta que contestaste antes, el campo *Nombre de equipo* contiene el nombre que identifica al equipo concreto dentro del dominio, y el campo *Nombre completo de equipo* contiene el identificador del equipo seguido del identificador del dominio al que pertenece.

H Indica el dominio DNS al que pertenecen los equipos del laboratorio

–Pregunta 18–

El nombre de este dominio ha sido asignado por los gestores de la red de la Universidad. *edv* significa Edificio Departamental de Viesques, y por consiguiente, todos los equipos que se encuentran en este edificio se nombran con este identificador de dominio.

H Pulsa el botón *Más...* para ver el nombre del equipo más desglosadamente. Ahora observarás el campo *Sufijo principal DNS del equipo*, en el que se indica el dominio DNS al que pertenece el equipo y el campo *Nombre NetBIOS del equipo*, que contiene el identificador del equipo en el dominio.

El concepto de NetBIOS viene de las antiguas plataformas Windows, que se comunicaban utilizando el protocolo NetBIOS en vez de TCP/IP. Esto ya no tiene mucha importancia, ya que ahora las plataformas Windows se comunican usando TCP/IP.

H Cierra todas las ventanas abiertas, cancelado, ya que no vamos a hacer ningún cambio en el nombre del equipo.

Una vez analizada la configuración del nombre de red de un equipo, cabe plantearse la siguiente reflexión: ¿qué importancia tiene dicha configuración para

la visibilidad del equipo en la red, es decir, por el hecho de configurar un equipo con un nombre de red, es automáticamente visible en la red con dicho nombre?

La respuesta es NO en las redes TCP/IP. Para alcanzar un equipo, lo que es importante es que aquél que quiera alcanzarlo conozca su dirección IP. Ahora bien, si el equipo que queremos alcanzar tiene asignado un nombre DNS registrado en un servidor DNS, podremos obtener su IP consultando al servidor DNS correspondiente.

Lo que hace que un equipo sea reconocido en una red con un nombre es que dicho nombre se encuentre registrado en un servidor DNS. No obstante, resulta obvio que las buenas prácticas de configuración de un equipo implican que la configuración del nombre de red de un equipo coincida con el nombre registrado para el equipo en el servidor DNS correspondiente.

Vamos a realizar algunas pruebas relativas al nombre de red de los equipos y su relación con los servidores DNS. Haremos pruebas de conectividad entre los ordenadores XP y Windows Server de tu puesto de trabajo.

H Comprueba que en el ordenador XP de tu mesa tienes iniciada una sesión como *AlumnoAdmin*. Si no es así, iníciala.

H Verifica que en el ordenador Windows Server de tu mesa tienes abierta una sesión como *Administrador*. Si no es así, iníciala.

H En la máquina XP quieres comprobar la conectividad con la máquina Windows Server a través de su nombre DNS. Para ello, debes comprobar primero si el nombre DNS de la máquina Windows Server se encuentra registrado. En la máquina XP abre una consola y ejecuta *nslookup*. Esta herramienta se conecta con el servidor DNS de la universidad. La idea ahora es preguntarle a *nslookup* si el nombre DNS de la máquina Windows Server (*atcxxx.edv.uniovi.es*) se encuentra registrado. Haz esta consulta. Como el nombre está registrado, *nslookup* te contestará con la dirección IP de la máquina. Haz *Ping* desde la máquina XP a la máquina Windows Server utilizando el nombre DNS de ésta. Comprueba que hay conectividad.

H Ahora vas a cambiar la configuración del nombre de red en la máquina Windows Server. En esta máquina selecciona la pestaña *Nombre de equipo* en *Propiedades de sistema*. Pulsa *Cambiar* y en el campo *Nombre de equipo* sustituye el nombre *ATCXXX* por *PEPEXXX*. Pulsa *Aceptar* para guardar la nueva configuración. Entonces tendrás que reiniciar el equipo para que los cambios surtan efecto. Espera hasta que el equipo Windows Server haya arrancado completamente e inicia sesión en él como *Administrador*.

H Pasa de nuevo a la máquina XP. Vas a probar la conectividad desde esta máquina a la máquina Windows Server. En la máquina XP haz *Ping* a la máquina Windows Server utilizando su nuevo nombre DNS, es decir, *pepexxx.edv.uniovi.es*. ¿Hay conectividad?

La respuesta debe ser NO. La máquina XP no encuentra el nuevo nombre con el que hemos configurado la máquina Windows Server. Esto es debido a que este nuevo nombre no está registrado en el servidor DNS.

H En la máquina XP haz *Ping* a la máquina Windows Server utilizando su nombre DNS antiguo, es decir, *atcxxx.edv.uniovi.es*. ¿Qué ocurre? ¿Hay conectividad?

La respuesta debe ser SÍ. No importa que localmente el nombre de la máquina Windows Server haya cambiado. Cuando los clientes externos intentan acceder a ella por su

antiguo nombre, reciben una respuesta satisfactoria del DNS, es decir, una IP, y acceden a la máquina utilizando dicha IP. Este experimento demuestra que la visibilidad de un equipo en la red es debida al nombre registrado para el equipo en los servidores DNS y no al nombre de red que se configura en el equipo. No obstante, según se indicó anteriormente, las buenas prácticas de configuración de los sistemas indican que ambos nombres deben coincidir.

H En la máquina Windows Server vuelve a configurar el nombre de red del equipo con su nombre original. Entonces reinicia el equipo para que los cambios surtan efecto.