Práctica 8		**Fecha:**
Nombre ordenador par:		**Hora:**
Alumnos		
DNI:	Nombre:	Apellidos:
DNI:	Nombre:	Apellidos:

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.

Material necesario

Todo el material necesario le será suministrado al alumno durante la realización de la práctica.

Introducción

Arranca el ordenador impar con el CD de Linux mientras vas leyendo la introducción

En el estudio de las comunicaciones entre ordenadores son especialmente relevantes los conceptos de protocolo y 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*.

La arquitectura de protocolos más habitual en la actualidad es 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 diferentes[1]. 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. Finalmente, 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 Controller*). La tecnología de NICs utilizada actualmente de forma estándar es Ethernet, que usa el protocolo de comunicación CSMA/CD.

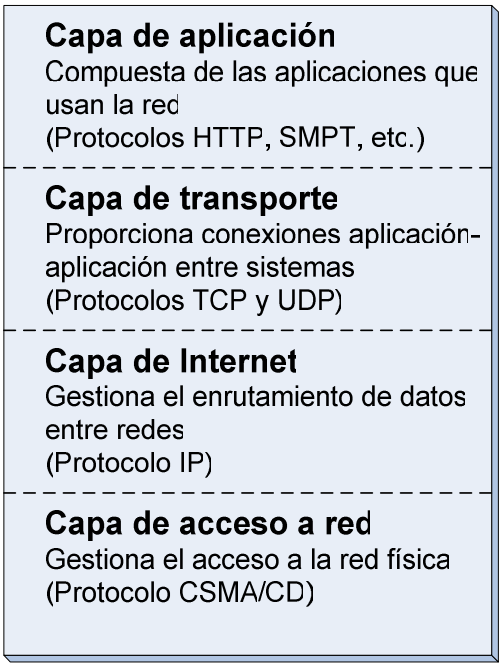

Figura 1: Arquitectura de protocolos TCP/IP

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 controlador (*driver*), que recibe el nombre de *controlador de protocolos*. Como todo controlador, el controlador de protocolos se integra en el núcleo del sistema operativo. El software de la capa de acceso a red (que contiene el protocolo CSMA/CD) se implementa en

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

el controlador 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.

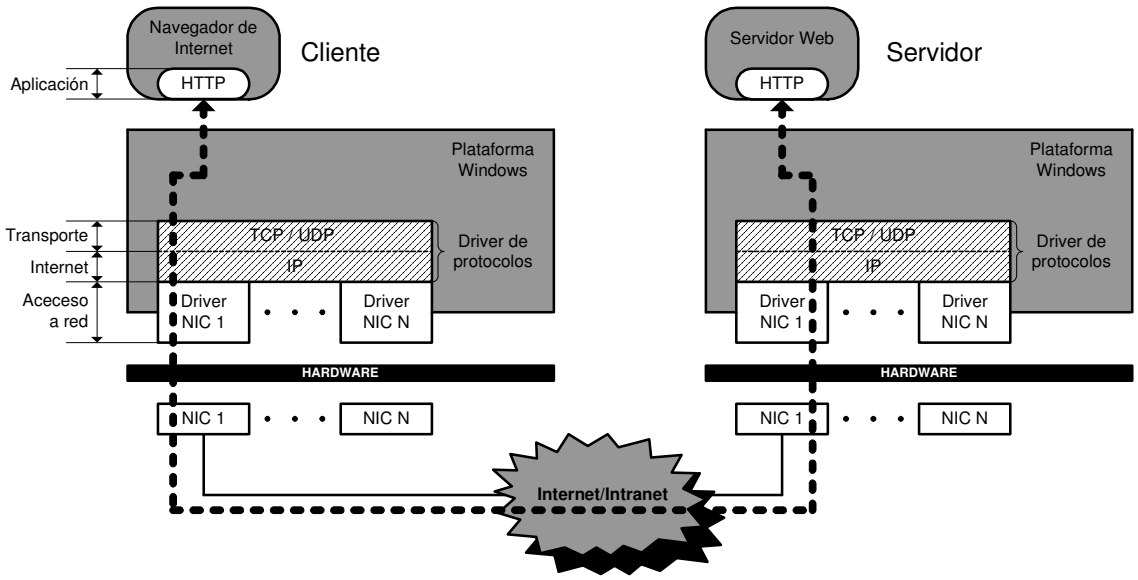

Figura 2: Organización del software de comunicaciones TCP/IP en la plataforma Windows

Desarrollo

1. La dirección IP

La dirección IP es un valor de 32 bits (4 bytes) que identifica unívocamente 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 7.35 en la subred 150.20.240.0.

- 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, rellena esta información:

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, a veces se utiliza 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.

- Indica a continuación la máscara de subred utilizada en la dirección 150.20.7.35/18:

2. La interfaz de red

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

En la figura 4 se muestra un conjunto de conectores del computador 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.

Observa el área de tarjetas de expansión de un ordenador del laboratorio. 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.

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.

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?

Configuración de las interfaces

Inicia sesión como *administrador* en el ordenador par de tu mesa de trabajo.

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.

- 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 encontrase 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.
- 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.
- 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.

- 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. 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.

- 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 instalado[2]. 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.

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.

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

Configuración básica del protocolo TPC/IP

Debido a que de forma estándar las comunicaciones 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.

- 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*, pula 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.

- 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.

[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.

- 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*.

- 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 la configuración TCP/IP de esta conexión.
- 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 estaos valores y según los 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.

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 encontrase y establecer comunicaciones entre ellos sin necesidad de utilizar ningún dispositivo intermediario. Sin embargo, cuado 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.

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

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 esta web utilizando el nombre DNS *www.uniovi.es* que su correspondiente dirección IP.

- 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*.

- 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*. El navegador lo que necesita es la dirección IP del servidor, así que 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 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*.

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

Servidor DNS preferido:
Servidor DNS alternativo:

3. Diagnóstico de la red

El software de 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 comprobar el correcto funcionamiento de una conexión de red, ya que 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*, si no se utilizan otros parámetros, 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.

- Abre una consola CMD. Ahora para probar la conectividad con la puerta de enlace, ejecuta el comando *Ping* seguido de su dirección IP: *ping 156.35.151.205*

  Ping debe indicar que hay conectividad con la puerta de enlace, mostrando que hay respuesta desde éste a los paquetes de datos enviados.

- 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.

- 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 cuyo nombre DNS es *pin.epsig.uniovi.es*. Ejecuta la orden *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:

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: es dejar en blanco el campo *Puerta de enlace predeterminada* de la configuración del protocolo TCP/IP y analizar cómo afecta este cambio de configuración a la conectividad del servidor con otros sistemas:

- 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 156.35.151.120 (el ordenador que está en la mesa del profesor), comprobando que hay conectividad. Después haz *Ping* a *pin.epsig.uniovi.es* pero con la dirección IP que contestaste antes. Contesta las siguientes preguntas:

¿Hay conectividad con el servidor *pin.epsig.uniovi.es*?
¿Qué mensaje muestra el comando *Ping*?

Vamos a analizar los resultados de este experimento. Has eliminado la puerta de enlace en el servidor de tu mesa. Tras esto, observas que puedes seguir accediendo al ordenador del

profesor ya no puedes acceder al servidor *pin.epsig.uniovi.es*. ¿Por qué tu ordenador 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 del profesor se encuentra en la misma subred IP que tu ordenador. Dicha subred es la 156.35.151.0. Por el hecho de estar ambos ordenadores en la misma subred, tu ordenador no necesita hacer uso de su puerta de enlace para alcanzar al del profesor. 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.

- Vuelve a dejar el campo Puerta de enlace predeterminada con el valor que tenía anteriormente.
- 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.

- 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.

- 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 ordenador par.

- 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*.

4. 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.

- Vas a ver el nombre de red del equipo par 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:

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.

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

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.

- 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. NetBIOS es un protocolo propio de Windows.
- 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.

5. Configuración de un router Linux utilizando NAT

1.1 Introducción

En esta parte de la práctica vas a utilizar el ordenador impar que arrancaste con Linux al principio de la sesión. La tarjeta de red integrada en la placa base estará conectada a Internet (red pública) y la tarjeta de red PCI se conectará a una red local (red privada). En nuestro caso la red local va a estar constituida por un solo ordenador: el ordenador par de la mesa. Esta configuración sería fácilmente extensible a múltiples ordenadores en la red local utilizando un *hub* al que iría conectada la tarjeta de la red privada del *router*. De hecho, esta es una configuración muy habitual, aunque en muchas ocasiones en lugar de utilizar un PC con Linux se utiliza un dispositivo específicamente diseñado para este cometido, siendo habitual que utilice también algún tipo de Linux, pero con la administración sólo a través de una interfaz web. Los conceptos (direcciones privadas, públicas, enrutamiento) son por lo tanto los mismos.

En esta ocasión vamos a suponer que se dispone de una dirección pública, proporcionada por el proveedor de Internet (*Internet Service Provider*, ISP), como Telefónica, Telecable, etc. En concreto, vamos a usar la dirección del ordenador impar, 156.35.151.xxx.

Para la red privada vamos a utilizar uno de los rangos de direcciones reservados para este uso, en concreto el 192.168.0.0/16. Muchos ordenadores en todo el mundo pueden tener la misma dirección en este rango, siempre y cuando no sea una dirección que se mande a Internet. De hecho, ese es el cometido del *router* en nuestro caso: recibir los paquetes de la red 192.168.0.0/16 y enviarlos con su dirección (156.35.151.xxx), que sí es válida para Internet. También tiene que hacer el proceso inverso: recibir paquetes de Internet y reenviarlos a los ordenadores de la red local correspondiente. Para distinguir de quién es cada paquete, utiliza puertos distintos del *router* para distintos ordenadores. De esta manera, cuando recibe un paquete por cierto puerto, sabe que se corresponde con cierto ordenador de la red local y se lo reenvía.

1.2 Conexión y configuración de las tarjetas de red

- Desconecta el cable de red del ordenador par de la pared y conéctalo a la tarjeta PCI del ordenador impar.

- Configura la tarjeta de red conectada a la pared (eth0) del equipo impar con su dirección pública (la que tiene habitualmente). Comprueba que tienes acceso a Internet ejecutando la orden *ping www.google.com*.

- Ahora debes configurar la otra tarjeta de red (eth1) con una dirección privada. En concreto, vas a utilizar la dirección 192.168.2.1, con máscara de subred 255.255.255.0. Deja la entrada para *gateway* vacía. No te olvides de arrancar la tarjeta de red mediante la orden *ifup eth1*.

- Ahora vas a configurar el ordenador par para que esté en la misma subred local privada que el ordenador impar. Pon la dirección 192.168.2.3. ¿Qué valor le tienes que poner como máscara de subred, cómo puerta de enlace y como DNS?

Máscara de subred: Puerta de enlace: DNS:

- Comprueba que el ordenador par puede acceder al *router* de su red privada ejecutando la orden *ping 192.168.2.1*. ¿Qué orden tienes que dar en el ordenador blanco para comprobar que puede acceder al ordenador negro?

- Ejecútala y comprueba que funciona. Si es así, ya tienes los dos ordenadores conectados correctamente y se pueden comunicar entre sí. Pero el ordenador par sólo puede acceder a la red local. Vamos a comprobarlo.

Ejecuta en el ordenador negro la orden *ping* 156.35.141.2 para intentar acceder a *pin.epsig.uniovi.es*, un ordenador conectado a Internet con una dirección pública. Deberás obtener un mensaje de error.

E so es debido a que las peticiones llegan hasta el ordenador impar pero este no las redirige a Internet. No puede hacerlo sin más porque la dirección del ordenador par no es válida en Internet.

1.3 Configuración de las tablas de encaminamiento

En Linux, se pueden definir reglas para trabajar con los paquetes que llegan por la red. Una lista ordenada de reglas a aplicar se denomina «cadena» (*chain*). Las cadenas, a su vez, se agrupan en tablas, sirviendo cada tabla para un propósito distinto. Estas son las tablas disponibles:

- **filter:** Sirve para filtrar paquetes. Permite utilizar *iptables* como un cortafuegos. Es la tabla por defecto.

- **nat:** Sirve para hacer traducción de direcciones de red (*Network Address Translation*), técnica que se explicará más adelante.

- **mangle:** Sirve para cambiar los contenidos de los paquetes, típicamente las cabeceras.

- **raw:** Sirve para marcar paquetes que no se desea que tengan seguimiento de la conexión (*connection tracking*). Es una tabla relativamente nueva que no siempre está presente.

Cada regla tiene una especificación que permite saber a qué paquetes se aplica y, opcionalmente, puede tener un objetivo que especifique qué hacer con el paquete si hay que aplicar la regla. Todos los paquetes que entran o salen del ordenador pasan al menos por una cadena. De esta forma, se pueden encaminar paquetes, aceptarlos o descartarlos, permitiendo así tener, además de un *router*, un cortafuegos. Cuando un paquete pasa por una regla, si

cumple su especificación, se le aplica el objetivo; si no, se aplica la política por defecto (*policy*).

Hay tres cadenas por defecto en la tabla *filter*:

- INPUT: Paquetes que llegan con destino la dirección de la máquina.
- OUTPUT: Paquetes que salen de la máquina.
- FORWARD: Paquetes que llegan a la máquina con la dirección de otra máquina.

A estas cadenas se les pueden aplicar dos políticas: ACCEPT (aceptar) y DROP (denegar).

Para mostrar las reglas que está aplicando un equipo, se puede ejecutar (como superusuario) la orden *iptables -L*. Ejecútala en el ordenador impar. ¿Qué política se sigue para las tres cadenas por defecto de la tabla por defecto (*filter*)?

Lo que debemos hacer es añadir una cadena para que cambie los paquetes que vengan del ordenador impar con una dirección privada y vayan hacia el exterior, de forma que tomen la dirección (pública) del ordenador par, utilizando un puerto distinto. A esto se le denomina en general NAT (*Network Address Translation*, traducción de direcciones de red) y, dentro de *iptables*, *masquerading* (enmascaramiento).

Vamos a indicar que se active el NAT con estas órdenes que debes ejecutar como superusuario (para ello, ejecuta antes *sudo –s*):

```
iptables --table nat --append POSTROUTING --out-interface eth0 -j
MASQUERADE

iptables --append FORWARD --in-interface eth1 -j ACCEPT

echo 1 > /proc/sys/net/ipv4/ip_forward
```

- La última línea sirve para que se active el encaminamiento en el núcleo, pero es también necesario reiniciar las interfaces de red. Para ello, para e inicia (con *ifdown* e *ifup* respectivamente) las dos interfaces de red.
- Vuelve a probar en el ordenador par la orden ping 156.35.14.2. ¿Cuál es la respuesta?

Sólo queda un problema: ahora mismo no puedes conectarte desde un ordenador de Internet a un servicio en el ordenador impar, ya que no tienes una dirección pública por la que conectarte. Una de las soluciones a este problema es volver a utilizar NAT, pero ahora de tal manera que se redirijan las peticiones un puerto concreto del ordenador impar al ordenador par.

- Descarga, en el ordenador par, la versión binaria para Win32 sin SSL del servidor web apache desde la dirección http://httpd.apache.org/download.cgi.

- Instálalo sólo para el usuario actual y utilizando el puerto 8080.
- Descubre, utilizando la orden *man* o buscando en Internet, qué orden tienes que dar para que se pueda acceder desde un ordenador exterior (por ejemplo, otro de los ordenadores del laboratorio conectado a Internet) al servidor web que has instalado. ¿Qué orden ha sido necesaria?

6. Finalización de la práctica

- Desinstala apache.
- Desconecta el cable que une los dos ordenadores y vuélvelo a conectar a la pared.
- Reconfigura el ordenador negro al que le habías cambiado la configuración de red con su configuración original. Comprueba que el equipo puede acceder a Internet.