

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.

Material necesario

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

Análisis de información en la red

1. Preparación

Una herramienta básica para detectar problemas de configuración en redes es el analizador de protocolos. En esta parte de la práctica se va a utilizar un analizador de protocolos denominado Wireshark. Copia de \\ATC150\\Software\\Redes al ordenador par el instalador para Windows de 32 bits de Wireshark e instala el programa. Copia también el archivo **captura.pcap** al ordenador par.

Un analizador de protocolos se puede usar de distintas formas en función de los objetivos pretendidos. Así, un administrador de sistemas puede utilizarla para buscar problemas de congestión; un administrador de seguridad para encontrar posibles fallos de seguridad; un desarrollador de protocolos para realizar tareas de depuración; o un estudiante puede utilizar la herramienta para la comprensión y estudio de los distintos protocolos de red.

Inicia el programa Wireshark para analizar tramas de red. En la pantalla de presentación se muestran las diferentes opciones de trabajo y configuración del programa. En la opción "Interface List" se muestra la lista de interfaces de red disponibles en nuestra máquina y a los que Wireshark tiene acceso. La opción "Capture options" permite configurar opciones de la captura en tiempo real de las tramas de red. "Sample Captures" permite acceder a una página web en la que se encuentra una colección de capturas interesantes realizadas por usuarios del programa. La opción "Open" permite acceder a un archivo que contenga una captura realizada con el programa. Selecciona esta opción para abrir el archivo **captura.cap**.

En el panel superior se muestra el listado de las tramas de red o paquetes que contiene el archivo, en el segundo panel se muestran los detalles, a nivel de protocolo, de la trama que seleccionemos y, en el tercer panel, tenemos los bytes concretos que conforman dicha trama.

2. Opciones de presentación

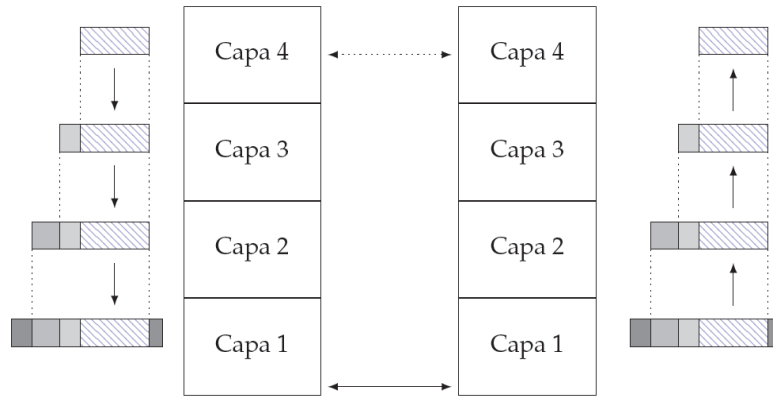
En el panel superior la información está organizada en columnas, las cuales tienen las siguientes etiquetas:

- **No.:** Es el número de orden de la trama. La primera trama que se capturó tiene el número 1, la siguiente el 2, y así sucesivamente.
- **Time:** Es una referencia al instante en el que se capturó la trama.
- **Source:** Dirección de origen de la trama. En este campo el aspecto de la información mostrada depende del tipo de trama.
- **Destination:** Dirección de destino de la trama. Como en el caso anterior, la información mostrada va a depender del tipo de trama.
- **Protocol:** Protocolo que contiene la trama capturada. Wireshark muestra el protocolo de más alto nivel que logra identificar. Así, por ejemplo, aunque todos los paquetes TCP o UDP tienen que ir dentro de un datagrama IP, la información que se muestra en este campo no es IP sino UDP o TCP, según corresponda.
- **Info:** Información que contiene la trama. Cuando son datos de usuario, muestra unos pocos bytes nada más.

Las cabeceras de las columnas son botones que nos permiten alterar la forma de presentación de los datos. Cada vez que pulsamos sobre una de ellas nos permite cambiar la ordenación de los datos de mayor a menor, y viceversa.

3. La arquitectura de protocolos en capas

Cuando queremos enviar una nota a una persona en otra ciudad metemos la nota en un sobre, escribimos la dirección de la persona en el exterior, hacemos llegar el sobre al servicio de correos, el cual lo transporta a la otra ciudad y allí un servicio de reparto lo entrega a la persona deseada. No se nos ocurre llevar la nota en persona y, desde luego, no esperamos que la otra persona venga a nuestro domicilio a entregarnos la nota de respuesta. De la misma manera cuando un programa que está ejecutándose en una máquina quiere enviar un dato a otro programa que está ejecutándose en otra máquina, no lo hace directamente sino que utiliza distintos servicios intermedios para hacerlo. Estos servicios de transporte intermedios configuran una arquitectura de protocolos en capas en la que, como podemos comprobar en la figura siguiente, cada capa por la que atraviesa el dato, añade una cierta cantidad de bytes al paquete para poder realizar su trabajo (en el ejemplo del correo es el equivalente al sobre, la dirección, el remite, el código postal, el sello, etc.).



Vamos a utilizar el programa Wireshark para analizar las distintas capas y cuáles son los bytes que añade cada capa cuando dos aplicaciones quieren transferir información a través de una red de telecomunicaciones basada en TCP/IP. Vamos a utilizar como ejemplo de aplicaciones un servidor Web y un navegador que le solicita una página.

El archivo **captura.pcap** contiene la captura de una sesión de comunicaciones entre el navegador y el servidor web. La sesión consiste en el envío, por parte del navegador, de una petición de un archivo al servidor web y de la respuesta de éste con el envío del archivo.

Lo que ves en el primer panel de Wireshark son las 13 tramas de datos que se han tenido que intercambiar entre la máquina del navegador y la máquina del servidor web para que el navegador reciba el archivo. Escribe **http** en el campo "Filter" y pulsa *Apply* para aplicar un filtro que sólo muestre los paquetes relacionados con el protocolo HTTP ("Hyper Text Transfer Protocol"), que es el que utilizan los navegadores y los servidores web para comunicar entre sí. Los dos paquetes que han quedado en el primer panel son los únicos que contienen la información que se intercambiaron directamente el navegador y el servidor web.

El intercambio entre el navegador y el servidor se inicia con el envío por parte del navegador de una petición GET al servidor con el nombre del archivo que desea. A esa petición responde el servidor con OK y el archivo, si lo tiene, o con ERROR si no lo tiene. En este caso, ha enviado el archivo.

En el panel superior de Wireshark marca el primer paquete. En el panel intermedio se muestra, interpretado, lo que contiene el paquete. Cada una de las líneas del panel intermedio (excepto la primera, que da información general) representa una capa en la arquitectura de protocolos que ha atravesado la información en su camino entre el navegador y el servidor web. En el panel inferior vemos los bytes que conforman realmente ese paquete. En cada fila se muestran 16 bytes. La columna de la izquierda muestra la dirección (desplazamiento con respecto al inicio del paquete) del primer byte mostrado en esa fila, las dos columnas del centro muestran los bytes del paquete en hexadecimal y la columna de la izquierda muestra su interpretación como ASCII.

Pulsa sobre las palabras "Hypertext Transfer Protocol" en el panel intermedio. Verás que en el panel inferior se han marcado de azul una serie de bytes: son los que forman parte del protocolo HTTP. Son fáciles de reconocer porque los primeros bytes son los códigos ASCII de la petición del navegador **GET /hola.html**.

Mueve la barra de desplazamiento del panel inferior hacia arriba y hacia abajo. Comprobarás que hay bytes que no están seleccionados en azul. Eso significa que el paquete contiene más bytes que los correspondientes al protocolo HTTP. Son los bytes que han añadido las demás capas de protocolo.

Aunque en el panel intermedio "HyperText Transfer Protocol" se encuentra en la línea inferior, su posición en la arquitectura de protocolos es la más alta, la más cercana a los programas de usuario, es la correspondiente a la capa de aplicación.

Pulsa ahora sobre las palabras "Transmission Control Protocol" en el panel intermedio. Acabas de descender un nivel en la arquitectura de protocolos y te has colocado en la capa de transporte. Verás que en el tercer panel se han seleccionado un conjunto diferente de bytes (mueve la barra de desplazamiento si lo necesitas) que son la cabecera del protocolo TCP.

Comprueba, alternado la selección entre "HyperText Transfer Protocol" y "Transmission Control Protocol", que los bytes de HTTP están justo a continuación de los correspondientes a la cabecera del protocolo TCP. Esto significa que los bytes de HTTP son los datos que transporta TCP.

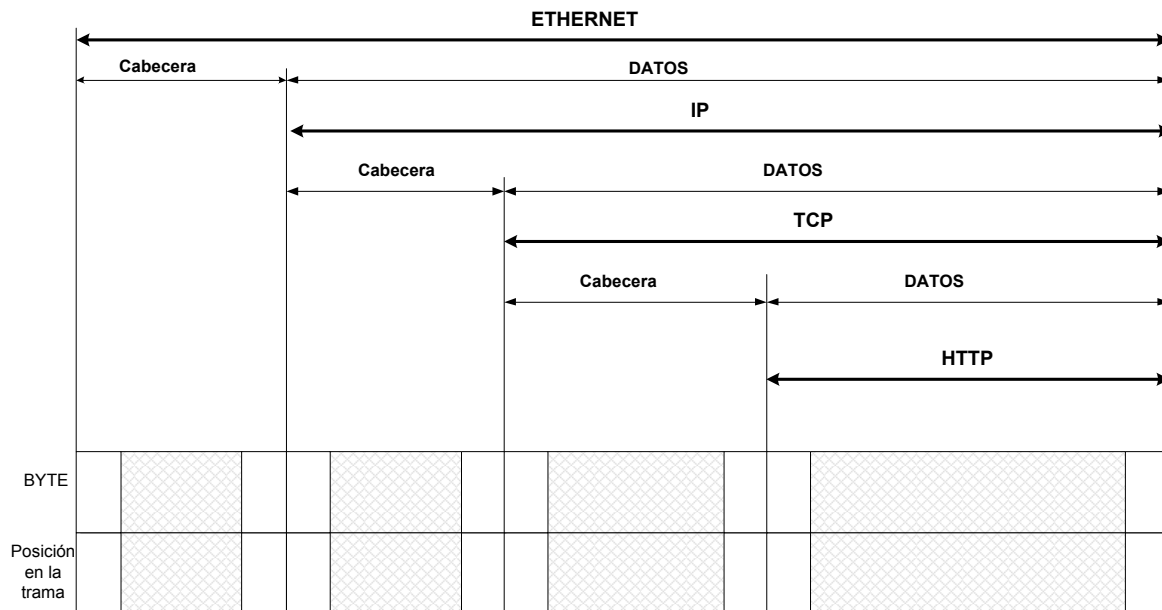
Pulsa ahora sobre las palabras "Internet Protocol" en el panel intermedio. Nuevamente, en el tercer panel se han seleccionado un conjunto diferente de bytes (mueve la barra de desplazamiento si lo necesitas). Has vuelto a descender un nivel en la arquitectura de protocolos y ahora te has colocado en la capa de red o internet. Comprueba, alternado la selección entre "Internet Protocol" y "Transmission Control Protocol", que los bytes de la cabecera de TCP están también a continuación de los correspondientes a la cabecera del protocolo IP. De nuevo eso significa que los bytes de TCP son los datos que transporta IP.

Pulsa ahora sobre "Ethernet II" en el panel intermedio. Como era de esperar, en el tercer panel se ha seleccionado un conjunto diferente de bytes (mueve la barra de desplazamiento si lo necesitas). Lo has hecho otra vez. Has descendido un nivel en la arquitectura de protocolos y ahora te has colocado en la capa de enlace. Como antes has hecho, comprueba, alternado la selección entre "Internet Protocol" y "Ethernet II", que los bytes de IP están a continuación de los correspondientes a la cabecera de la trama de Ethernet. Como en los casos anteriores, eso significa que los bytes de IP son los datos que transporta Ethernet.

Si repasamos todos los pasos anteriores podemos ver que en el nivel más bajo tenemos una trama Ethernet que, en su campo de datos, transporta un datagrama IP. A su vez, el datagrama IP, en su campo de datos, transporta un segmento TCP que, en su campo de datos, lleva unas instrucciones del protocolo HTTP. Esas instrucciones HTTP son la información que quería enviar el navegador al servidor web. Esta encapsulación de unos datos dentro de otros es el resultado de organizar los protocolos en una arquitectura en capas.

Alterna la pulsación sobre los distintos niveles de protocolo en el panel intermedio para ver la selección de los bytes en el tercer panel hasta que te quede claro el concepto.

En la figura siguiente se muestra un esquema del encapsulamiento de protocolos en el interior de la trama. Rellena, en los huecos de la fila etiquetada con BYTE, el valor del primer y último byte de cada protocolo implicado. En la fila de abajo, indica en qué posición de la trama se encuentra cada uno de los bytes de la fila superior. La posición escríbela también en hexadecimal ya que es así como la obtienes de Wireshark.



4. La capa de aplicación. Protocolo HTTP

Vamos a analizar el intercambio empezando por la capa más alta de la arquitectura de protocolos, la capa de aplicación.

En el panel superior de Wireshark marca el primer paquete. En el panel intermedio pulsa sobre los símbolos menos de todos los campos que estén abiertos.

Pulsa en el panel intermedio sobre la línea correspondiente al protocolo HTTP para seleccionar sus bytes y después pulsa sobre el símbolo más que hay a la izquierda de "HyperText Transfer Protocol". Vemos que el panel inferior no se ha modificado (sigue mostrando en azul los bytes correspondientes al protocolo HTTP) pero en el panel intermedio se nos muestra con más detalle el significado de cada byte. Si vamos pulsando sobre cada una de las líneas que nos han aparecido, podemos ver en el panel inferior qué bytes son los que proporcionan esa información. Podemos comprobar cómo el navegador web envía bastante información adicional al servidor web además de la ruta del fichero a obtener. ¿Qué navegador y qué sistema operativo se han usado para realizar la petición?

Pulsa ahora sobre la segunda trama del panel superior. Es la respuesta del servidor Web. Pulsa sobre el símbolo más a la izquierda del protocolo HTTP. Como verás, el servidor responde con el código 200 que corresponde a una respuesta correcta (OK).

Pulsa el más que hay a la izquierda de la línea denominada "Line-based text data" en el segundo panel. Los bytes que se marcan en azul en el tercer panel corresponden con el archivo HTML enviado por el servidor web al navegador. Puedes ver el archivo tanto en el segundo panel como en el tercero.

5. La capa de transporte. Protocolo TCP

Hemos visto que los bytes que corresponden al protocolo HTTP, que es el que usan el navegador y el servidor web para conversar, son sólo una parte de los bytes que componen el

Puerto de origen:

Puerto destino:

Pulsando sobre los campos "Source port" y "Destination port" en el segundo panel de Wireshark puedes comprobar que has hecho correctamente el apartado anterior. Por convenio, todos los servidores web utilizan el puerto 80 para recibir las peticiones de los navegadores web; de esta manera, únicamente tenemos que conocer la máquina para localizar al servidor web. Es un *puerto bien conocido*. Fíjate que el puerto de origen es en el que está esperando el navegador la respuesta. Este puerto se asigna aleatoriamente en cada petición: no hace falta que sea bien conocido y que esté fijo porque el que inicia la petición es el navegador y le puede decir al servidor en qué puerto va a esperar la respuesta.

Obtén ahora el valor del campo "Número de secuencia". Mirando en el tercer panel, ¿qué bytes son?

Obtén con qué número decimal se corresponden. Comprueba en el segundo panel que Wireshark propone un valor distinto para este campo. La razón de esta divergencia es que, para facilitar la comprensión del intercambio de datos, Wireshark indica los números de secuencia con respecto al primero de la comunicación, que, como se verá más adelante, es el F749AD04h.

Comprueba el valor que da Wireshark al campo "Número de reconocimiento". Como en el caso anterior, Wireshark indica un número relativo y no el valor real.

Selecciona el campo "Header length" que es como Wireshark denomina al campo "Localización datos". De los bits que Wireshark resalta en azul en el tercer panel (50h), sólo los cuatro primeros bits (5h) son de este campo; los otros cuatro bits se corresponden con el campo "Reservado". Como puedes comprobar, Wireshark indica que la longitud es 20 bytes y no 5. La razón es que lo que indica el campo (5) es el número de bloques de 32 bits (8 bytes) que tiene la cabecera y $5 \times 8 = 20$.

A continuación tenemos 8 campos de longitud 1 bit que Wireshark denomina "Flags". Según el panel intermedio, ¿qué campos están activos?

El siguiente campo es "Tamaño de la ventana". Según el panel intermedio, ¿cuál es el tamaño en este caso?

Solo quedan los campos "Suma de comprobación" y "Puntero urgente", ya que hemos llegado a la conclusión de que esta trama TCP no dispone del campo "Opciones", y no los vamos a analizar.

5.1. Establecimiento de conexión en TCP

Podemos ver que el paquete en el que el navegador envía la petición GET al servidor web es el cuarto que se intercambian entre las dos máquinas. Antes de enviar la petición, las capas

de transporte de las máquinas del cliente y del servidor han tenido que establecer una conexión.

Selecciona el primer paquete del primer panel de Wireshark. En el segundo panel, expande la información correspondiente a TCP. ¿Qué flags están a 1?

Este es el primer datagrama que se envía al establecer una conexión. Si buscas el valor del campo "Número de secuencia" verías que es F749AD04h. Fíjate que Wireshark lo interpreta como el valor 0 para que sea más fácil seguir el intercambio de segmentos TCP y que esta es la razón de que para el paquete del GET pusiera el número de secuencia relativo 1.

Selecciona el segundo paquete en el primer panel. Este paquete lo envía la máquina del servidor web como respuesta a la petición de conexión de la máquina del navegador. Analizando los flags se puede observar que la máquina acepta la conexión (ACK) y, a su vez, intenta establecer una conexión enviando un SYN. Si determinases el valor del campo "Número de reconocimiento" verías que es F749AD05h, lo que Wireshark interpreta como 1. Con este valor el servidor le está diciendo al navegador que ha recibido correctamente el byte 0 de la conexión y que está preparado para recibir el byte 1.

Si determinases el "Número de secuencia" verías que vale 80C5B30Dh. Como este es el primer paquete que el servidor le envía al navegador, Wireshark interpretará ese número como el paquete 0 en ese sentido.

Selecciona el tercer paquete en el primer panel. Comprueba que el campo ACK está a 1 y que el campo "Número de reconocimiento" se corresponde con el esperado.

Una vez intercambiados estos tres paquetes entre la máquina del cliente y la del servidor, se ha establecido una conexión "full duplex" entre ambas máquinas. Esto quiere decir que existen dos conexiones activas:

1. La conexión que "lleva" los datos del cliente al servidor. Esos datos están identificados a partir del número de secuencia que envió el cliente al servidor en el primer paquete.
2. La conexión que "lleva" los datos desde la máquina del servidor a la del cliente. Estos datos están identificados por el número de secuencia que estableció el servidor en el primer paquete que envió al cliente (paquete número 2 del primer panel de Wireshark) y que es distinto del que usa el cliente.

También hemos de fijarnos que en cada datagrama que envía el cliente al servidor, además de incluir el número de secuencia de sus datos, incluye también (en el campo "Número de reconocimiento") el número de reconocimiento, que es el número de secuencia que corresponde con el último dato recibido del servidor. El servidor hace lo propio con cada datagrama que envía al cliente. De esta manera, en cada datagrama que se intercambian, no sólo se identifican los datos que se envían, sino que además se identifican los datos que se han recibido.

De la misma forma que se establecen conexiones, también se terminan. Fíjate en los paquetes números 8, 10 y 11 (el paquete 9 es una comunicación con otra máquina que no tiene que ver con la conexión que estamos analizando aquí). Se han generado al cerrar la

página en el navegador. Los flags que están a 1 en estos paquetes son los necesarios para cerrar una conexión.

1.1 La capa de red. El protocolo IP

La capa inmediatamente inferior a la capa de transporte es la capa de red. En la arquitectura de protocolos TCP/IP el protocolo que se encuentra en el nivel de red es "Internet Protocol" o IP. Vamos a utilizar Wireshark para analizar algunos campos de este protocolo. En la figura siguiente tenemos un esquema del contenido de un datagrama IP:

0	7 8		15 16		23 24		31
Versión	IHL	Tipo de servicio		Longitud total			
Identificación				DF	MF	Desplazamiento del fragmento	
Tiempo de vida		Protocolo		Suma de comprobación			
Dirección de origen							
Dirección de destino							
Opciones							
...							

En el panel superior del analizador de protocolos selecciona el primer paquete. Pulsa el botón menos de todos los campos en el panel intermedio. Pulsa sobre las palabras "Internet Protocol" para que en el panel inferior se seleccionen los bytes correspondientes a la cabecera del datagrama. Los bytes que han quedado sin seleccionar por debajo son los datos que transporta el datagrama.

Pulsa sobre el más en el panel intermedio y expande el protocolo IP. ¿Qué valor tiene el campo "Identificación" en hexadecimal?

Este es el número del datagrama IP.

De los flags del protocolo IP, ¿cuál está activo?

¿Cuál es el valor en decimal del "Tiempo de vida" de este datagrama? ¿Qué significa eso?

Selecciona el campo con la dirección IP de origen. ¿Cual es su valor en hexadecimal?

Comprueba con la calculadora hexadecimal que la conversión a decimal de cada uno de sus bytes da lugar a la misma dirección en formato X.Y.Z.W que muestra el programa. Como puedes observar, el datagrama también tiene la dirección IP de destino.

7. La capa de enlace. Protocolo Ethernet

Todas las tramas que contiene el archivo se han capturado en una red local formada por dos ordenadores y un enrutador, conectados entre sí por una red Ethernet. Por lo tanto, todas las tramas capturadas serán Ethernet y todos los protocolos de nivel superior estarán encapsulados dentro de una trama Ethernet. El formato de estas tramas se muestra a continuación:

Preámbulo	Delimitador	MAC destino	MAC origen	Etiqueta 802.1Q	EtherType o tamaño	Carga útil	CRC
7 bytes 10101010	1 byte 10101011	6 bytes	6 bytes	4 bytes opcionales	2 bytes	46-1500 bytes	4 bytes

De los elementos que conforman la trama Ethernet, Wireshark no nos puede presentar ni los 7 bytes del preámbulo, ni el byte delimitador, ni los 4 bytes del CRC ya que esos elementos solo le sirven a la capa física para identificar la información útil de la trama pero nunca son transmitidos "hacia arriba" en la arquitectura de protocolos y no llegan al programa de captura. El resto de campos sí se pueden analizar dentro del programa. Vamos a ver una trama en detalle:

Pulsa y selecciona la trama número 1. Oculta pulsando sobre menos todos los campos que pudieran estar expandidos en el panel intermedio. Selecciona la segunda línea, la que comienza con la palabra Ethernet. Verás que en el tercer panel se seleccionan 14 bytes que corresponden a los datos de la cabecera de una trama Ethernet.

Expande la información correspondiente al protocolo Ethernet pulsando en el símbolo más que hay a la izquierda de la palabra Ethernet. Comprobarás que han aparecido tres líneas más. Si pulsas sobre cualquiera de ellas verás en el panel inferior los bytes de la trama que se corresponden con esa información.

Pulsa sobre la línea que comienza por la palabra Type. Verás que se seleccionan dos bytes en la trama del tercer panel con los valores 08 00. En el segundo panel se nos informa del significado, en el protocolo Ethernet, de esos dos bytes: indican que los datos que se transportan en la trama Ethernet son del protocolo IP.

Pulsa sobre la línea que empieza por la palabra Destination. Verás en el tercer panel que se seleccionan 6 bytes que son los que se corresponden con la dirección Ethernet de la tarjeta de destino de la trama. ¿Qué valor tienen esos bytes?

Puedes comprobar que también se puede obtener la dirección Ethernet del origen.

Las direcciones Ethernet de las interfaces de red son únicas. A cada fabricante se le asigna un rango de direcciones para que las asigne a las tarjetas que fabrica. De esa manera, conociendo la dirección Ethernet de una interfaz se puede saber cuál ha sido el fabricante. ¿Sabrías decir quién es el fabricante de la tarjeta Ethernet origen de la trama?

8. Visión global

Ahora que ya hemos visto con detalle todas las capas, vamos a recapitular con una visión global. Para esto resulta muy útil el panel superior de Wireshark. En él puedes observar cómo la petición de una página web se ha traducido en diez tramas. Las otras tres que hay en la captura son comunicaciones con otras máquinas, como puedes comprobar analizando las direcciones.

Las tres primeras tramas sirvieron para establecer la comunicación. Puedes ver que en el campo info se muestran los datos fundamentales del protocolo: los puertos¹, qué flags están activos, los números de secuencia, el tamaño de la ventana, etc. La cuarta trama es la petición HTTP y la quinta el ACK a esa petición. La sexta es la respuesta del servidor con la página web y la séptima, el ACK a la trama anterior. Finalmente, como se ha visto en una sección previa, las tramas 8, 10 y 11 realizan la desconexión.

En general, para trabajar con Wireshark deberías empezar analizando este panel superior, posiblemente utilizando filtros para ver sólo la información de los protocolos o máquinas que te interesen.

Configuración TCP/IP

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 FDX. ¿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 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.
- 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 instalado¹. 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*, 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.

- 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.

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

¹ 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.

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 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.

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.

- 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 el campo *Puerta de enlace predeterminada*. Cierra, aceptando, todas las ventanas de configuración para que se aplique la nueva configuración. Ahora haz *Ping* a 156.35.151.150 (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 uno de ellos:

Nombre de equipo:

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.