Redes

Ingeniería Informática (9185)

Manual de la Práctica 1:

Introducción a las redes de computadores

Francisco Andrés Candelas Herías

Jorge Pomares Baeza

Grupo de **I**nnovación **E**ducativa en **A**utomática

Universitat d'Alacant
Universidad de Alicante

1. Objetivos

- Realizar la captura de cualquier paquete de datos que se desee empleando el software del monitor de red.
- Interpretar el funcionamiento de los protocolos Ethernet, ARP e IP en base a la información capturada por el monitor de red.
- Reconocer los diferentes niveles de la arquitectura TCP/IP y qué funcionalidad tienen en la comunicación de datos.
- Conocer el esquema de direccionamiento empleado por el protocolo IP.

2. Introducción

La primera práctica de la asignatura Redes pretende introducir al alumno en las redes de computadores de forma práctica. Para ello se analizará el estudio de una Red de Área Local (LAN) que emplea la arquitectura de red TCP/IP. Esta arquitectura de red se ha convertido en un estándar para los sistemas de transmisión de datos actuales y proporciona la tecnología base para multitud de aplicaciones: correo electrónico, servidores WWW, servidores FTP, IRC, comercio electrónico, acceso a bases de datos remotas, tecnología WAP, etc.

Para el estudio del funcionamiento de una arquitectura de red, la detección de fallos y la gestión eficiente de la misma, es fundamental conocer qué información está circulando por el medio. En el momento en que un usuario detecta que no existe comunicación entre el servidor y un cliente hay que proceder con una metodología para detectar donde está el fallo en la comunicación. Ésta consiste en determinar en qué nivel de la arquitectura de red se produce el fallo y proceder a subsanarlo. Ello es posible gracias al empleo de un "*monitor de red*".

El monitor de red es un software que altera el funcionamiento normal de un adaptador de red o dispositivo de comunicaciones de un equipo. Los adaptadores de red empleados en el laboratorio de prácticas de Redes son tarjetas de red Ethernet. En una red Ethernet cada adaptador de red, que está conectado al bus de E/S del PC, puede leer cualquier paquete de información que circula por el medio físico, dado que éste está compartido por todos los PC's de la red. Sin embargo, el software del adaptador de red (los drivers de la tarjeta) evitan que el usuario pueda interpretar esos paquetes, de forma que sólo realiza el procesamiento de los paquetes que van dirigidos a él. Las tarjetas de red Ethernet pueden alterar su funcionamiento pasando a un modo denominado promiscuo, de forma que interpretan todos los paquetes o tramas que circulan por el medio físico. Un software que habilita esta funcionalidad y permite mostrar al usuario todos los paquetes que circulan por el medio se denomina monitor de red.

Mediante el empleo del monitor de red es posible analizar cuál es el formato de los paquetes que circulan por el medio físico, entendiendo así el funcionamiento de los protocolos de diferente nivel que coexisten en la arquitectura de red.

3. Topología de la red del laboratorio

En el esquema inferior se muestra la topología de la red de comunicaciones del laboratorio de prácticas en el aula L24 del edificio Politécnica I de la EPSA. La red está formada por la interconexión de diferentes segmentos de red. Cada segmento de red está conectado a los demás segmentos a través de un dispositivo denominado router o

encaminador. En la asignatura Redes adoptaremos la interpretación de segmento de red en el nivel de red de la arquitectura. Por ello, un segmento de red será el conjunto de dispositivos que comparten una misma dirección de red IP (dado que empleamos la arquitectura de red TCP/IP).

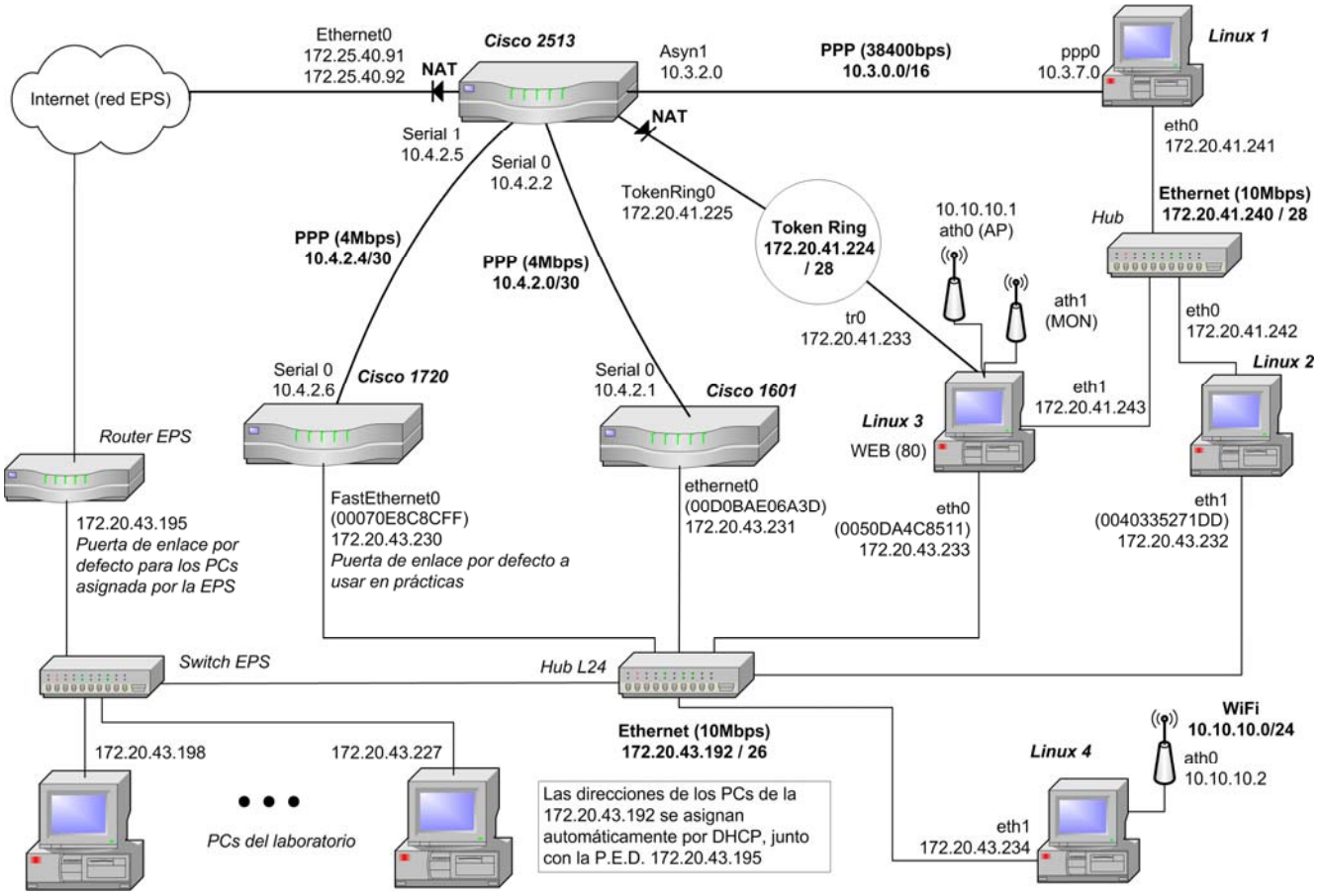

Figura 1: Topología de la red del laboratorio L24

El segmento principal corresponde a la red en que se encuentran los PC's de los alumnos. Algunas de las máquinas están conectadas entre sí empleando un dispositivo denominado *hub* o concentrador.

Un *hub* es un dispositivo que dispone de una serie de puertos donde conectar los PC's de la red empleando cables par trenzado (con conectores RJ-45, similares a los conectores RJ-11 empleados en el cable par paralelo de telefonía) y que emplea el protocolo Ethernet para intercambiar información entre las diferentes estaciones. En el protocolo Ethernet cada adaptador de red (tarjeta de comunicaciones) de cada PC está identificado con una dirección única (dirección MAC) y cuando dos estaciones quieren intercambiar información lo hacen transmitiendo bloques de datos en los que se indican la dirección MAC del PC que envía los datos y la dirección MAC del que los recibe.

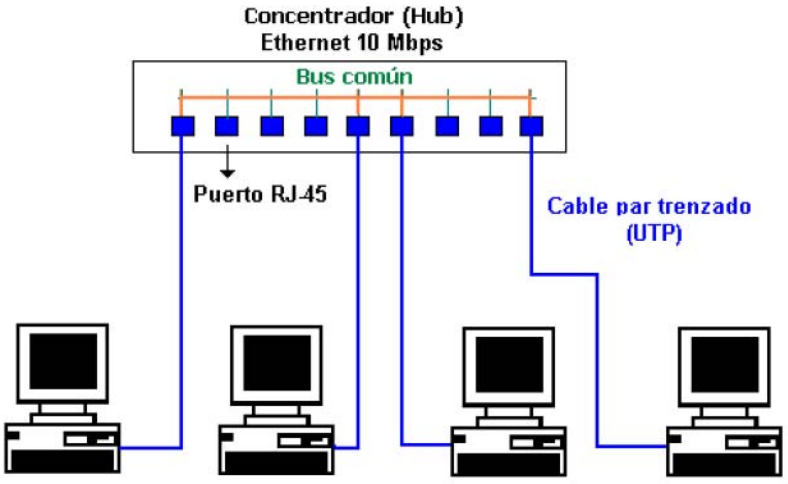

Figura 2: Esquema de un Hub.

Una alternativa más eficiente del *hub* es el conmutador o *switch*, que es el que se utiliza para interconectar los PC's de los alumnos. Debido al elevado número de PC's existentes en el laboratorio se han dispuesto varios *switch* conectados entre sí (conexión en cascada), de forma que es posible construir una red Ethernet lo suficientemente grande.

El *switch* establece internamente conexiones entre los puertos donde están conectados los PC's que quieren intercambiar información. Para ello dispone de una malla de interconexión entre todos los puertos y dependiendo de a qué destino va dirigida la información que se recibe por un puerto, ésta se envía sólo al puerto donde está conectado el PC destinatario.

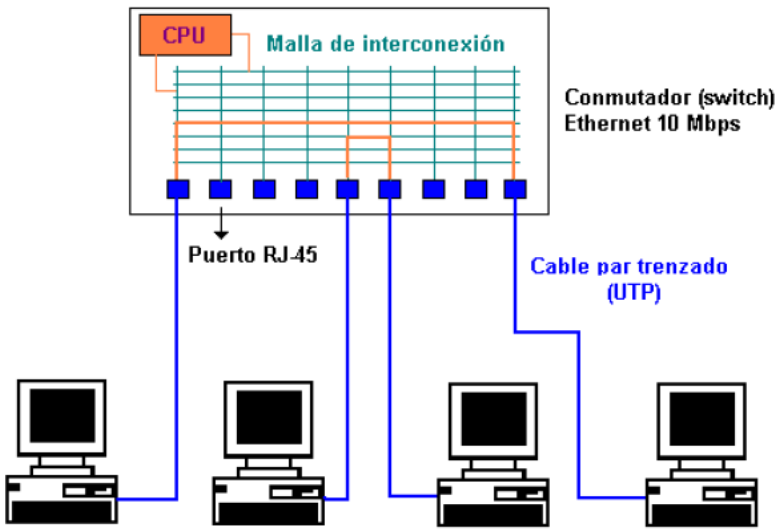

Figura 3: Esquema de un switch.

El *switch* proporciona un nivel de seguridad superior al *hub* en el medio físico compartido. El *hub* actúa como repetidor de todos los paquetes que llegan enviándolas a todas las máquinas, mientras que el *switch* envía los paquetes sólo a las máquinas destinatarias, por lo que las demás estaciones no podrán capturar con un monitor de red esta información, ya que no es accesible físicamente. Además, el *switch* realiza un mejor aprovechamiento del medio físico, ya que permite la transmisión simultánea de información entre pares de máquinas diferentes, mientras que en el *hub* esto no es posible, ya que cuando

dos o más estaciones tratan de transmitir información simultáneamente se producen colisiones, presentando un retardo en el envío de la información y por tanto una velocidad de transferencia efectiva menor.

El router **CISCO 1720** interconecta la red Ethernet con una red PPP. Para comunicar las máquinas de la red Ethernet con las de la red PPP es necesario un protocolo que permita la interconexión entre dos segmentos de red. Este protocolo es el protocolo IP. Cada segmento de red tendrá una dirección de red IP y todas las máquinas que estén en un mismo segmento de red tendrán el mismo valor de dirección de red en su dirección IP. Para diferenciar las máquinas dentro de un mismo segmento de red cada una de ellas tiene asociada una dirección de máquina que se indica en la dirección IP. En posteriores apartados se hablará con más detalle de las direcciones IP.

PPP son las siglas de **Point to Point Protocol**: Protocolo Punto a Punto. Es un protocolo que se emplea para construir un segmento de red que consta de sólo dos máquinas unidas entre sí por un canal de comunicación. En un segmento de red PPP sólo existirán por tanto dos máquinas: las de los dos extremos. El segmento PPP en el router **CISCO 1720**, que emplea una velocidad de transmisión de 4 Mbps, está conectado al router **CISCO 2513** y éste a su vez con el router **CISCO 1601** empleando otro enlace PPP a 4 Mbps. El router **CISCO 1601** está conectado de nuevo a la red Ethernet de los alumnos, por lo que se establece un bucle en la topología de la red de prácticas.

Existe otro bucle en la topología del laboratorio. Éste se establece desde el router **CISCO 2513** con un enlace PPP al equipo **Linux 1**, un PC con sistema operativo Linux Slackware configurado con funcionalidades de router, a una velocidad de 38400 bps. El equipo **Linux 1** está conectado a su vez a una red Ethernet a 10 Mbps donde hay un equipo adicional, el **Linux 2** configurado también con funcionalidades de router. El bucle se cierra al conectar el equipo **Linux 2** a la red Ethernet de los alumnos. El estudio de la existencia de bucles en redes TCP/IP es especialmente interesante, ya que proporciona tolerancia a fallos en la caída de los enlaces (existe un camino alternativo para alcanzar un destino) pero una configuración incorrecta puede producir la presencia de paquetes que circulan indefinidamente en la red.

Existe además otro equipo que realiza funciones de router, el **Linux 3**, que permite interconectar la red de los Alumnos con la Ethernet a 10 Mbps existente entre **Linux 1** y **Linux 2**, también se conecta al router **CISCO 2513** mediante una red Token Ring a 16 Mpbs.

Esta configuración de red sería cerrada si no fuera porque el router **CISCO 2513** está conectado a Internet, y a través de él los alumnos pueden acceder al exterior. El **CISCO 2513** está conectado a los routers de la red de la Universidad de Alicante que dan paso a Internet.

Finalmente hay que indicar que por defecto los ordenadores del laboratorio L24, tiene como puerta de enlace por defecto, equipo al que mandar los paquetes que no vayan dirigidos a su red, una máquina de la EPS. Para poder utilizar correctamente el esquema anterior hay que cambiar la puerta de enlace por defecto. Ejecutando el archivo "c:\pracredes.bat" se cambia la ruta por defecto para que sea el **CISCO 1720**.

4. Iniciación al monitor de red

El monitor de red que se empleará en las prácticas de la asignatura es el Wireshark versión 0.99.6a que permitirá, empleando una interfaz gráfica, acceder a los paquetes que circulan por el medio físico.

Wireshark es un software multiplataforma de captura de paquetes muy extendido y de libre distribución bajo licencia GNU. Al igual que un gran número de herramientas utilizadas por administradores de red, se basa en unas librerías comunes conocidas como 'pcap' o 'winpcap' dependiendo de la plataforma utilizada.

El formato de los ficheros de captura que Wireshark utiliza, es compatible con otras herramientas tales como tcpdump, tcptrace, tcpflow, snort, ntop y un largo etc., especializadas en el tratamiento de capturas de paquetes.

Se podrían enumerar las siguientes ventajas:

- Interfaz gráfica de usuario.
- Compatible en lectura y escritura con capturas realizadas mediante otros analizadores como tcpdump.
- Sintaxis de Filtrado de paquetes muy flexible y potente.
- Funciona tanto en entornos Linux/Unix como en Windows.
- Se pueden intercambiar las capturas realizadas en máquinas Windows y Linux/Unix.

Para realizar una captura y exploración de la información que circula por la red pueden seguirse los pasos básicos que se comentan en sucesivos apartados. Si se desea más información sobre el funcionamiento del programa se puede acudir a su ayuda, que es bastante completa. Sin embargo, para obtener información sobre los protocolos, direccionamiento, tipos de redes, etc. hay que acudir a la bibliografía adecuada.

4.1. Inicio de una captura de paquetes que circulan por la red

Al iniciar el programa, en la barra de menús seleccionar la opción '*Capture*' y a continuación *'Options*' (puede emplearse también la secuencia de teclado CTRL+K). De esta forma se inicia la ventana de control de la captura de paquetes en la red, donde hay que indicar una serie de parámetros:

1. **Interface**. Ha de seleccionarse el interfaz de red que se empleará para capturar información. En el laboratorio de prácticas este interfaz es el dispositivo Ethernet, que vendrá indicado como '3Com Etherlink', y es el que conecta el PC a la red Ethernet del aula.

2. **Capture packets in promiscuous mode**. Esta opción permite activar el modo promiscuo en el interfaz de red. Ethernet es una red de difusión, que se caracteriza porque el medio físico es compartido por todas las estaciones en la red. En el modo de funcionamiento normal, las tarjetas Ethernet sólo almacenan y procesan los paquetes que van dirigidos a sus direcciones MAC. Sin embargo, dado que todos los paquetes circulan por el mismo medio físico, es posible activar un modo de funcionamiento en la tarjeta de red que permita almacenar todos los paquetes que circulan en la red, independientemente de la dirección de destino. Este es el denominado modo promiscuo y que deberá estar activado en la tarjeta de red para la realización de las prácticas.

3. **Limit each packet to**. Esta opción está desactivada por defecto, y permite limitar la cantidad de información que se almacena de cada paquete capturado. En las prácticas necesitaremos analizar el contenido completo de cada paquete que circula, por lo que se mantendrá desactivada esta opción.

4. **Capture Filter**. Esta opción permite especificar un filtro para la captura de paquetes. Empleado filtros podemos indicar qué tipo de paquetes queremos capturar de

la red. Los filtros de captura se indican con una sintaxis que se especifica en el apartado 4.3.

5. **Capture File(s): "File"**. Esta opción permite especificar un fichero donde se almacenará la información capturada con el monitor de red para un análisis posterior de los paquetes.

6. **Display Options**. Esta opción permite definir los parámetros que se muestran durante la captura. Conviene desactivar la opción "Update list of packets in real time", ya que si esta opción esta activa y hay mucho tráfico en la red se podrían perder algunos paquetes. La opción "Hide capture info dialog" se debe desactivar y así tendremos, durante la captura, un resumen del tipo y cantidad de paquetes que se están capturando.

7. **Name Resolution**. Esta opción permite que el programa transforme las direcciones de los equipos contenidas en los paquetes por su nombre. Esta traducción se puede hacer ha distintos niveles. Se recomienda desactivar todas las resoluciones de nombres para poder analizar los paquetes directamente.

El resto de parámetros de la captura no son necesarios para la realización de las prácticas y pueden ser consultados en la ayuda. Finalmente, para iniciar la captura de información pulsar el botón '*Start*'. En ese instante se inicia la captura de paquetes que circulan por el medio físico, mostrando qué porcentaje de paquetes capturados corresponde a cada tipo de información. La captura se lleva a cabo hasta que es detenida por parte del usuario con el botón '*Stop*'.

4.2. Visualización de la captura

Una vez pulsado el botón '*Stop*' de la ventana de captura, los paquetes capturados son visualizados en la ventana principal de Wireshark y en el caso de haber indicado un fichero de captura se almacenan también en éste. La ventana principal de Wireshark se divide en tres secciones horizontales.

En la primera se visualizan los paquetes capturados, empleando para cada uno de ellos una línea. Por cada paquete se indica el orden de captura (1º, 2º, 3º, etc.), el tiempo transcurrido en segundos desde el inicio de la captura, la dirección de origen y destino del paquete, el protocolo de nivel más alto que transporta el paquete e información característica que transporta el paquete.

En la sección horizontal inferior aparece el desglose del paquete por protocolos. Para cada protocolo se visualiza un línea que puede desplegarse pinchando en el símbolo '+' de la izquierda y acceder al contenido de los campos de la cabecera del protocolo.

En la última sección horizontal se visualiza el contenido del paquete en formato hexadecimal y ASCII. Cuando en la sección horizontal central se selecciona alguna cabecera de protocolo o algún campo de las cabeceras, se sombrea la porción del paquete al que corresponde en la sección inferior. De esta forma es posible identificar la posición de las cabeceras de los protocolos en el paquete capturado.

4.3. Filtrado de paquetes

Cuando se realiza una captura de información en una red de difusión como Ethernet, existirá gran cantidad de información que no precisemos para el análisis del estado de funcionamiento de la red. Un filtro hace referencia a un conjunto de reglas que deben cumplir las tramas o paquetes de la red para poder ser capturados o visualizados. Las reglas pueden estar dadas en base a las direcciones origen y/o destino, tipo de protocolo o pattern matching,

que hace referencia a que el contenido de un byte o grupo de bytes dentro de un paquete coincida con unos valores especificados.

El filtrado de paquetes puede realizarse durante la captura o durante la visualización de la captura definiendo los filtros de captura y de visualización respectivamente. Aunque puede realizarse el filtrado de información en la captura y la visualización, es recomendable realizar la captura de información sin filtros y filtrar en la visualización. Ello es debido a que si filtramos paquetes en la captura corremos el riesgo de perder algún paquete que puede ser útil para comprender qué está sucediendo en la red. Sin embargo, si filtramos en la visualización y no disponemos de toda la información necesaria en ese filtrado, siempre podemos buscar en toda la captura la información que podamos necesitar.

Los filtros de visualización se pueden definir a través del menú '*Analyze*' -> '*Display Filter*' o seleccionando el botón '*Filter*' que aparece en la parte inferior izquierda de la ventana principal de Wireshark. La definición de un filtro consiste en una expresión que indica las condiciones que debe verificar un paquete. Estas condiciones están relacionadas con las características de los protocolos presentes en el paquete. El formato de estas expresiones sigue el estándar del software tcpdump (un monitor de red de libre distribución en modo texto disponible para varios sistemas operativos), aunque Wireshark nos proporciona una herramienta muy útil para definirlos sin conocer la sintaxis de tcpdump.

Una vez abierta la ventana de filtros de visualización, podemos añadir un filtro utilizando el botón '*Expression...*'. Este botón despliega un cuadro de diálogo donde podemos asociar a las características de cada protocolo una relación del tipo ==, >, <, >=, <=, !=, contiene o existe, con un valor determinado. Por ejemplo, si queremos capturar todos los paquetes cuya dirección MAC de origen es 00:02:10:3F:45:F4, seleccionamos el protocolo Ethernet y dentro de éste el campo eth.src. A continuación se indica qué relación se va a emplear, en nuestro caso ==. Y al indicarla podremos especificar un valor de comparación, que será 00:02:10:3F:45:F4. Pulsando en '*OK*' aparecerá la expresión eth.src == 00:02:10:3F:45:F4 en la sección '*Filter string*' de la ventana de filtros de captura. Para crear el filtro asociado a esa expresión, debe indicarse un nombre para el filtro en la sección '*Filter name*' y pulsar el botón '*New*'.

Para aplicar el filtro creado sobre una captura, seleccionamos el filtro desde el botón '*Filter*' en la parte inferior izquierda de la ventana principal de Wireshark. Seleccionamos el nombre del filtro y pulsamos el botón '*OK*'. En ese momento, aparecerán en la ventana de visualización sólo los paquetes que verifican el filtro. Para no filtrar y visualizar de nuevo todos los paquetes capturados pulsar el botón '*Clear*' que hay en la parte inferior de la ventana principal de Wireshark.

Un filtro puede constar de más de una expresión relacionándolas con los operadores and, or y not. Si queremos filtrar los paquetes que envía o recibe la estación con dirección MAC 00:02:10:3F:45:F4, tendríamos que indicar en el filtro la expresión eth.src == 00:02:10:3F:45:F4 or eth.dst == 00:02:10:3F:45:F4.

Algunos ejemplos de la sintaxis de filtrado en Wireshark son los siguientes:

Tráfico de Difusión o 'broadcast'

Para realizar un filtro de visualización que seleccione todos las tramas de difusión presentes en una captura realizada, se puede especificar diréctamente la sintaxis del filtro, o a través de la ventana de creación de filtros, pulsando la casilla <Expression...>:

En la casilla <filter>, ejecutar: eth.dst eq ff:ff:ff:ff:ff:ff

O en la casilla <Expression...>, seleccionar el filtro a través de los menús desplegables buscando la dirección destino ethernet ff:ff:ff:ff:ff:ff en los paquetes capturados.

Filtro por dirección ip en general

En la casilla <filter>, ejecutar: ip.addr eq 193.145.232.129

O en la casilla <Expression...>, seleccionar el filtro a través de los menús desplegables buscando la dirección ip 193.145.232.129 en los paquetes capturados.

Filtro por dirección ip destino

En la casilla <filter>, ejecutar: ip.dst eq 193.145.232.129

O en la casilla <Expression...>, seleccionar el filtro a través de los menús desplegables seleccionando la dirección ip destino 193.145.232.129 en los paquetes capturados.

Filtro por dirección ip origen

En la casilla <filter>, ejecutar: ip.src eq 193.145.232.129

O en la casilla <Expression...>, seleccionar el filtro a través de los menús desplegables seleccionando la dirección ip origen 193.145.232.129 en los paquetes capturados.

Filtro por dirección ip destino y oigen (ip del alumno)

En la casilla <filter>, ejecutar: ip.dst eq 193.145.232.129 and ip.src == 172.20.43.<n> (donde n es el último prefijo IP utilizado por la máquina del alumno).

O en la casilla <Expression...>, seleccionar el filtro a través de los menús desplegables seleccionando la dirección ip origen 193.145.232.129 en los paquetes capturados.

Filtro por prefijo ip origen

En la casilla <filter>, ejecutar: ip.src eq 193.145.0.0/24 (Filtra todos los paquetes ip cuya dirección IP origen comience por 193.145. .

O en la casilla <Expression...>, seleccionar el filtro a través de los menús desplegables seleccionando la dirección ip origen 193.145.0.0/16 en los paquetes capturados.

Filtro por tamaño de paquete

En la casilla <filter>, ejecutar: ip.len < 100 o ip.len lt 100 (paquetes con tamaño inferior a 100 byes). Los operadores válidos son: eq , ne , gt, lt, ge, le o ==, !=, >, <, >=, <=. Es decir, igual que, distinto de, mayor que, menor que, mayor o igual y menor o igual.

También puede usarse la notación hexadecimal 0x, como por ejemplo 0x0a.

O en la casilla <Expression...>, seleccionar el filtro a través de los menús desplegables buscando atributos de la cabecera ip.

Filtrado de todos los paquetes TCP con el bit SYN igual a 1 (Establecimientos de conexión)

En la casilla <filter>, ejecutar: tcp.flags & 0x02 o tcp.flags & 2 (Esta selección permite conocer el número de intentos de conexión realizados entre dos máquinas). El campo flags se compone de 6 bit, cada uno con significado propio. El bit SYN se utiliza para establecer una conexión TCP o socket y se emplea únicamente al inicio de cada conexión, ocupando la segunda posición del campo flags. Por ello, al realizar el and lógico con el valor 0x02 (en binario 000010), podemos comprobar el estado lógico de ese bit independiente del resto.

O en la casilla <Expression...>, seleccionar el filtro a través de los menús desplegables seleccionando el atributo 'flags' == 0x02 de la cabecera tcp.

Filtrado de todos los paquetes IP con el campo TTL mayor o igual a 64

En la casilla <filter>, ejecutar: ip.ttl >= 0x64 o ip.ttl >= 100 .

O en la casilla <Expression...>, seleccionar el filtro a través de los menús desplegables seleccionando el atributo ttl == 0x064 de la cabecera ip.

Filtrado de todos los paquetes http que contengan el texto aula24

En la casilla <filter>, ejecutar: http contains aula24 .

O en la casilla <Expression...>, seleccionar el filtro http correspondiente.

Para una mayor comprensión acerca de la sintáxis de filtrado, se recomienda el acceso al siguiente URL: http://www.wireshark.org/docs/

5. Protocolos de comunicación en lan's

5.1. Prococolo de nivel de enlace Ethernet

Ethernet es una red de área local con tecnología de difusión basada en un bus común. Originariamente fue introducida por el fabricante Novell y consistía en un bus de cable coaxial al que se conectaban los equipos de la red empleando derivadores en forma de T. Esta Ethernet original permitía velocidades de transferencia de hasta 10 Mbps y presentaba el problema clásico de colisiones de las redes de difusión. El esquema de funcionamiento para la transmisión de datos en una red Ethernet es muy sencillo: Cualquier estación que desea transmitir datos escucha durante un cierto tiempo el canal. Si no se detecta actividad de transmisión se procede con la transmisión de las señales de datos al medio físico. Este sistema resulta efectivo cuando el número de equipos en la red es bajo pero si el número es demasiado alto entonces se producen con frecuencia colisiones, ya que la probabilidad de que dos o más estaciones detecten simultáneamente el medio físico libre y transmitan es más alta.

La colisión es detectada por la estación que transmite los datos al comprobar que por el medio físico circula una señal de interferencia (debido a la superposición de varias señales de datos) y procede a resolver el problema. Para ello espera un tiempo aleatorio y vuelve a transmitir la información. De esta forma se consigue que el paquete de datos se transmita sin esperar a comprobar de nuevo el medio físico y dado que se espera un tiempo aleatorio, la probabilidad de volver a colisionar es baja. Sin embargo este esquema funcionará cuando el volumen de tráfico (cantidad de información transmitida) y el número de equipos en la red no sea muy alto (inferior a unos 25), ya que en caso contrario la red entra en un estado de permanente colisión y no es posible la transmisión de información.

Este inconveniente de colisiones se superó con la introducción del *switch*, que sustituye el bus común por una malla de interconexión que evita muchas de las colisiones. Este mejora en Ethernet, denominada Ethernet conmutada, permitió el desarrollo de sistemas que permitieran transmitir datos a mayor velocidad, pasando de 10 Mbps a 100 Mbps en las redes Fast Ethernet conmutada, 1000 Mbps (1 Gbps) en la Gigabit Ethernet y 10000 Mbps (10 Gpbs) en la red 10 Gigabit Ethernet.

Existen básicamente dos tipos de paquetes dentro de Ethernet. La denominada IEEE 802.3 y la Ethernet. La utilización de una u otra depende del protocolo utilizado. Así, TCP/IP utiliza la encapsulación denominada Ethernet (RFC 894 - Request for comments nº 894), mientras que el protocolo utilizado por Novell, el IPX/SPX, utiliza la encapsulación 802.3.

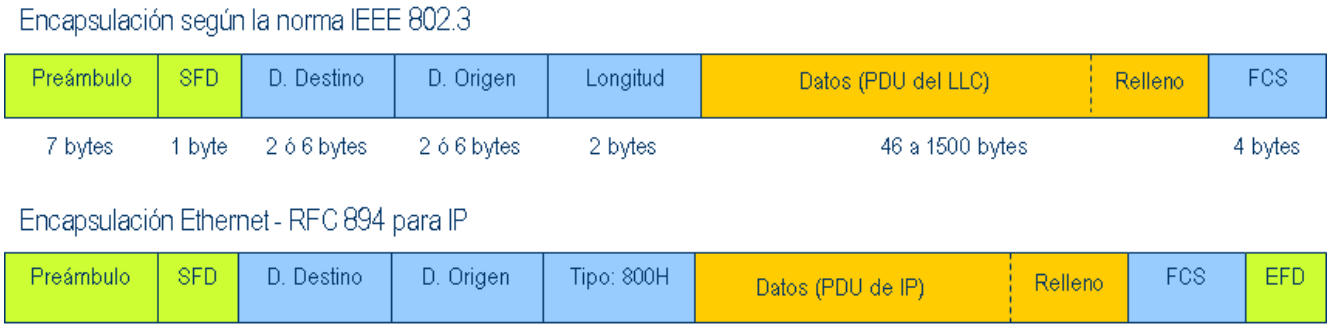

Figura 4: Encapsulación según normal IEEE 802.3 y Ethernet.

El tamaño máximo de trama (MTU)

Como puede verse en la figura anterior, existe un límite en el tamaño del paquete tanto para Ethernet como para IEEE 802.3. Los tamaños máximos para datos (datagrama IP) son de 1500 y 1492 bytes respectivamente. Esta característica de la capa de enlace se conoce como **MTU** (**Maximum Transfer Unit**).

Si un datagrama IP es mayor que el MTU de la capa de enlace, IP utiliza un mecanismo denominado fragmentación, consistente en romper el datagrama en pequeños fragmentos de manera que cada uno de ellos sea menor que el MTU. Ethernet es incapaz de realizar la fragmentación de un paquete de información procedente de la capa de red superior (datagrama IP), por lo que la capa de red tiene que enviar paquetes del tamaño adecuado a la capa de enlace Ethernet.

El MTU varía en función del tipo de enlace, y depende de diversos factores como la tasa de error media (BER), política de acceso al medio, velocidad de transmisión etc.

Las direcciones MAC

Cuando un paquete Ethernet es enviado a una estación de la red se necesita conocer la dirección de la estación en la red Ethernet. A ésta dirección de cada estación en una red Ethernet se la denomina dirección física, dirección **MAC** (**Media Access Control**), dirección Ethernet o dirección del adaptador de red, dependiendo de la bibliografía consultada.

Consiste en un valor de 48 bits (6 bytes), de forma que los 3 primeros bytes de la izquierda son fijados para cada fabricante de adaptadores y los 3 siguientes los establece el fabricante del mismo. Este esquema permite que cada fabricante de adaptadores Ethernet proporcione direcciones MAC diferentes, por lo que cada dirección MAC es única e irrepetible. Esta condición es necesaria para que en una red Ethernet puedan coexistir estaciones con adaptadores de diferentes fabricantes, ya que es necesario identificar a cada máquina de la red de forma única.

Dado que Ethernet es una red de difusión, cada adaptador de red debe ser capaz de procesar paquetes dirigidos a dos direcciones MAC: La suya propia y la dirección de broadcast o dirección difusión. Ésta se caracteriza por tener los 48 bits a 1, con lo cual queda como FF:FF:FF: FF:FF:FF expresada en hexadecimal.

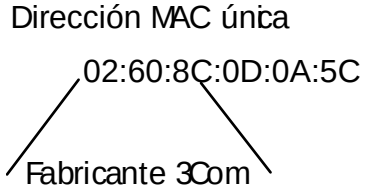

Figura 5: Esquema de una dirección MAC.

Un paquete ethernet con dirección de destino la dirección de broadcast será atendida por todas las estaciones conectadas sobre el mismo segmento. Esta particularidad es utilizada ampliamente por el protocolo ARP que veremos mas adelante.

Ethernet permite además un esquema de direccionamiento con multidifusión. Para ello es posible asignar a un adaptador Ethernet una dirección MAC de grupo. Para indicar una dirección MAC de grupo, la dirección MAC debe tener el valor 01:xx:xx:xx:xx:xx, tomando x los valores asociados al grupo. El esquema de multidifusión no se estudiará en las prácticas de esta asignatura.

5.2. El protocolo ARP

El esquema de direccionamiento de Ethernet es sólo valido cuando se intercambia información dentro del mismo segmento de difusión. En una red con arquitectura TCP/IP (Internet) nos vamos a encontrar con una estructura que no es la de una red de difusión, sino la interconexión de numeras redes de difusión y equipos remotos empleando una red punto a punto. Ello supone la necesidad de un mecanismo de encaminamiento de la información a través de esta red punto a punto. El mecanismo de encaminamiento lo proporciona la capa de red de la arquitectura, en nuestro caso el protocolo IP. Una de las características de este protocolo es establecer un esquema de direccionamiento en el que cada equipo en Internet tiene una dirección única. Esta dirección se denomina dirección IP y en una red Ethernet conectada a Internet cada equipo tendrá asociada una dirección IP y una dirección MAC.

Dado que para enviar información en una red Ethernet es necesario conocer la dirección MAC del destino y la información procedente de Internet indicará una dirección IP de destino, se hace necesario un mecanismo dinámico de asociación de direcciones MAC (direcciones del nivel de enlace) con direcciones IP (direciones del nivel de red). Este mecanismo se especifica en el protocolo **ARP** (**Address resolution protocol**) recogido en el documento estándar de Internet RFC 826.

Veamos el esquema de funcionamiento del protocolo ARP en el siguiente segmento de red.

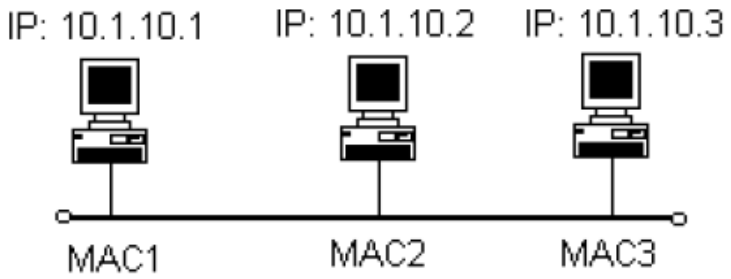

Figura 6: Esquema de red.

Si la estación 10.1.10.1 desea enviar un paquete de datos a la estación 10.1.10.2 debe crear un datagrama IP en el que se indique la dirección origen y destino de esos datos. Este paquete lo podemos representar con la siguiente sintaxis: “10.1.10.1 -> 10.1.10.2 | datos”. De esta forma indicamos que la estación 10.1.10.1 transmite un datagrama IP a la estación 10.1.10.2 con los datos “datos”. Este datagrama ha de ser enviado al medio físico dentro de un paquete Ethernet en el que se debe indicar la dirección MAC de destino y de origen. En principio la estación 10.1.10.1 sólo conoce su dirección MAC y la dirección IP de destino, por lo que tiene que determinar la dirección MAC de destino del paquete Ethernet. ARP permite

determinar cuál es la dirección MAC de la estación que tiene una cierta dirección IP. Para ello se desencadena el envío de una serie de paquetes ARP en la red.

En primer lugar la estación 10.1.10.1 tiene que preguntar a todas las estaciones de la red quién tiene la dirección IP 10.1.10.2. Como desconoce las direcciones MAC del resto de estaciones empleará la dirección de broadcast Ethernet para enviar un paquete que sea procesado por todas las estaciones de la red y en el que se pregunte ¿qué estación posee la dirección IP 10.1.10.2 ? Este paquete lo representaremos con la sintaxis:

MAC1 -> FF:...:FF | ARP Request | ¿ 10.1.10.2 ?

Este paquete se denomina petición ARP y será procesado por todas las estaciones de la red.

La estación que contenga la dirección IP 10.1.10.2 contestará al remitente indicando cuál su dirección MAC. A este paquete de respuesta se la denomina respuesta ARP y lo representaremos por la sintaxis:

MAC2 -> MAC1 | ARP Reply | 10.1.10.2 <=> MAC2

De esta forma, la estación 10.1.10.1 ya puede transmitir en el segmento Ethernet el datagrama IP, que representaremos con la sintaxis:

MAC1 -> MAC2 | 10.1.10.1 -> 10.1.10.2 | datos

La memoria cache de ARP

Sin embargo, el intercambio de paquetes ARP cada vez que una estación tiene que transmitir un datagrama IP supone un aumento de tráfico en la red que impide que otras estaciones puedan transmitir. Resulta lógico que una vez que una estación aprende la dirección MAC asociada a una cierta dirección IP almacene esta información en una tabla donde pueda consultarla posteriormente. Esta tabla se denomina memoria caché de ARP y se encarga de mantener las correspondencias entre las direcciones IP y las MAC. Esta tabla se encuentra vacía al iniciar el sistema y cada vez que se añade una nueva entrada ésta se mantiene durante un cierto tiempo. Si pasado este tiempo la estación no ha empleado esa entrada de la tabla, ésta será borrada. El establecer un tiempo de expiración para una entrada en la tabla permite que si una estación modifica su dirección IP o MAC ésta sea aprendida de nuevo de forma automática. El plazo normal de expiración de una entrada en la tabla ARP es de 20 minutos para sistemas Unix y de unos 2 minutos para Windows. Por tanto, en sistemas Windows existirá un peor aprovechamiento de la red de comunicaciones al intercambiarse paquetes ARP más frecuentemente.

Para visualizar el intercambio de paquetes ARP podemos emplear la aplicación ping. Esta aplicación envía un datagrama IP a una estación de la red y espera que ésta le envie otro datagrama IP de respuesta. El formato de empleo de la aplicación ping es el siguiente: “ping -n 1 dirección_IP” En primer lugar podemos comprobar el estado de la tabla caché de arp ejecutando el comando *arp -a* en una ventana de “símbolo del sistema”. El comando visualiza las asociaciones de direcciones IP y MAC que conoce la estación.

Al ejecutar el comando “ping -n 1 172.20.43.231” podemos comprobar que la tabla caché de arp ha sido modificada, añadiendo una entrada para la dirección IP 172.20.43.231. Al cabo de unos minutos podemos comprobar que la entrada desaparece de la tabla.

Si al ejecutar el comando empleamos el monitor de red para capturar la información, podemos comprobar como aparecen paquetes ARP si la dirección IP de destino no está en la tabla caché, mientras que si está no aparecerán paquetes ARP al ejecutar el comando ping.

5.3. El protocolo de nivel de red IP

El protocolo de nivel de red IP tiene como objetivo conseguir que los paquetes de información puedan ser encaminados a través de una red de computadores formada por la interconexión de diferentes segmentos físicos (Internet). Con un protocolo de nivel de enlace, como es Ethernet, sólo es posible que la información sea intercambiada dentro del mismo segmento físico. Para que la información pueda pasar de un segmento físico a otro es necesario un sistema de direccionamiento que permita la comunicación entre equipos de redes diferentes. Ésta es una de las funcionalidades del protocolo IP, establecer un sistema de direccionamiento global para todos los equipos que conforman la red. El protocolo IP ha evolucionado en el tiempo dando lugar a varias versiones del mismo. En Redes de Computadores nos centraremos en la versión 4 de este protocolo (IPv4), en funcionamiento en la inmensa mayoría de equipos de usuario conectados a Internet, pero se está procediendo a la implantación de la última versión de IP (IPv6) en los troncales (backbone) de Internet, y en toda la red de Internet.

El direccionamiento IP se fundamenta en las denominadas direcciones IP. Cada una de estas direcciones consiste en un valor de 32 bits que es único y permite distinguir dos partes en la dirección: la parte de red y la parte de máquina. Todas las estaciones que están en una misma red IP tendrán los mismos valores de parte de red en su dirección IP y valores diferentes en la parte de máquina. El valor de 32 bits se expresa dividiéndolo en cuatro grupos de 8 bits separados por puntos: x.x.x.x, donde el valor x estará en el rango de 0 a 255.

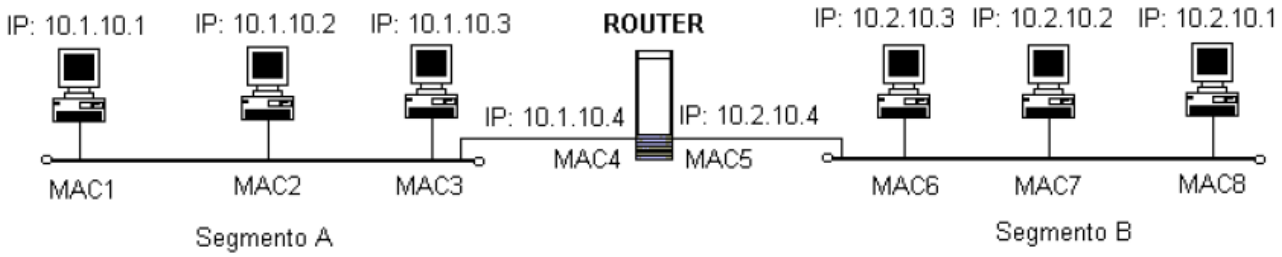

Figura 7: Esquema de red con dos segmentos.

En el esquema anterior se muestra la interconexión de dos segmentos de red con arquitectura TCP/IP. El dispositivo que los interconecta se denomina *router* o encaminador y será el dispositivo encargado de determinar, para cada paquete que le llega, a qué segmento de red hay que enviarlo. Dado que un *router* interconectará dos o más segmentos de red, éste dispondrá de un adaptador o tarjeta de red por cada segmento que une, y para cada adaptador se especificará una dirección MAC y una dirección IP. En cada segmento, todas las direcciones IP disponen de una parte común que se denomina parte de red y siempre será un conjunto de bits de la parte inicial de la dirección IP. En el caso anterior, en el segmento A la parte de red son los primeros 16 bits de la dirección IP: 10.1, y en el segmento B también los 16 primeros: 10.2. Nótese como la parte de red de las direcciones IP son diferentes en cada segmento. Los últimos 16 bits de la dirección IP se corresponden con la parte de máquina, que dentro de cada segmento o red IP es diferente para todas las estaciones. Este es el esquema de direccionamiento de Internet: diferentes redes IP interconectadas entre sí empleando routers.

Sin embargo, la identificación de la parte de red y de máquina de una dirección IP no se realiza averiguando las partes comunes de todas las direcciones en una red, sino que se especifica con un valor adicional de 32 bits que se denomina máscara de red. La máscara de red es un valor de 32 bits en los que los primeros n bits que son parte de red en la dirección IP se ponen a valor 1, y el resto correspondientes a la parte de máquina a valor 0. Para el

segmento A la máscara de red asociada será: 11111111.11111111.00000000.00000000, es decir 255.255.0.0, o de forma abreviada también se puede expresar como /16. De esta forma, con una dirección IP y la máscara de red asociada podemos determinar qué direcciones IP pertenecen a la misma red.

Sea la dirección IP 120.12.3.4 con máscara de red 255.255.0.0, las direcciones asociadas a la misma red serán:

120.12.0.0

120.12.0.1

....

120.12.0.255

120.12.1.0

120.12.1.1

.....

120.12.254.254

120.12.254.255

120.12.255.0

120.12.255.1

.....

120.12.255.255

De todas estas direcciones IP (las de la red 120.12) existen dos que no pueden ser asignadas a estaciones de la red ya que están reservadas. Una de ellas es la denominada dirección de red que es la dirección IP de la red que tiene todos los bits de la parte de máquina a valor 0. En el caso anterior, la dirección de red es 120.12.0.0. Esta dirección se emplea en los routers para establecer rutas de encaminamiento de los paquetes. La otra dirección reservada es la denominada dirección de *broadcast* y es la dirección IP de la red que tiene todos los bits de la parte de máquina a valor 1. El objetivo de esta dirección es análogo al de la dirección de broadcast de nivel de enlace: si una estación recibe un datagrama IP dirigido a la dirección IP de broadcast de su red procesará el paquete. Para el caso anterior, la dirección de broadcast será 120.12.255.255.

El valor de la máscara de red asociada a una dirección IP no es arbitrario, existe una definición de direcciones IP donde para cada dirección IP se especifica una máscara de red y por tanto una parte de red y de máquina en la dirección IP. Esta definición de máscaras asociadas a direcciones IP se muestra a continuación:

Figura 8: Clases de redes IP según la dirección.

En este diagrama se definen 5 grupos de direcciones IP dependiendo del valor de los primeros bits de la dirección IP. Para cada grupo de direcciones IP se ha definido una máscara de red que indica qué parte de la dirección IP se asigna a la red y qué parte a las máquinas. Por ejemplo, la clase C está formada por las direcciones IP cuyos tres primeros bits toman el valor binario 110. Estas direcciones IP estarán definidas en el rango binario desde 11000000.0000000.00000000.00000000 a 11011111.11111111.1111111.1111111, es decir desde 192.0.0.0 hasta 223.255.255.255. Dado que la máscara de red asociada es 255.255.255.0, tenemos disponibles 21 bits para especificar valores de redes diferentes y 8 para especificar máquinas dentro de cada red. Por tanto, dispondremos de 221 (2.097.152) redes de clase C y dentro de cada una podemos especificar 28 - 2 (254) máquinas diferentes (la dirección de red y broadcast no son asignables a máquinas en la red).

Teniendo en cuenta el esquema de direccionamiento anterior, las direcciones IP de la figura 7 tienen una máscara de red asociada de 8 bits, es decir 255.0.0.0. Sin embargo se ha indicado que la máscara asociada es 255.255.0.0 para así establecer dos redes diferentes. Este mecanismo, por el cual a partir de una red (10.0.0.0) se definen dos redes diferentes (10.1.0.0 y 10.2.0.0) se denomina ampliación de la máscara de red, pasando a crear subredes dentro de una red. Este mecanismo se emplea cuando en una red no pueden coexistir todas las máquinas en un mismo segmento físico y es necesario crear varias subredes. Para ello se amplia la máscara de red en un número suficiente de bits para especificar las nuevas subredes.

Sea la red 192.168.100.0/24 (el término /24 indica que la máscara de red tiene los primeros 24 bits puestos a 1, es decir tendrá el valor 255.255.255.0). Si se desea establecer 3 subredes dentro de esa red con el mismo número de estaciones en cada una de ellas, será necesario ampliar en 2 bits la máscara de red dado que con dos bits podemos establecer cuatro combinaciones diferentes. De esta forma las 4 cuatro subredes (una de las cuales no se emplearía) que se obtendrían serían:

192.168.100.00000000 o 192.168.100.0/26

192.168.100.01000000 o 192.168.100.64/26

192.168.100.10000000 o 192.168.100.128/26

192.168.100.11000000 o 192.168.100.192/26

La nueva máscara de red para cada una de las subredes creadas tendrá ahora 26 bits y su valor será 255.255.255.11000000 o 255.255.255.192. Los rangos de direcciones IP para cada subred serían entonces:

Red 192.168.100.0/26

Desde 192.168.100.00000001 o 192.168.100.1 hasta 192.168.100.00111110 o 192.168.100.62

Dirección de la subred red: 192.168.100.0

Dirección de broadcast de la subred: 192.168.100.63

Red 192.168.100.64/26

Desde 192.168.100.01000001 o 192.168.100.65 hasta 192.168.100.01111110 o 192.168.100.126

Dirección de la subred red: 192.168.100.64

Dirección de broadcast de la subred: 192.168.100.127

Red 192.168.100.128/26

Desde 192.168.100.10000001 o 192.168.100.129 hasta 192.168.100.10111110 o 192.168.100.190

Dirección de la subred red: 192.168.100.128

Dirección de broadcast de la subred: 192.168.100.191

Red 192.168.100.192/26

Desde 192.168.100.11000001 o 192.168.100.193 hasta 192.168.100.11111110 o 192.168.100.254

Dirección de la subred red: 192.168.100.192

Dirección de broadcast de la subred: 192.168.100.255

Parámetros de configuración en una máquina con arquitectura TCP/IP

Con el esquema de direccionamiento IP anterior podemos determinar qué parámetros de configuración de red son necesarios para una máquina que desee intercambiar información en una red con arquitectura TCP/IP.

Dirección IP: Dirección asignada en la red a la estación.

Máscara de red: Máscara de red asociada a la dirección IP, que puede estar ampliada en el caso de una subred.

Además de estos dos parámetros es necesario un tercero que se denomina puerta de enlace (P.E.) o *default gateway* (D.G). Este parámetro es la dirección IP de un equipo en la red que proporciona acceso a otras redes. Sin este parámetro una máquina de una red TCP/IP sólo puede intercambiar información dentro de la propia red. La puerta de enlace en una red TCP/IP será siempre un *router* que realiza la interconexión con el resto de redes que existen. La existencia de la puerta de enlace afecta al mecanismo de funcionamiento de ARP.

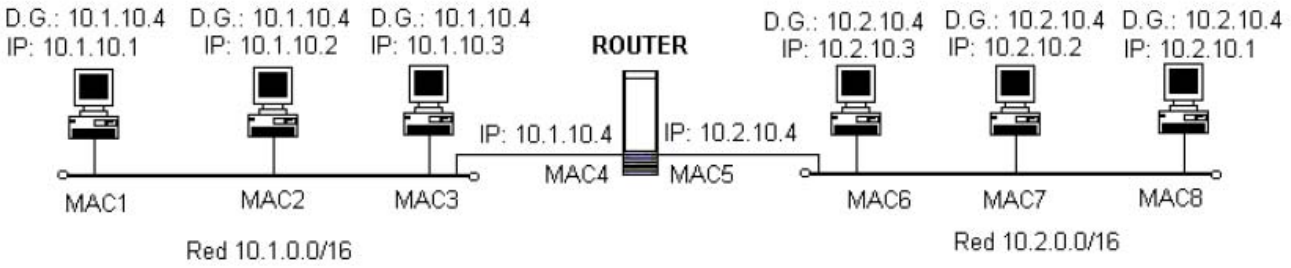

Figura 9: Esquema de red a nivel IP.

En el esquema de la red de la figura 9 se representa dos redes TCP/IP interconectadas por un *router*. Cuando las estaciones intercambian datagramas IP con datos han de indicar en la cabecera del datagrama la dirección IP de origen y la dirección IP de destino. Este datagrama lo denotaremos con la sintaxis: IP_origen -> IP_destino | datos. Todo datagrama IP se enviará encapsulado dentro de un paquete del nivel de enlace (en este caso Ethernet) donde se especificarán las direcciones MAC de origen y de destino. El funcionamiento de ARP para proporcionar la dirección MAC de destino será diferente si el datagrama IP va dirigido a una estación de la propia red IP o de otra red IP.

Supóngase que la estación 10.1.10.1 quiere enviar un datagrama IP a la estación 10.1.10.2. La estación de origen construirá el datagrama 10.1.10.1 -> 10.1.10.2 | datos. Este datagrama será encapsulado y enviado en un paquete Ethernet, para lo que hay que determinar la dirección MAC de la estación 10.1.10.2.

En primer lugar, la estación ha de determinar si el paquete va dirigido a una estación de su red IP o no. Para ello comprueba los bits correspondientes a la parte de red de la dirección IP de destino según la máscara de red de la estación. Dado que la máscara de red de la estación 10.1.10.1 es 255.255.0.0, la estación comprueba el valor de los primeros 16 bits de la dirección 10.1.10.2. Si esos primeros 16 bits coinciden con los 16 primeros bits de la dirección de la estación de origen (10.1.10.1), entonces la dirección de destino pertenece a la misma red que la de origen. De hecho, los primeros 16 bits de las direcciones 10.1.10.1 y 10.1.10.2 coinciden, luego la estación de destino estará en el mismo segmento físico y se buscará en ese segmento la dirección MAC del destino.

Por tanto ARP desencadenará la siguiente secuencia de paquetes:

MAC1 -> FF:...:FF | ARP Request | ¿ 10.1.10.2 ?

MAC2 -> MAC1 | ARP Reply | 10.1.10.2 <=> MAC2

Y de esta forma se enviará el datagrama IP

MAC1 -> MAC2 | 10.1.10.1 -> 10.1.10.2 | datos

Supóngase ahora que la estación 10.1.10.1 quiere enviar otro datagrama IP a la estación 10.2.10.3. El datagrama IP construido será “10.1.10.1 -> 10.2.10.3 | datos”. La estación 10.1.10.1 comprueba los 16 primeros bits de la dirección de destino (10.2) y verifica que no se corresponden con los suyos. De esta forma la estación 10.1.10.1 sabe que la estación de destino no se encuentra en su propia red y por tanto ha de enviar el datagrama IP a una estación de su red que pueda encaminarlo al destino: esta estación es la puerta de enlace. Por tanto el datagrama IP ha de encapsularse en un paquete Ethernet dirigido a la puerta de enlace. Para ello hay que determinar la dirección MAC de la puerta de enlace con la siguiente secuencia de paquetes ARP:

MAC1 -> FF:...:FF | ARP Request | ¿ 10.1.10.4 ?

MAC4 -> MAC1 | ARP Reply | 10.1.10.4 <=> MAC4

De esta forma el paquete Ethernet enviado por la estación 10.1.10.1 será:

MAC1 -> MAC4 | 10.1.10.1 -> 10.2.10.3 | datos

Es muy importante notar que el datagrama IP mantiene su dirección IP origen y destino sin modificar, ya que el datagrama ha de alcanzar el destino y conservar la información del remitente. El direccionamiento de nivel de enlace (direcciones MAC) permite que el datagrama alcance el siguiente salto en cada segmento de red para alcanzar el destino.

Cuando el datagrama "10.1.10.1 -> 10.2.10.3 | datos" es procesado por el router, éste es capaz de determinar que el destinatario está en la red 10.2.0.0/16 a la que está conectado directamente. Por ello, en el segmento de red 10.2.0.0 se desencadenará la secuencia de paquetes ARP:

MAC5 -> FF:...:FF | ARP Request | ¿ 10.2.10.3 ?

MAC6 -> MAC5 | ARP Reply | 10.2.10.3 <=> MAC6

Y el router enviará el paquete Ethernet con el datagrama IP a su destinatario:

MAC5 -> MAC6 | 10.1.10.1 -> 10.2.10.3 | datos

Un parámetro de configuración adicional en una máquina conectada a una red TCP/IP son los denominados servidores de nombres de dominio o *domain name servers* (DNS). Cuando se accede a un servidor web con un navegador el usuario introduce un nombre en la forma www.nombre.dominio (www.ua.es). Este nombre denota a un servidor de hipertexto de una organización en una región (Servidor de hipertexto de la Universidad de Alicante en España).

Al acceder a un servidor web se produce el intercambio de datagramas IP entre el cliente y el servidor, pero para ello es necesario conocer la dirección IP del servidor. De esta función se encargan los servidores de nombres de dominio. Cada proveedor de acceso a Internet dispone de servidores de nombres que realizan una traducción de nombre de dominio a direcciones IP para sus clientes. Estos servidores de nombres están dispuestos en una estructura jerárquica, de forma que si un servidor no conoce un cierto nombre lo consulta a otro servidor de nombres.

En la Universidad de Alicante, los servidores de nombres tienen las direcciones IP 193.145.233.5 y 193.145.233.6.

Formato del datagrama IP

Un datagrama IP consta de una cabecera y un cuerpo de datos. En la cabecera se incorpora la información de control para el funcionamiento del protocolo como son las direcciones IP de origen y de destino. El formato del datagrama IP queda representado en la figura siguiente.

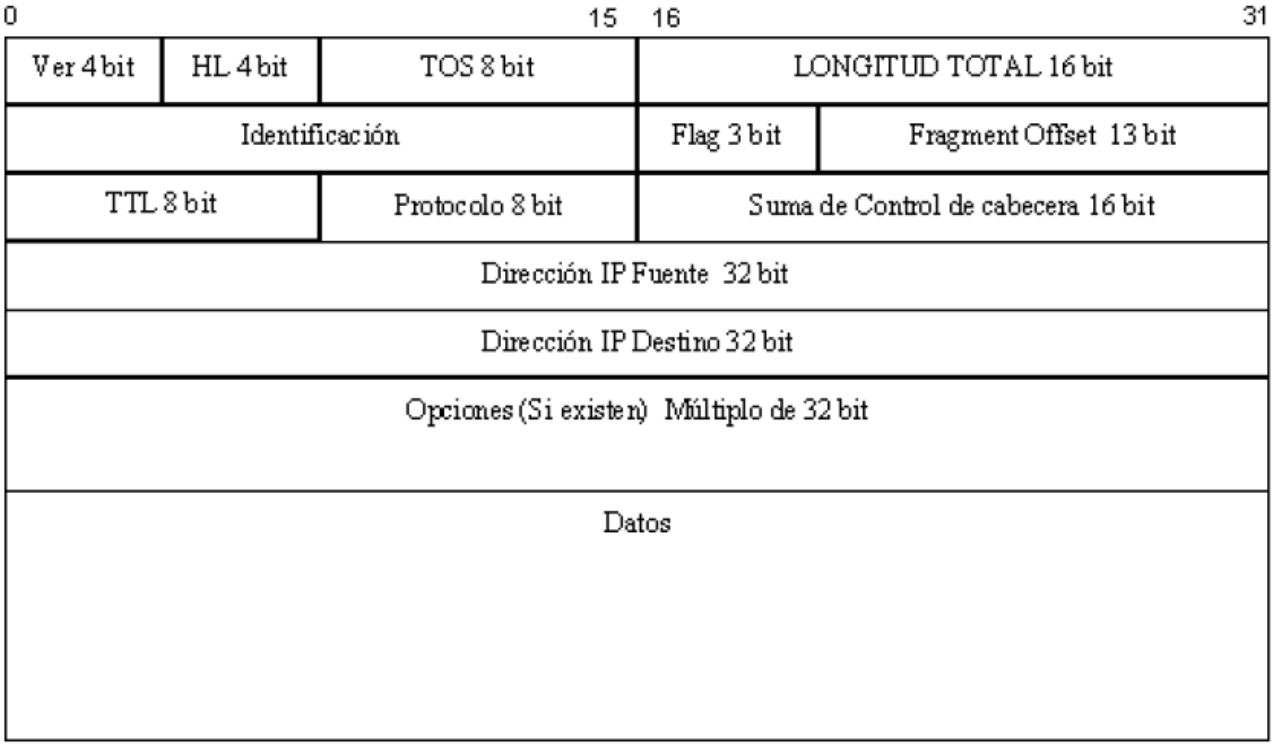

Figura 10: Formato de una trama IP.

El bit más significativo está marcado como 0 en el lado izquierdo, mientras que el menos significativo de la palabra de 32 bits se etiqueta como 31 en el lado derecho. Los octetos de cada palabra de 32 bits se transmiten empezando por el 0 hasta el 31.

El campo **Ver** indica la versión del protocolo IP en el datagrama y tiene una longitud de 4 bits.

El campo **HL** indica el número de bytes que componen la cabecera, incluyendo las opciones eventuales. Puesto que su tamaño es de 4 bits, tendremos que: (24 -1) x 32 bits por palabra = 60 bytes de longitud máxima en la cabecera IP. Este campo posee habitualmente el valor 5 (cuando no existen opciones).

TOS (Type of service) indica el Tipo de Servicio. Actualmente los 3 primeros bits son ignorados, los 4 siguientes representan el TOS y el último está inutilizado y su valor debe ser siempre 0.

El campo **Longitud Total** contiene el tamaño en octetos de todo el datagrama IP (cabecera y datos). Gracias a él y al campo HL podemos conocer donde empieza y termina la porción de datos. Como utiliza 16 bits, se puede deducir que el tamaño máximo o MTU de un datagrama IP será de 65535 bytes.

El mecanismo de fragmentación utilizado por IP emplea los siguientes 3 campos. El primero, **Identificación**, permite marcar de forma única cada datagrama enviado por una máquina. Se incrementa normalmente en cada nuevo envío. Cuando se produce una fragmentación, este valor es copiado en cada uno de los trozos o fragmentos que componen el datagrama original. El campo **flag** de 3 bits, activa entonces uno de ellos (el número 2) conocido como '*more fragments*' tomando el valor 1 en todos los trozos excepto en el último. El campo **Frame Offset** contiene el índice del fragmento a partir del datagrama original. Además, el nuevo campo Longitud Total de cada fragmento se actualiza al valor adecuado.

Existe un bit (el número 1) en el campo **flag** conocido como **Don't fragment**. Si está activado a 1, IP no producirá ninguna fragmentación eliminando el datagrama y enviando un mensaje de error ICMP a la fuente Para evitar que un datagrama quede atrapado en algún bucle dentro de la red (p. ej. Por problemas con los protocolos de encaminamiento) existe un tiempo de vida representado mediante el campo TTL (*Time to Live*). Se inicializa a un cierto valor por el remitente y se decrementa en una unidad por cada router que atraviesa. Cuando alcanza el valor 0, el datagrama se elimina y un mensaje ICMP es enviado a la fuente indicando el suceso.

IP identifica el protocolo (TCP, UDP, ICMP,...) al cual debe hacer llegar la información a través del campo Protocolo.

La Suma de Control abarca únicamente la cabecera IP. Se calcula como una suma sin acarreo sobre 16 bits de todos los bytes que componen la cabecera IP considerándolos como una secuencia de palabras de 16 bits. El motivo es claro. Un router debe procesar grandes cantidades de paquetes por unidad de tiempo. Generalmente, el único valor que se modifica a cada datagrama es el TTL, decrementándolo en una unidad. El cálculo de la suma de control puede ser realizado de forma incremental disminuyendo drásticamente el tiempo de proceso de cada datagrama por las pasarelas intermedias.

Como ya se comentó anteriormente, cada datagrama contiene la dirección IP del destinatario y la del remitente.

El campo Opciones es una lista de longitud variable con información específica del datagrama.

5.4. Protocolos de nivel superior

En la figura siguiente se pueden observar las distintas capas de que consta la arquitectura de red TCP/IP, así como los protocolos de cada nivel y las interacciones entre ellos:

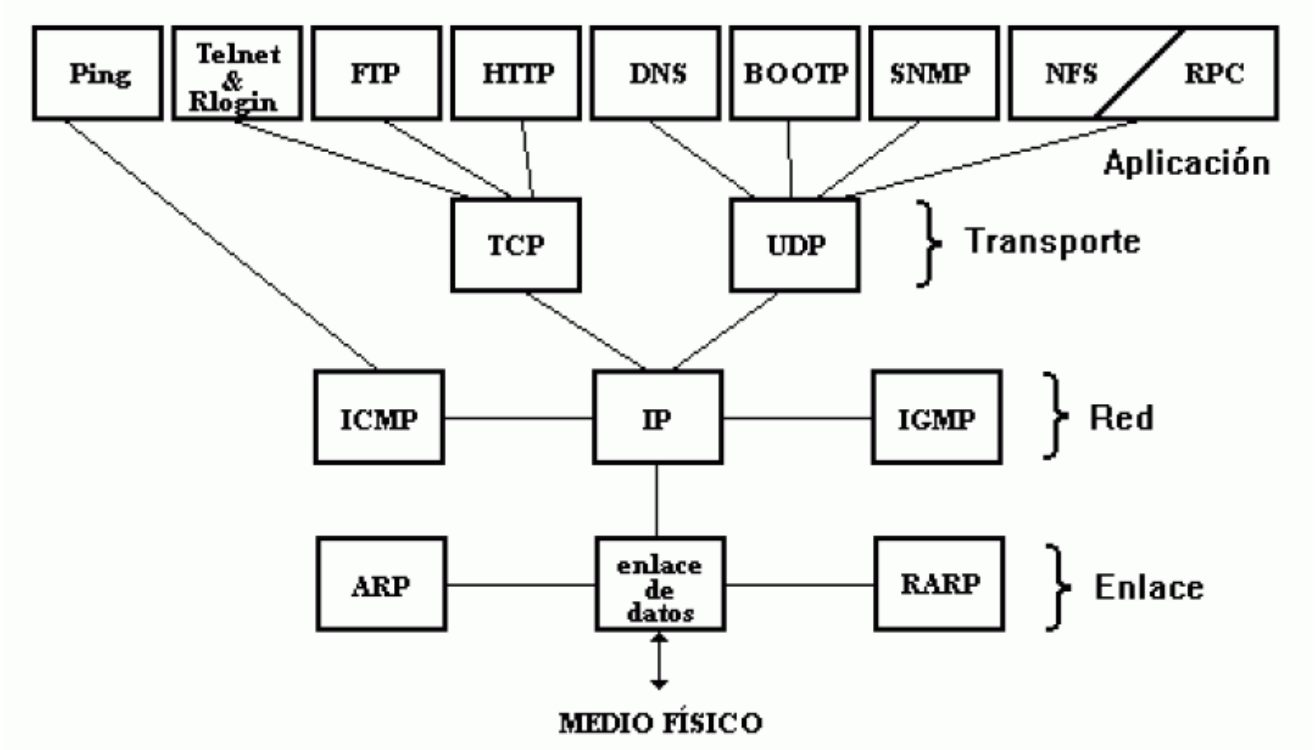

Figura 11: Protocolos según el nivel OSI.

Una vez que se han capturado un conjunto de paquetes podemos proceder a su filtrado para visualizar sólo aquellas que contengan un protocolo determinado. Los protocolos que nos interesan son TCP, UDP, HTTP, DNS e ICMP.

Generación de paquetes empleando protocolos TCP, UDP, HTTP, DNS e ICMP

TCP

El protocolo TCP se encuentra ubicado en la capa de transporte del modelo TCP/IP. Es un protocolo orientado a conexión. TCP asegura que los datos llegan a su destino mediante mecanismos de control, además estos datos son recibidos en el receptor en el mismo orden con el que se envían.

Para poder visualizar este tipo de paquetes ponemos en funcionamiento el Monitor de Red y seguidamente hacemos uso del Navegador, conectándonos a una página web arbitraria. http es el protocolo del nivel de aplicación utilizado en Internet por los navegadores para la transferencia de ficheros de tipo hipertexto (páginas web). El protocolo HTTP utiliza en el nivel de transporte el protocolo TCP. Deteniendo la captura de datos del Monitor fácilmente podemos filtrar y visualizar este tipo de paquetes (TCP y HTTP). Hay que tener en cuenta que si navegamos a una página visitada anteriormente el navegador puede tenerla en cache, con lo que no generaría ningún paquete ya que usaría la versión almacenada.

UDP

UDP es, al igual que TCP, un protocolo de transporte, pero mucho más sencillo ya que no está orientado a la conexión. UDP no ofrece ninguna garantía de fiabilidad pues no existe la seguridad de que los paquetes lleguen a su destino. Dada esta falta de fiabilidad parece lógico pensar que debemos utilizar siempre TCP, sin embargo esto no es del todo cierto, puesto que existen casos en los que el uso de UDP está recomendado por su sencillez y bajo consumo de recursos.

Para poder observar los paquetes UDP solicitamos el servicio DNS, protocolo para resolver los nombres de dominio de Internet, obteniendo la dirección IP asociada a una dirección de Internet (por ejemplo www.ua.es). Este servicio se ejecuta automáticamente cuando por ejemplo solicitamos una página web en nuestro navegador, realizamos un telnet, etc...

ICMP

El protocolo ICMP se estudiará detenidamente en la práctica 2 de la asignatura y está asociado a mensajes de test y error que se producen en la red. La aplicación ping permite el envío de datagramas IP que contienen un mensaje ICMP de información.

6. Cuestiones

6.1. Análisis de una captura de datos

A partir de un fichero de captura de tráfico en la red se determinará cierta información que aparece la misma. Para ello se necesita generar tráfico para poder obtener un fichero con información capturada.

En primer lugar se iniciará el monitor de red y se realizarán las siguientes acciones para generar tráfico:

- Abrimos una sesión del navegador al URL http://dfists.ua.es
- Desde una ventana de "Símbolo del sistema", se ejecuta el comando ping 172.20.43.230, que permite comprobar la conectividad de una máquina remota.
- Ejecutamos desde una ventana de "Símbolo del sistema", el comando "ping –l 1800 172.20.43.230". Con este comando se envían paquetes con 1800 bytes de datos.
- Ejecutamos desde una ventana de "Símbolo del sistema", el comando "tracert 172.25.40.91", que permite comprobar los saltos que recorren los paquetes para llegar a ese destino.
- Accedemos al buscador GOOGLE y escribimos la cadena de búsqueda aula24. Ignoramos el resultado del buscador.

A continuación se detiene la captura pulsando 'STOP' en el menú emergente de captura y se almacena la captura mediante la opción <File> <Save> utilizando como nombre de fichero LAB24_P1.cap.

Ahora disponemos de una captura que vamos a poder filtrar con un filtro de visualización. Con esta captura se debe responder a las siguientes cuestiones:

1. Calcula el porcentaje de tramas ethernet de difusión existentes en la captura. (Tramas de difusión/Tramas totales * 100).
2. Calcula el porcentaje de paquetes IP existentes en la captura.
3. Calcula el porcentaje de paquetes no IP existentes en la captura.
4. Calcula el porcentaje de paquetes IP enviados por el equipo del alumno.
5. Calcula el porcentaje de paquetes IP recibidos por el equipo del alumno.
6. Captura todos los paquetes IP que contengan la cadena 'abcd' y lleven la dirección IP de tu máquina.
7. Respecto a los paquetes obtenidos en el apartado anterior, ¿pertenecen a algún protocolo en concreto? Explica qué aplicación o programa ha podido generar esos paquetes.
8. Captura todos aquellos paquetes que contengan el campo *protocol* de la cabecera IP igual a 17.
9. Respecto a los paquetes capturados en el apartado anterior, ¿pertenecen al mismo protocolo de transporte? o ¿aparecen varios diferentes? Enumera los protocolos de transporte que aparecen.
10. Localiza todos los paquetes que contengan el campo TTL (Time to Live) de la cabecera IP igual a 1.

11. Localiza todos los paquetes que contengan el campo TTL (Time to Live) de la cabecera IP igual a 2.
12. Respecto de los apartados 10 y 11, ¿Qué protocolo aparece? ¿Qué aplicación puede haberlos generado y por qué?
13. Determina en cuantos paquetes aparece la cadena 'aula24'. ¿A qué aplicación están asociados?
14. Determina qué porcentaje de los paquetes IP capturados están fragmentados (paquetes con el bit *MORE FRAGMENTS* activo).

6.2. Direccionamiento IP

Se desean establecer 7 subredes dentro de la red 193.145.230.0/24 con el mismo número de equipos. Determina en cuantos bits hay que ampliar la máscara de red y cuáles son los rangos de direcciones IP para todas las subredes resultantes.

Se desean establecer 5 subredes dentro de la red 130.20.0.0/22. Determina en cuantos bits hay que ampliar la máscara de red y cuáles son los rangos de direcciones IP para todas las subredes resultantes.

6.3. Protocolo ARP

Verificar la configuración del equipo comprobando la dirección de la puerta de enlace ejecutando el comando:

C:\WINDOWS\netstat -rn

Se debe comprobar que aparece una línea de la forma:

Destino de red	Máscara de red	Puerta de acceso
0.0.0.0	0.0.0.0	172.20.43.230

Si la información anterior no aparece hay que crearla ejecutando el siguiente comando:

C:\pracredes

Comprobar con el comando "netstat –rn" que ahora sí aparece la línea indicada.

1. Verifica la presencia de paquetes ARP en la red ejecutando el comando "ping -n 1 172.20.43.231" y que la secuencia de las mismas se corresponde con la descrita en el enunciado de la práctica. Comprobar que en la tabla ARP (comando arp -a) aparece la entrada correspondiente y que si se ejecuta de nuevo el comando "ping -n 1 172.20.43.231" no aparecen paquetes ARP. Para que aparezcan de nuevo paquetes ARP hay que esperar que se borre la entrada automáticamente o borrarla directamente con el comando "arp –d 172.20.43.231".
2. Verifica el funcionamiento de ARP enviando un paquete IP a la máquina de tu compañero. Ejecuta el comando "ping -n 1 IP_compañero" y determina los paquetes ARP y echo, echo reply que aparecen. ¿Cuántas secuencias ARP aparecen al hacer un ping a la dirección de tu compañero? ¿Cómo cambian las tablas ARP de tu máquina y la de tu compañero? ¿Por qué tu compañero no te envía paquetes ARP?
3. Verifica el modo de funcionamiento de ARP cuando se envía un datagrama a otra red. Para ello ejecuta el comando "ping -n 1 10.4.2.5". Verifica de qué estación intenta averiguar ARP su dirección MAC. Ten en cuenta que sólo podrá visualizarse la secuencia ARP correspondiente a tu segmento físico.

4. Determina a través de qué estación de la red 172.20.43.192/26 procede el paquete de respuesta al ejecutar el comando ping a los siguientes destinos. Para ello hay que determinar la dirección MAC de origen del paquete de respuesta y ver en la tabla caché de ARP a que máquina se corresponde en la red.

   ping -n 1 10.4.2.6

   ping -n 1 10.4.2.5

   ping -n 1 10.4.2.2

   ping -n 1 10.3.7.0

   ping -n 1 10.3.2.0

   ping -n 1 172.20.41.241

   ping -n 1 172.20.41.242

7. Documentación complementaria

- RFC 791. Internet Protocol v4 specification.
- RFC 826. Ethernet Address Resolution Protocol.
- RFC 1883. Internet Protocol v6 specification.