Introducción a Redes y a TCP/IP sobre Tecnología Ethernet

REDES (9359)

ING. TÉCNICA EN INFORMÁTICA DE SISTEMAS

CURSO 2010/2011

(*Este documento es una versión en papel de la versión completa en formato web-SCORM publicada a través de la plataforma Moodle-UA*)

Pablo Gil Vázquez (Pablo.Gil@ua.es)
Grupo de Innovación Educativa en Automática

Universitat d'Alacant
Universidad de Alicante

1.1 Introducción

La primera práctica de la asignatura Redes pretende introducir al alumno en las redes de computadores de forma práctica. Para ello se realizará 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.

Con la realización de esta práctica el alumno debe adquirir conocimientos que le permitan:

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

1.2. Arquitectura de red TCP/IP

1.2.1 Introducción

En 1969 la agencia ARPA (Advanced Research Projects Agency) del Departamento de Defensa (DoD, Department of Defense) de los Estados Unidos inició un proyecto de interconexión de ordenadores mediante redes telefónicas. Al ser un proyecto desarrollado por militares en plena guerra fría, un principio básico de diseño era que la red debía poder resistir la destrucción de parte de su infraestructura (por ejemplo a causa de un ataque nuclear), de forma que dos nodos cualesquiera pudieran seguir comunicados siempre que hubiera alguna ruta que los uniera. Esto se consiguió en 1972 creando una red de conmutación de paquetes denominada ARPAnet, la primera de este tipo que operó en el mundo. La conmutación de paquetes unida al uso de topologías malladas mediante múltiples líneas punto a punto dio como resultado una red altamente fiable y robusta.

ARPAnet fue creciendo paulatinamente, y pronto se hicieron experimentos utilizando otros medios de transmisión de datos, en particular, enlaces por radio y vía satélite; los protocolos existentes tuvieron problemas para interoperar con estas redes, por lo que se diseñó un nuevo conjunto o pila de protocolos, y con ellos una arquitectura. Este nuevo conjunto se denominó TCP/IP (Transmission Control Protocol/Internet Protocol) nombre que provenía de los dos protocolos mas importantes que componían la pila; los nuevos protocolos fueron especificados por vez primera por Cerf y Kahn en un artículo publicado en 1974. A la nueva red, que se creó como consecuencia de la fusión de ARPAnet con las redes basadas en otras tecnologías de transmisión, se la denominó Internet.

La aproximación adoptada por los diseñadores del TCP/IP fue mucho más pragmática que la de los autores del modelo OSI. Mientras que en el caso de OSI se emplearon varios años en definir con

mucho cuidado una arquitectura de capas donde la función y servicios de cada una estuvieran perfectamente definidas, en el caso de TCP/IP la operación fue a la inversa, pues primero se especificaron los protocolos, y luego se definió el modelo como una simple descripción de los protocolos ya existentes. Por este motivo el modelo TCP/IP es mucho más simple que el OSI. También por este motivo el modelo OSI se utiliza a menudo para describir otras arquitecturas, como por ejemplo la TCP/IP, mientras que el modelo TCP/IP nunca suele emplearse para describir otras arquitecturas que no sean la suya propia.

En el modelo TCP/IP se pueden distinguir cuatro capas:

- La capa host-red: Acceso al medio y físico.
- La capa interred o red.
- La capa de transporte.
- La capa de aplicación.

En la figura 1 se aprecian las capas de la arquitectura. En los siguientes puntos se comentarán cada una de ellas.

1.2.2 La capa host-red

Esta capa engloba realmente las funciones de la capa física y la capa de enlace del modelo OSI. El modelo TCP/IP no dice gran cosa respecto a ella, salvo que debe ser capaz de conectar el host a la red por medio de algún protocolo que permita enviar paquetes IP. Se podría afirmar que para el modelo TCP/IP esta capa se comporta como una 'caja negra'. Cuando surge una nueva tecnología de red (por ejemplo ATM) una de las primeras cosas que aparece es un estándar que especifica de que forma se pueden enviar sobre ella paquetes IP; a partir de ahí la capa internet ya puede utilizar esa tecnología de manera transparente.

1.2.3 La capa internet IP

Esta capa es el 'corazón' de la red. Su papel equivale al desempeñado por la capa de red en el modelo OSI, es decir, se ocupa de encaminar los paquetes de la forma más conveniente para que lleguen a su destino, y de evitar que se produzcan situaciones de congestión en los nodos intermedios. Debido a los requisitos de robustez impuestos en el diseño, la capa Internet da únicamente un servicio de conmutación de paquetes no orientado a conexión. Los paquetes pueden llegar desordenados a su destino, en cuyo caso es responsabilidad de las capas superiores en el nodo receptor la reordenación para que sean presentados al usuario de forma adecuada.

A diferencia de lo que ocurre en el modelo OSI, donde los protocolos para nada intervienen en la descripción del modelo, la capa Internet define aquí un formato de paquete y un protocolo, llamado IP (Internet Protocol), que se considera el protocolo 'oficial' de la arquitectura, siendo el más popular de todos.

1.2.4 La capa de transporte

Esta capa recibe el mismo nombre y desarrolla la misma función que la cuarta capa del modelo OSI, consistente en permitir la comunicación extremo a extremo (host a host) en la red. Aquí se definen dos protocolos:

- TCP (Transmission Control Protocol) ofrece un servicio fiable, con lo que los paquetes (aquí llamados segmentos) llegan ordenados y sin errores. TCP se ocupa también del control de flujo extremo a extremo, para evitar que por ejemplo un host rápido sature a un receptor mas lento. Ejemplos de protocolos de aplicación que utilizan TCP son el SMTP (Simple Mail Transfer Program, correo electrónico) y el FTP (File Transfer Protocol).
- UDP (User Datagram Protocol) que da un servicio no orientado a conexión y no fiable. UDP no realiza control de errores ni de flujo. Una aplicación típica donde se utiliza UDP es la transmisión de voz y vídeo en tiempo real; aquí el retardo que introduciría el control de errores produciría mas daño que beneficio: es preferible perder algún paquete que retransmitirlo fuera de tiempo. Otro ejemplo de aplicación que utiliza UDP es el NFS (Network File System); aquí el control de errores y de flujo se realiza en la capa de aplicación.

1.2.5 La capa de aplicación

Esta capa desarrolla las funciones de las capas de sesión, presentación y aplicación del modelo OSI. La experiencia ha demostrado que las capas de sesión y presentación son de poca utilidad, debido a su escaso contenido, por lo que la aproximación adoptada por el modelo TCP/IP parece más acertada.

La capa de aplicación contiene todos los protocolos de alto nivel que se utilizan para ofrecer servicios a los usuarios. Entre éstos podemos mencionar tanto los 'tradicionales', que existen desde que se creó el TCP/IP:

- Terminal virtual (TelNet).
- Transferencia de ficheros (FTP).
- Correo electrónico (SMTP).
- Servidor de nombres (DNS).

Así como los mas recientes:

- Servicio de news (NNTP).
- Web (HTTP), el Gopher, etc.

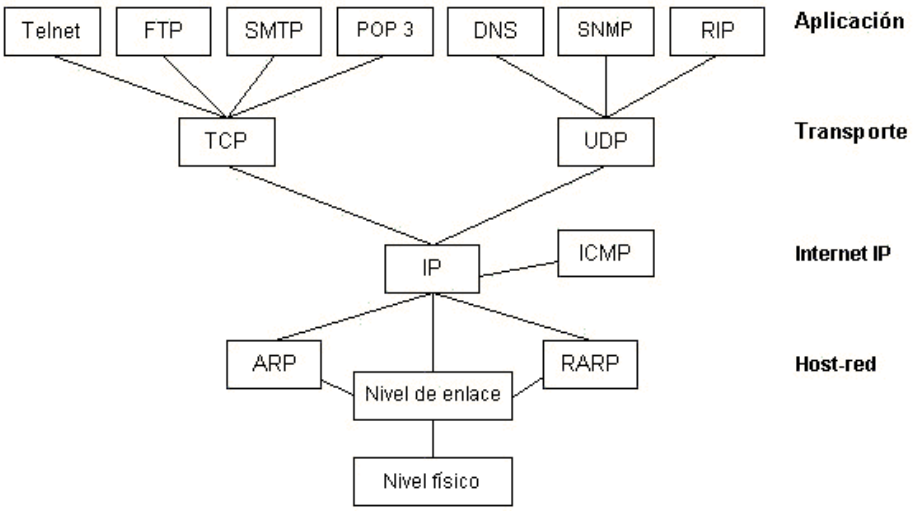


Figura 1. Arquitectura de protocolos TCP/IP.

1.3. Dispositivos de interconexión de redes

1.3.1 Introducción

Los dispositivos de interconexión de redes han permitido el crecimiento de redes LAN de modo que hoy en día, la mayor parte de redes de comunicación de datos en universidades, industrias y empresas están constituidas por conjuntos redes de área local interconectadas, y a su vez el conjunto de todas ellas forman la red mundial conocida como Internet. Existen diversos dispositivos de interconexión, cada uno de ellos con una función específica. Así, se dispone de dispositivos para interconectar redes con distinta arquitectura o con una misma arquitectura, a un determinado nivel dentro de dicha arquitectura. Entre los dispositivos de interconexión de redes, conviene destacar los que a continuación se detallan.

1.3.2 Repetidor (nivel físico de OSI)

A medida que las señales eléctricas se transmiten por un cable tienden a degradarse proporcionalmente a la longitud del cable. Este fenómeno se conoce como atenuación. Un repetidor es un dispositivo sencillo que se instala para amplificar las señales del cable, de forma que se pueda extender la longitud de la red. El repetidor normalmente no modifica la señal, sólo la amplifica para poder retransmitirla por el segmento de cable extendido (figura 2).

Un repetidor básicamente es un dispositivo "no inteligente" con las siguientes características:

- Regenera las señales de la red para que lleguen mas lejos.
- Los repetidores funcionan sobre el nivel más bajo de la jerarquía de protocolos.
- Los segmentos conectados a un repetidor forman parte de la misma red.

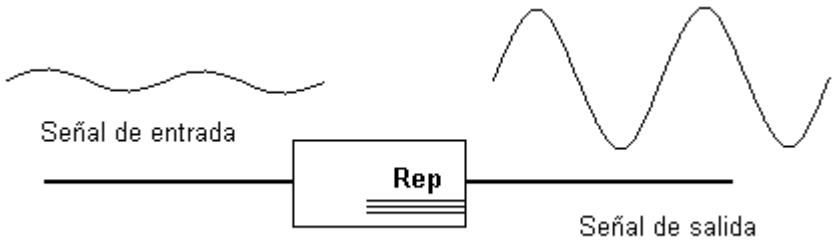


Figura 2. Repetidor. Este dispositivo de interconexión regenera la señal atenuada.

1.3.3 Hub (nivel físico de OSI)

Dispositivo que interconecta hosts dentro de una red (figura 3). Es el dispositivo de interconexión más simple que existe. Sus principales características son:

- Se trata de un equipo con muchas conexiones donde se centraliza todo el cableado de una red, es decir, un dispositivo con muchos puertos de entrada y salida.
- Suele regenerar la señal.

Físicamente parece una topología en estrella, pero internamente es un bus.

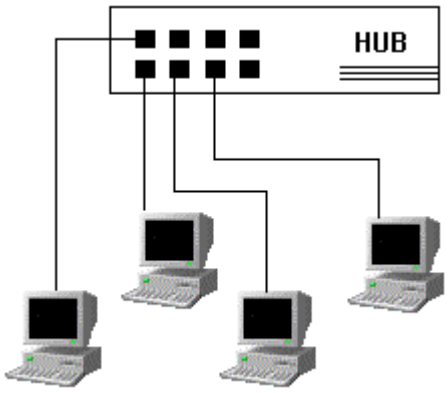


Figura 3. Concentrador de cableado empleado en las redes Ethernet 10baseT, 100BaseT.

1.3.4 Bridge (nivel de enlace de OSI)

Un puente añade un nivel de inteligencia a una conexión entre redes. Trabaja a nivel de enlace. Es especialmente útil para:

- Ampliar la extensión de la red, o el número de nodos que la constituyen.
- Reducir la carga en una red con mucho tráfico, uniendo segmentos diferentes de una misma red.
- Unir redes con la misma topología y método de acceso al medio.

1.3.5 Switch (nivel de enlace de OSI)

Un switch es básicamente un puente con muchos puertos. Es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red.

- Es usualmente más usado para enviar información dentro de una red que para enviarla de una red a otra.
- Al igual que los puentes, realiza funciones de filtrado.
- Permite transmisiones simultáneas entre pares de estaciones.

1.3.6 Router (nivel de red de OSI)

Trabajan a nivel de red, con lo cual ofrecen la posibilidad de intercambiar tramas entre redes muy distintas. Se emplean fundamentalmente para constituir redes de área extensa (figura 4).

Los routers realizan la función de encaminamiento: son capaces de elegir la ruta más eficiente que debe seguir un paquete en el momento de recibirlo, mediante la consulta de tablas de dirección de red. La forma que tienen de funcionar es la siguiente:

- Cuando llega un paquete al router, éste examina la dirección destino y lo envía hacia allí a través de una ruta predeterminada.
- Si la dirección destino pertenece a una de las redes que el router interconecta, entonces envía el paquete directamente a ella; en otro caso enviará el paquete al router más próximo a la dirección destino.
- Para saber el camino por el que el router debe enviar un paquete recibido, examina sus propias tablas de encaminamiento.

Cada segmento de red conectado a través de un router tiene una dirección de red diferente.

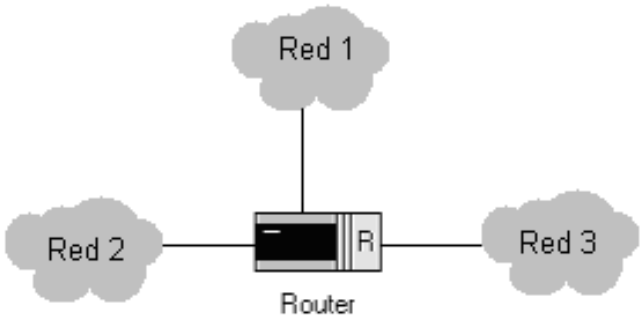


Figura 4. Interconexión de redes a través de un router.

1.4. Tecnología Ethernet

Ethernet es el nombre que se le ha dado a una popular tecnología LAN de conmutación de paquetes inventada por Xerox PARC a principios de los años setenta. Posteriormente fue normalizada por el IEEE, denominándose IEEE 802.3. Sin lugar a dudas Ethernet es la tecnología LAN más popular.

1.4.1 Descripción general

La red Ethernet es una tecnología de BUS (por tanto, difusión) de 10 Mbps, 100 Mbps, 1000Mbps o 10Gbps, basada en la filosofía de "entrega con el menor esfuerzo". Es un Bus, todas las estaciones comparten el mismo canal de comunicación y es de difusión porque todos los equipos reciben todas las transmisiones. El esquema de acceso a Ethernet es conocido como *Carrier Sense Múltiple Acces with Collision Detect* (CSMA/CD), o lo que es lo mismo, acceso a la red utilizando el acceso múltiple de percepción de portadora con detección de colisión. Esta estrategia de acceso al medio consiste, básicamente, en que cada componente de la red o nodo escucha antes de transmitir los paquetes de información. De hecho, si dos nodos transmiten al mismo tiempo se produce una colisión. Al captar una colisión, la computadora interrumpe la transmisión y espera a que la línea quede libre. Uno de los ordenadores pasa entonces a transmitir los datos, logrando el control de la línea y completando la transmisión de los datos. Actualmente, con el uso de conmutadores se reduce en gran medida las colisiones y aumenta el rendimiento de la red (Ethernet conmutada).

Resumiendo, Ethernet es una tecnología pasiva de espera y de escucha. Las colisiones entre paquetes suelen ser frecuentes en la red y los hosts tienen que disputarse el tiempo de transmisión.

El diseño original de Ethernet utilizaba cable coaxial para la conexión de todos los dispositivos. Los avances en la tecnología han hecho posible construir redes Ethernet que no precisen el blindaje eléctrico de un cable coaxial. Llamada *twister pair Ethernet* (Ethernet de par trenzado), esta tecnología permite que un ordenador acceda a Ethernet a través de pares de cables de cobre (similar a los empleados en tecnología telefónica). Técnicamente esta variación se conoce como Ethernet 10Base-T (10 MBps, codificación en banda base y par trenzado).

En la figura 5 se observa el hardware de Ethernet empleado en los hosts: una tarjeta de red de bajo coste frente al mayor coste presente en tecnologías como token ring. La configuración de la tarjeta de red en cada PC posibilita su correcto funcionamiento en red. En la figura 6 se muestra un ejemplo de configuración para una máquina con sistema operativo MS Windows 2000.

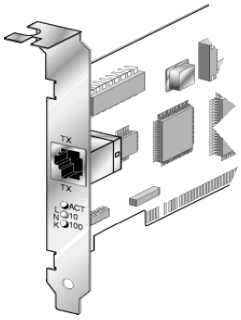


Figura 5. Tarjeta de red Ethernet 100baseT.

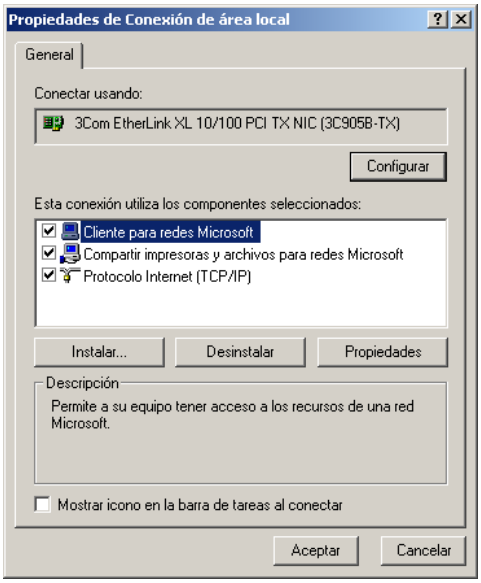


Figura 6: Configuración de Ethernet en un PC.

La ventaja de usar cables de par trenzado (figura 7) radica en que reducen mucho los costes de instalación y protegen a los ordenadores de los riesgos de desconexión del coaxial en cualquier punto de la red, ya que se emplean cables individuales de pares trenzados desde cada computadora hasta el concentrador (hub).

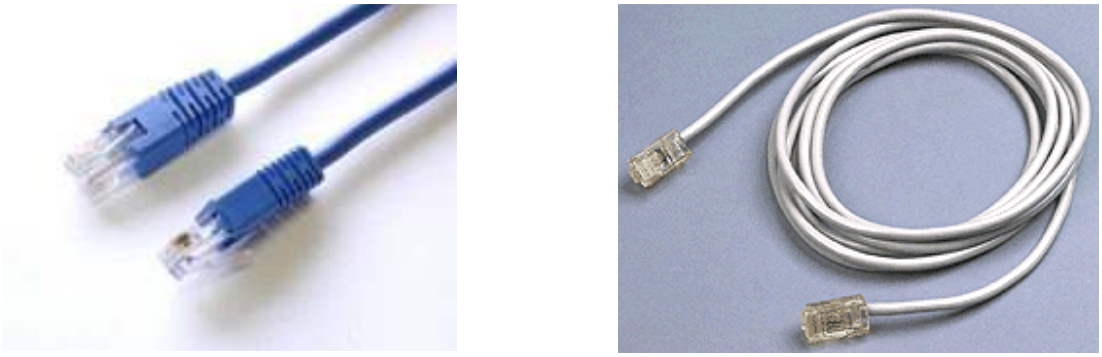


Figura 7. Cable de par trenzado con terminación RJ45.

1.4.2 Trama Ethernet

El formato de datos en Ethernet se denomina trama. Ethernet emplea varios tipos de trama, lo que puede ocasionar problemas en la red si no se han configurado correctamente todos los nodos con la misma tecnología. Entre diferentes tipos de tramas Ethernet: IEEE 802.3, Ethernet SNAP y Ethernet II, esta última es la empleada para protocolos TCP/IP y es la trama Ethernet que será estudiada en el laboratorio de prácticas (figura 8).

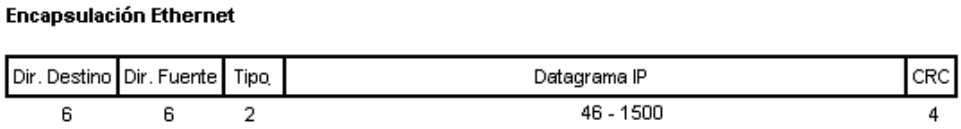


Figura 8. Formato de la trama Ethernet II, empleada en el laboratorio.

La trama posee longitud variable, pero no es menor de 64 bytes ni mayor a 1518 bytes (incluyendo encabezado, datos y CRC). Como en todas las redes de conmutación de paquetes, cada trama Ethernet contiene un campo con direccionamiento fuente y destino. El campo 'Tipo' de la trama contiene un entero de 16 bits que identifica el tipo de trama. Las tramas de Ethernet II tienen en tipo el valor de 2048. El final de la trama contiene una detección de errores 'CRC' (verificación por redundancia cíclica).

1.4.2.1 El tamaño máximo de trama (MTU)

Como puede observarse en la figura 8, existe un límite en el tamaño de la trama para Ethernet. Los tamaños máximos para datos (datagrama IP) son de 1500 bytes. Esta característica de la capa de enlace se conoce como MTU.

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. Este parámetro 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.

1.4.2.2 Las direcciones MAC

Cuando un datagrama es enviado hacia una estación o un servidor determinado se necesita conocer la dirección física de la tarjeta o hardware de red Ethernet del equipo de destino. Según la bibliografía consultada, esta dirección puede aparecer también como dirección Ethernet, dirección MAC, etc.

Las direcciones MAC son una combinación de 48 bits, de forma que los 3 primeros bytes de la izquierda identifican al fabricante de la tarjeta, y los 3 siguientes aseguran un identificador único para cada tarjeta del fabricante. De aquí se deduce que utilizando los comandos adecuados, es fácil conocer la procedencia de cada tarjeta conectada a la red. La dirección MAC es única e irrepetible (figura 9).

Toda tarjeta de red, debe ser capaz de responder a 2 direcciones: La suya propia, y la dirección de **Broadcast**. Esta última se caracteriza por tener los 48 bits a 1, con lo cual queda como FF:FF:FF: FF:FF:FF.

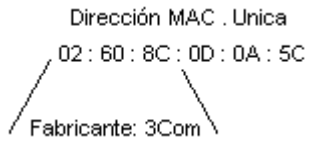


Figura 9. Numeración MAC de una tarjeta para el fabricante 3COM.

Una trama Ethernet enviada a la dirección de Broadcast será atendida por todas las estaciones conectadas al mismo segmento. Esta particularidad es utilizada ampliamente por el protocolo ARP que se comentará a continuación.

1.5. El protocolo ARP

1.5.1 Introducción

Puesto que un enlace de datos como Ethernet o Token Ring posee su propio esquema de direccionamiento (a menudo sobre 48 Bits), cada protocolo de red deberá de amoldarse a él. Una red como Ethernet puede ser usada de forma simultánea por diferentes capas de red, como los protocolos OSI, IP, IPX de Netware (Novell), IDP de XNS (Xerox), DDP de Appletalk (Apple)...

En el seno de una Red Local, cuando una trama Ethernet se envía de una máquina a otra, es la dirección de 48 Bits (dirección MAC) quien determina a qué interfaz físico va destinada. El *driver* de la tarjeta de red nunca se preocupa de la dirección IP de destino contenido dentro del datagrama IP.

La especificación ARP (*Address Resolution Protocol*), contenida en la RFC 826 es quien se encargará de efectuar una correspondencia dinámica entre la dirección MAC y la dirección de destino IP que se especifica en niveles superiores.

ARP es un protocolo de nivel de enlace que se apoya sobre Ethernet para poder circular por el medio. Posee, por tanto, un nivel de encapsulación, tal y como se observa en la figura 10.

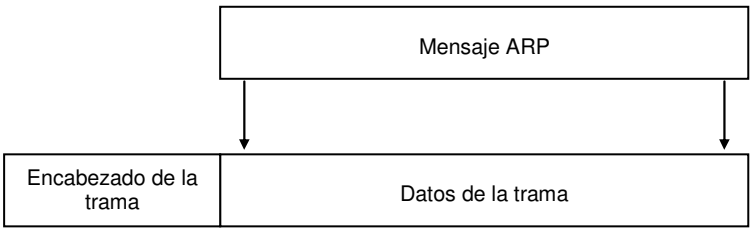


Figura 10. Encapsulación del mensaje ARP en una trama de Ethernet.

Por ejemplo, cada vez que se ejecuta la orden:

c:\> telnet 10.3.7.0

en una maquina 'A' hacia una máquina destino 10.3.7.0 'B', se desencadena la siguiente serie de acontecimientos :

- El cliente telnet pide a su TCP utilizar esta dirección para establecer una conexión.
- TCP envía una petición de conexión a la máquina remota emitiendo un datagrama IP a su dirección IP.

- ARP envía una trama especial Ethernet, de tamaño muy corto, llamada 'petición ARP o ARP Request' a cada máquina de la Red Local. Este proceso se conoce como 'Broadcast'. La petición ARP contiene la dirección IP de la máquina destino, y equivaldría a formular la pregunta:
    - "Si Usted es propietario de esta dirección IP, por favor respóndame devolviendo su dirección MAC". (figura 11).

- La capa ARP de la máquina destino recibe el 'Broadcast' (como el resto de máquinas de la red), verifica que el solicitante pide su dirección IP y emite una 'respuesta ARP'. Esta respuesta contiene la dirección IP y la dirección MAC correspondiente. (figura 12).
- La respuesta ARP es recibida por la máquina y el datagrama IP que produjo la petición ARP puede ser emitido al destino B (‘Arp Reply’).

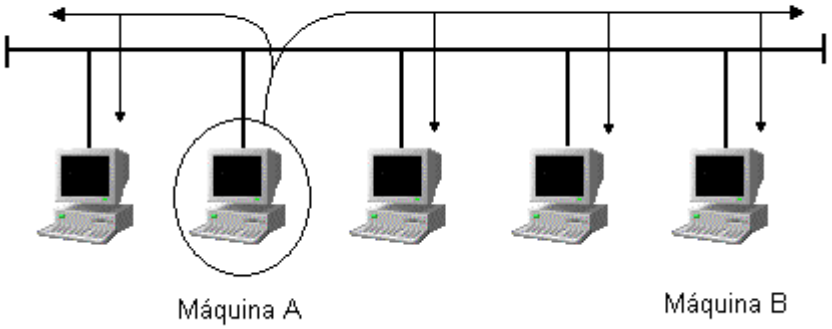


Figura 11. Petición ARP desde una máquina ‘A’ al resto de máquinas del segmento de red, (Broadcast).

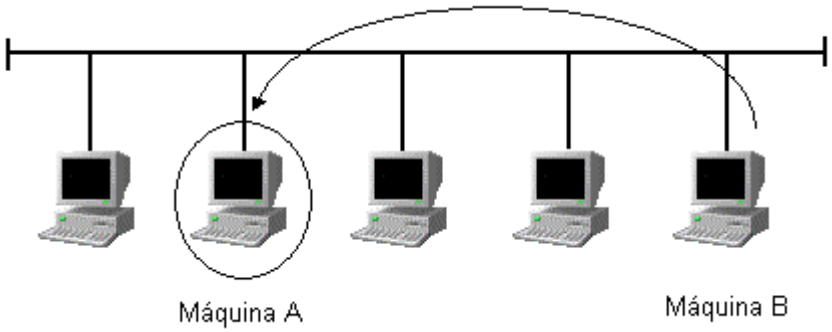


Figura 12. Respuesta ARP desde una máquina ‘B’ a la máquina origen ‘A’.

Más adelante en el apartado 1.5.4 se puede ver un análisis del procedimiento y las tramas y paquetes generados con mayor nivel de detalle.

1.5.2 La memoria caché de ARP

El mantenimiento de una memoria caché ARP en cada máquina es esencial para el correcto funcionamiento de ARP. Esto permite las correspondencias entre las direcciones IP y las físicas (MAC). El plazo normal de expiración de una entrada en la tabla ARP depende del sistema operativo de la máquina, normalmente es de 20 segundos después de su creación.

A modo de ejemplo práctico vamos a realizar un 'telnet 10.3.7.0' sobre nuestro servidor. A continuación ejecutar el siguiente comando:

C:\>WINDOWS> arp -a

El resultado dependerá de en qué condiciones se encuentre la red. Sería muy probable obtener una serie de líneas similares a las siguientes:

172.20.43.231 00:D0:BA:E0:6A:3D
10.3.7.0 00:40:33:52:71:88

El comando 'arp' posee una serie de opciones que permiten efectuar distintos ajustes en la memoria caché de ARP.

1.5.3 ARP - proxy

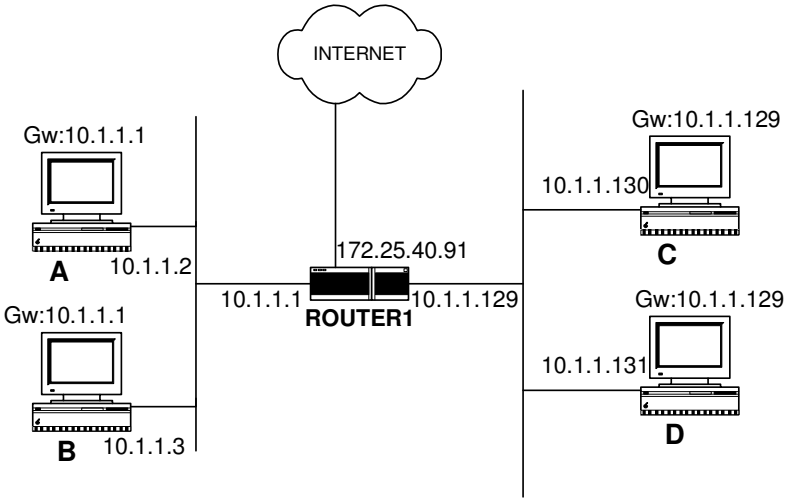
El ARP-Proxy o proxy-ARP es un protocolo de resolución de direcciones proxy. Es una variación del protocolo ARP en el cual un dispositivo intermedio (por ejemplo, un router) envía una respuesta ARP en nombre de un nodo extremo al host solicitante. ARP proxy puede disminuir el uso del ancho de banda en enlaces WAN de baja velocidad.

Se conoce también como ARP delegado: un encaminador puede contestar una solicitud ARP como si fuera la máquina destino, cuando esa máquina destino es alcanzable a través de dicho encaminador.

1.5.4 Ejemplo de Intercambio de paquetes ARP.

Para ilustrar el intercambio de paquetes ARP entre redes de difusión cuando estas están unidas por enlaces punto a punto, se va a emplear el ejemplo de la Figura 13. Supóngase que se dispone de un conjunto de máquinas (A y B) unidas todas ellas mediante una topología en bus y por otro lado otro conjunto de máquinas (C y D), también unidas entre sí mediante otra topología en bus. A su vez, ambas redes se unen entre sí mediante un dispositivo Router. El Router, en tal caso, determina dos segmentos de red distintos.

Si por ejemplo se desease que la máquina B enviase algún tipo de mensaje a la máquina D que está situada en otro segmento de red, B necesitaría conocer la dirección MAC del puerto del Router1 correspondiente a la dirección IP 10.1.1.1. Esto es así, porque éste es el puerto del Router (con esa dirección IP) que está configurado como puerta de enlace de la máquina B. Y por lo tanto, es el encaminador que conoce como llegar a la máquina destino D.



Dirección IP	Dirección MAC
10.1.2.2	MAC A
10.1.1.3	MAC B
10.1.1.1	MAC R1a
10.1.1.129	MAC R1b
10.1.1.130	MAC C
10.1.1.131	MAC D

Figura 13. Topología de red para el intercambio de paquetes entre 2 segmentos de red.

De modo, que siempre que B quiera enviar algún tipo de mensaje a D y éste tenga que ser encapsulado en tramas, se requerirá como dirección de destino la MAC del Router1 correspondiente a la Ip 10.1.1.1. Así, el mensaje que va destinado a D y que irá encapsulado en una trama Ethernet dispondrá, de acuerdo a la Figura 8, del formato:

Cabecera Ethernet		*Cabecera IP*	
MAC ORIGEN	*MAC DESTINO*	*IP ORIGEN*	*IP DESTINO*
MAC B	*MAC ROUTER1a*	*10.1.1.3*	*10.1.1.131*

Pero, para que ese mensaje pueda encapsularse de esa manera, será necesario que B conozca la dirección MAC de destino, es decir conozca la dirección MAC del Router1 que corresponde a la Ip 10.1.1.1. Por lo tanto, el primer paso que ejecuta la máquina B es comprobar si en su tabla ARP dispone de esa información. En caso afirmativo, la extrae y construye la trama Ethernet de datos que se ha mostrado anteriormente. Sin embargo, en caso negativo, es necesario que alguien proporcione esa información a la máquina B, para que esta pueda construir la trama Ethernet de datos que encapsula el mensaje que se quiere enviar.

Cabecera Ethernet		*Cabecera IP*	
MAC ORIGEN	*MAC DESTINO*	*IP ORIGEN*	*IP DESTINO*
MAC B	*¿?*	*10.1.1.3*	*10.1.1.131*

Es en este momento, dónde comienza la ejecución del protocolo ARP. Protocolo que se emplea para averiguar ese dato que le falta a B para poder envíar la trama de datos Ethernet a D.

Para ello, en primer lugar, y tras comprobar B que la dirección Ip de la máquina D no pertenece a su segmento de datos, accede a su tabla ARP en busca de la MAC del dispositivo encaminador que le proporcione salida hasta D. Posteriormente, y tras comprobar que tampoco dispone de esa información, no conoce la MAC del Router1 correspondiente a la 10.1.1.1, entonces genera el siguiente paquete ARP:

ARP 'Request'

Cabecera Ethernet		*Paquete ARP*
MAC ORIGEN	*MAC DESTINO*	*DATOS (información)*
MAC B	*BROADCAST*	*¿Quién tiene la IP10.1.1.1?*

Con este paquete, la máquina B pretende averiguar la dirección MAC correspondiente a la dirección Ip 10.1.1.1. Y lo hace, enviando un paquete ARP, encapsulado en una trama Ethernet, preguntando quien tiene la dirección Ip 10.1.1.1. y cuya dirección MAC de destino, es la de todas las máquinas que están conectadas a la misma red que B.

A continuación, si alguna de las máquinas conoce la dirección MAC correspondiente a la dirección por la que se pregunta, (Ip 10.1.1.1), contestará al paquete ARP con un segundo paquete ARP, denominado paquete 'Arp Reply'. En dicho paquete se proporciona la MAC del interfaz correspondiente a la Ip 10.1.1.1. Es obvio, que la máquina que conoce la dirección MAC de 10.1.1.1 es la máquina a la que pertenece ese interfaz. Por lo tanto, el paquete generado tendrá el formato:

ARP 'Reply'

Cabecera Ethernet		*Paquete ARP*
MAC ORIGEN	*MAC DESTINO*	*DATOS (información)*
MAC ROUTER1	*MAC B*	*IP: 10.1.1.1<->MAC: MAC Router1*

Una vez, la máquina B recibe el paquete 'Arp Reply' almacena la MAC de la Ip: 10.1.1.1 en su tabla ARP, y a continuación construye la trama Ethernet con los datos del mensaje:

Cabecera Ethernet		*Cabecera IP*	
MAC ORIGEN	*MAC DESTINO*	*IP ORIGEN*	*IP DESTINO*
MAC B	*MAC ROUTER1a*	*10.1.1.3*	*10.1.1.131*

Dicha trama de datos, llegará hasta el Router1 que a su vez tendrá que encaminarla hasta hacerla llegar hasta su destino final, la máquina D con dirección Ip: 10.1.1.131. De nuevo, en este momento, se vuelve a repetir el mismo proceso que se ha realizado con anterioridad. Es decir, para enviar la trama de datos del mensaje a la nueva red es necesario que el Router1 conozca la dirección MAC de la máquina D.

De ahí se deduce que el primer paso que ejecuta la máquina Router1 es comprobar si en su tabla ARP dispone de esa información. En caso afirmativo, la extraería y construiría la trama Ethernet de datos que se muestra a continuación:

Cabecera Ethernet		*Cabecera IP*	
MAC ORIGEN	*MAC DESTINO*	*IP ORIGEN*	*IP DESTINO*
MAC Router1b	*MAC D*	*10.1.1.3*	*10.1.1.131*

Por el contrario, en caso negativo, es necesario que alguien proporcione esa información a la máquina Router1, para que esta pueda construir la trama Ethernet de datos que encapsula el mensaje que se quiere enviar a D.

Cabecera Ethernet		*Cabecera IP*	
MAC ORIGEN	*MAC DESTINO*	*IP ORIGEN*	*IP DESTINO*
MAC Router1b	*¿?*	*10.1.1.3*	*10.1.1.131*

Nuevamente, debe ejecutarse el protocolo ARP. Protocolo que se emplea para averiguar ese dato que le falta a Router1 para poder envíar la trama de datos Ethernet a D.

Para ello, la máquina Router1 comprueba que la dirección Ip: 10.1.1.131 de la máquina D pertenece a uno de sus segmentos de red y accede a su tabla ARP en busca de la MAC de la máquina D. Posteriormente, y tras comprobar que tampoco dispone de esa información, no conoce la MAC de D correspondiente a la 10.1.1.131, entonces genera el siguiente paquete ARP:

ARP 'Request'

Cabecera Ethernet		*Paquete ARP*
MAC ORIGEN	*MAC DESTINO*	*DATOS (información)*
MAC Router1b	*BROADCAST*	*¿Quién tiene la IP10.1.1.131?*

Con este paquete, la máquina Router1 pretende averiguar la dirección MAC correspondiente a la dirección Ip 10.1.1.131. Y lo hace, enviando un paquete ARP, encapsulado en una trama Ethernet, preguntando quien tiene la dirección Ip 10.1.1.131. y cuya dirección MAC de destino, es la de todas las máquinas que están conectadas a la misma red que la interfaz del Router1 10.1.1.129.

A continuación, si alguna de las máquinas conoce la dirección MAC correspondiente a la dirección por la que se pregunta, (Ip 10.1.1.131), contestará al paquete ARP con un segundo paquete ARP, denominado paquete 'Arp Reply'. En dicho paquete se proporciona la MAC del interfaz correspondiente a la Ip 10.1.1.131. Es obvio, que la máquina que conoce la dirección MAC de 10.1.1.131 es la máquina a la que pertenece ese interfaz. Por lo tanto, el paquete generado tendrá el formato:

ARP 'Reply'

Cabecera Ethernet		*Paquete ARP*
MAC ORIGEN	*MAC DESTINO*	*DATOS (información)*
MAC D	*MAC Router1b*	*IP: 10.1.1.131<->MAC: MAC D*

Una vez, la máquina Router1 recibe el paquete 'Arp Reply' almacena la MAC de la Ip: 10.1.1.131 en su tabla ARP, y a continuación construye la trama Ethernet con los datos del mensaje:

Cabecera Ethernet		*Cabecera IP*	
MAC ORIGEN	*MAC DESTINO*	*IP ORIGEN*	*IP DESTINO*
MAC Router1b	*MAC D*	*10.1.1.3*	*10.1.1.131*

1.6. El datagrama de Internet

La analogía entre una red física y una red compuesta de varias redes (TCP/IP) es alta. En una red física como Ethernet la unidad de transferencia es una trama que contiene un encabezado y los datos, en donde el encabezado posee información de direccionamiento hardware origen y destino. La red de redes (Internet) denomina a su unidad de datos básica datagrama IP. Como una trama común de red física, un datagrama se divide en áreas de encabezado y datos. También, como en una trama, el encabezado del datagrama contiene la dirección de la fuente y destino del mensaje. Este tipo de dirección se conoce como dirección IP, es una dirección software, frente a la hardware MAC impresa en el dispositivo físico de la red.

El datagrama IP viaja por la red encapsulado en la trama física (figura 14):

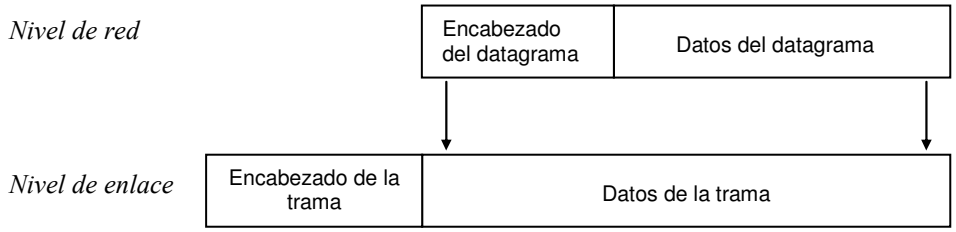


Figura 14. Encapsulación del datagrama IP en una trama Ethernet.

La cabecera de un datagrama IP es mucho más compleja que el encabezamiento de una trama física, es decir, posee muchos más campos de control.

El formato del datagrama IP queda representado en la figura 15. El tamaño de la cabecera es de 20 bytes, a no ser que presente opciones.

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.

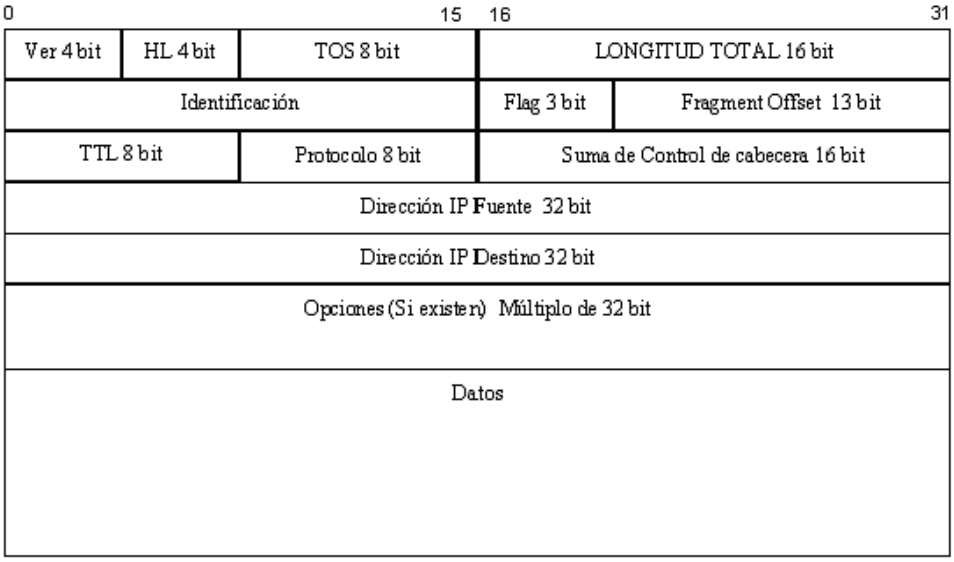


Figura 15. Formato del datagrama IP.

La versión en curso actual de IP es la 4 también conocida como IPv4 aunque ya ha comenzado a ser operativa la IPv6. El campo **ver** sobre 4 bits transporta esta información.

El campo **HL** indica el número de grupos de cuatro bytes que componen la cabecera, incluyendo las opciones eventuales. Puesto que su tamaño es de 4 bits, tendremos que la longitud máxima de la cabecera IP es de 60 bytes. Este campo posee habitualmente el valor 5 (cuando no existen opciones) correspondiente a 20 bytes.

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. 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 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 **fragment offset** contiene el índice del fragmento a partir del datagrama original. Además, el nuevo campo **longitud total** de cada fragmento es actualizado a su nuevo valor.

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 (Problemas con los protocolos de encaminamiento, p.ej.) 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,etc.) 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. Sin embargo, otros protocolos como TCP, UDP, ICMP utilizan códigos de redundancia cíclica (CRC) basados en algoritmos más sofisticados. El motivo es claro. Un router debe procesar grandes cantidades de paquetes por unidad de tiempo. Generalmente, el único valor que 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.

1.7. Direccionamiento IP

1.7.1 Introducción

Las direcciones MAC permiten identificar máquinas dentro de un mismo segmento, pero ello no es suficiente para satisfacer las necesidades de comunicación dentro de una red que puede estar compuesta por miles de ellos (Internet). Se necesita, pues, un protocolo de red que permita hacer llegar a su destino una unidad de información, datagrama IP en nuestro caso, que a lo largo de su recorrido pueda atravesar redes con protocolos de enlace muy dispares (Ethernet, Token Ring, Token Bus, líneas punto a punto con SLIP, PPP, HDLC y un sinfín de combinaciones a través de otras redes como RDSI o Frame Relay).

Las direcciones IP tienen una longitud de 32 bits, organizadas en 4 grupos de 8 bits cada uno. Se dividen fundamentalmente en dos partes: La porción de la red y la porción de la máquina (figura 16).

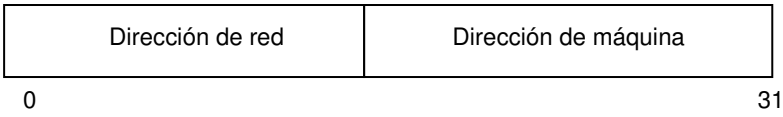


Figura 16. Formato de direcciones IP. Parte de red y parte de máquina.

La porción de red identifica generalmente a un grupo de máquinas que comparten el mismo protocolo de enlace dentro de un segmento de red. El campo de máquina hace referencia a todas aquellas estaciones conectadas a la misma red. El tamaño de cada parte depende del valor de los bits de mayor peso, tal y como se muestra en la figura 17:

Figura 17. Clase de direcciones IP. En uso actualmente la A, B y C.

De aquí surge una clasificación en 5 tipos de redes en función del contenido de cada uno de los campos de dirección, tal y como se ilustró en la figura anterior, si bien, en la práctica sólo las clases A, B y C son las empleadas. La clase E se ha utilizado en años anteriores para propósitos experimentales, y fue diseñada en su momento para futuras ampliaciones, antes de la aparición de IP v6.

Dentro del direccionamiento IP, al igual que en las direcciones MAC, existe una dirección de Broadcast definida con todos los bits correspondientes a la porción de máquina a 1. Es decir, la dirección 134.215.255.255 sería una dirección de Broadcast perteneciente a la red 134.215. A diferencia de MAC, dentro de IP las redes también poseen direcciones que se obtienen con todos los bits de la porción de

máquina a 0. Continuando con el ejemplo anterior, la dirección 134.215.0.0 correspondería a la dirección IP de la red 134.215.

Cada interfaz IP situado dentro de una misma máquina, tiene una dirección propia IP. Significa que si tuviéramos una tarjeta de red en el servidor, y una conexión SLIP asociada a uno de sus puertos serie, éste presentaría dos direcciones IP. Podríamos acceder a él a través de cualquiera de ellas siempre que sus tablas de enrutamiento lo permitiesen.

1.7.2 La máscara de subred

Todo interface IP, necesita como mínimo dos parámetros: La dirección IP y su máscara asociada. La máscara se compone de 32 bits. Éstos se superponen bit a bit a la dirección IP de tal forma que aquellos cuyo valor es 1, indican que la porción correspondiente a la dirección es la parte de red. El valor 0 señala la parte de máquina. Esta información es muy importante, pues un datagrama con destino IP cuya porción de red (definida por la máscara) no coincida con la que presenta la fuente del mensaje será enviado a la máquina conocida como puerta de enlace. Lógicamente, existe siempre una máscara por defecto asociada a la dirección IP, en función de la clase. Por ejemplo, la dirección 10.2.45.1 pertenece a la red 10.0.0.0 de clase A. Su máscara por defecto deberá ser 255.0.0.0:

11111111.00000000.00000000.00000000 en notación binaria.

En la figura 18 se muestra una ventana de dialogo de TCP/IP de un PC en donde se identifica la dirección IP asignada al PC, la máscara de subred, así como la puerta de enlace predeterminada, la máquina por la que saldrán los datagramas al exterior.

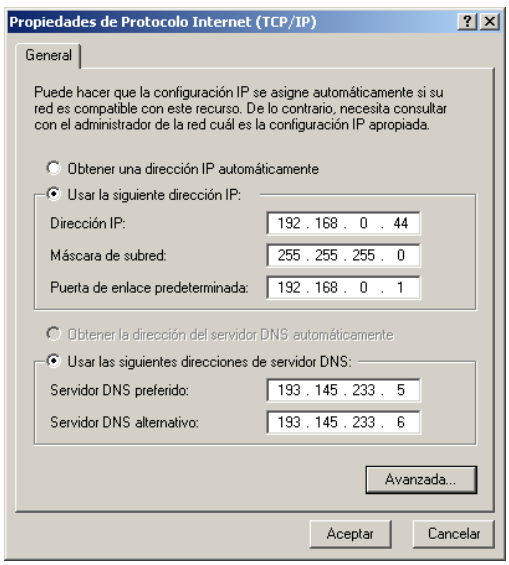


Figura 18. Configuración de direcciones IP, máscara y puerta de enlace un PC.

Cuando se dispone de un único segmento de red resulta muy sencillo gestionar las direcciones IP de las máquinas. Por ejemplo, para una red de clase A, todas las máquinas conectadas llevarían la máscara 255.0.0.0 y se numerarían 10.2.45.1, 10.7.23.124, 10.0.12.253 etc..., manteniendo la porción de la red siempre igual a 10. Se dispondría por tanto de 2^{24} máquinas menos 2: La dirección de Broadcast 10.255.255.255 y la dirección de la red 10.0.0.0 no válidas para numerar máquinas. Pero si quisiéramos

crear subredes, por ejemplo 3 (figura 19), dentro de esta red necesitaríamos ampliar la máscara como mínimo 2 bits más para tener así 4 subredes, una más de las necesarias. De este modo quedaría una máscara de 11111111.11000000.00000000.00000000 o **255.192.0.0**. Dispondríamos en este caso de las siguientes subredes con la siguiente numeración:

- 00001010.00000000.00000000.00000000 ó **10.0.0.0**
- 00001010.01000000.00000000.00000000 ó **10.64.0.0**
- 00001010.10000000.00000000.00000000 ó **10.128.0.0**
- 00001010.11000000.00000000.00000000 ó **10.192.0.0**

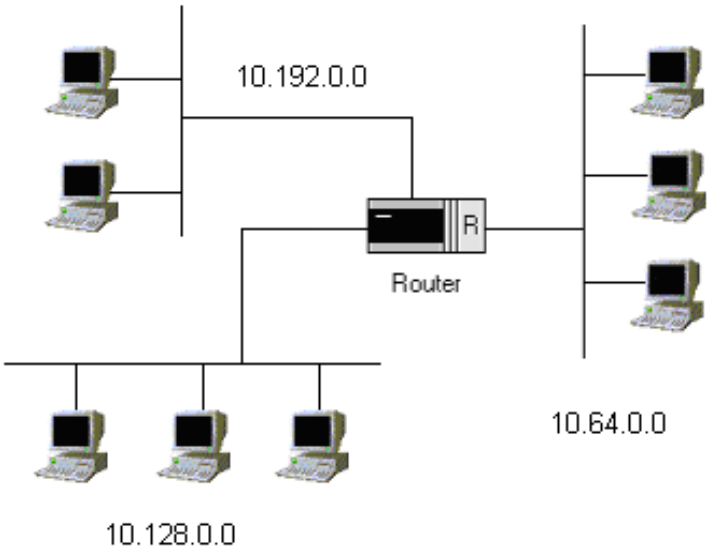


Figura 19. División de una red de clase A en tres subredes con máscara asociada 255.192.0.0.

El número de máquinas por cada una de estas subredes sería 2^{22} menos 2. Por tanto, cada vez que se amplía la máscara, se pierden 2 direcciones IP en cada subred (Broadcast y red).

Resumiendo, se ha considerado que una dirección IP está compuesta de dos identificadores, uno para la red y otro para la máquina. El ámbito de cada uno de ellos depende de la clase a la que pertenece esa dirección o de la máscara de red asociada.

1.7.3 Direcciones IP públicas y privadas

Una consideración a tener en cuenta por parte del administrador de red de una organización es elegir la clase de dirección IP a instalar y si ésta será pública o privada, es decir, si las direcciones de las máquinas podrán ser accesibles desde el exterior o si, por el contrario, serán direcciones locales a la red LAN gestionada por el administrador.

Para las clases de direcciones A, B y C se definen unos rangos de direcciones privadas para redes locales que, evidentemente, no podrán ser empleados para direccionamiento público de máquinas. Los rangos de direcciones son los siguientes:

Clase **A**: 10.0.0.0

Clase **B**: 171.16.0.0, 171.17.0.0, ..., 171.31.0.0 (*16 redes*)

Clase **C**: 192.168.0.0, 192.168.1.0, ..., 192.168.255.0 (*256 redes*)

1.7.4 Proceso de elección de direcciones IP

En ocasiones, se hace necesario construir un conjunto de subredes a partir de un determinado rango de direcciones IP y asignar direcciones nuevas a cada uno de los dispositivos o máquinas que se interconectan en dicha topología de red. A continuación, mediante un ejemplo se va tratar de ilustrar de forma detallada este proceso.

Supóngase, que el administrador del sistema informático de una empresa nos proporciona una dirección IP y una máscara asociada a esa dirección IP. Por ejemplo, IP: 128.32.64.0 con una máscara asociada de 255.255.254.0. Y se nos pide que a partir del rango de IPs que se pueden configurar en esa red con esa IP y esa máscara, construyamos una red formada por 4 subredes más pequeñas unidas por un dispositivo de tipo Router e identifiquemos el rango de direcciones IP que pueden ser empleados en cada subred construida.

Como curiosidad, convendría determinar cuál es el rango de máquinas que tiene la red inicial antes de aplicar variaciones de configuración en ésta. Así, observando la máscara se puede comprobar que se tienen 9 bits a valor 0, y por lo tanto 9 bits que permiten direccionar máquinas. Si además se sabe que cada bit puede adoptar dos valores '0' o '1', entonces se tienen 2^9-2 posibles direcciones de máquina a configurar en esa red.

Como primer paso, comentar que para que a partir de una dirección de red se puedan construir 4 subredes, será necesario utilizar bits para identificar subredes que antes se empleaban para direccionar máquinas. Así, atendiendo a la máscara 255.255.254.0., se hace necesario reservar **2** bits para subred que antes eran para red para formar 4 subredes, porque $\log_2 4 =$**2**. El proceso aplicado es el siguiente:

La red 128.32.64.0 tiene una máscara asociada 255.255.254.0.

Si se pone la máscara en binario tenemos:

11111111.11111111.11111110.00000000

Ampliar 2 bits la máscara supone, que la nueva máscara en formato binario será:

11111111.11111111.11111111.100000000

Transformando la máscara de binario a decimal, se obtiene que la nueva máscara una vez ampliada en dos bits es 255.255.255.128. Dicha máscara de red será la nueva máscara para cada una de las 4 subredes que se van a direccionar.

A continuación, y para construir las subredes, partimos de la dirección de red inicial 128.32.64.0. Se transforma ésta a binario y se toman los bits que ocupan la misma posición que los ampliados en la máscara de red, como sigue:

La dirección de red en binario es:

10000000.00100000.01000000.00000000

Los bits de red que ocupan la misma posición que los ampliados en la máscara de red son:

10000000.00100000.0100000X.X0000000

Se construyen todas las combinaciones posibles de código con esos dos bits.

10000000.00100000.01000000.00000000
10000000.00100000.01000000.10000000
10000000.00100000.01000001.00000000
10000000.00100000.01000001.10000000

Y si se transforman a decimal, se tiene:

Subred1: 128.32.64.0
Subred2: 128.32.64.128
Subred3: 128.32.65.0
Subred4: 128.32.65.128

En segundo lugar, una vez se han construido las cuatro subredes posibles al ampliar en dos bits la máscara de red. Se hace necesario determinar cuales son las direcciones IP para configurar máquinas en cada una de de esas subredes. El rango de direcciones IP configurables para cada subred estará comprendido entre dos direcciones de red consecutivas. El rango de direcciones comenzará en una dirección por encima de la dirección de red de valor inferior, y terminará en 2 direcciones por debajo de la siguiente dirección de red superior.

Así, el rango para esas direcciones de red será:

Subred1:	128.32.64.0	Rango: 128.32.64.1—128.32.64.126
Subred2:	128.32.64.128	Rango: 128.32.64.129—128.32.64.254
Subred3:	128.32.65.0	Rango: 128.32.65.1—128.32.65.126
Subred4:	128.32.65.128	Rango: 128.32.65.129—128.32.65.254

1.8. Topología de prácticas

La topología de la red del laboratorio de prácticas de la Escuela Politécnica Superior de la Universidad de Alicante está formada por la interconexión de varios segmentos de red. La interpretación del concepto de segmento de red depende del nivel dentro de la arquitectura en que se considere. Se adoptará en estas prácticas que un segmento de red será el conjunto de dispositivos que se ubican bajo una misma tecnología de acceso al medio o nivel de enlace. Todos estos equipos compartirán una misma dirección de red IP.

La figura 20 muestra el laboratorio de prácticas y en el esquema de la figura 21 se detalla la estructura de la red de comunicaciones. Cada segmento de red está conectado a los demás segmentos a través del dispositivo denominado router o encaminador.

El segmento principal corresponde a la red en la que se encuentran los PC's de los alumnos. Todas las máquinas están conectadas entre sí empleando un dispositivo denominado HUB (figura 22a), que proporciona una topología aparentemente en estrella (internamente es un BUS).

El protocolo Ethernet está presente en las tarjetas de red Ethernet instaladas en cada una de las máquinas que requieren esta tecnología (figura 22b).

La red del laboratorio consta de 5 subredes la **172.20.43.192/26,** la **172.20.41.240/28,** la **10.4.2.4/30,** la **10.4.2.0/30** y la **10.3.0.0/16**. La subred de los PC's de los alumnos pertenece a la subred 172.20.43.192 con máscara de 26 bits, del tipo 255.255.255.192. Todos los PC's de los alumnos están numeran desde 172.20.43.198 hasta 172.20.43.227 siendo la dirección de broadcast 172.20.43.255. Existen tres máquinas, CISCO 1720, CISCO 1601 y Linux 2 que interconectan la subred 172.20.43.192 con las otras subredes del laboratorio. En la topología de la red se puede observar como los equipos de interconexión disponen de una dirección IP en cada uno de los enlaces en los que están presentes.

Figura 20. Laboratorio de prácticas de la EPS. Universidad de Alicante.

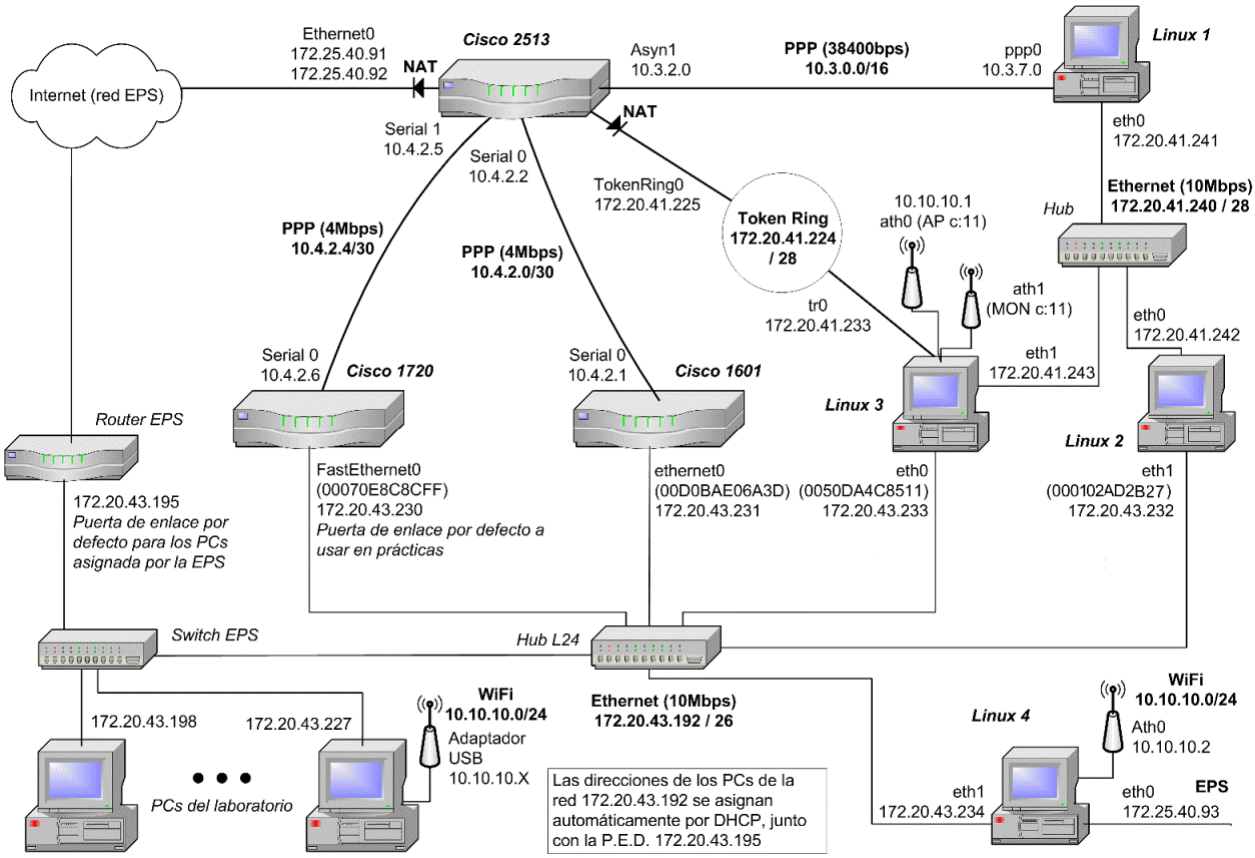
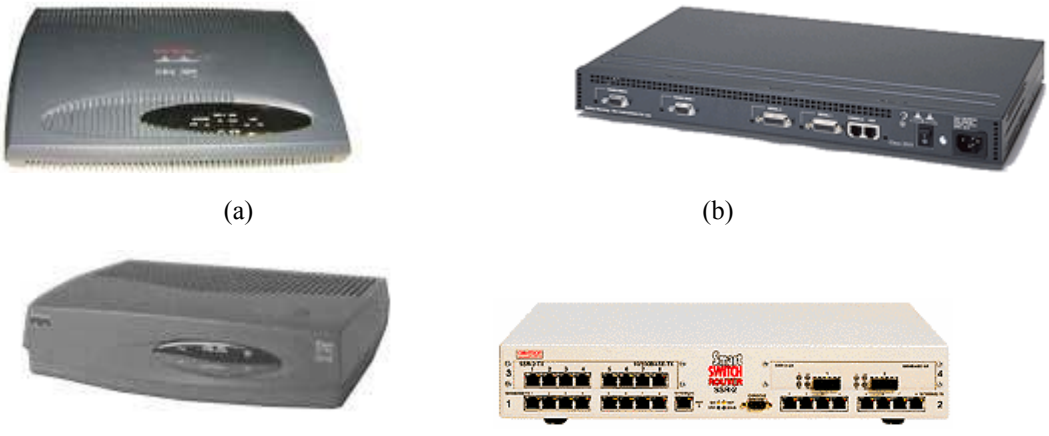


Figura 21. Esquema de la red del laboratorio.

Todos los PC's de los alumnos están conectados al medio físico mediante un dispositivo SWITCH. Por otro lado, el router CISCO 1601 (figura 23.a) se une al medio físico compartido por tres máquinas: Linux2, Linux3 y Linux4 mediante un dispositivo HUB. A su vez, este dispositivo HUB se une a un SWITCH, al que también se conecta el PC Profesor (172.20.43.223). Todo el tráfico de este SWITCH sale al exterior a través del router CISCO 1720 (figura 23.c) que, al igual que el router CISCO 1601, interconecta la red Ethernet con otras subredes del laboratorio, como las 10.4.2.4/30, 10.4.2.0/30 y 10.3.0.0/16 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. Se recuerda que cada segmento de red tendrá una dirección de red IP y todas las máquinas que estén en un mismo segmento de red tendrán la misma dirección de red o subred (dependiendo de si forman una red o sólo una subred). Para diferenciar las máquinas dentro de un mismo segmento de red, cada una de ellas tiene asociada una dirección de máquina.

Figura 22. a) Concentrador de cableado, Hub. b) Tarjeta de red Ethernet instalada en los equipos.

PPP son las siglas de Point to Point Protocol: Protocolo Punto a Punto. Este segmento PPP, que emplea una velocidad de transmisión de 4 Mbps, está también conectado a otro segmento PPP que trabaja a una velocidad de 38400 bps (subred 10.3.0.0/16). El dispositivo que las interconecta es el router CISCO 2513 (figura 23.b).



(a) (b)

(c) (d)

Figura 23. Routers en la red del laboratorio. (a) Router CISCO 1601. (b) Router CISCO 2513. (c) Router CISCO 1720. (d) Smart Switch Router CABLETRON.

En el otro extremo de la red PPP hay un PC con sistema operativo Linux, Linux1, que interconecta ese segmento con otra red Ethernet 10baseT (subred 172.20.41.240/28) que mediante un HUB une Linux1 con Linux2 y Linux3. Esta máquina, Linux 1, también es un router, pues interconecta dos segmentos de red. La diferencia entre el router CISCO y el router Linux es que el router CISCO es un dispositivo orientado y diseñado para la interconexión de redes, por lo que presenta mejores prestaciones y mayor rapidez en el procesamiento de los paquetes que el PC con el sistema operativo Linux. Finalmente, el segmento de Ethernet 172.20.41.240/28 está conectado al segmento Ethernet de los PCs de los alumnos a través de otro router, el Linux 2. Además, en el esquema de la figura 21 hay configurada una red 10.10.10.0/24 que permite encaminar el tráfico a través de accesos inalámbricos entre el Linux 3 y el Linux4.

Esta configuración de red sería cerrada si no fuera porque el router CISCO 2513 está conectado al exterior del laboratorio, y a través de él los alumnos pueden acceder a la red de la Universidad. El CISCO 2513 está conectado a los routers de la red Ethernet de la Universidad de Alicante que dan paso a Internet, concretamente, la conexión exterior se realiza a través del CABLETRON de la Escuela Politécnica. Es posible observar en el esquema de la figura 21 como el router CISCO 2513 dispone de cuatro direcciones IP diferentes, uno por cada red o subred en la que está conectado.

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 más empleados en el laboratorio 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 accede al contenido 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 todas las tramas 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.

Ejercicios de captura

Cuestión 1. Captura de tramas

a. Conecta a la página web www.google.com y ejecuta el monitor de red Wireshark.

b. Identifica el tipo de dispositivo de red (interface de captura).

c. Aprende a cambiar el modo de captura a promiscuo y no promiscuo. Observa las diferencias en la captura.

d. Aprende a variar el número máximo de bytes de trama que se quieren capturar. Por defecto 68 bytes.

e. Aprende a visualizar los datos al tiempo que se captura. *Update list packets in real time*

Cuestión 2. Identificación de la información de captura

a. Conéctate a la página web, www.eps.ua.es y haz una captura de tramas con el monitor Wireshark.

- Identifica cada uno de los parámetros de la captura: número de paquetes, tiempo de captura, dirección origen y destino de cada paquete, tipo de paquete e información de datos del paquete.
- Identifica los paquetes contenidos en una determinada trama capturada de acuerdo a su nivel en la arquitectura TCP/IP (paquete IP, paquete TCP,etc.)
- Comprueba los datos ASCII de una trama y comparalos con la información que contiene la página web. Marca las tramas que contienen esa información.
- Emplea la opción *Analyze->follow tcp stream* y estudia las tramas que salen.

Cuestión 3. Marcado y grabación de capturas

a. Familiarizase con las capturas, activando o desactivando posibles protocolos susceptibles de ser capturados.

- Para ello captura www.wanadoo.es, y marca las tramas http. Después, realiza la misma captura desactivando todos los protocolos menos el http. *Analyze-> Enabled Protocols.* Observa las diferencias.

b. Aprende a aislar un paquete mostrándolo en una ventana independiente.

- Para ello emplea la opción *View->show packet in new window* para aislar un paquete TCP de entre todos los obtenidos en la captura anterior.
- Graba el paquete capturado y marcado, en un fichero.

Cuestión 4. Filtros de visualización y captura

a. Captura las tramas durante el proceso de conexión a www.ua.es, realiza los siguientes filtros para visualizar únicamente las tramas que se piden. Guarda la sintaxis de los filtros, en cada caso, con la opción *Analyze->Display filtres.*

- Filtra las tramas dirigidas a tu máquina.
- Filtra las tramas que proceden de tu máquina.
- Filtra las tramas que proceden de la máquina de un determinado compañero.
- Filtra las tramas que sean de broadcast.
- Filtra las tramas que emplean el protocolo IP.
- Filtra las tramas que emplean el protocolo TCP y cuyo puerto origen es 80.
- Filtra las tramas que contienen paquetes IP de una longitud mayor que 90.
- Filtra las tramas Ethernet con longitud mayor que 1400

b. Conecta al servidor www.ya.com y captura, únicamente, las siguientes tramas:

- Las tramas dirigidas a tu máquina.
- Las tramas que procedan de tu máquina.
- Las tramas que proceden de la máquina 172.20.43.230.
- Las tramas con MAC de destino del tipo broadcast.
- Las tramas con IP de destino del tipo broadcast.
- Las tramas que emplean puerto 80.
- Las tramas que emplean protocolo TCP y puerto destino es el 80.
- Las tramas que tengan una longitud superior a 90 y empleen protocolo IP.

Ejercicios de topología y dispositivos

Cuestión 5. Topologías y dispositivos

a. ¿Qué dispositivos de interconexión posee la topología presentada en la figura 21? Identifícalos y enumera sus características.

b. ¿Qué diferencias adviertes entre SWITCH y HUB?

c. ¿Qué diferencias adviertes entre ROUTER y BRIDGE?

Ejercicios de ARP

Cuestión 6. Protocolo ARP sobre la configuración del Laboratorio

a. Visualizar la dirección MAC e IP de la máquina de ensayos, ejecutando el comando:

C:\WINDOWS\ipconfig /all

Activar la captura de tramas en el programa monitor de red.

En la máquina del alumno se lanzarán peticiones 'echo' a través del programa ping a la dirección IP 172.20.43.230, borrando previamente de la tabla ARP local la entrada asociada a esa dirección IP:

C:\>WINDOWS>arp –a Estado de la memoria caché de Arp

C:\>WINDOWS>arp –d <dirección ip> Borrado de una dirección IP en la tabla arp.

C:\>WINDOWS>ping –n 1 172.20.43.230

Dentro del monitor de red detener la captura y visualizarla. Introducir un filtro para visualizar sólo tramas ARP asociadas a la máquina del alumno

- ¿Cuántas tramas intervienen en la resolución ARP?
    - Descríbase la secuencia de tramas involucradas, justificando todas las direcciones MAC e IP que aparecen.
- ¿Cuál es el estado actual de la memoria caché de ARP?
- Volver a ejecutar el comando ping a la misma máquina y observar la secuencia de tramas ARP. ¿Aparecen las mismas tramas ARP? ¿Por qué?

b. Ejecutar el comando *ping -n* con diferentes direcciones IP de los compañeros asistentes a prácticas. ¿Qué ocurre con la memoria caché de ARP?

c. Ejecutar el comando *ping -n* con las siguientes direcciones IP: 10.3.7.0, 10.4.2.1, 10.4.2.5, 172.20.41.241. Y para cada una de las ejecuciones responde a las siguientes preguntas:

- ¿Cuántas tramas intervienen en la resolución ARP? ¿Cuántas tramas que encapsulan ARP de las que intervienen en la resolución ARP pueden ser capturadas desde la máquina del alumno? Descríbase la secuencia de tramas involucradas, justificando todas las direcciones MAC e IP que aparecen.
- ¿Qué ocurre con la memoria caché de ARP? ¿Qué diferencia existe con respecto al ejercicio anterior?

Cuestión 7. Protocolo ARP de acuerdo a la topología de la Figura 24

a. Describe la secuencia de tramas ARP generadas cuando la máquina A ejecuta el comando 'ping –n 1 10.1.2.2'. Para ello supóngase que las tablas ARP de todas las máquinas están vacías. ¿Cuántas tramas intervienen en la resolución ARP? ¿Cuáles son las direcciones MAC de dichas tramas? ¿Qué tipos de paquetes ARP encapsulan esas tramas? ¿Qué información transportan?

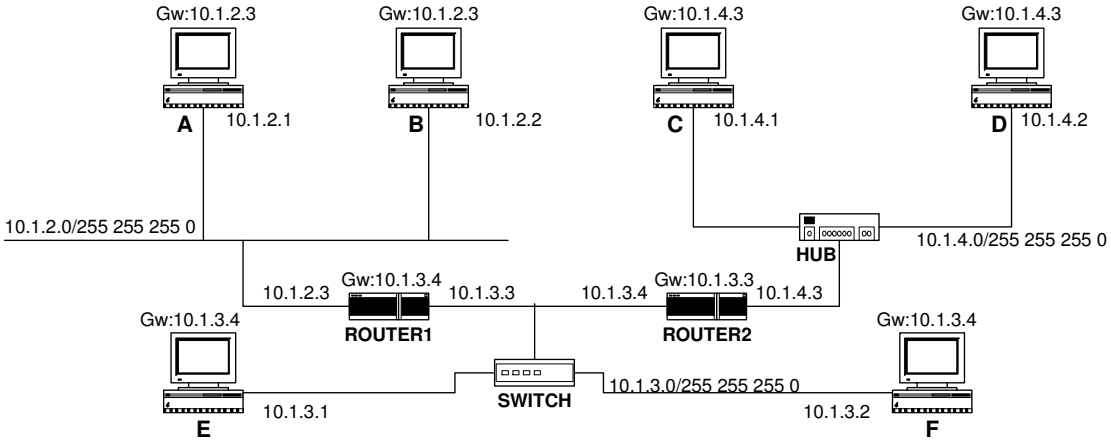


Figura 24. Topologia de red LAN com vários segmentos de red y dispositivos de interconexión.

b. Describe la secuencia de tramas ARP generadas cuando la máquina A ejecuta el comando 'ping –n 1 10.1.4.1'. Para ello supóngase que las tablas ARP de todas las máquinas están vacías. ¿Cuántas tramas intervienen en la resolución ARP? ¿Cuáles son las direcciones MAC de dichas tramas? ¿Qué tipos de paquetes ARP encapsulan esas tramas? ¿Qué información transportan?

c. Describe la secuencia de tramas ARP generadas cuando la máquina A ejecuta el comando 'ping –n 1 10.1.4.1'. Para ello supóngase que la máquina Router2 conoce la dirección MAC de C. ¿Cuántas tramas intervienen en la resolución ARP? ¿Cuáles son las direcciones MAC de dichas tramas? ¿Qué tipos de paquetes ARP encapsulan esas tramas? ¿Qué información transportan?

d. Describe la secuencia de tramas ARP generadas cuando la máquina A ejecuta el comando 'ping –n 1 10.1.2.4'. Para ello supóngase que las tablas ARP de todas las máquinas están vacías. ¿Cuántas tramas intervienen en la resolución ARP? ¿Cuáles son las direcciones MAC de dichas tramas? ¿Qué tipos de paquetes ARP encapsulan esas tramas? ¿Qué información transportan?

Ejercicios de Direccionamiento

Cuestión 8. Direccionamiento IP

a. Sea la dirección de red IP 125.145.64.0 con máscara asociada 255.255.254.0. Ampliar la máscara de subred en dos bits, indicando el nuevo valor. Determina el rango de direcciones IP que puede emplearse para numerar máquinas en cada una de las subredes obtenidas en la ampliación.

b. Determina el rango de direcciones IP para las máquinas de las subredes que se obtienen de ampliar en dos bits la dirección de red 130.0.0.0.

c. Dada la dirección de red IP 10.32.0.0 con máscara asociada 255.254.0.0. Se quiere ampliar la máscara en dos bits. ¿Cuál es la nueva máscara?¿Cuántas subredes se pueden configurar? Determinar sus direcciones IP. ¿Cuántas máquinas se pueden configurar en cada una de las subredes? Determinar el rango de direcciones IP para numerar máquinas en cada una de las subredes obtenidas en la ampliación.

Cuestión 9. Análisis de datagramas IP

a. Analizar los datagramas IP capturados con el monitor de red cuando se accede a las siguientes páginas web: http://www.dfists.ua.es, http://www.aurova.ua.es, http://www.elmundo.es, http://www.elpais.com

- ¿Cuál es su longitud?
- ¿Qué aparece en el campo de Protocolo?
- Identifica la clase de dirección asociada a cada dirección IP fuente o destino.
- Identifica el valor de los puertos origen y destino que aparecen en la cabecera del protocolo del nivel de transporte asociado al protocolo de aplicación http.

- ¿ Cuál es la IP de los servidores web que proporcionan esos site?

b. A partir de la captura de tramas realizada mediante el uso del monitor de red y representada en la figura 25.

- Identificar la dirección IP origen y destino. ¿Cuáles son? ¿A qué clase pertenece cada una?
- Identificar los puertos origen y destino.
- Indicar la longitud de datos de la trama Ethernet.

```
+ FRAME: Base frame properties
  ETHERNET: ETYPE = 0x0800 : Protocol = IP:  DOD Internet Protocol
  + ETHERNET: Destination address : 00D0BAE06A3D
  + ETHERNET: Source address : 0050DA4C850F
    ETHERNET: Frame Length : 54 (0x0036)
    ETHERNET: Ethernet Type : 0x0800 (IP:  DOD Internet Protocol)
    ETHERNET: Ethernet Data: Number of data bytes remaining = 40 (0x0028)
  IP: ID = 0xF402; Proto = TCP; Len: 40
    IP: Version = 4 (0x4)
    IP: Header Length = 20 (0x14)
   + IP: Service Type = 0 (0x0)
    IP: Total Length = 40 (0x28)
    IP: Identification = 62466 (0xF402)
   + IP: Flags Summary = 0 (0x0)
    IP: Fragment Offset = 0 (0x0) bytes
    IP: Time to Live = 128 (0x80)
    IP: Protocol = TCP - Transmission Control
    IP: Checksum = 0x88B8
    IP: Source Address = 10.1.10.1
    IP: Destination Address = 193.145.232.129
    IP: Data: Number of data bytes remaining = 20 (0x0014)
  TCP: ...R.., len:    0, seq:   1765060-1765060, ack:   1765060, win:    0, src: 1077  dst:   80
    TCP: Source Port = 0x0435
    TCP: Destination Port = Hypertext Transfer Protocol
    TCP: Sequence Number = 1765060 (0x1AEEC4)
    TCP: Acknowledgement Number = 1765060 (0x1AEEC4)
    TCP: Data Offset = 20 (0x14)
   + TCP: Flags = 0x04 : ...R..
    TCP: Window = 0 (0x0)
    TCP: Checksum = 0x0F89
    TCP: Urgent Pointer = 0 (0x0)
```

Figura 25. Captura de tramas con el monitor de red.

c. Analizar los datos capturados por el monitor de red cuando se emplean diferentes aplicaciones de Internet. Comprobar qué protocolos intervienen en aplicaciones HTTP, FTP, TELNET, DNS, etc. ¿Cuáles son los protocolos de transporte involucrados en la captura?