Redes I

Examen Integrador 2da Fecha 06/2016

Emiliano Salvatori

Noviembre 2019

1. ¿Qué entiende por protocolo? ¿Cuáles son las características de una red de paquetes conmutados?

Existen dos métodos fundamentales que permiten transportar los datos a través de una red de enlaces y conmutadores: la conmutación de circuitos y la conmutación de paquetes. En las **redes de conmutación de circuitos**, los recursos necesarios a lo largo de una ruta (buffers, velocidad de transmisión del enlace) que permiten establecer la comunicación entre los sistemas terminales están reservados durante el tiempo que dura la sesión entre dichos sistemas terminales. En las **redes de conmutación de paquetes**, estos recursos no están reservados; los mensajes de una sesión utilizan los recursos bajo petición y, en consecuencia, pueden tener que esperar (es decir, ponerse en cola) para poder acceder a un enlace de comunicaciones.

1.1. Conmutación de paquetes

Un paquete es un grupo de información que consta de dos partes: los datos propiamente dichos y la información de control, que indica la ruta a seguir a lo largo de la red hasta el destino del paquete. La **conmutación de paquetes** es un método de agrupar los datos transmitidos a través de una red digital en paquetes que se componen de un encabezado y una carga útil. Los datos en el encabezado son utilizados por el hardware de red para dirigir el paquete a su destino donde la carga útil es extraída y utilizada por el software de la aplicación. La conmutación de paquetes es la base principal de las comunicaciones de datos en redes informáticas de todo el mundo.

Las aplicaciones distribuidas intercambian mensajes para llevar a cabo sus tareas. Los mensajes pueden contener cualquier cosa que el diseñador del protocolo desee. Los mensajes pueden realizar una función de control (por ejemplo, los mensajes de saludo "Hola" del ejemplo anterior sobre establecimiento de la comunicación) o pueden contener datos, como por ejemplo un mensaje de correo electrónico, una imagen JPEG o un archivo de audio MP3. En las redes de computadoras modernas, el origen divide los mensajes largos en fragmentos de datos más pequeños que se conocen como paquetes. Entre el origen y el destino, cada uno de estos paquetes viaja a través de los enlaces de comunicaciones y de los conmutadores de paquetes (de los que existen dos tipos predominantes: los routers y los switches de la capa de enlace). Los paquetes se transmiten a través de cada enlace de comunicaciones a una velocidad igual a la velocidad de transmisión máxima del enlace.

La mayoría de los conmutadores de paquetes emplean el método de transmisión de almacenamiento y reenvío en las entradas de los enlaces. **Transmisión de almacenamiento y reenvío** significa que el conmutador tiene que recibir el paquete completo antes de poder comenzar a transmitir el primer bit del paquete al enlace de salida. Por tanto, los conmutadores de paquetes de almacenamiento y reenvío añaden un retardo de almacenamiento y reenvío en la entrada de cada enlace existente a lo largo de la ruta que debe seguir el paquete. Veamos el tiempo que se tarda en enviar un paquete de L bits desde un host a otro host en una red de conmutación de paquetes. Supongamos que existen Q enlaces entre los dos hosts, y que la velocidad en cada uno de ellos es igual a R bps. Suponemos que éste es el único paquete presente en la red. En primer lugar, el paquete tiene que enviarse a través del primer enlace que sale del host A, lo que consume un tiempo de $\frac{L}{R}$ segundos. A continuación, tiene que ser transmitido por cada uno de los $Q-1$ enlaces restantes; es decir, se tiene que almacenar y reenviar $Q-1$ veces, añadiéndose cada vez un retardo de almacenamiento y reenvío de $\frac{L}{R}$. Por tanto, el retardo total es igual a $\frac{Q*R}{L}$

Cada conmutador de paquetes tiene varios enlaces conectados a él y para cada enlace conectado, el conmutador de paquetes dispone de un buffer de salida (también denominado cola de salida), que almacena los paquetes que el router enviará a través de dicho enlace. El buffer de salida desempeña un papel clave en la conmutación de paquetes. Si un paquete entrante tiene que ser transmitido a través de un enlace, pero se encuentra con que el enlace está ocupado transmitiendo otro paquete, el paquete entrante tendrá que esperar en el buffer de salida. Por tanto, además de los retardos dé almacenamiento y reenvío, los paquetes se ven afectados por los retardos de cola del buffer de salida. Estos retardos son variables y dependen del nivel de congestión de la red. Puesto

que la cantidad de espacio en el buffer es finita, un paquete entrante puede encontrarse con que el buffer está completamente lleno con otros paquetes que esperan a ser transmitidos. En este caso, se producirá una pérdida de paquetes, bien el paquete que acaba de llegar o uno que ya se encuentra en la cola será descartado.

2. ¿Qué entiende por Modelo de Capas? ¿Cuáles son sus características?

El modelo TCP/IP, describe un conjunto de guías generales de diseño e implementación de protocolos de red específicos para permitir que un equipo pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando como los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario. Existen protocolos para los diferentes tipos de servicios de comunicación entre equipos.

El uso de un modelo en capas para describir protocolos de red y operaciones incluyen los siguientes beneficios:

- Ayuda en el diseño de protocolos.
- Fomenta la competencia, ya que los productos de distintos proveedores pueden trabajar en conjunto.
- Evita que los cambios en la tecnología o en las funcionalidades de una capa afecten otras capas superiores e inferiores.
- Proporciona un "lenguaje común" para describir las funciones y capacidades de red.

Los modelos TCP/IP y OSI son los modelos principales que representan el tipo básico de modelos de red en capas:

- **Modelo de protocolo**: este tipo de modelo coincide con precisión con la estructura de una suite de protocolos determinada. El modelo TCP/IP es un protocolo modelo porque describe las funciones que ocurren en cada capa de protocolos dentro de una suite de TCP/IP. TCP/IP también es un ejemplo de un modelo de referencia.
- **Modelo de referencia**: este tipo de modelo es coherente con todos los tipos de servicios y protocolos de red al describir qué es lo que se debe hacer en una capa determinada, pero sin regir la forma en que se debe lograr. El modelo OSI en un modelo de referencia de internetwork muy conocido, pero también es un modelo de protocolo para la suite de protocolo OSI.

Las capas de protocolos presentan ventajas conceptuales y estructurales. Como hemos visto, las capas proporcionan una forma estructurada de estudiar los componentes del sistema. Además, la modularidad facilita la actualización de los componentes del sistema. Un potencial inconveniente de la estructura de capas es que una capa puede duplicar la funcionalidad de la capa inferior. Por ejemplo, muchas pilas de protocolos proporcionan una función de recuperación de errores tanto por enlace como extremo a extremo. Un segundo potencial inconveniente es que la funcionalidad de una capa puede precisar información (por ejemplo, un valor de una marca temporal) que sólo existe en otra capa, y esto viola el objetivo de la separación en capas.

Cuando los protocolos de las distintas capas se toman en conjunto se habla de pila de protocolos. La pila de protocolos de Internet consta de cinco capas: capa física, capa de enlace, capa de red, capa de transporte y capa de aplicación, como se muestra en la siguiente imagen:

a. Pila de protocolos de Internet de cinco capas

Pila de Protocolos

Capa de Aplicación

La capa de aplicación es donde residen las aplicaciones de red y sus protocolos. Un protocolo de la capa de aplicación está distribuido a lo largo de varios sistemas terminales, estando la aplicación en un sistema terminal que utiliza el protocolo para intercambiar paquetes de información con la aplicación de otro sistema terminal. A este paquete de información de la capa de aplicación se denomina **mensaje**.

Capa de Transporte

La capa de transporte de Internet transporta los mensajes de la capa de aplicación entre los puntos terminales de la aplicación. En Internet, existen dos protocolos de transporte, TCP y UDP, pudiendo cada uno de ellos transportar los mensajes de la capa de aplicación. TCP ofrece a sus aplicaciones un servicio orientado a la conexión. Este servicio proporciona un suministro garantizado de los mensajes de la capa de aplicación al destino y un mecanismo de control del flujo (es decir, adaptación de las velocidades del emisor y el receptor).

El protocolo UDP proporciona a sus aplicaciones un servicio sin conexión. Es un servicio básico que no ofrece ninguna fiabilidad, ni control de flujo, ni control de congestión. Denominaremos a los paquetes de la capa de transporte como **segmentos**

Capa de Red

La **Capa de Red** de Internet es responsable de trasladar los paquetes de la capa de red, conocidos como datagramas, de un host a otro. El protocolo de la capa de transporte (TCP o UDP) de Internet de un host de origen pasa un segmento de la capa de transporte y una dirección de destino a la capa de red, al igual que damos al servicio de correo postal una caita con una dirección de destino. Luego, la capa de red proporciona el servicio de suministrar el segmento a la capa de transporte del host de destino.

La capa de red de Internet incluye el conocido protocolo IP, que define los campos del datagrama, así como la forma en que actúan los sistemas terminales y los routers sobre estos campos. Existe un único protocolo IP y todos los componentes de Internet que tienen una capa de red deben ejecutar el protocolo IP. La capa de red de Internet también contiene los protocolos de enrutamiento que determinan las rutas que los datagramas siguen entre los orígenes y los destinos. Internet dispone de muchos protocolos de enrutamiento. Internet es una red de redes y, dentro de una red, el administrador de la red puede ejecutar cualquier protocolo de enrutamiento que desee. Aunque la capa de red contiene tanto el protocolo IP como numerosos protocolos de enrutamiento, suele hacerse referencia a ella simplemente como la capa IP, lo que refleja el hecho de que IP es el pegamento de todo Internet.

Capa de Enlace

La capa de red de Internet encamina un datagrama a través de una serie de routers entre el origen y el destino. Para trasladar un paquete de un nodo (host o router) al siguiente nodo de la ruta, la capa de red confía en los servicios de la **Capa de Enlace**. En concreto, en cada nodo, la capa de red pasa el datagrama a la capa

de enlace, que entrega el datagrama al siguiente nodo existente a lo largo de la ruta. En el siguiente nodo, la capa de enlace pasa el datagrama a la capa de red.

Puesto que normalmente los datagramas necesitan atravesar varios enlaces para viajar desde el origen hasta el destino, un datagrama puede ser manipulado por distintos protocolos de la capa de enlace en los distintos enlaces disponibles a lo largo de la ruta. Por ejemplo, un datagrama puede ser manipu lado por Ethernet en un enlace y por PPP en el siguiente enlace. La Capa de Red recibirá un servicio diferente por parte de cada uno de los distintos protocolos de la capa de enlace. Se denomina a los paquetes de esta capa como **Tramas**.

Capa de Física

Mientras que el trabajo de la capa de enlace es mover las tramas completas de un elemento de la red hasta el elemento de red adyacente, el trabajo de la capa física es el de mover los bits individuales dentro de la trama de un nodo al siguiente. Los protocolos de esta capa son de nuevo dependientes del enlace y, por tanto, dependen del medio de transmisión del enlace (por ejemplo, cable de cobre de par trenzado o fibra óptica monomodo). Por ejemplo, Ethernet dispone de muchos protocolos de la capa física: uno para cable de cobre de par trenzado, otro para cable coaxial, otro para fibra, etc. En cada caso, los bits se desplazan a través del enlace de forma diferente.

3. ¿Cuáles son las características principales de la Capa de Red?

Funciones de la capa de Red

La función de la capa de red es por tanto tremendamente simple: transporta paquetes desde un host emisor a un host receptor. En la realización de esta tarea podemos identificar dos importantes funciones de la capa de red:

- **Reenvío (forwarding)**: Cuando un paquete llega al enlace de entrada de un router, éste tiene que pasar el paquete al enlace de salida apropiado. Por ejemplo, un paquete que llega procedente de Hl al router Rl debe ser reenviado al siguiente router de la ruta hacia H2.

  Reenvio/Forwarding: Tiene que ver con lo anerior, es mover paquetes desde una entrada del router a la salida del mismo. Cuando un paquete llega al enlace de entrada de un router, éste tiene que pasar el paquete al enlace de salida apropiado.

- **Enrutamiento (routing)**: La capa de red tiene que determinar la ruta o camino que deben seguir los paquetes a medida que fluyen de un emisor a un receptor. Los algoritmos que calculan estas rutas se conocen como algoritmos de enrutamiento. Un algoritmo de enrutamiento debe determinar, por ejemplo, la ruta por la que fluirán los paquetes para ir de H1 a H2.

  Ruteo/Enrutamiento/Routing: Determina una ruta de una punta a la otra, desde origen a destino. La capa de red tiene que determinar la ruta o camino que deben seguir los paquetes a medida que fluyen de un emisor a un receptor. Los algoritmos que calculan estas rutas se conocen como algoritmos de enrutamiento. Un algoritmo de enrutamiento debe determinar, por ejemplo, la ruta por la que fluirán los paquetes para ir de un Host situado en la ciudad/pais A, hasta otro situado en la ciudad/país B.

Ejemplo práctico de Reenvío y Enrutamiento

Un paralelismo con lo anterior se puede poner cuando un usuario quiere realizar un viaje en auto por el país. Decidir la ruta que se tomará para llegar a determinada provincia desde la casa del usuario sería el *enrutamiento*. En cambio, llegado a una ciudad (que sería para el ejemplo como ser un router), decidir por qué calle tomar para dar con la ruta que me llevará al próximo pueblo sería el *reenvío*.

El reenvío hace referencia a la acción local que realiza un router al transferir un paquete desde una interfaz de un enlace de entrada a una interfaz del enlace de salida apropiada. El enrutamiento hace referencia al proceso que realiza la red en conjunto para determinar las rutas terminal a terminal que los paquetes siguen desde el origen al destino.

Para saber la mejor ruta los ruters corren algoritmos que van a determinar la mejor ruta para ir de un host a otro, una vez que terimna el algoritmo gnera una tabla de reenvio, esa tabla está conformada como si fuera un algoritmo de Dijkstra. Evalúa dándole determinado peso entre routers.

Todo router tiene una tabla de reenvío. Un router reenvía un paquete examinando el valor de un campo de la cabecera del paquete entrante y utilizando después ese valor para indexarlo dentro de la tabla de reenvío del router. El resultado de la tabla de reenvío indica a cuál de las interfaces del enlace de salida del router será reenviado el paquete. Dependiendo del protocolo de la capa de red, este valor de la cabecera del paquete podría ser la dirección de destino del paquete o una indicación de la conexión a la que pertenece el paquete

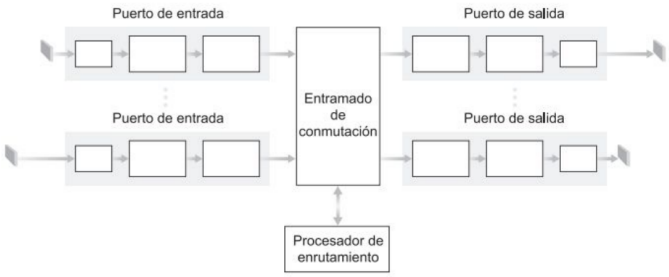
Una vez que el router pasa el paquete a otro, se olvida del paquete que envió. Si cada router corre el mismo algoritmo proporcionado por el protocolo que se ejecute,todos llegan a la misma conclusión de que la mejor ruta es una, y en base a ello es que se genera la tabla de reenvío; la problemática es que todos corran el mismo algoritmo y saber cuál usar.

Cada ruter corre el algoritmo, genera la tabla, determina la mejor ruta, envía los paquetes; los algoritmos se corren cada determinado tiempo, para que se actualice la tabla de ruteo; y todo esto se denomina *Ruteo dinámico. Ruteo estático*: es cuando se define vía hardware por dónde debe salir un paquete determinado.

4. ¿Cuáles son las funciones de un Router? Realice un diagrama en bloques de un Router y describa sus modulos?

Función de un Router

La función principal de un router es la *transferencia real de paquetes desde los enlaces de entrada de un router a los apropiados enlaces de salida.*



En un router se pueden identificar cuatro componentes:

1. **Puertos de entrada**: El puerto de entrada realiza varias funciones. Lleva a cabo las funciones de la capa física (representadas por el recuadro situado más a la izquierda del puerto de entrada y el recuadro más a la derecha del puerto de salida en la Figura) consistentes en la terminación de un enlace físico de entrada a un router. Realiza las funciones de la capa de enlace de datos (representadas por los recuadros centrales de los puertos de entrada y de salida) necesarias para interoperar con las funciones de la capa de enlace de datos en el lado remoto del enlace de entrada. También realiza una función de búsqueda y reenvío (el recuadro más a la derecha del puerto de entrada y el recuadro más a la izquierda del puerto de salida) de modo que un paquete reenviado dentro del entramado de conmutación del router emerge en el puerto de salida apropiado. Los paquetes de control (por ejemplo, paquetes que transportan la información del protocolo de enrutamiento) son reenviados desde un puerto de entrada al procesador de enrutamiento. En la práctica, suelen agruparse varios puertos en una única tarjeta de línea (line card) dentro del router.

2. **Entramado de conmutación**: El entramado de conmutación conecta los puertos de entrada del router a sus puertos de salida. Este entramado de conmutación está completamente contenido dentro del router.

3. **Puertos de salida**: Un puerto de salida almacena los paquetes que le han sido reenviados a través del entramado de conmutación y los transmite al enlace de salida. Así, el puerto de salida lleva a cabo la función inversa de la capa física y de la capa de enlace de datos que el puerto de entrada. Cuando un enlace es bidireccional (es decir, transporta tráfico en ambas direcciones), un puerto de salida del enlace normalmente estará emparejado con otro puerto de entrada de dicho enlace en la misma tarjeta de línea.

4. **Procesador de enrutamiento**: El procesador de enrutamiento ejecuta los protocolos de enrutamiento mantiene la información de enrutamiento y las tablas de reenvío y realiza funciones de gestión de red dentro del router.

5. ¿Para qué se utiliza el comando ipconfig?¿Cómo se utiliza?

ipconfig en Microsoft Windows es una aplicación de consola que muestra los valores de configuración de red de TCP/IP actuales y actualiza la configuración del protocolo DHCP y el sistema de nombres de dominio (DNS). También existen herramientas con interfaz gráfica denominadas winipcfg y wntipcfg. El papel desempeñado por estas herramientas es similar al de las diversas implementaciones de ifconfig en UNIX y sistemas operativos tipo UNIX.

El comando permite mostrar la configuración de red del ordenador en que se utilizó. Se puede añadir que la diferencia entre IPCONFIG e IPCONFIG/ALL es que el primero muestra sólo la información básica de red del ordenador y el segundo muestra toda la información disponible por el SO.

Para utilizarlo es necesario abrir una terminal en Windows y teclear o *ipconfig* o *ipconfig/all*. La información más relevante que se puede ver es:

- La dirección IP local que tiene la computadora asignada por el router.
- La puerta de enlace predeterminada. Esta es la información mas común por la cual se utiliza el comando IPCONFIG. La puerta de enlace predeterminada puede servir para poder entrar a la configuración del router.
- Los servidores DNS asignados al equipo. Estos pueden estar configurados manualmente o de forma automática, dependiendo del caso pueden ser fijos o variar dependiendo de la configuración del router y del proveedor de servicios de Internet.
- La MAC Address del PC.

6. Detalle las características del protocolo IP. ¿A qué capa pertenece? ¿Qué es un número IP? ¿Qué es una IP privada? ¿Cómo funciona el protocolo NAT?

Protocolo IP

El protocolo de IP (Internet Protocol) es la base fundamental de la Internet. Este protocolo corre sobre la **Capa de Red**, portando datagramas de la fuente al destino.

El nivel de transporte parte el flujo de datos en datagramas. Durante su transmisión se puede partir un datagrama en fragmentos que se montan de nuevo en el destino. Las principales características de este protocolo son:

- Protocolo orientado a no conexión.
- Fragmenta paquetes si es necesario.
- Direccionamiento mediante direcciones lógicas IP de 32 bits.
- Si un paquete no es recibido, este permanecerá en la red durante un tiempo finito.
- Realiza el "mejor esfuerzo"para la distribución de paquetes.
- Tamaño máximo del paquete de 65635 bytes.

Sólo ser realiza verificación por suma al encabezado del paquete, no a los datos éste que contiene.

El Protocolo Internet proporciona un servicio de distribución de paquetes de información orientado a no conexión de manera no fiable. La orientación a **no conexión** significa que los paquetes de información, que será emitido a la red, son tratados independientemente, pudiendo viajar por diferentes trayectorias para llegar a su destino. El término **no fiable** significa más que nada que no se garantiza la recepción del paquete.

La unidad de información intercambiada por IP es denominada datagrama. Tomando como analogía los marcos intercambiados por una red física los datagramas contienen un encabezado y una área de datos. IP no especifica el contenido del área de datos, ésta será utilizada arbitrariamente por el protocolo de transporte.

Dirección IP

Para que en una red dos computadoras puedan comunicarse entre sí ellas deben estar identificadas con precisión Este identificador puede estar definido en niveles bajos (identificador físico) o en niveles altos (identificador lógico) de pendiendo del protocolo utilizado. TCP/IP utiliza un identificador denominado dirección internet o dirección IP, cuya longitud es de 32 bites. La dirección IP identifica tanto a la red a la que pertenece una computadora como a ella misma dentro de dicha red.

Puesto que todos los hosts y todos los routers son capaces de enviar y recibir datagramas IP, IP requiere que cada interfaz de host y de router tenga su propia dirección IP. Por tanto, técnicamente, una dirección IP está asociada con una interfaz, en lugar de con el host o con el router que contiene dicha interfaz (el límite entre el host y el enlace físico se denomina **interfaz**).

Las direcciones IP tienen una longitud de 32 bits (lo que equivale a 4 bytes), por lo que existen un total de 2^{32} direcciones.IP posibles. Aproximando 2^{10} a 10^3, es fácil ver que hay unos 4.000 millones direcciones IP posibles. Estas direcciones normalmente se expresan utilizando la notación decimal con punto, en la que cada byte de la dirección se escribe en formato decimal y separada medíante un punto del resto de los bytes de la dirección.

La dirección IP es el identificador de cada host dentro de su red de redes. Cada host conectado a una red tiene una dirección IP asignada, la cual debe ser distinta a todas las demás direcciones que estén vigentes en ese momento en el conjunto de redes visibles por el host. En el caso de Internet, no puede haber dos ordenadores con 2 direcciones IP (públicas) iguales. Pero sí podríamos tener dos ordenadores con la misma dirección IP siempre y cuando pertenezcan a redes independientes entre sí (sin ningún camino posible que las comunique).

Clasificación de las direcciones IP:

- **Direcciones IP públicas**: Son visibles en todo Internet. Un ordenador con una IP pública es accesible (visible) desde cualquier otro ordenador conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública.
- **Direcciones IP privadas (reservadas)**: Son visibles únicamente por otros hosts de su propia red o de otras redes privadas interconectadas por routers. Se utilizan en las empresas para los puestos de trabajo. Los ordenadores con direcciones IP privadas pueden salir a Internet por medio de un router (o proxy) que tenga una IP pública. Sin embargo, desde Internet no se puede acceder a ordenadores con direcciones IP privadas.

A su vez las direcciones IP pueden ser:

- **Direcciones IP estáticas (fijas)**: Un host que se conecte a la red con dirección IP estática siempre lo hará con una misma IP. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet con objeto de que estén siempre localizables por los usuarios de Internet. Estas direcciones hay que contratarlas.
- **Direcciones IP dinámicas**: Un host que se conecte a la red mediante dirección IP dinámica, cada vez lo hará con una dirección IP distinta. Las direcciones IP públicas dinámicas son las que se utilizan en las conexiones a Internet mediante un módem. Los proveedores de Internet utilizan direcciones IP dinámicas debido a que tienen más clientes que direcciones IP (es muy improbable que todos se conecten a la vez).

Protocolo NAT

Dado el aumento de dispositivos en los últimos años conectados a internet (dispositivos móviles, subredes domésticas, Internet de las cosas, etc), fue necesario encontrar alguna forma para poder proporcionar a cada nuevo dispositivo un acceso a una dirección IP para poder establecer comunicación con Internet.

La **traducción de direcciones de Redes (NAT)** permite asignar direcciones IP de forma simple sin la necesidad de que cada usuario requiera gestionar de forma manual su red doméstica.

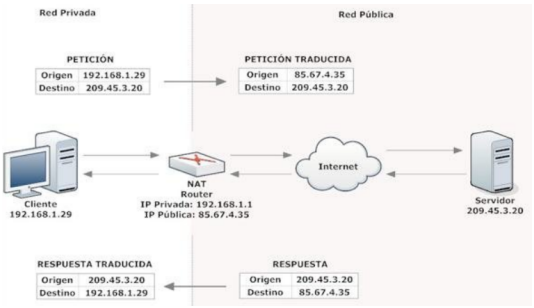
El router NAT no parece un router a ojos del mundo exterior. En su lugar, el router NAT se comporta de cara al exterior como un único dispositivo con una dirección IP única. En la Figura 4.22, todo el tráfico que sale del router doméstico hacia Internet tiene una dirección IP de origen igual a 138.76.29.7, y todo el tráfico que entra en él tienen que tener la dirección de destino 138.76.29.7. En resumen, el router NAT oculta los detalles de la red doméstica al mundo exterior. (Como nota al margen, posiblemente se esté preguntando dónde obtienen las computadoras de la red doméstica sus direcciones y dónde obtiene el router su dirección IP única. A menudo, la respuesta a ambas preguntas es la misma: ¡DHCP! El router obtiene su dirección del servidor DHCP del ISP y el router ejecuta un servidor DHCP para proporcionar direcciones a las computadoras, dentro del espacio de direcciones de la red doméstica controlada por el router NAT-DHCP.)

Si todos los datagramas que llegan al router NAT procedentes de la WAN tienen la misma dirección IP de destino (específicamente, la de la interfaz WAN del router NAT), entonces ¿cómo sabe el router a qué host interno debería reenviar un datagrama dado? El truco consiste en utilizar una tabla de traducciones NAT almacenada en el router NAT, e incluir los números de puerto, así como las direcciones IP en las entradas de la tabla. Considere el ejemplo de la Figura 4.22. Suponga que un usuario de una red doméstica

Explicación de Internet

Internet en sus inicios no fue pensado para ser una red tan extensa, por ese motivo se reservaron solo 32 bits para direcciones, el equivalente a 4.294.967.296 direcciones únicas, pero el hecho es que el número de máquinas conectadas a Internet aumentó exponencialmente y las direcciones IP se agotaban. Por ello surgió la NAT o Network Address Translation (en castellano, Traducción de Direcciones de Red)

La idea es sencilla, hacer que redes de ordenadores utilicen un rango de direcciones especiales (IPs privadas) y se conecten a Internet usando una única dirección IP (IP pública). Gracias a este ¿parche¿, las grandes empresas sólo utilizarían una dirección IP y no tantas como máquinas hubiese en dicha empresa. También se utiliza para conectar redes domésticas a Internet.



¿Cómo funciona?

- **Estática**: Una dirección IP privada se traduce siempre en una misma dirección IP pública. Este modo de funcionamiento permitiría a un host dentro de la red ser visible desde Internet. (Ver imagen anterior)
- **Dinámica**: El router tiene asignadas varias direcciones IP públicas, de modo que cada dirección IP privada se mapea usando una de las direcciones IP públicas que el router tiene asignadas, de modo que a cada dirección IP privada le corresponde al menos una dirección IP pública.

  Cada vez que un host requiera una conexión a Internet, el router le asignará una dirección IP pública que no esté siendo utilizada. En esta ocasión se aumenta la seguridad ya que dificulta que un host externo ingrese a la red ya que las direcciones IP públicas van cambiando.
- **Sobrecarga**: La NAT con sobrecarga o PAT (Port Address Translation) es el más común de todos los tipos, ya que es el utilizado en los hogares. Se pueden mapear múltiples direcciones IP privadas a través de una dirección IP pública, con lo que evitamos contratar más de una dirección IP pública. Además del ahorro económico, también se ahorran direcciones IPv4, ya que aunque la subred tenga muchas máquinas, todas salen a Internet a través de una misma dirección IP pública.

  Para poder hacer esto el router hace uso de los puertos. En los protocolos TCP y UDP se disponen de 65.536 puertos para establecer conexiones. De modo que cuando una máquina quiere establecer una conexión, el router guarda su IP privada y el puerto de origen y los asocia a la IP pública y un puerto al azar. Cuando llega información a este puerto elegido al azar, el router comprueba la tabla y lo reenvía a la IP privada y puerto que correspondan.

7. Dada la red 150.21.10.0. Se necesitan definir 12 subredes. Indique la máscara utilizada y las direcciones de las dos primeras subredes. Luego tome una de ellas e indique el rango de direcciones asignables en esa subred, dirección de red y Broadcast

Pimero se obtiene el número en binario:

$$10010110 \cdot 00010101 \cdot 00001010 \cdot 00000000$$

Se busca la cantidad de bits que se deben resguardar para poder obtener las redes: $2^4 = 16$ redes posibles, ya que $2^3 = 8$ y no alcanza. Por lo que se deben resguardar los últimos 4 bits de la dirección de red.
Obteniéndose lo siguiente:

$$10010110 \cdot 00010101 \cdot 00001010 \cdot 0000hhhh$$

Por lo que la máscara de subred será:

$$150 \cdot 21 \cdot 10 \cdot 0/28$$

Ya que los 28 bits más significativos de la izquierda estarán reservados para la red.

Indicar para cada subred: Dirección de Subred, Máscara de Subred, y Dirección de Broadcast

Red 0

Por lo tanto la **Red 0** tendría las siguientes características:

- **Dirección de Red**: 150.21.10.0/28

$$10010110 \cdot 00010101 \cdot 00001010 \cdot 00000000$$

- **Dirección de Broadcast**: No tiene
- **Dispositivos disponibles**: 1

Red 1

Por lo tanto la **Red 1** tendría las siguientes características:

- **Dirección de Red**: 150.21.10.1/28

$$10010110 \cdot 00010101 \cdot 00001010 \cdot 00000001$$

- **Dirección de Broadcast**: No tiene
- **Dispositivos disponibles**: 1

Red 2

Por lo tanto la **Red 2** tendría las siguientes características:

- **Dirección de Red**: 150.21.10.2/28

$$10010110 \cdot 00010101 \cdot 00001010 \cdot 00000010$$

- **Dirección de Broadcast**: 150.21.10.3/28

$$10010110 \cdot 00010101 \cdot 00001010 \cdot 00000011$$

- **Dispositivos disponibles**: 2

Red 3

Por lo tanto la **Red 3** tendría las siguientes características:

- **Dirección de Red**: 150.21.10.4/28

$$10010110 \cdot 00010101 \cdot 00001010 \cdot 00000100$$

- **Dirección de Broadcast**: 150.21.10.7/28

$$10010110 \cdot 00010101 \cdot 00001010 \cdot 00000111$$

- **Dispositivos disponibles**: $(2^2) = 4$
- **Dispositivos disponibles sin Broadcast y Red**: $(2^2) - 2 = 2$

Red 4

Por lo tanto la **Red 4** tendría las siguientes características:

- **Dirección de Red**: 150.21.10.8/28

$$10010110 \cdot 00010101 \cdot 00001010 \cdot 00001000$$

- **Dirección de Broadcast**: 150.21.10.15/28

$$10010110 \cdot 00010101 \cdot 00001010 \cdot 00001111$$

- **Dispositivos disponibles**: $(2^3) = 8$
- **Dispositivos disponibles sin Broadcast y Red**: $(2^3) - 2 = 6$

8. ¿Qué algoritmos de enrutamiento conoce? Detalle sus principios de funcionamiento

En términos generales, una forma de clasificar los algoritmos de enrutamiento es dependiendo de si son **globales** o **descentralizados**:

- **Un algoritmo de enrutamiento global** calcula la ruta de coste mínimo entre un origen y un destino utilizando el conocimiento global y completo acerca de la red. Es decir, el algoritmo toma como entradas la conectividad entre todos los nodos y todos los costes de enlace. Esto requiere por tanto que el algoritmo de alguna forma obtenga esta información antes de realizar realmente el cálculo. El cálculo en sí puede hacerse en un sitio (un algoritmo de enrutamiento global centralizado) o replicarse en varios sitios. La característica distintiva aquí, sin embargo, es que un algoritmo global dispone de toda la información acerca de la conectividad y de los costes de los enlaces. En la práctica, los algoritmos con información de estado global a menudo se denominan algoritmos de **Estado de Enlaces (LS, Link-State)**, ya que el algoritmo tiene que ser consciente del coste de cada enlace de la red.

- En un algoritmo de **enrutamiento descentralizado**, el cálculo de la ruta de coste mínimo se realiza de manera iterativa y distribuida. Ningún nodo tiene toda la información acerca del coste de todos los enlaces de la red. En lugar de ello, al principio, cada nodo sólo conoce los costes de sus propios enlaces directamente conectados. Después, a través de un proceso iterativo de cálculo e intercambio de información con sus nodos vecinos (es decir, los nodos que están en el otro extremo de los enlaces a los que él mismo está conectado), cada nodo calcula gradualmente la ruta de coste mínimo hacia un destino o conjunto de destinos. El algoritmo de enrutamiento descentralizado que estudiaremos se denomina algoritmo de **vector de distancias (DV, Distance-Vector)**, porque cada nodo mantiene un vector de estimaciones de los costes (distancias) a todos los demás nodos de la red.

Algoritmo de enrutamiento por Vector de Distancias (DV)

Mientras que el algoritmo LS es un algoritmo que emplea información global, el algoritmo por Vector de Distancias (DV) es iterativo, asincrono y distribuido.

- Es **distribuido** en el sentido de que cada nodo recibe información de uno o más de sus vecinos directamente conectados, realiza un cálculo y luego distribuye los resultados de su cálculo de vuelta a sus vecinos.

- Es **iterativo** porque este proceso continúa hasta que no hay disponible más información para ser intercambiada entre los vecinos. (Además, el algoritmo también finaliza por sí mismo, es decir, no existe ninguna señal que indique que los cálculos deberían detenerse; simplemente se detienen).

- El algoritmo es **asincrono**, en el sentido de que no requiere que todos los nodos operen sincronizados entre sí.

Como tendremos oportunidad de ver, un algoritmo asincrono, iterativo, distribuido y que finaliza por sí mismo es mucho más interesante y divertido que un algoritmo centralizado.

Algoritmo de enrutamiento de Estado de Enlaces(LS)

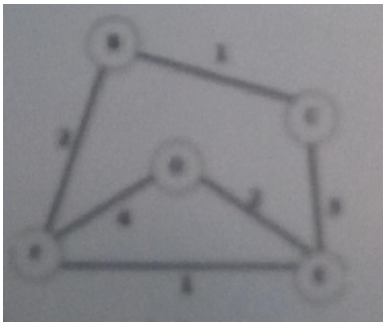
Recuerde que en un algoritmo de Estado de Enlaces, la topología de la red y el coste de todos los enlaces **son conocidos**; es decir, están disponibles como entradas para el algoritmo LS.

En la práctica, esto se consigue haciendo que cada nodo difunda paquetes del estado de los enlaces a todos los demás nodos de la red, con cada paquete de estado de enlace conteniendo las identidades y los costes de sus enlaces conectados. En la práctica (por ejemplo, con el protocolo de enrutamiento OSPF de Internet), esto suele conseguirse mediante un algoritmo de difusión de estado de enlaces

El resultado de difundir la información de los nodos es que todos los nodos tienen una visión completa e idéntica de la red. Cada nodo puede entonces ejecutar el algoritmo LS y calcular el mismo conjunto de rutas de coste mínimo que cualquier otro nodo.

El algoritmo de enrutamiento de Estado de Enlaces que presentamos a continuación se conoce como algoritmo de Dijkstra, en honor a su inventor. El algoritmo de Dijkstra calcula la ruta de coste mínimo desde un nodo (el origen, al que denominaremos u) hasta todos ios demás nodos de la red. El algoritmo de Dijkstra es iterativo y tiene la propiedad de que después de la k-ésima iteración del algoritmo, se conocen las rutas de coste mínimo hacia k nodos de destino y entre las rutas de coste mínimo a todos los nodos de destino, estas k rutas tendrán los k costes más pequeños.

9. Dado el siguiente gráfico calcule el costo mínimo desde el nodo B hasta todos los demás mediante el algoritmo de Estados de Enlace. Realice la tabla de ruteo del nodo B



10. ¿Cuáles son los servicios que debe otorgar la Capa de Enlace? ¿En qué consiste el protocolo CSMA/CD? ¿Qué es una dirección MAC?

Para la Capa de Enlace, nos resultará conveniente referirnos a los hosts y los routers simplemente como **nodos** ya que, no nos va a preocupar especialmente si un determinado nodo es un router o un host. También nos referimos a los canales de comunicación que conectan nodos adyacentes a lo largo de la ruta de comunicaciones con el nombre de enlaces. Para que un datagrama pueda ser transferido desde el host de origen al de destino, debe moverse a través de cada uno de los enlaces individuales que forman la ruta terminal a terminal.

Entre los posibles servicios que un protocolo de la capa de enlace puede ofrecer se incluyen:

- **Entramado**: Casi todos los protocolos de la capa de enlace eticapsulan cada datagrama de la capa de red dentro de una trama de la capa de enlace antes de transmitirla a través del enlace. Una trama consta de un campo de datos, en el que se inserta el datagrama de la capa de red, y de una serie de campos de cabecera. (Una trama también puede incluir campos de cola; sin embargo, utilizaremos el término campos de cabecera para referimos tanto a los de cabecera como a los de cola.) La estructura de la trama está especificada por el protocolo de la capa de enlace.

- **Acceso al enlace**: Un protocolo de control de acceso al medio (MAC, Médium Access Control) especifica las reglas que se utilizan para transmitir una trama a través del enlace. Para los enlaces punto a punto que tengan un único emisor en un extremo del enlace y un único receptor en el otro extremo, el protocolo MAC es muy simple (o no existe): el emisor puede enviar una trama siempre que el enlace esté inactivo. El caso más interesante es cuando hay varios nodos compartiendo un mismo enlace de difusión, en cuyo caso se presenta el denominado problema del acceso múltiple. En ese caso, el protocolo MAC sirve para coordinar la transmisión de las tramas de los múltiples nodos.

- **Entrega fiable**: Cuando un protocolo de la capa de enlace proporciona un servicio de entrega fiable, garantiza que va a transportar cada datagrama de la capa de red a través del enlace sin que se produzcan errores. Recuerde que ciertos protocolos de la capa de transporte (como TCP) también proporcionan un servicio de entrega fiable. De forma similar a los servicios de entrega fiable de la capa de transporte, el servicio de entrega fiable de la capa de enlace suele implementarse mediante reconocimientos y retransmisiones (véase la Sección 3.4). A menudo se utiliza un servicio de entrega fiable de la capa de enlace en aquellos enlaces que suelen presentar altas tasas de error, como por ejemplo en los enlaces inalámbricos, con el objetivo de corregir los errores localmente (en el enlace en el que se producen los errores), en lugar de obligar a que un protocolo de la capa de transporte o de ia de aplicación realice una retransmisión de datos terminal a terminal. Sin embargo, la entrega fiable en la capa de enlace puede considerarse una sobrecarga innecesaria en aquellos enlaces que tengan una baja tasa de errores de bit, incluyendo los enlaces de fibra, los coaxiales y muchos enlaces de cobre de par trenzado. Por esta razón, muchos protocolos de la capa de enlace para enlaces cableados no proporcionan un servicio de entrega fiable.

- **Control de flujo**: Los nodos situados en cada extremo de un enlace tienen una capacidad limitada de almacenamiento en buffer de las tramas. Esto puede ser un problema cuando el nodo receptor puede recibir las tramas a más velocidad de la que puede procesarlas. Sin un control de flujo, el buffer del receptor puede

desbordarse con lo que las tramas se per derían. De forma similar a lo que sucede en la capa de transporte, el protocolo de la capa de enlace puede proporcionar un mecanismo de control de flujo para evitar que el nodo emisor al otro lado del enlace abrume al nodo receptor situado en el otro extremo.

- **Detección de errores**: El hardware de la capa de enlace en un nodo receptor pudiera llegar a decidir, incorrectamente, que un bit contenido en una trama es cero cuando fue transmitido como un uno, y viceversa. Dichos errores de bit se introducen debido a la atenuación de las señales y al ruido electromagnético. Puesto que no existe ninguna necesidad de reenviar un datagrama que contenga un error, muchos protocolos de la capa de enlace proporcionan un mecanismo para detectar dichos errores de bit. Esto se lleva a cabo haciendo que el nodo transmisor incluya bits de detección de errores en la trama y que el nodo receptor realice una comprobación de errores. Recuerde de los Capítulos 3 y 4 que las capas de transporte y de red de Internet también ofrecen una forma limitada de detección de errores: la suma de comprobación de Internet. La detección de errores en la capa de enlace normalmente es más sofisticada y se implementa en hardware.
- **Corrección de errores**: La corrección de errores es similar a la detección de errores, salvo porque el receptor no sólo detecta si hay bits erróneos en la trama, sino que también determina exactamente en qué puntos de la trama se han producido los errores (y luego corrige esos errores). Algunos protocolos proporcionan corrección de errores en la capa de enlace sólo para la cabecera del-paquete en lugar de para el paquete completo. Habla remos de la detección y corrección de errores en la Sección 5.2.
- **Semiduplex y fullduplex**: Con la transmisión fullduplex, los nodos de ambos extremos de un enlace pueden transmitir paquetes al mismo tiempo. Sin embargo, con la transmisión semiduplex un mismo nodo no puede transmitir y recibir al mismo tiempo.

¿En qué consiste el protocolo CSMA/CD?

El protocolo **CSMA/CD**: protocolo de acceso múltiple de Ethernet. El mismo, realiza lo siguiente:

1. Un adaptador puede comenzar a transmitir en cualquier instante; es decir, no existe el concepto de partición de tiempo.
2. Un adaptador nunca transmite una trama cuando detecta que algún otro adaptador está transmitiendo; es decir, utiliza un mecanismo de sondeo de portadora.
3. Un adaptador que está transmitiendo aborta su transmisión tan pronto como detecta que otro adaptador también está transmitiendo; es decir, utiliza un mecanismo de detección de colisiones.
4. Antes de intentar llevar a cabo una retransmisión, un adaptador espera un intervalo de tiempo aleatorio que normalmente es más pequeño que el tiempo que se tarda en trans mitir una trama.

Estos mecanismos proporcionan a CSMA/CD un rendimiento mucho mejor que el del protocolo ALOHA con particiones en un entorno LAN. De hecho, si el retardo máximo de propagación entre estaciones es muy pequeño, la eficiencia de CSMA/CD puede aproximarse al 100 por ciento. Observe también que el segundo y tercer mecanismos de la lista anterior requieren que los adaptadores de Ethernet sean capaces de (1) detectar cuándo algún otro adaptador está transmitiendo y (2) detectar una colisión mientras están transmitiendo. Los adaptadores Ethernet realizan estas dos tareas midiendo los niveles de tensión antes y durante las transmisiones.

Dentro de un adaptador específico,el protocolo CSMA/CD opera de la siguiente forma:

1. El adaptador obtiene un datagrama de la capa de red, prepara una trama Ethernet y la coloca en un buffer del adaptador.
2. Si el adaptador detecta que el canal está inactivo (es decir, durante 96 periodos de bit el adaptador no recibe intensidad de señal procedente del canal), comienza a transmitir la trama. Si el adaptador detecta que el canal está ocupado, espera hasta comprobar que no hay intensidad de señal (más otros 96 periodos de bit) y luego comienza a transmitir la trama.
3. Mientras está transmitiendo, el adaptador monitoriza la presencia de señales proceden tes de otros adaptadores. Si el adaptador transmite la trama completa sin detectar ninguna señal procedente de otros adaptadores, concluye que ha terminado su trabajo con esa trama.
4. Si el adaptador detecta intensidad de señal procedente de otros adaptadores mientras está transmitiendo, deja de transmitir su trama y transmite una señal de interferencia (jam) de 48 bits.

5. Después de abortar la transmisión de la trama (es decir, de transmitir la señal de interferencia), el adaptador entra en la fase de espera exponencial (backoff exponencial). Específicamente, a la hora de transmitir una determinada trama, después de experimentar la n-ésima colisión para esa trama, el adaptador selecciona un valor aleatorio para K del conjunto $0, 1, 2, ..., 2m - 1$, donde m = min(n,10). El adaptador espera entonces $K \cdot 512$ periodos de bit y vuelve al Paso nº 2.

Direcciones MAC

En las redes de computadoras, la dirección MAC (siglas en inglés de Media Access Control) es un identificador de 48 bits (6 bloques de dos caracteres hexadecimales (8 bits)) que corresponde de forma única a una tarjeta o dispositivo de red. Se la conoce también como dirección física, y es única para cada dispositivo. Está determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (primeros 24 bits) utilizando el *organizationally unique identifier*. [1]

La mayoría de los protocolos que trabajan en la **Capa de Enlace** del modelo OSI usan una de las tres numeraciones manejadas por el IEEE: MAC-48, EUI-48, y EUI-64, las cuales han sido diseñadas para ser identificadores globalmente únicos. No todos los protocolos de comunicación usan direcciones MAC, y no todos los protocolos requieren identificadores globalmente únicos.

Las direcciones MAC son únicas a nivel mundial, puesto que son escritas directamente, en forma binaria, en el hardware en su momento de fabricación. Debido a esto, las direcciones MAC son a veces llamadas burned-in addresses, en inglés.

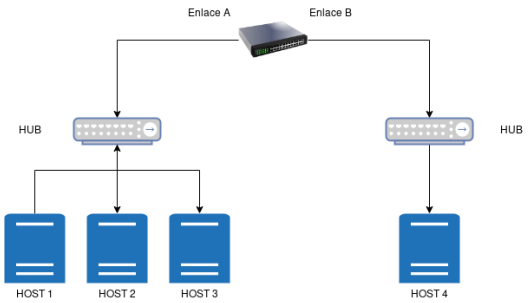
Si nos fijamos en la definición como cada bloque hexadecimal son 8 dígitos binarios (bits), tendríamos: $6^8 = 48$ bits únicos

En la mayoría de los casos no es necesario conocer la dirección MAC, ni para montar una red doméstica, ni para configurar la conexión a internet, usándose esta sólo a niveles internos de la red. Sin embargo, es posible añadir un control de hardware en un conmutador o un punto de acceso inalámbrico, para permitir sólo a unas MAC concretas el acceso a la red. En este caso, deberán conocerse las MAC de los dispositivos para añadirlos a la lista. Dicho medio de seguridad se puede considerar un refuerzo de otros sistemas de seguridad, ya que teóricamente se trata de una dirección única y permanente, aunque en todos los sistemas operativos hay métodos que permiten a las tarjetas de red identificarse con direcciones MAC distintas de la real.

Cuando un adaptador de un emisor quiere enviar una trama a otro adaptador de destino, inserta la dirección MAC del de destino en la trama y luego la envía a través de la red LAN. Si la red LAN es una LAN de difusión (como por ejemplo, 802.11 o Ethernet), la trama será recibida y procesada por todos los demás adaptadores de la LAN. En particular, cada adaptador que reciba la trama comprobará si la dirección MAC de destino contenida en la trama se corresponde con su propia dirección MAC. Si existe una correspondencia, el adaptador extraerá el datagrama incluido en la trama y lo pasará hacia arriba por la pila de protocolos para entregárselo a su nodo padre. Si no hay una correspondencia entre ambas direcciones, el adaptador descarta la trama, sin pasar el datagrama de la capa de red hacia arriba por la pila de protocolos. De este modo, sólo el nodo de destino será interrumpido cuando se reciba la trama.

Sin embargo, en ocasiones un adaptador de un emisor sí que quiere que todos los demás adaptadores de la LAN reciban y procesen la trama que va a enviar. En este caso, el adaptador emisor inserta una dirección de difusión MAC especial en el campo de la dirección de destino de la trama. Para las redes LAN que utilizan direcciones de 6 bytes (como las LAN Ethernet y de paso de testigo), la dirección de difusión es una cadena compuesta por 48 unos (1) consecutivos, es decir: FF:FF:FF:FF:FF:FF en notación hexagecimal.

11. Adicional: Se requiere realizar la tabla ARP de la siguiente red



[1] El identificador único de organización o organizationally unique identifier (OUI) es un número de 24 bits comprado a la Autoridad de Registro del Instituto de Ingeniería Eléctrica y Electrónica (IEEE). Este identificador único, identifica a cada empresa u organización (llamados asignados) a nivel mundial y reserva un bloque en cada posible identificador derivado (como las direcciones MAC, direcciones de grupos, identificadores para el Protocolo de acceso a subredes, etc.)

Definición del Protocolo ARP

En red de computadoras, el protocolo de **Resolución de Direcciones (ARP, del inglés Address Resolution Protocol)** es un protocolo de comunicaciones de la capa de red, responsable de encontrar la dirección de hardware (Ethernet MAC) que corresponde a una determinada dirección IP. Para ello se envía un paquete (ARP request) a la dirección de difusión de la red (broadcast, MAC = FF FF FF FF FF FF) que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (ARP reply) con la dirección Ethernet que le corresponde. Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo y la carga.

Se debe tener en cuenta que sólo los Switchs mantienen esta tabla ARP y no así los dispositivos HUB.

Se definen los datagramas enviados dentro de la red

Mensaje	Dispositivos que reciben	Cómo se completa tabla ARP
1 envía 3	1, 2, 3, 4	1 se encuentra en Interfaz A
3 envía 1	1, 2, 3	3 se encuentra en Interfaz A
2 envía 4	1, 2, 3, 4	2 se encuentra en Interfaz A
4 envía 2	1, 2, 3	4 se encuentra en Interfaz B
3 envía 4	1, 2, 3, 4	-
4 envía 2	1, 2, 3	-

Tabla ARP del Switch

HOST	Interface
1	A
2	A
3	A
4	B