Contenido

Autor: M. Celeste Weidmann

¡Copia este texto!

Direccionamiento IP

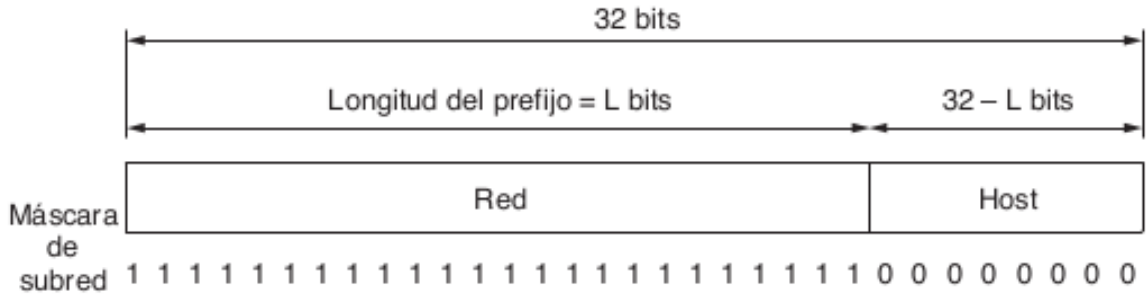
Una dirección IP es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red de un dispositivo (computadora, tablet, notebook, smartphone) que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP. En un paquete IP, el encabezado contiene una dirección de 32 bits (IPv4) o 128 bits (IPv6)

IPv4

Protocolo IP versión 4. Un datagrama IPv4 consiste en dos partes: el encabezado y el cuerpo o carga útil. El encabezado tiene una parte fija de 20 bytes y una parte opcional de longitud variable. El campo Versión lleva el registro de la versión del protocolo al que pertenece el datagrama. La versión 4 es la que domina Internet en la actualidad, al incluir la versión al inicio de cada datagrama, es posible tener una transición entre versiones a través de un largo periodo de tiempo. El encabezado transporta información vital, como las direcciones. Los campos Dirección de origen y Dirección de destino indican la dirección IP de las interfaces de red de la fuente y del destino.

Una característica que define a IPv4 consiste en sus direcciones de 32 bits. Cada host y enrutador de Internet tiene una dirección IP que se puede usar en los campos Dirección de origen y Dirección de destino de los paquetes IP. Es importante tener en cuenta que una dirección IP en realidad no se refiere a un host, sino a una interfaz de red, por lo que si un host está en dos redes, debe tener dos direcciones IP. Sin embargo, en la práctica la mayoría de los hosts están en una red y, por ende, tienen una dirección IP. En contraste, los enrutadores tienen varias interfaces y, por lo tanto, múltiples direcciones IP.

A diferencia de las direcciones Ethernet, las direcciones IP son jerárquicas. Cada dirección de 32 bits está compuesta de una porción de red de longitud variable en los bits superiores, y de una porción de host en los bits inferiores. La porción de red tiene el mismo valor para todos los hosts en una sola red, como una LAN Ethernet. Esto significa que una red corresponde a un bloque contiguo de espacio de direcciones IP. A este bloque se le llama prefijo o parte de red de una dirección IP. La longitud del prefijo corresponde a una máscara binaria de 1s en la porción de red. Cuando se escribe de esta forma, se denomina máscara de subred. Se puede aplicar un AND a la máscara de subred con la dirección IP para extraer sólo la porción de la red.



Las direcciones IP se escriben en notación decimal con puntos. En este formato, cada uno de los 4 bytes se escribe en decimal, de 0 a 255. El tamaño se determina mediante el número de bits en la porción de red; el resto de los bits en la porción del host pueden variar.

Por convención, el prefijo se escribe después de la dirección IP como una barra diagonal seguida de la longitud en bits de la porción de red.

Las direcciones IP se dividen en clases para definir las redes de tamaño pequeño, mediano y grande. Las direcciones Clase A se asignan a las redes de mayor tamaño. Las direcciones Clase B se utilizan para las redes de tamaño medio y las de Clase C para redes pequeñas. El primer paso para determinar qué parte de la dirección identifica la red y qué parte identifica el host es identificar la clase de dirección IP.

Para contrarestar las direcciones IP con las direcciones MAC, veamos las principales características. Las direcciones MAC son direcciones físicas, son asignadas por el fabricante y tienen una estructura plana. En cambio las direcciones IP, son lógicas, la asignación la realiza el administrador de la red, y tienen una estructura jerárquica (RED,HOST).

La división en clases o classful se utilizó para adaptarse a redes de distintos tamaños y para ayudar a clasificarlas. Cada dirección IP completa de 32 bits se divide en la parte de la red y parte del host. Un bit o una secuencia de bits al inicio de cada dirección determinan su clase. Son cinco las clases de direcciones IP. De estas 5 clases de direcciones ip, 3 de uso comercial (clase A, B y C) y 2 de uso reservado (clase D y E).

En 1992, la Fuerza de tareas de ingeniería de Internet (IETF) identificó los siguientes problemas: Agotamiento de las direcciones de red IPv4 no asignadas. (el espacio de Clase B estaba a punto de agotarse) y un aumento en el tamaño de las tablas de enrutamiento de Internet a medida que las redes Clase C se conectaban en línea. La inundación resultante de nueva información en la red amenazaba la capacidad de los Routers de Internet para ejercer una efectiva administración.

Las direcciones de la forma 127.xx.yy.zz se reservan para las pruebas de loopback. Los paquetes que se envían a esa dirección no se ponen en el cable; se procesan en forma local y se tratan como si fueran paquetes entrantes. Esto permite enviar paquetes al host sin que el emisor conozca su número, lo cual es útil para realizar pruebas.

IPv6

IPv6 (IP versión 6) es un diseño de reemplazo para cambiar a direcciones ip más grandes. Puesto que utiliza direcciones de 128 bits, es muy poco probable que se vayan a agotar en un futuro previsible. Sin embargo, IPv6 ha demostrado ser muy difícil de implementar. Es un protocolo de capa de red diferente que en realidad no congenia internamente con IPv4, a pesar de tantas similitudes.

Además de incrementar la cantidad de direcciones ip disponibles, IPv6 incorpora una simplificación en el encabezado. Sólo contiene siete campos (en comparación con los 13 de IPv4). Este cambio permite a los enrutadores procesar los paquetes con más rapidez y, por ende, mejora la velocidad de transmisión real y el retardo.

La mayor parte de los sistemas operativos, desde el año 2001 aproximadamente, tienen algún tipo de soporte de IPv6. Es cierto, que en algunos casos, inicialmente no se trataba de un soporte “comercial”, sino versiones de prueba, aunque se incorporaban a sistemas operativos de “producción”. Cada vez es más frecuente que diversas plataformas o sistemas operativos, no solo incorporen IPv6, sino que además sea activado por defecto por el fabricante, sin requerir intervención alguna por parte del usuario.

En Linux, IPv6 esta soportado a partir de versión del kernel 2.4.x. Para comprobar si esta instalado:

```
$ test -f /proc/net/if_inet6 && echo "Kernel actual soporta IPv6"
```

Para instalar el módulo IPv6:

```
$ modprobe ipv6
```

Se puede comprobar el módulo con:

```
$ lsmod |grep -w 'ipv6' && echo "modulo IPv6 cargado"
```

También se puede configurar la Carga/descarga automática del modulo (/etc/modules.conf o /etc/conf.modules):

```
$ nano /etc/modules.conf
```

alias net-pf-10 ipv6 #habilita carga bajo demanda alias net-pf-10 off #deshabilita carga bajo demanda

Se puede realizar la configuración permanente, por ejemplo, para Debian: Con el módulo IPv6 cargado se edita /etc/network/interfaces

iface eth0 inet6 static pre-up modprobe ipv6

address 2001:DB8:1234:5::1:1

Elimina completamente la autoconfiguración:

up echo 0 > /proc/sys/net/ipv6/conf/all/autoconf netmask 64

El encaminador esta autoconfigurado y no tiene dirección fija.

Se encuentra gracias a

(/proc/sys/net/ipv6/conf/all/accept_ra).

Si no habrá que configurar el GW:

gateway 2001:DB8:1234:5::1

Se reinicia o:

```
$ ifup --force eth0
```

Máscara de red

Las direcciones IP tienen asociada una mascara de red. Esta máscara es de 32 bits, los bits 1 indican la porción de red y los bits 0 indican la porción de host.

Aplicando una máscara de subred (también llamada máscara de red, o simplemente netmask, en inglés) se puede especificar tanto al anfitrión (host), como a la red a la que

pertenece. Tradicionalmente, las máscaras de subred se expresan utilizando formas decimales separadas por puntos, a la manera de una dirección IP. Por ejemplo, 255.255.255.0 sería una máscara común. Las máscaras de subred se expresan más sucintamente utilizando notación CIDR, la que simplemente enumera la cantidad de bits en la máscara después de la barra ascendente (/). De esta manera, 225.225.225.0 puede simplificarse en /24.

Supongamos que tenemos un rango de direcciones IP desde 10.0.0.0 hasta 10.255.255.255. Si todas ellas formaran parte de la misma red, su máscara de red sería: 255.0.0.0. Que también se podría expresar como: 10.0.0.0/8.

Máscara de red para direcciones IP clase A: 255.0.0.0 Máscara de red para direcciones IP clase B: 255.255.0.0 Máscara de red para direcciones IP clase C: 255.255.255.0

Una máscara de red representada en binario son 4 octetos de bits (11111111.11111111.11111111.11111111). La representación utilizada se define colocando en 1 todos los bits de red (máscara natural) y en el caso de subredes, se coloca en 1 los bits de red y 0 los bits de host usados por las subredes. Así, en esta forma de representación (10.0.0.0/8) el 8 sería la cantidad de bits puestos a 1 que contiene la máscara en binario, comenzando desde la izquierda. Para el ejemplo dado (/8), sería 11111111.00000000.00000000.00000000 y en su representación en decimal sería 255.0.0.0.

Una máscara de subred determina el tamaño de una red dada. Al usar una máscara de red /24, hay 8 bits reservados para anfitriones: (32 bits en total—24 bits de máscara de red = 8 bits para anfitriones). Esto permite hasta 256 direcciones de anfitrión (2 8 = 256). Por convención, el primer valor se toma como la dirección de la red (.0 ó 00000000), y el último se toma como la dirección de difusión (.255 ó 11111111). Esto deja 254 direcciones libres para anfitriones en esta red.

Las máscaras de subred funcionan aplicando lógica AND al número IP de 32 bits. En notación binaria, los bits “1” de la máscara indican la porción de la dirección de red, y los “0”, la porción de la dirección del anfitrión. Un AND lógico se efectúa comparando los dos bits. El resultado es “1” si los dos bits comparados son también “1”. De lo contrario, el resultado es “0”. A continuación exponemos todos los resultados posibles de la operación AND binaria entre dos bits.

Subredes

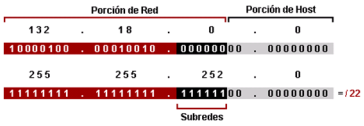
Para evitar conflictos, los números de red se administran a través de una corporación sin fines de lucro llamada ICANN (Corporación de Internet para la Asignación de Nombres y Números, del inglés. Internet Corporation for Assigned Names and Numbers). Esta corporación ha delegado partes de este espacio de direcciones a varias autoridades regionales, las cuales reparten las direcciones IP a los ISP y otras compañías. Éste es el proceso por el cual se asigna un bloque de direcciones IP a una compañía. La solución es dividir el bloque de direcciones en varias partes para uso interno en forma de múltiples redes, pero actuar como una sola red para el mundo exterior. A estas partes de la red se les llama subredes.

Las subredes se introdujeron para asignar de manera flexible bloques de direcciones dentro de una organización.

Cuando llega un paquete, el enrutador analiza su dirección de destino y verifica a qué subred pertenece. Para ello, el enrutador aplica un AND a la dirección del destino con la máscara para cada subred y verifica que el resultado sea el prefijo correspondiente.

En el caso más simple, se puede dividir una red en subredes de tamaño fijo (todas las subredes tienen el mismo tamaño). Sin embargo, por la escasez de direcciones IP, hoy en día frecuentemente se usan subredes de tamaño variable.

La conexión en subredes permite crear múltiples redes lógicas que existen dentro de una red única Clase A, B o C. Si no crea una subred, solamente se podrá utilizar una red de la red de Clase A, B o C, lo que es poco realista. Cada link de datos de una red debe tener una identificación de red única, siendo cada nodo de ese link miembro de la misma red. Si se divide una red principal (clase A, B, o C) en subredes menores, se podrá crear una red de subredes interconectadas. Cada link de datos de esta red tendrá entonces una identificación única de red/subred. Cualquier dispositivo o gateway, que conecte n redes/subredes tendrá n direcciones IP distintas, una por cada red/subred que interconecte. Para crear subredes en una red, amplíe la máscara natural usando algunos de los bits de la parte de identificación de host de la dirección para crear una identificación de subred.



CIDR

Classless Interdomain Routing (CIDR) se presentó para mejorar tanto la utilización del espacio de direcciones como la escalabilidad de ruteo en Internet. Era necesario debido al rápido crecimiento de Internet y al crecimiento de las tablas de ruteo IP contenidas en los routers de Internet.

CIDR se aparta de las clases IP tradicionales (Clase A, Clase B, Clase C y así sucesivamente). En CIDR, una red IP se representa mediante un prefijo, que es una dirección IP y alguna indicación de la longitud de la máscara. Por longitud se entiende el número de bits de máscara contiguos del extremo izquierdo que están establecidos en uno. Por lo tanto, la red 172.16.0.0 255.255.0.0 se puede representar como 172.16.0.0/16. CIDR también representa una arquitectura de Internet más jerárquica, donde cada dominio toma sus direcciones IP de un nivel superior. Permite que se realice el resumen de los dominios al nivel más alto.

NAT: Traducción de Dirección de Red

A esta altura, hemos leído varias veces que las direcciones IP son escasas, y es que con IPv4 lo son. Un ISP podría tener una dirección con prefijo de /16, lo cual le da 65 534 números de host. Si tiene más clientes que esos, tiene un problema. Esta escasez ha conducido a técnicas para usar las direcciones IP con moderación. Un método es asignar dinámicamente una dirección IP a una computadora cuando ésta se encuentra encendida y usa la red, y tomar de vuelta la dirección IP cuando el host se vuelve inactivo. Así, la dirección IP se puede asignar a otra computadora que se active en ese momento.

El problema de quedarse sin direcciones IP no es uno teórico que podría ocurrir en cierto momento en un futuro distante. Está ocurriendo justo aquí y ahora. La solución a largo plazo es que toda la Internet migre a IPv6, que cuenta con direcciones de 128 bits. Esta transición está ocurriendo lentamente, pero pasarán años antes de que el proceso esté completo. Mientras tanto, para sobrevivir se requería una solución rápida. Esta solución, que se utiliza ampliamente en la actualidad, se conoce como NAT (Traducción de Dirección de Red, del inglés Network Address Translation).

La idea básica detrás de NAT es que el ISP asigne a cada hogar o negocio una sola dirección IP (o a lo más, una pequeña cantidad de éstas) para el tráfico de Internet. Dentro de la red del cliente, cada computadora obtiene una dirección IP única, la cual se utiliza para enrutar el tráfico interno. Sin embargo, justo antes de que un paquete salga de la red del cliente y vaya al ISP, la dirección IP única interna se traduce a la dirección IP pública compartida. Esta traducción hace uso de los tres rangos de direcciones IP que se han declarado como privados. Las redes pueden utilizarlos de manera interna como deseen. La única regla es que no pueden aparecer paquetes que contengan estas mismas direcciones en Internet.

Los tres rangos reservados son:

- 10.0.0.0 - 10.255.255.255/8 - (16,777,216 hosts)
- 172.16.0.0 - 172.31.255.255/12 - (1,048,576 hosts)
- 192.168.0.0 - 192.168.255.255/16 - (65,536 hosts)

Dentro de las premisas del cliente, cada máquina tiene una dirección única de la forma 10.x.y.z. Sin embargo, antes de que un paquete salga de las premisas del cliente, pasa a través de una caja NAT que convierte la dirección IP de origen interna, a la dirección IP verdadera del cliente. A menudo, la caja NAT se combina en un solo dispositivo con un firewall (corta fuegos) que proporciona seguridad controlando cuidadosamente lo que entra y sale por la red de la compañía. También es posible integrar la caja NAT en un enrutador o módem ADSL.

Para contactar con los anfitriones en la Internet, las direcciones ip deben convertirse en direcciones IP globales, enrutables. Esto se logra por medio de la técnica que estamos describiendo, Traducción de Direcciones de Red Network Address Translation, o NAT.

Un dispositivo NAT es un enrutador que manipula las direcciones de paquetes en lugar de simplemente remitirlas. En un enrutador NAT, la conexión a Internet usa una (o más) direcciones IP enrutadas globalmente, mientras que la red privada usa una dirección IP del rango de las direcciones privadas del RFC1918. El enrutador NAT permite que la/las direcciones IP sean compartidas con todos los usuarios internos, que usan todos direcciones privadas. Convierte los paquetes desde una forma de direcciones a otra, a medida que los paquetes se transmiten. Desde la perspectiva de los usuarios, estos van a estar directamente conectados a Internet sin necesidad de software o drivers especiales. Simplemente usan el enrutador NAT como la pasarela por defecto, y direccionan los paquetes, como lo harían normalmente. El enrutador NAT traduce los paquetes dirigidos hacia afuera para que puedan usar las direcciones IP globales a medida que salen de la red, y los vuelve a traducir cuando se reciben desde Internet.

Direcciones Privadas y Públicas

La estabilidad de la Internet depende de forma directa de la exclusividad de las direcciones de red utilizadas públicamente. Las direcciones IP repetidas hacen que el router no pueda realizar su trabajo de seleccionar la mejor ruta. Es necesario que cada dispositivo de la red tenga una dirección exclusiva. Hizo falta un procedimiento para asegurar que las direcciones fueran, de hecho, exclusivas. En un principio, una organización conocida como el Centro de información de la red Internet (InterNIC) manejaba este procedimiento. InterNIC ya no existe y la Agencia de asignación de números de Internet (IANA) la ha sucedido. IANA administra, cuidadosamente, la provisión restante de las direcciones IP para garantizar que no se genere una repetición de direcciones utilizadas de forma pública. La repetición suele causar inestabilidad en la Internet y compromete su capacidad para entregar datagramas a las redes.

Direcciones IP Públicas

Dirección IP pública identifica el equipo en internet. Es única, no se puede repetir. Las direcciones IP públicas son exclusivas. Dos máquinas que se conectan a una red pública nunca pueden tener la misma dirección IP porque las direcciones IP públicas son globales y están estandarizadas. Todas las máquinas que se conectan a la Internet acuerdan adaptarse al sistema. Hay que obtener las direcciones IP públicas de un proveedor de servicios de Internet (ISP) o un registro, a un costo. Con el rápido crecimiento de Internet, las direcciones IP públicas comenzaron a escasear.

Direcciones IP Privadas

Las direcciones IP privadas son una solución al problema del agotamiento de las direcciones IP públicas. Como ya se ha mencionado, las redes públicas requieren que los hosts tengan direcciones IP únicas. Sin embargo, las redes privadas que no están conectadas a la Internet pueden utilizar cualquier dirección de host, siempre que cada host dentro de la red privada sea exclusivo. Existen muchas redes privadas junto con las redes públicas.

El RFC 1918 asigna tres bloques de la dirección IP para uso interno y privado. Estos tres bloques consisten en una dirección de Clase A, un rango de direcciones de Clase B y un rango de direcciones de Clase C. Las direcciones que se encuentran en estos rangos no se enrutan hacia el backbone de la Internet. Los routers de Internet descartan inmediatamente las direcciones privadas. Si se produce un direccionamiento hacia una intranet que no es pública, un laboratorio de prueba o una red doméstica, es posible utilizar las direcciones privadas en lugar de direcciones exclusivas a nivel global. La conexión de una red que utiliza direcciones privadas a la Internet requiere que las direcciones privadas se conviertan a direcciones públicas. Este proceso de conversión se conoce como Traducción de direcciones de red (NAT). En general, un router es el dispositivo que realiza NAT, como mencionamos previamente.

Existen ciertas direcciones en cada clase de dirección IP que no están asignadas y que se denominan direcciones privadas. Las direcciones privadas pueden ser utilizadas por los hosts que usan traducción de dirección de red (NAT) para conectarse a una red pública o por los hosts que no se conectan a Internet. En una misma red no pueden existir dos direcciones

iguales, pero sí se pueden repetir en dos redes privadas que no tengan conexión entre sí o que se conecten mediante el protocolo NAT. Las direcciones privadas son:

- Clase A: 10.0.0.0 a 10.255.255.255 (8 bits red, 24 bits hosts).
- Clase B: 172.16.0.0 a 172.31.255.255 (16 bits red, 16 bits hosts). 16 redes clase B contiguas, uso en universidades y grandes compañías.
- Clase C: 192.168.0.0 a 192.168.255.255 (24 bits red, 8 bits hosts). 256 redes clase C continuas, uso de compañías medias y pequeñas además de pequeños proveedores de internet ISP).

Muchas aplicaciones requieren conectividad dentro de una sola red, y no necesitan conectividad externa. En las redes de gran tamaño a menudo se usa TCP/IP. Las direcciones privadas se pueden utilizar junto con un servidor de traducción de direcciones de red (NAT) para suministrar conectividad a todos los hosts de una red que tiene relativamente pocas direcciones públicas disponibles. Según lo acordado, cualquier tráfico que posea una dirección destino dentro de uno de los intervalos de direcciones privadas no se enrutará a través de Internet.

Es muy probable, que la computadora o dispositivo que esten utilizando para descargar el apunte que estan leyendo ahora mismo, tenga una dirección privada. Al final de esta unidad veremos como identificar la dirección ip que tiene la máquina que estas utilizando.

Asignación IP Estático y Dinámico

La asignación de direcciones IP privadas en una organización se puede realizar de manera estática o dinámica.

Asignación Estática

La asignación estática funciona mejor en las redes pequeñas con poca frecuencia de cambios. De forma manual, el administrador del sistema asigna y rastrea las direcciones IP para cada computador, impresora o servidor de una red interna. Es fundamental llevar un buen registro para evitar que se produzcan problemas con las direcciones IP repetidas. Esto es posible sólo cuando hay una pequeña cantidad de dispositivos que rastrear.

Es muy común que los servidores reciban una dirección IP estática de modo que las estaciones de trabajo y otros dispositivos siempre sepan cómo acceder a los servicios requeridos. Otros dispositivos que suelen recibir direcciones IP estáticas son las impresoras en red, servidores de aplicaciones y routers.

Asignación Dinámica

La asignación dinámica de direcciones ip, se realiza a través del protocolo DHCP (Protocolo de configuración dinámica del host), este permite que un host obtenga la dirección IP de forma dinámica sin que el administrador de red tenga que configurar un perfil individual para cada dispositivo.

Con DHCP, cada red debe tener un servidor DHCP responsable de la configuración. Al iniciar una computadora, ésta tiene integrada una dirección Ethernet u otro tipo de dirección de capa de enlace de datos en la NIC o placa de red, pero no cuenta con una dirección IP. Si

la PC está configurada para recibir la dirección IP de manera dinámica, esta difunde una solicitud de una dirección IP en su red. Para ello usa un paquete llamado DHCP DISCOVER. Este paquete debe llegar al servidor DHCP. Si el servidor no está conectado directamente a la red, el enrutador se configurará para recibir difusiones DHCP y transmitirlas al servidor DHCP en donde quiera que se encuentre.

Cuando el servidor recibe la solicitud, asigna una dirección IP libre y la envía al host en un paquete DHCP OFFER (que también se puede transmitir por medio del enrutador). Para que esto pueda funcionar incluso cuando los hosts no tienen direcciones IP, el servidor identifica a un host mediante su dirección Ethernet (la cual se transporta en el paquete DHCP DISCOVER).

Un problema que surge con la asignación automática de direcciones IP de una reserva es determinar qué tanto tiempo se debe asignar una dirección IP. Si un host sale de la red y no devuelve su dirección IP al servidor DHCP, esa dirección se perderá en forma permanente. Después de un tiempo, tal vez se pierdan muchas direcciones. Para evitar que eso ocurra, la asignación de direcciones IP puede ser por un periodo fijo de tiempo, una técnica conocida como arrendamiento. Justo antes de que expire el arrendamiento, el host debe pedir una renovación al DHCP. Si no puede hacer una solicitud o si ésta se rechaza, tal vez el host ya no pueda usar la dirección IP que recibió antes.

Algunos ejemplos comunes de la información que se configura incluyen la máscara de red, la dirección IP de la puerta de enlace predeterminada y las direcciones IP de los servidores DNS y de tiempo.

Protocolo ARP

Para que dos host se comuniquen en una red local, deben conocer las direcciones MAC respectivas. Es posible configurar manualmente cada anfitrión con una tabla de mapeo desde una dirección IP a una dirección MAC, pero normalmente el Protocolo de Resolución de Direcciones (ARP, en inglés) se usa para determinar esto de manera automática. Cuando se usa ARP, el anfitrión transmite a los otros anfitriones la pregunta: “¿Quién tiene la dirección MAC para una determinada IP ?” Cuando el anfitrión que tiene dicha dirección IP ve una solicitud ARP de su propia dirección IP, le responde con su dirección MAC.

Direcciones MAC

Repasando, la dirección MAC (siglas en inglés de media access control; en español "control de acceso al medio") es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo. Está determinada y configurada por el IEEE (los primeros 24 bits) y el fabricante (los últimos 24 bits) utilizando el organizationally unique identifier.

Lecturas recomendadas de la unidad 4:

- Redes de Computadoras. Tanenbaum. Capítulo 5.6.2 "Direcciones IP".
- Redes Inalámbricas para países en desarrollo. Capitulo 3. pags 46 a 49.

Bibliografia

- Redes de Computadoras. Andrew S. Tanenbaum, David J. Wetherall. Capítulo 4.
- https://es.wikipedia.org/wiki/Direcci%C3%B3n_IP
- https://es.wikipedia.org/wiki/M%C3%A1scara_de_red
- https://es.wikipedia.org/wiki/Subred