Direcciones IP y su asignación

Por MsC. Marcos Antonio Pérez García, Especialista en Telemática, Gerencia de Coordinación y Control, DDAR, ETECSA
marcos.perez@etecsa.cu

Introducción

En la planificación, desarrollo y dimensionamiento de las redes a paquetes basadas en el Protocolo Internet (IP) es esencial el conocimiento de los conceptos básicos del protocolo que la sustenta. Así, mediante la comparación de los dos protocolos fundamentales que en la actualidad se aplican o están en fase de aplicación a nivel mundial —el Protocolo Internet versión 4 (IPv4) y el Protocolo Internet versión 6 (IPv6)—, este trabajo expone aspectos medulares para su comprensión.

Se explica, también, la forma en que, a escala global, se asignan las direcciones IP, los organismos internacionales que intervienen en el proceso y, por último, se introducen brevemente algunos conceptos relacionados con el gobierno de Internet.

Protocolos de Internet, IPvX

La Internet es la red mundial de computadoras no relacionadas que sólo pueden comunicarse de forma apropiada si se atienen a un conjunto de reglas o protocolos. Es de suponer que lo más básico en Internet son las direcciones del Protocolo Internet o IP.

Las direcciones IP se refieren a un único número que se le asigna a cada computadora conectada a la Internet. Al número IP se le denomina "dirección" porque tiene los mismos propósitos de las direcciones de una casa o edificio, es decir, permite que cada computadora en Internet sea localizada por un esquema numérico.

Por lo general, los abonados de los Proveedores de Servicios de Internet o ISP —del inglés, *Internet Service Provider*— se encuentran familiarizados con el uso de dirección IP. Sin embargo, no es así con los conceptos de direcciones estáticas y direcciones dinámicas. En realidad, para brindar conexión a la Internet global, cada ISP tiene un único diapasón de direcciones IP disponibles por lo que cuando se inicia una conexión, se asigna automáticamente una dirección IP dinámica que persiste mientras dure esta.

Las direcciones IP también se clasifican en públicas y privadas. Las primeras son necesarias para la conexión de una computadora a la Internet Global, las segundas sirven para identificar los dispositivos en una red, por ejemplo, privada o LAN —del inglés, *Local Area Network*—. Se requiere de un dispositivo conversor de direcciones o NAT —*Net-*

work Address Translation— para que un dispositivo de la LAN con dirección privada tenga acceso a la Internet.

A los efectos de este artículo se han agrupado los protocolos IP bajo el genérico de IPvX —Protocolo de Internet versión "X"— aunque sólo se analizan los dos que, en estos momentos, se emplean a escala mundial: el IPv4 —ampliamente extendido— y el IPv6 —en desarrollo—; el IPv5 fue un protocolo que se desarrolló para soportar fundamentalmente video y audio.

Las direcciones IPv4 tienen 32 bits agrupados en 4 grupos de 8 bits, por lo que el conjunto global se extiende desde la dirección 0.0.0.0 a la 255.255.255.255. En teoría habría un espacio de 4.294, 967,296 direcciones. En un inicio se pensó que esto era más que suficiente, sin embargo, las direcciones se asignan en bloques o subredes y todas ellas se consideran ya ocupadas —se usen o no—, además en un principio se asignaron con mucha facilidad las clases "A" y "B".

El IPv6, también conocido como IPng —del inglés, *Next Generation Internet Protocol*—, es la nueva versión del protocolo IP y fue diseñado por la IETF —del inglés, *Internet Engineering Task Force*— para reemplazar, de forma gradual, la versión actual del IPv4. En esta versión se mantuvieron las funciones del IPv4 que son utilizadas, mientras que las que no son utilizadas o se usan con poca frecuencia, se quitaron o se hicieron opcionales, agregándosele nuevas características.

El motivo básico para crear el IPv6 fue la posibilidad de falta de direcciones del IPv4. Esta previsión se desarrolló fundamentalmente a partir del 2001, en que comenzaron a circular comentarios advirtiendo que la tecnología inalámbrica —que incluye aplicaciones domésticas como los refrigeradores inteligentes— agotarían el espacio de direcciones que suministra el IPv4, en particular en regiones como Europa y Asia que tenían asignadas una cantidad de direcciones relativamente pequeña. Así, mientras que, en el año 2002, en los Estados Unidos existían en operación más de 3 x 10^9, en China y Corea tenían asignadas 38, 527,000 y 23, 559,000 direcciones respectivamente con una población significativamente mayor.

Esta realidad impulsó el desarrollo y la expansión del IPv6 que, con un espacio de direcciones de 128 bits, ofrece un aumento en capacidad de unos 25,000 trillones de trillones en comparación con el IPv4 que, con un espacio de direcciones de 32 bits, ofrece una capacidad de unos 4,3 billones de direcciones de las cuales, según la ICANN —*Internet Corporation for Assigned Names and Numbers*—, dos tercios de las mismas ya están asignadas. Se pronostica que ambos protocolos funcionen en paralelo por unos 20 años.

Se supone que con tal abundancia de direcciones provista por el IPv6 pueda eliminarse el NAT que, irónicamente, permitió "ocultar" detrás de una simple dirección IP múltiples dispositivos. Otros dos aspectos relevantes del IPv6 apuntan, por un lado, que fue específicamente diseñado teniendo en cuenta los dispositivos móviles: la movilidad se implementa en un protocolo especial denominado IP Móvil, que permite *roaming* entre redes diferentes sin perder la dirección IP establecida; y, por otro lado, que tiene un mayor grado de seguridad intrínseco que se logra mediante un protocolo especial denominado IPsec, que permite autenticación, encriptación y compresión.

Protocolo IPv4 y su direccionamiento

Cuando se desarrolló el protocolo se creó lo que se conoce como jerarquía de dirección de dos niveles (Figura 1), una parte del campo de

dirección de 32 bits identifica la red —prefijo de la red— y la otra los terminales que son residentes de esa red.

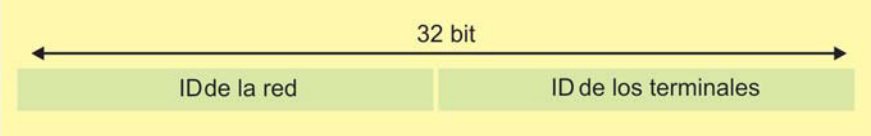

Figura 1 Jerarquía de dirección de dos niveles del IPv4

Nótese que todos los terminales de una red comparten el mismo prefijo pero tienen una dirección diferente, mientras que *terminales* de redes diferentes pueden tener la misma dirección pero prefijos de red distintos.

Con el propósito de proveer la flexibilidad necesaria para la expansión de redes de diferentes tamaños, los diseñadores de Internet decidieron que el espacio de direcciones IP debe ser dividido en tres clases de direcciones: clase A, clase B y clase C. Cada clase tiene su **frontera** en diferentes lugares de la dirección de 32 bits, entre el prefijo de red y el ID del terminal (Figura 2).

Uno de los aspectos fundamentales de la división en clases es que cada dirección contiene un código que identifica el punto en que se dividen el prefijo de red y las ID de los terminales. Por ejemplo, si los primeros dos bits de una dirección IP es 10, el punto de división cae entre los bits 15 y 16. Esto simplificó, al principio de Internet, los sistemas de encaminamiento pues en su comienzo los protocolos de encaminamiento no suministraban la **máscara** con la cual cada *router* identifica el largo del prefijo de red.

Redes clase A (prefijo /8)

Cada clase A tiene un prefijo de red de 8 bits con el bit más significativo con el valor 0 lo que deja 7 bits para el número de las redes, seguido de 24 bits para el número de los terminales. A la clase A también se le llama /8 por el número de bits de su prefijo.

La clase A define hasta un máximo de 126 redes. A los cálculos (2^8) se le sustrae 2 por que la 0.0.0.0 se le reserva como ruta por omisión (*default*) y a la 127.0.0.0 se le reserva para la función de realimentación interna —*internal loopback*—.

En cuanto al número de terminales la clase A tiene un máximo de 16,777,214 terminales por red, pues a los cálculos se le sustrae 2 debido a que todos 0 es la **propia red** y todos 1 es para **difusión** (*broadcast*).

Como la clase A contiene 2^{31} (2,147,483,648) direcciones individuales y el espacio de direcciones total del protocolo IPv4 contiene un máximo de 2^{32} (4,294,967,296) direcciones, el espacio de direcciones /8 contiene el 50 % del total de direcciones *unicast* del espacio de direcciones IPv4.

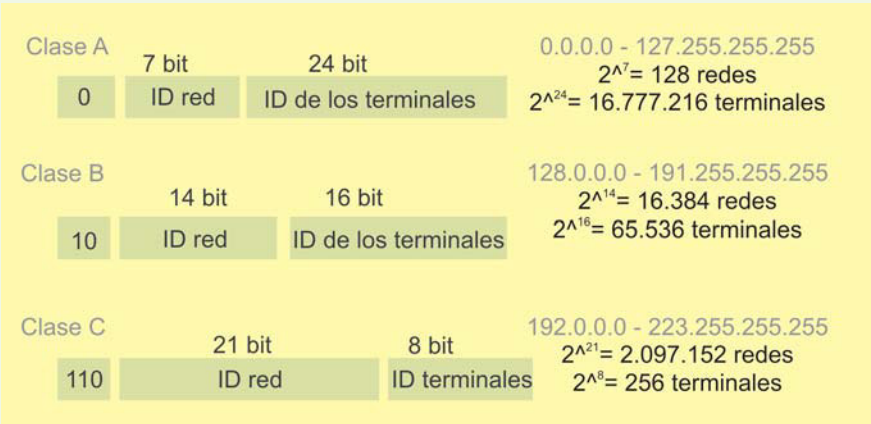

Figura 2 Principales formatos de las direcciones IP

Redes clase B (prefijo /16)

Cada clase B tiene un prefijo de red de 16 bits con los dos bits más significativos con el valor 1-0, lo que deja 14 bits para el número de las redes, seguido de 16 bits para el número de los terminales. A la clase B también se le llama /16 por el número de bits de su prefijo.

Con la clase B se pueden definir hasta un máximo de 16,384 redes y 65,534 terminales por red. El bloque entero de direcciones /16 contiene 2^{30} (1,073,741,824) direcciones y representa el 25 % del total del espacio de direcciones *unicast* del IPv4.

Redes clase C (prefijo /24)

Cada clase C tiene un prefijo de red de 24 bits con los tres bits más significativos con el valor 1-1-0, lo que deja 21 bits para el número de las redes, seguido de 8 bits para el número de terminales. A la clase C también se le llama /24 por el número de bits de su prefijo.

Notación decimal de las direcciones Internet IPv4

Para hacer más sencilla la lectura de las direcciones Internet IPv4 se desarrolló la notación en cuatro números decimales, cada uno separado por un punto. En esta notación se divide el espacio de direcciones en cuatro campos, cada uno especificado de forma independiente como un número decimal separado por puntos. La figura 3 muestra una típica dirección clase B con la notación decimal separada por puntos.

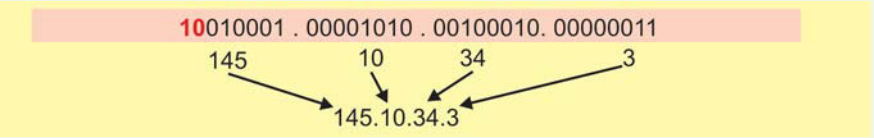

Figura 3 Notación decimal de direcciones IPv4

La tabla 1 muestra los intervalos de los valores decimales separados por puntos que pueden ser asignados a cada una de las tres principales clases del IPv4. La notación xxx representa el campo de número de direcciones de terminales que pueden ser asignadas por el administrador de la red local.

Clase	Intervalo en notación decimal
A (prefijo /8)	1.xxx.xxx.xxx hasta la 126.xxx.xxx.xxx
B (prefijo /16)	128.0.xxx.xxx hasta la 191.255.xxx.xxx
C (prefijo /24)	192.0.0.xxx hasta la 223.255.255.xxx

Tabla 1 Intervalo de direcciones de cada clase en notación decimal

Direcciones reservadas

Del espacio de direcciones de la IPv4, la IANA —*Internet Assigned Number Authority*— no asignará las siguientes direcciones:

Clase A	10.0.0.0 – 10.255.255.255
Clase B	172.16.0.0 – 172.31.255.255
Clase C	192.168.0.0 – 192.168.255.255

Se recomienda utilizar estas direcciones para las redes IP privadas. Las direcciones privadas se quedan en la red privada y no se traspasan o encaminan hacia la Web, es decir, a Internet, pues los *routers* que cumplan con la recomendación RFC 1918, cuando reciben una dirección privada en el encabezamiento de los paquetes, las descarta incluso sin acudir a las tablas de encaminamiento.

Subredes

La IETF, mediante la RFC 950, definió una norma para subdividir las clases A, B y C en lo que se llamó la creación de subredes (*subnetting*). El procedimiento fue creado para superar algunos de los problemas que estaba experimentando el direccionado jerárquico de dos niveles. Por ejemplo el crecimiento considerable de las tablas de encaminamiento de Internet, así como la petición de una nueva dirección de red para la instalación de redes adicionales dentro de una organización.

Para aminorar ambos problemas se creó un nuevo nivel jerárquico en la estructura del direccionamiento IP. Con la adición del nuevo nivel es posible crear subredes dentro de una misma red. La figura 4 ilustra el concepto básico de subred que consiste en dividir el campo de las direcciones de los terminales en dos partes: la del número de subredes y la del número de terminales.

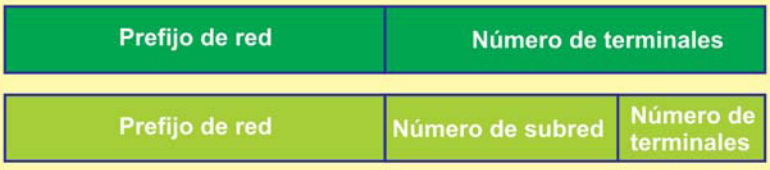

Figura 4 Comparación entre las jerarquías de dos y tres niveles

Con la estructura de subred se garantiza que su estructura nunca sea visible desde el exterior de la organización interna de la red. El encaminamiento de Internet a cualquier subred de una dirección IP es el mismo, no importa cual sea la subred en la que se encuentre el terminal de destino. Esto es posible debido a que todas las subredes de una red dada usan el mismo prefijo de la red, pero con números diferentes de subred.

En realidad los *routers* internos de la red necesitan diferenciar entre las subredes no así los *routers* de Internet, debido a que todas las subredes de una organización se encuentran comprendidas en una sola entrada de la tabla de encaminamiento. Esto permite al administrador de una red establecer cualquier estructura interna de la red de su organización sin comprometer el tamaño de las tablas de encaminamiento de Internet. Además posibilita a las organizaciones expandir nuevas subredes sin tener que obtener nuevas direcciones de Internet.

La figura 5 muestra la estructura de una red con varias subredes utilizando el concepto de direccionamiento de subred para una dirección

Figura 5 Varias subredes usando una sola dirección clase B (/16)

de red de clase B (/16). El *router* acepta todo el tráfico de la dirección Internet de la red 130.5.0.0, y dirige el tráfico hacia las subredes definidas por el tercer octeto del direccionamiento.

Prefijo de red extendido

Los *routers* de Internet usan solo el **prefijo de red** como dirección de destino para encaminar el tráfico hacia una organización. Por su parte los *routers* dentro de la organización usan el **prefijo de red extendido** para encaminar el tráfico interno. El prefijo de red extendido está compuesto del prefijo de red más el número de subred.

Para identificar el prefijo de red extendido se utiliza la **máscara de subred**. Por ejemplo, si un administrador dispone de un /16 con dirección 130.5.0.0 y quiere utilizar todo el tercer octeto para representar el número de subred, debe especificar una máscara de subred 255.255.255.0. Los bits en la máscara se establecen en 0 si el sistema debe identificar esos bits como parte del número de terminal (Figura 6).

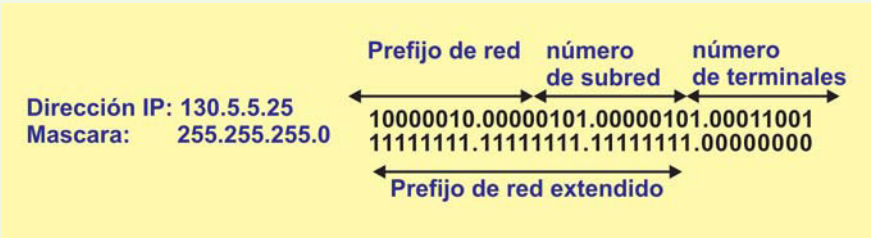

Figura 6 Máscara de subred

Ninguno de los protocolos estándar de encaminamiento de Internet contiene un campo de un byte en el encabezamiento conteniendo el número de bits del prefijo de red extendido.

Consideraciones para el diseño de las subredes

Para desplegar un plan de direccionamiento de una organización requiere de una planificación cuidadosa. Por lo tanto, deben tenerse en cuenta varias preguntas claves: ¿cuántas subredes se necesitan ahora?, ¿cuántas subredes se necesitarán en el futuro?, ¿cuántos terminales se encuentran en la mayor de las redes hoy? Y ¿cuántos terminales necesitará la mayor de las subredes en el futuro?

El **primer paso** en el proceso de planificación es ver el máximo número de subredes requerido y redondearlo a la potencia de dos más cercana. Por ejemplo, si la organización requiere de nueve subredes 2^3 (u 8) no dan un espacio de direcciones suficiente para las subredes, por lo tanto, el administrador necesita redondear a 2^4 (ó 16).

Mejor aún es prever el crecimiento, de ese modo, si se requieren hoy 14 subredes, 16 pueden no ser suficientes en los próximos años cuando se necesite agregar la subred 17. En este caso es conveniente seleccionar 2^5 (ó 32) como el máximo número de subredes.

El **segundo paso** es asegurar que exista suficiente espacio de direcciones para los terminales para la mayor de las subredes de la organización. Si la subred mayor necesita 50 direcciones de terminales hoy, 2^5 (ó 32) no suplirá suficiente espacio de direcciones por lo que el administrador de la red necesitará redondear a 2^6 (ó 64).

El **paso final** es asegurar que la asignación de direcciones de la organización provea suficientes bits para desplegar el plan de direccionamiento de las subredes. Por ejemplo, si a la organización se le

ha asignado un simple /16, puede fácilmente expandir 4 bits para cada número de subred y 6 bits para cada número de terminal. Sin embargo, si lo que tiene disponible son varias /24 y se necesitan desarrollar nueve subredes, entonces, habría que —usando 2 bits— "definir cuatro subredes en" cada uno de sus /24 y construir la red combinando las subredes en tres /24 números de redes.

Una solución alternativa sería emplear, para la conectividad interna, los números de redes del espacio de direcciones privadas previstos por la IETF y usar un NAT para el acceso externo a Internet. Es de notar lo laborioso y complejo de conformar un plan de direcciones IP para la red de una organización. Esta complejidad se multiplicaría considerablemente para una red de telecomunicaciones basada en el protocolo IP.

A modo de ejemplo, se considerará que se le ha asignado a una organización el número de red 193.1.1.0/24 y que se necesitan definir seis subredes de las cuales la mayor requiere de 25 terminales:

El primer paso es definir la máscara de subred para determinar el número de bits requerido para definir las seis subredes. Debido a que las direcciones de las redes sólo pueden ser divididas en subredes empleando números binarios, estas deben ser creadas en bloques de potencia de dos: 2 (2^1), 4 (2^2), 8 (2^3), etc. En consecuencia, es imposible definir un bloque de direcciones IP que contenga exactamente seis subredes. En este caso, debería definirse un bloque de 8 (2^3) quedando dos direcciones de subredes para un crecimiento futuro.

Para 8 direcciones se requieren de tres bits para su enumeración. Como en este ejemplo la organización tiene que dividir en subredes un /24 se necesitarán tres bits más, o sea, un prefijo de red extendido de un /27. Un prefijo de red extendido /27 puede ser expresado utilizando la notación decimal mediante 255.255.255.224 (Figura 7).

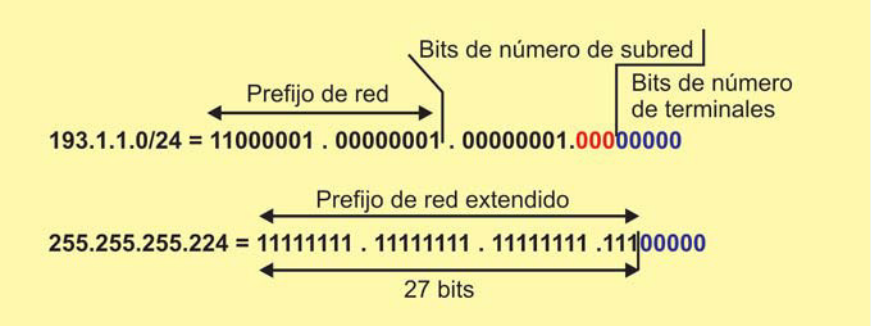

Figura 7 Definición de la máscara de subred/largo de prefijo extendido

El prefijo de red extendido de 27 bits deja 5 bits para definir las direcciones de terminales para cada subred. Esto significa que cada subred con un prefijo de 27 bits representa un bloque contiguo de 2^5 (32) direcciones IP individuales. Pero recordando que no se pueden usar las direcciones con todo en 0 ni con todo en 1, existen 30 ($2^5 - 2$) direcciones de terminales asignadas para cada subred.

La figura 8 representa los números de las ocho subredes del ejemplo. La porción subrayada de cada dirección identifica el prefijo de red extendido, la porción en rojo identifica los 3 bits que representan el campo de número de la subred.

Subred	Notación binaria	Notación decimal
Red básica asignada	11000001.00000001.00000001.00000000	193.1.1.0/24
Subred No. 0	11000001.00000001.00000001.000 00000	193.1.1.0/27
Subred No. 1	11000001.00000001.00000001 001 00000	193.1.1.32/27
Subred No. 2	11000001.00000001.00000001 010 00000	193.1.1.64/27
Subred No. 3	11000001.00000001.00000001 011 00000	193.1.1.96/27
Subred No. 4	11000001.00000001.00000001 100 00000	193.1.1.128/27
Subred No. 5	11000001.00000001.00000001.101 00000	193.1.1.160/27
Subred No. 6	11000001.00000001.00000001.110 00000	193.1.1.192/27
Subred No. 7	11000001.00000001.00000001.111 00000	193.1.1.224/27

Figura 8 Representación de los números, en binario y decimal, de las ocho subredes

Protocolo IPv6 y su direccionamiento

Las direcciones en IPv6 son de 128 bits e identifican subredes individuales o conjuntos de estas y se clasifican en tres tipos:

Unicast: identifican a una sola interfaz de red. Un paquete enviado a una dirección *unicast* es entregado sólo a la interfaz identificada con dicha dirección.

Anycast: identifican a un conjunto de interfaces. Un paquete enviado a una dirección *anycast*, será entregado a alguna de las interfaces identificadas con la dirección del conjunto al cual pertenece esa dirección *anycas*t.

Multicast: identifican un grupo de interfaces. Cuando un paquete es enviado a una dirección *multicast* es entregado a todas las interfaces del grupo identificadas con esa dirección.

En IPv6 no existen direcciones *broadcast*, su funcionalidad ha sido mejorada por las direcciones *multicast*.

Representación de las direcciones en IPv6

La representación de las direcciones cambia enormemente y pasan de estar representadas por 4 octetos separados por puntos a estar divididas en grupos de 16 bits —representados como 4 dígitos hexadecimales— separados por el carácter dos puntos (:). El esquema usado de asignación es similar al explicado con anterioridad para el IPv4 —clases A, B y C—, pero con los bloques y la capacidad de división mucho mayor.

Existen tres formas de representar las direcciones IPv6 como cadena de texto:

- x:x:x:x:x:x:x:x donde cada x es el valor hexadecimal de 16 bits, de cada uno de los 8 campos que definen la dirección. No es necesario escribir los ceros a la izquierda de cada campo, pero al menos debe existir un número en cada campo.

Ejemplos:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

1080:0:0:0:8:800:200C:4174

- Como será común utilizar esquemas de direccionamiento con largas cadenas de bit 0, existe la posibilidad de usar sintácticamente el símbolo **::** para representarlos. El uso de **::** indica uno o más grupos de 16 bits de ceros. Dicho símbolo podrá ser representado una sola vez en cada dirección**.**

Ejemplos:

1080:0:0:0:8:800:200C:417A	dirección *unicast*
FF01:0:0:0:0:0:0:101	dirección *multicast*
0:0:0:0:0:0:0:1	*loopback address*
0:0:0:0:0:0:0:0	*unspecified address*

Que pueden ser representadas como:

1080::8:8:800:200C:417A	dirección *unicast*
FF01::101	dirección *multicast*
::1	*loopback address*
::	*unspecified address*

◆ Para escenarios con nodos IPv4 e IPv6 es posible utilizar la siguiente sintaxis:

x:x:x:x:x:x:d.d.d.d**,** donde **x** representa valores hexadecimales de las seis partes más significativas —de 16 bits cada una— que componen la dirección y las **d** son valores decimales de las 4 partes menos significativas —de 8 bits cada una—, de la representación estándar del formato de direcciones IPv4.

Ejemplos:

0:0:0:0:0:0:13.1.68.3

0:0:0:0:0:FFFF.129.144.52.38

O en la forma comprimida:

::13.1.68.3

::FFFF:129.144.52.38

Al igual que en IPv4 para que las direcciones sean más amigables se les ha dividido en dos partes: los bits que identifican la red y subred, y los bits que identifican la interfaz de los dispositivos, así en la representación

2001:638:A01:2::/64

los primeros 64 bits —más a la izquierda— de esta dirección se utilizan como la dirección de la red, y los últimos 64 bits —más a la derecha— se utilizan para identificar el dispositivo en la red. A los bits de la red se les denomina comúnmente **prefijo** y el prefijo en este ejemplo es de 64 bits. Los prefijos identificadores de subredes, *routers* e intervalos de direcciones IPv6 son expresados de forma análoga que la utilizada en IPv4, es decir, el esquema es similar lo único que los campos contienen más bits.

En IPv6 (Figura 9), lo común es que los proveedores asignen un /48, donde se fijan los primeros 48 bits, los 16 restantes para subredes —por lo tanto, 65,535 posibles subredes— y los 64 restantes para asignación de los dispositivos terminales.

Figura 9 Comparación entre el espacio de direcciones del IPv4 y de IPv6

Mecanismos de transición básicos

Los mecanismos de transición son un conjunto de mecanismos y protocolos implementados en terminales y *routers*, junto con algunas guías operativas de direccionamiento diseñadas para hacer la transición de Internet al IPv6 con la menor interrupción posible.

Existen dos mecanismos básicos:

1. *Dual Stack* que provee soporte completo para IPv4 e IPv6 en *terminales* y *routers*.

2. *Tunneling* que encapsula paquetes IPv6 dentro de encabezamientos (*headers*) IPv4 que son transportados a través de infraestructura de encaminamiento IPv4.

Estos mecanismos están diseñados para ser usados por terminales y *routers* IPv6 que necesitan interoperar con terminales IPv4 y utilizar infraestructuras de encaminamiento IPv4. No obstante, IPv6 también puede ser usado en escenarios donde no se requiere interoperabilidad con IPv4. Los nodos diseñados para esos ambientes no necesitan usar ni implementar estos mecanismos.

Asignación de las direcciones IP en el ámbito internacional

La IANA, entidad contratada por el Departamento de Defensa de los Estados Unidos, delega grandes bloques de direcciones y asigna responsabilidades a los Registros de Internet Regionales —*Regional Internet Registries* (RIR)—. En el sistema actual de administración las direcciones IP son concedidas de acuerdo con los principios bien conocidos de asignación, siempre que se demuestre la necesidad de nuevas direcciones.

La distribución de direcciones IP para el acceso a Internet es una función coordinada entre operadores de Internet bajo acuerdos consensuados. La administración de los recursos de direcciones de Internet se organiza a nivel regional por cinco RIR:

◆ APNIC —*Asian Pacific Network Information Centre*— que sirve la región Asia Pacífico.

◆ ARIN —*American Registry Internet Numbers*— que sirve Norte América y partes del Caribe.

- AfriNIC —*Africa Network Information Centre*— para el continente africano.
- RIPE NCC —*Reseaux IP Européens National Coordination Centre*— para Europa, el Oriente Próximo y Asia Central.
- LACNIC —*Latin American and Caribbean Network Information Centre*— para América Latina y partes del Caribe.

Los RIR se fundaron y son gobernados por unas 8 000 organizaciones en el ámbito mundial, que representan a los usuarios de los recursos de direcciones de Internet. Los procedimientos y principios de asignación se desarrollan en foros abiertos a los miembros de los RIR, así como partes interesadas, incluyendo los gobiernos. Esta coordinación evita políticas incompatibles que puedan entrar en conflictos entre países o redes, además, reduce la fragmentación del espacio de direcciones y su consecuente impacto global.

Debido a la importancia en los aspectos sociales, económicos y de la propia seguridad de los países que representa Internet, existe la tendencia que, en el ámbito nacional, la administración de los recursos de direcciones de Internet sea una responsabilidad del Ministerio que rige las políticas de las telecomunicaciones y tecnología de la información reteniendo, de esa forma, el poder de regular sobre un aspecto crítico para el desarrollo del país. Por su parte, varias naciones han organizado Registros Nacionales de Internet para la administración de los recursos a ellas asignados.

Criterios generales para determinar el número y clase de direcciones IP en las redes basadas en paquetes

Las direcciones IP son consustanciales con las redes de paquetes basadas en el Protocolo Internet (IP) protocolo que, a su vez, constituye el pilar de las Redes de Nueva Generación. Las direcciones IP no se estructuran de forma geográfica, de ese modo, el prefijo de un bloque de direcciones IP identifica una red que puede ser de cualquier tamaño y de cualquier extensión física: global, regional, nacional o local.

La determinación del tipo de direcciones IP y su número requerido se cuantifican cuando se define la arquitectura y el proyecto de redes basados en el protocolo IP. En esa fase se realiza la segmentación de las clases disponibles en diferentes subclases en dependencia de cuántas redes se requieren levantar y cuántos equipos terminales —PC, *routers*, *gateways*, LANs, etc.— se encuentran en cada red. Esto se amplía en caso de que se quieran utilizar terminales de voz IP.

Las direcciones privadas se quedan en la red privada y no se traspasan o encaminan hacia la Web, es decir, a Internet pues los *routers* que cumplan con la recomendación RFC 1918, cuando reciben una dirección privada en el encabezamiento de los paquetes, las descarta incluso sin acudir a las tablas de encaminamiento.

Las direcciones IP privadas son más seguras porque no se puede acceder a ellas desde otras redes diferentes de las que están asignadas. Puede utilizarse este tipo de dirección hasta el punto de acceso a Internet. En este punto hay que asignar direcciones públicas y crear la función NAT para traducir una dirección privada a una dirección pública. La función NAT puede activarse en cualquier equipo IP —*router*, *access controller*, etc.—.

Para un cliente con acceso conmutado o dedicado a Internet hay que asignarle una dirección pública y una dirección privada, si el acceso es a través de una red IP privada que después se conecta a Internet a través de la función NAT.

En redes grandes con muchos equipos, se le asigna una subclase grande con muchas direcciones IP, redes pequeñas con algunos equipos se le asigna una subclase con algunas direcciones IP.

Otro aspecto a decidir es la selección entre el IPv6 y el IPv4. Por las ventajas aquí mencionadas del IPv6, este protocolo sería una opción a considerar. No obstante, y en general, existen en casi todas las redes dispositivos que operan con IPv4 por lo que la adquisición de terminales y *routers* IPv6 deben poder interoperar con terminales IPv4 y utilizar infraestructuras de encaminamiento IPv4. De introducirse el IPv6, existen dos aspectos que no pueden ignorarse: el protocolo IP Móvil relacionado con el *roaming* de los terminales celulares, y el protocolo especial denominado IPsec concerniente con la seguridad.

Movilidad sobre IPv6

Esta movilidad se basa en la posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad, tema que en IPv4 resulta complicado. Esto se hace generando una dirección secundaria, basada en la posición, sin afectar la dirección original.

La idea es la de identificar a un nodo móvil con su dirección de partida —o *home address*—, con independencia de su punto de conexión a Internet en cada instante. Los nodos IPv6 almacenan información de vinculación entre la dirección de partida y la posición actual, a modo de caché y, por lo tanto, son capaces de enviar los paquetes destinados

al nodo móvil, a su dirección de origen, y encaminados de manera transparente a su dirección actual.

Seguridad

La seguridad en IPv4 fue un agregado, con varios problemas en las implementaciones que complican la certeza de cierto tipo de transacciones. Incluso, soluciones como los *firewalls* afectan la conectividad de las redes en muchas ocasiones.

IPv6 provee autenticación, seguridad, encriptado y salvaguarda de la integridad de los datos. La autenticación estandarizada en IPv6 garantiza que un paquete realmente proviene de la dirección Internet. También provee de una encriptación de extremo a extremo a nivel de capa de red, garantizando que el paquete nunca sea violado.

Los organismos internacionales y las direcciones IP

La IETF es una comunidad internacional de ingenieros, operadores e investigadores, que desarrolla actividades relacionadas con Internet a través de grupos de trabajo y es el principal organismo, a escala mundial, del comportamiento y desarrollo de Internet.

El ICANN —*Internet Corporation for Assigned Names and Numbers*— es el organismo internacional responsable de asignar el espacio de direcciones del Protocolo Internet, asignar los identificadores de protocolo, administrar los sistemas de nombre de dominio del nivel superior como los genéricos (gTLD) y los de código de países (ccTLD), y de las funciones administrativas del sistema de servidores raíz. Estos servicios se realizaban originalmente, bajo contrato del gobierno de los Estados Unidos por la IANA.

La UIT-T es un fórum donde gobiernos y el sector privado coordinan y producen normas de alta calidad para las redes de telecomunicaciones mundiales y servicios asociados. Es una agencia especializada dentro del sistema de las Naciones Unidas.

Debido a la importancia en los aspectos sociales, económicos y de la propia seguridad de los países que representa Internet existe una fuerte presión, expresada en los encuentros mundiales para la sociedad de la información —*World Summit of Information Society* (WSIS)—, para que la UIT-T, como órgano adscrito al sistema de las Naciones Unidas, asuma el control de las direcciones IP dentro del marco de lo que se ha dado en llamar **el gobierno de Internet**.

El gobierno de Internet comprende temas como: distribución del recurso de direcciones de Internet y acuerdos sobre las normas, políticas, procedimientos en caso de disputas, etc. Estas y otras cuestiones vertidas en el marco de las WSIS provienen, fundamentalmente, de los países en vías de desarrollo. Como es un asunto controvertido en el que se tratan temas económicos e intereses geopolíticos, tardará tiempo en encontrar una solución con un consenso. Nótese que se trata, principalmente, el gobierno porque las definiciones técnicas de Internet que rigen, esencialmente, por las normas de la IETF.

Conclusiones

Las direcciones IP son consustanciales con las redes de paquetes basadas en el Protocolo Internet (IP) que, a su vez, constituye el pilar en el que se basan las Redes de Nueva Generación (NGN).

La significativa expansión de los servicios móviles —incluyendo las aplicaciones domésticas, la aparición de las NGN y la asimetría en el número de direcciones IP asignadas entre los países que aplicaron primero Internet

y el resto— motivó la aparición de un nuevo protocolo de Internet: la versión 6 ó IPv6.

La existencia de dos protocolos —IPv4 e IPv6—, la convergencia entre redes de telecomunicaciones, datos y móviles, más el surgimiento de nuevas aplicaciones, preocupa y ocupa tanto a los operadores de telecomunicaciones, proveedores de servicios Internet como a reguladores y organismos de Normalización internacionales. Ante estas disyuntivas podrían considerarse, entre las mejores prácticas a seguir, las siguientes:

- La determinación del tipo de direcciones IP así como su número requerido se cuantifica cuando se define la arquitectura y el proyecto de redes basados en el protocolo IP.
- Considerar la opción IPv6.
- Definir el, o, los mecanismos de transición adecuados del IPv4 al IPv6.
- Incluir, en la opción IPv6, los protocolos relativos a los móviles y a la seguridad.

Bibliografía

"ICANN, funciones y logros" (2006). Disponible en: http://www.icann.org. (Consulta: enero/2006).

"IP Address Services" (IANA). Disponible en: http://www.iana.org/ipaddress/ip-addresses.htm. (Consulta: febrero/2006).

Pérez García, Marcos, "Metodología para la asignación de direcciones IP". Documento DDAR: IT-04-003/06-02, ETECSA, mayo/2006.

RFC 1009, - Variable Subset Mask (VLSM). Disponible en: http://www.ietf.org/rfc/rfc1009.txt, (Consulta: febrero/2006).

RFC 1034 - Domain Names - concepts and facilities. Disponible en: http://www.ietf.org/rfc/rfc1034.txt. (Consulta: marzo/2006).

RFC 1918 - Address Allocation for Private In. Disponible en http://www.ietf.org/rfc/rfc1918.txt. (Consulta: marzo/2006).

RFC 2375 - IPv6 Multicast Address Assignments. Disponible en: http://www.ietf.org/rfc/rfc2375.txt. (Consulta: mayo/2006).

RFC 2401 - Security Architecture for the Internet Protocol. Disponible en: http://www.ietf.org/rfc/rfc2401.txt. (Consulta: abril/2006).

RFC 2411 - IP Security. Roadmap. Disponible en: http://www.ietf.org/rfc/rfc2411.txt. (Consulta: marzo/2006).

RFC 2460 - Internet Protocol Vesion 6 (IPv6). Disponible en: ftp://ftp.rfc-editor.org/in-notes/rfc2460.txt. (Consulta: abril/2006).

RFC 2461 - Neighbor Discovey for IP Version 6 (IPv6). Disponible en: http://www.ietf.org/rfc/rfc2461.txt. (Consulta: mayo/2006).

RFC 2526 - Reserved IPv6 Subnet Anycast Addresses. Disponible en: http://www.ietf.org/rfc/rfc2526.txt. (Consulta: abril/2006).

RFC 3024 - Reverse Tunneling for Mobile IP. Disponible en: http://www.ietf.org/rfc/rfc3024.txt. (Consulta: marzo/2001).

RFC 3027 - Protocol Complications with the IP Network Address Translator. Disponible en: http://www.ietf.org/rfc/rfc3027.txt (Consulta: abril/2001).

RFC 3587 - IPv6 Global Unicast Address Format. Disponible en: http://www.ietf.org/rfc/rfc3587.txt. (Consulta: marzo/2001).