1206

DOMINIOS Y DIRECCIONES EN REDES IP

Referido a la administración de dominios y direcciones IP; a la asignación dinámica y al manejo de los sockets.

1- DIRECCIONES IP

1.1- CLASES DE DIRECCIONES IP

Dentro de una red IP las direcciones son gestionadas tanto por el **IANA** (*Internet Assigned Numbers Authority*) que asigna las direcciones públicas, como por el usuario que maneja las direcciones en el interior de su red. La dirección IP ocupa 32 bits (4 Bytes) que permite identificar la red y el host individual. El formato de las direcciones puede ser de 5 tipos de acuerdo con la Clase que se indica en la **Tabla 01**.

Tabla 01. Clases de direcciones IP (IP-Address).

Clase A.	0+7bit+24bit. Corresponde a un número de dirección de Network (7 bit asignados por IANA) y otro número para el Host (24 asignados por el administrador de la red). Aplicable solo para grandes redes. El IAB solo puede designar 128 (2^7) redes de este tamaño. Numera desde 0.0.0.0 hasta 127.255.255.255. Sin embargo, ante la falta de direcciones IPv4 se ha decidido particionar la clase A para asignarlas a varios usuarios. Por ejemplo, La dirección de HP de Argentina es del tipo 15.59.x.y. En tanto que, la dirección MAC de HP es 08-00-09 (la dirección MAC de Siemens es en cambio: 08-00-06).
Clase B.	10+14bit+16bit. Aplicable a redes medianas y numera desde 128.0.0.0 hasta 191.255.255.255. Por ejemplo, la empresa Telefónica de Argentina tiene asignado un número de este tipo de red: 168.226.x.x (los dos bytes finales son asignados por el operador de la red).
Clase C.	110+21bit+8bit. Para pequeñas redes. Se trata de 4 Bytes: los 3 primeros Bytes indican la dirección de red y el último Byte numera el Host dentro del nodo. Un router de red IP se identifica mediante los 3 primeros Bytes y sus puertas con el Byte final. En esta configuración el primer valor válido es 192.0.0.0 y el último es 223.255.255.255.
Clase D.	1110+28 bits. Ocupa la numeración 224.0.0.0 hasta 239.255.255.255. Es utilizada para direcciones *multicast* (grupo de usuarios de servicios IP).
Clase E.	11110+27 bits. Ocupa desde 240.0.0.0 hasta 247.255.255.255. Este set de direcciones se encuentra sin aplicación. La dirección 255.255.255.255 es una dirección de *broadcast*.

La dirección IP puede escribirse mediante la notación decimal punteada *Dotted* (44.123.230.224) que esta es la preferida por su simplicidad. También se han usado la notación hexadecimal (2C.7B.E6.E0), la notación estilo C de Unix (Cx2C7BE6E0) y la notación binaria (00101100.01111101.11100110.11100000).

CLASE D (*Multicast*). El IANA ha reservado la clase D de direcciones IP para grupos multicast. Esta clase de direcciones consiste en la secuencia 1110 y 28 bits de dirección (5 bits no usados y 23 de dirección). Expresado en la notación normal se trata desde 224.0.0.0 hasta 239.255.255.255. Algunas direcciones se encuentran reservadas y no pueden ser utilizadas.

En las direcciones MAC se ha reservado el prefijo 01-00-5E (hexadecimal) para direcciones IP multicast. De esta forma casi todos los últimos 3 Bytes de IP y MAC son idénticos. Por ejemplo, la dirección IP: 224.10.8.5 corresponde a la dirección MAC: 01005E0A0805. En la siguiente secuencia, los bits en negrita no son usados y separan la zona de identificación multicast (anterior) de la dirección propiamente dicha de usuario (posterior).

IP Address			224=1110 **0000**	10=**0**000 1010	8=0000 1000	5=0000 0101
MAC Address	0.1=0000 0001	0.0=0000 0000	5.E=0101 **1110**	0.A=**0**000 1010	0.8=0000 1000	0.5=0000 0101

***MASK NET*.** La dirección IP contiene 4 sectores; el sector que define al host está determinado por la máscara de subnetwork. Los componentes son los siguientes:
-***Prefijo*** desde 1 a 5 bits para identificación del tipo de Clase (A a E). Así la secuencia 110 determina la clase C.
-***Network*** (de 7, 14 o 21 bits para las clases A a C); entonces la secuencia 110 inicial determina que la dirección de red es de 21 bits.
-***Sub-network***. Se trata de la diferencia con la dirección de host.

-***Host***. Para conocer la secuencia que identifica al host es necesario leer la máscara de red (*mask net*). Esta máscara identifica los bits que determinan el host y por ello, la subnetwork.

Estos dos últimos campos ocupan en total los 24, 16 o 8 bits que completan la dirección. Para poder distinguir entre la identificación de subnetwork y host se requiere una filtro de direcciones denominado *Mask Net*. Por ejemplo, para una dirección clase C (inicio 110) se tiene el formato (x para Network; y para Subnetwork; z para el Host) de la **Tabla 02**. Una dirección por el estilo se debe expresar como W.X.Y.Z/27; donde el /27 se refiere a la cantidad de unos en la máscara de red utilizada.

Tabla 02. Ejemplo de máscara de red.

	Byte 1	Byte 2	Byte 3	Byte 4	Decimal
Dirección IP	110x.xxxx	xxxx.xxxx	xxxx.xxxx	yyyz.zzzz	(192...) a (223...)
Mask Net	1111.1111	1111.1111	1111.1111	1110.0000	(255.255.255.224)

1.2- DIRECCIONES SIN CLASES

El crecimiento de las direcciones IP ocupadas ha obligado a dos tipos de soluciones: el VLSM y CIDR a corto plazo sobre el protocolo IP versión 4 y la ampliación del campo de direcciones en IP versión 6.

VLSM (*Variable Length Subnet Mask*).
En RFC-1009 se autoriza la construcción de redes donde la longitud de la máscara es variable dentro de la red. La limitación de utilizar siempre la misma máscara de subred es que se está limitado a un número fijo de direcciones de subred. Conceptualmente una red es dividida en subredes, cada subred es dividida en subredes y así sucesivamente. Esto puede reducir sustancialmente las tablas de ruta de los routers. El protocolo de routing OSPF soporta VLSM; el algoritmo que lo permite se denomina "*longest match*".

Ejemplo.
-El proceso se inicia sobre la red **140.25**.0.0/16 (binario: **10001100-00011001**-00000000-00000000) que permite los últimos 16 bits para direcciones de subred VLSM. En negritas se indican los bits fijos para la red; subrayado se indican los bits relacionados con /16.
-Se divide en subredes del tipo 140.25.0.0/20. Es decir que se han creado 16 subredes (4 bits).
-Se selecciona en el ejemplo la subred 140.25.**224**.0/20 (10001100-00011001-**1110**0000-0000000).
-Se la divide en subredes del tipo 140.25.224.0/24. Es decir se han creado 16 subredes (4 bits).
-Se selecciona en el ejemplo la subred 140.25.**238**.0/24 con la secuencia (10001100-00011001-1110**1110**-00000000).
-Se divide en subredes del tipo 140.25.238.0/27. Es decir se han creado 8 subredes (3 bits).
-Se selecciona en el ejemplo la subred 140.25.238.**64**/27 (10001100-00011001-11101110-**101**00000).
-Esta subred dispone de 30 direcciones de host (desde 140.25.238.66/27 a 140.25.238.94/27). La dirección inicial (140.25.238.65/27) se reserva para indicar la subred completa y la final (140.25.238.95/27) para broadcasting. Por ejemplo, la dirección de broadcasting en esta subred es (10001100-00011001-11101110-101**11111**).

CIDR (*Classless Inter-Domain Routing*).
En el año 1992 el IETF decide subdividir las direcciones clase A debido a que las direcciones clase C se encuentra casi exhausta. Por ejemplo, para el año 1992 se habían asignado 46 de las 126 direcciones clase A y 5467 de la 16382 de clase B. Para el año siguiente estos valores eran de 52 y 7133 respectivamente. En RFC-1519 del año 1993 se instruye el CIDR que elimina la división entre clase lo cual equivale en esencia a VLSM. Con posterioridad el crecimiento de direcciones fue incrementándose. De 130 web en junio de 1993 se pasó a 646.162 en enero de 1997.

2- ASIGNACION DE DIRECCIONES IP

2.1- DOMINIOS

La gestión de direcciones IP requiere de una serie de elementos interrelacionados: el servidor DNS permite asociar un nombre de usuario con la dirección IP; el servidor/router NAT permite asignar direcciones IP no-públicas en el interior de una red privada; el servidor DHCP permite asignar direcciones IP en forma dinámica a usuarios intermitentes y el *Dynamic DNS* permite actualizar el servidor de DNS cuando se asigna la dirección mediante DHCP. A continuación los detalles de estos elementos.

DNS (*Domain Name System*).
Este sistema permite organizar la información de routing entre una denominación (seudónimo) simple de recordar y el número de dirección IP verdadero (se denomina resolución de nombre). Hasta 1980 un solo computador (llamado Host.txt en California) realizaba esta función, pero el tráfico hacia la misma se tornó inmanejable. Entonces se introdujo un sistema distribuido. El nombre completo tiene como máximo 63 caracteres. De ellos 3 caracteres indican el domino (edu-educación, com-comercial, gov-gubernamental, org-organización, mil-militar, etc) y 2 el país (ar-Argentina, it-Italia, etc). La tabla de dominios memorizada en el servidor se denomina *DNS Cache*.

Por ejemplo, cuando un usuario de Internet selecciona un dominio (dirección DNS) de e-mail (rares@nss.com.ar) o de la dirección de web (www.nss.com.ar) el servidor realiza un chequeo de la base de datos para encontrar que esta dirección DNS es un seudónimo de la dirección IP (ejemplo 192.168.1.4). La dirección IP se envía hacia atrás para asegurar que el mensaje pueda ser reconocido en la red. Existen servidores que permiten reconocer la dirección DNS y reporta la IP correspondiente.

DNS opera sobre UDP por lo cual no existe una conexión propiamente dicha; solo sirve para resolver la relación entre dominio en formato de texto y la dirección IP asignada. Con posterioridad, la conexión es establecida sobre TCP hacia el servidor (por ejemplo de web).

Existe también la resolución inversa. Si se conoce solo la dirección IP (por ejemplo 192.168.1.0) mediante el comando inverso (1.1.168.192.in-addr.arpa) se obtiene el seudónimo.

NAT (*Network Address Translation*).
El problema más complejo de Internet es el reducido número de direcciones. La solución a largo plazo el IPv6 con un mayor número de bytes por dirección. La solución instrumentada sobre IPv4 son dos: el **CIDR** (*Classless InterDomain Routing*) y el **NAT**. El proceso NAT propone reducir el número de direcciones IP mediante el re-uso de direcciones privadas en todas las redes. De esta forma una red privada utiliza un direccionamiento propio y el router en el borde (*Stub Router*) de la red realiza la función de traducción y direccionamiento hacia la red pública (llamadas dirección local y dirección global).

El uso de NAT en el router de borde requiere el manipuleo de la información; por ejemplo, los checksum de IP y TCP cambian, además existen protocolos que llevan la dirección IP en el contenido (FTP lleva la dirección en código ASCII) y debe ser cambiada, etc. Esto introduce un retardo y un incremento de procesamiento pero a cambio se simplifica notablemente la gestión de direcciones. El funcionamiento de NAT puede ser estático o dinámico; en el estático el mapeo desde el conjunto de direcciones internas al conjunto externo se realiza manualmente. En el funcionamiento dinámico responde a diversas estrategias.

Una vez asignadas las direcciones privadas en el interior de la red, las mismas no cambian aun si se conectan a distintos ISP, con distintas direcciones públicas. Cuando NAT está implementado nunca el esquema de direcciones internas debe ser enviado al exterior pero lo contrario es deseable para que la Intranet tenga un conocimiento de la Internet.

El IANA determinó un set de direcciones para uso privado. Estas direcciones no son ruteadas por la Internet y se asignan para los componentes del interior. Como los router no distinguen las direcciones privadas se requiere el NAT para efectuar la traducción. Las direcciones reservadas por el IANA son las indicadas en la **Tabla 03.**

Tabla 03. Direcciones IP reservadas para aplicaciones en Intranet (NAT).

Clase	Desde	Hasta	Prefijo
A	10.0.0.0	10.255.255.255	10/8
B	172.16.0.0	172.16.255.255	172.16/12
C	192.168.0.0	192.168.255.255	192.168/16

NAT tiene la ventaja de conservar la legalidad de direcciones; es flexible para la conexión a nuevos ISP; impide el problema de superposición de direcciones IP debido al filtrado de direcciones privadas. Lamentablemente, el NAT reduce las opciones de seguridad debido a que tiene que intervenir sobre el paquete por lo que limita las posibilidades de la criptografía. Por otro lado se pierde la posibilidad de trazabilidad entre extremos y se incrementa el retardo por procesamiento de software.

2.2- ASIGNACION DINAMICA

DHCP (*Dynamic Host Configuration Protocol*).
Cuando un nuevo usuario se agrega a la red o se cambia de posición se requiere asignar una dirección IP y actualizar la base de datos del DNS. El protocolo DHCP fue diseñado por el IETF (standard en RFC-2131) para reducir los requerimientos de configuración. Además de asignar la dirección IP realiza una configuración automática de los parámetros necesarios para funcionar en la red donde se encuentra. DHCP trabaja sobre TCP y está basado en el protocolo **BOOTP** (*Bootstrap Protocol*) de RFC-0951, con algunas diferencias. El BOOTP permitía que clientes sin capacidad de memoria (disco rígido) pueda funcionar en TCP/IP.

Se utiliza un modelo *Client/Server* por lo que se dispone de uno o varios servidores DHCP. No se requiere de un servidor por subred por lo que el protocolo DHCP debe trabajar a través de routers. Más de un servidor pueden realizar las tareas de asignación de direcciones con el propósito de mejorar la eficiencia del sistema.

Las características generales de funcionamiento son las siguientes:
-El administrador de la red define en el servidor DHCP el set de direcciones IP que pueden ser asignadas. También se seleccionan los valores de los parámetros que deben ser seteados en el cliente.
-No requiere indicarse cuales de la direcciones IP están en uso; el protocolo RARP puede ayudar en esta función. Las direcciones IP que permanentemente se asignaban a la subred son distribuidas en forma dinámica entre los host. Otra forma es la asignación manual por parte del operador de la red con lo cual la asignación es permanente.
-Cuando un host se enciende realiza un pedido en forma broadcast a los servidores DHCP. El cliente puede seleccionar una de las respuestas (sin son varias) y enviar el requerimiento adicional de configuración. El server DHCP no fuerza los parámetros, es el host cliente el que solicita los parámetros configurables.
-El servidor asigna la dirección IP (y la mask de subred) por un tiempo determinado. El tiempo de asignación corresponde a un mensaje de 4 Bytes (*Timestamp*) en unidades de segundos; la secuencia FF.FF.FF.FF identifica a una asignación permanente sin límite de tiempo.
-En forma periódica el cliente debe renovar la solicitud de permanencia. Si no se renueva o el cliente efectúa un *shut-down* la dirección queda libre y será reciclada para se asignada a otro host.

Existen otros protocolos que se relacionan con la asignación dinámica de direcciones. El protocolo **RARP** permite descubrir cuales son las direcciones IP que han sido a signadas en la red. El protocolo **TFTP** provee un mecanismo de transporte de información desde el servidor de *Boot*. El **ICMP** provee información de host desde otros router mediante mensajes como el *redirect*.

DDNS (*Dynamic DNS Update*)**.**
Asociado a DHCP se encuentra el mecanismo **DDNS**. Permite la actualización automática del servidor DNS con el nombre y la dirección IP asignada en forma dinámica por el protocolo DHCP. Se refiere a RFC-2136 del año 1997. Este protocolo trabaja sobre TCP o UDP de acuerdo con el *request*. El formato del mensaje de actualización (*update*) contiene un encabezado de 12 Bytes que identifica al que efectúa el requerimiento y siguen diversos campos.

DHCP *FAILOVER*.
También en sociedad son DHCP se dispone de la técnica *DHCP Failover* que consiste en disponer de servidores duplicados funcionando como pares redundantes. Se dispone de un protocolo de comunicación simplificado para la operación en régimen normal, de interrupción de comunicación entre servidores y de falla del servidor asociado.

3- PORT y SOCKETS.

Mediante 2 Bytes se identifica la puerta (*Port*) de acceso al servicio origen en TCP/UDP. Se trata de direcciones TSAP que reservan la numeración desde 1 a 225 para los protocolos más conocidos (denominados *well-known*), como ser Echo:7, SMTP:25; FTP:21; Telnet:23; Gopher:70; y Web:80. El protocolo UDP identifica las aplicaciones SNMP:161; TFTP:69 y RPC-Sun:111. Desde la port 256 a 1023 se reserva para aplicaciones UNIX. Las aplicaciones propietarias llevan la dirección de port desde 1024 hasta 49151; las direcciones superiores a 40152 (hasta 2^{16}) se asignan en forma dinámica.

La combinación de la dirección IP y la port TCP/UDP es conocida como ***Socket*** cuya asignación puede estar predeterminada (para protocolos conocidos) o se asigna entre los valores no utilizados (para las aplicaciones nuevas). Por ejemplo IP= 199.238.200.110 y port= 80 identifica al servidor de web identificado como *www.technologypreview.com*.

Un problema se genera cuando una misma máquina abre dos o más sesiones desde la misma aplicación (por ejemplo, varias ventanas de web simultáneas sobre la miasma máquina). Para eliminar esta discordancia en el socket se utiliza la numeración de port *well-known* solo en el servidor de web; en tanto que el cliente selecciona una port no asignada distinta para cada sesión. Por esta razón es que las direcciones IP y la port (el socket) es incluido en cada datagrama entre ambas máquinas. Solo los servicios que operan entre pares pueden usar la misma dirección socket en ambos extremos.

Para completar el concepto de NAT se dispone del **PAT** (*Port Address Transation*) consistende traducir una dirección de puerta interna hacia el exterior de la red. En este caso la transacción se realiza entre rangos de direcciones originales (convención BSD): 1...511; 512...1023; 1024...4999; 5000...65535. Esto permite crear varias conexiones desde el interior de la red hacia el exterior con pocas direcciones públicas.