Redes IP Versión 6

INTRODUCCION

Desde principios de los 90, la IETF (Internet Engineering Task Force) investiga opciones para reemplazar la clásica versión 4 del protocolo IP, a fin de subsanar los problemas que se van detectando: falta de suficientes direcciones IP, excesivo volumen de las tablas de encaminamiento, poca atención al tipo de tráfico cursado, escasa seguridad y otros varios. En 1995 se presenta la versión 6 de IP y desde entonces sus características nuevas siguen sometidas a debate y discusión. Entre estas novedades destacan: nuevo formato de direccionamiento, aceleración del encaminamiento, soporte a la movilidad de máquinas, soporte al tráfico de tiempo real y seguridad integrada en el protocolo.

De esta forma nace la nueva versión del protocolo IP, llamada IPv6, aunque también es conocida como IPng (Internet Protocol Next Generation). Es la versión 6, debido a que la numero 5 no pasó de la fase experimental. La compatibilidad con la versión 4 es prácticamente total, ya que se han incluido características de compatibilidad. Algunas de las modificaciones, están encaminadas a mejorar la seguridad en la red, que apenas existia en la versión 4. En este trabajo se realizará una pequeña mención a la versión 4 de IP, que permitirá establecer un marco de comparación entre ambas versiones.

IP VERSIÓN 4

Es importante aclarar que de acuerdo al modelo OSI, es la CAPA DE RED la que se encarga de controlar la comunicación entre un equipo y otro. Esta conforma los paquetes IP que serán enviados por la capa inferior. Desencapsula los paquetes recibidos pasando a la capa superior la información dirigida a una aplicación.

El Protocolo IP proporciona un sistema de distribución que es poco fiable incluso en una base solida. El protocolo IP especifica que la unidad básica de transferencia de datos en el TCP/IP es el datagrama.

Los datagramas pueden ser retrasados, perdidos, duplicados, enviados en una secuencia incorrecta o fragmentados intencionadamente para permitir que un nodo con un buffer limitado pueda coger todo el datagrama. Es la responsabilidad del protocolo IP reensamblar los fragmentos del datagrama en el orden correcto. En algunas situaciones de error los datagramas son descartados sin mostrar ningún mensaje mientras que en otras situaciones los mensajes de error son recibidos por la maquina origen (esto lo hace el protocolo ICMP). El protocolo ICMP (Internet Control Message Protocol), proporciona el medio para que el software de hosts y gateways intermedios se comuniquen. El protocolo ICMP tiene su propio numero de protocolo (numero 1), que lo habilita para utilizar el IP directamente. La implementacion de ICMP es obligatoria como un subconjunto lógico del protocolo IP. Los mensajes de error de este protocolo los genera y procesa TCP/IP, y no el usuario.

El protocolo IP también define cual sera la ruta inicial por la que serán mandados los datos.

Cuando los datagramas viajan de unos equipos a otros, es posible que atraviesen diferentes tipos de redes. El tamaño máximo de estos paquetes de datos puede variar de una red a otra, dependiendo del medio físico que se emplee para su transmisión. A este tamaño máximo se le denomina MTU (Maximum Transmission Unit), y ninguna red puede transmitir un paquete de tamaño mayor a esta MTU. El datagrama consiste en una cabecera y datos.

- Longitud de la Cabecera

Este campo ocupa 4 bits, y representa el numero de octetos de la cabecera dividido por cuatro, lo que hace que

este sea el numero de grupos de 4 octetos en la cabecera.

- Versión

El campo versión ocupa 4 bits. Este campo hace que diferentes versiones del protocolo IP puedan operar en la Internet. En este caso se trata de la versión 4.

- Tipo de servicio

Este campo ocupa un octeto de la cabecera IP, y especifica la precedencia y la prioridad del datagrama IP. Los tres primeros bits del octeto indican la precedencia. Los valores de la precedencia pueden ser de 0 a 7. Cero es la precedencia normal, y 7 esta reservado para control de red. Muchos Gateways ignoran este campo. Los otros 4 bits definen el campo prioridad, que tiene un rango de 0 a 15. Las cuatro prioridades que están asignadas son: 0, (por defecto, servicio normal), 1 (minimizar el costo monetario), 2 (máxima fiabilidad), 4 (Maximizar la transferencia), 8 (El bit +4 igual a 1, define minimizar el retraso). Estos valores son utilizados por los routers para direccionar las solicitudes de los usuarios.

- Longitud Total

Este campo se utiliza para identificar el numero de octetos en el datagrama total.

- Identificación

El valor del campo identificación es un numero secuencial asignado por el Host origen. El campo ocupa dos octetos. Los números oscilan entre 0 y 65.535, que cuando se combinan con la dirección del Host forman un numero único en la Internet. El numero se usa para ayudar en el reensamblaje de los fragmentos de datagramas.

- Fragmentos Offset

Cuando el tamaño de un datagrama excede el MTU, este se segmenta. El fragmento Offset representa el desplazamiento de este segmento desde en inicio del datagrama entero.

- Flags

El campo flag ocupa 3 bits y contiene dos flags. El bit +5 del campo flags se utiliza para indicar el ultimo datagrama fragmentado cuando toma valor cero. El bit +7 lo utiliza el servidor origen para evitar la fragmentación. Cuando este bit toma valor diferente de cero y la longitud de un datagrama excede el MTU, el datagrama es descartado y un mensaje de error es enviado al Host de origen por medio del protocolo ICMP.

- Tiempo de Vida

El campo tiempo de vida ocupa un octeto. Representa el numero máximo de segundos que un datagrama puede existir en Internet, antes de ser descartado. Un Datagrama puede existir un máximo de 255 segundos. El numero recomendado para IP es 64. El originador del datagrama manda un mensaje ICMP cuando el datagrama es descartado.

- Protocolo

El campo protocolo se utiliza para identificar la capa de mayor nivel más cercana usando el IP. Este es un campo de 0 bits, que normalmente identifica tanto la capa TCP (valor 6), como la capa UDP (valor 17) en el nivel de transporte, pero puede identificar hasta 255 protocolos de la capa de transporte.

- Checksum

El checksum proporciona la seguridad de que el datagrama no ha sido dañado ni modificado. Este campo tiene una longitud de 16 bits. El checksum incluye todos los campos de todos los campos de la cabecera IP, incluido el mismo, cuyo valor es cero a efectos de calculo.

Un Gateways o nodo que efectue alguna modificación en los campos de la cabecera (por ejemplo en el tiempo de vida), debe recalcular el valor del checksum antes de enviar el datagrama.

Los usuarios del IP deben proporcionar su propia integridad en los datos, ya que el checksum es solo para la cabecera.

- Dirección de Origen

Este campo contiene un identificador de red (Netid) y un identificador de Host (Hostid). El campo tiene una longitud de 32 bits. La dirección puede ser de clase A, B, C. (ver Direcciones IP).

- Dirección de Destino

Este campo contiene el Netid y el Hostid del destino. El campo tiene una longitud de 32 bits. La dirección puede ser de clase A, B, C o D (ver Direcciones IP).

- Opciones

La existencia de este campo viene determinada por la longitud de la cabecera. Si esta es mayor de cinco, por lo menos existe una opción. Aunque un Host no esta obligado a poner opciones, puede aceptar y procesar opciones recibidas en un datagrama. El campo Opciones es de longitud variable. Cada octeto esta formado por los campos Copia, Clase de Opción y Numero de Opción.

El campo Copia sirve para que cuando un datagrama va a ser fragmentado y viaja a través de nodos o Gateways. Cuando tiene valor 1, las opciones son las mismas para todos los fragmentos, pero si toma valor 0, las opciones son eliminadas. Clase de Opción es un campo que cuando tiene valor 0, indica datagrama o control de red; Cuando tiene valor 2, indica depuración o medida. Los valores 1 y 3 están reservados para un uso futuro. El Numero de Opción indica una acción especifica.

- Padding

Cuando esta presente el campo Pad, consiste en 1 a 3 octetos puestos a cero, si es necesario, para hacer que el numero total de octetos en la cabecera sea divisible por cuatro.

- Datos

El campo datos consiste en una cadena de octetos. Cada octeto tiene un valor entre 0 y 255. El tamaño de la cadena puede tener un mínimo y un máximo, dependiendo del medio físico. El tamaño máximo esta definido por la longitud total del datagrama. El tamaño del campo Datos en octetos es igual a:

(Longitud Total del Datagrama) − (Longitud de la cabecera)

- Direcciones IP y máscaras de red

En una red TCP/IP los ordenadores se identifican mediante un número que se denomina **dirección IP**. Esta dirección ha de estar dentro del rango de direcciones asignadas al organismo o empresa a la que pertenece,

estos rangos son concedidos por un organismo central de Internet, el **NIC** (Network Information Center).

Las direcciones IP hacen que el envío de datos entre computadores se haga de forma eficaz, de un modo similar al que se utilizan los números de teléfonos.

Una dirección IP está formada por 32 bits, que se agrupan en octetos:

01000001 00001010 00000010 00000011

Para entender mejor utilizamos las direcciones IP en formato decimal, representando el valor decimal de cada octeto y separando con puntos:

129.10.2.3

Cada campo puede tener un valor comprendido entre 0 y 255. Esta compuesta por una dirección de red, seguida de una dirección de subred y de una dirección de host.

Las dirección de una máquina se compone de dos partes cuya longitud puede variar:

- **Bits de red:** son los bits que definen la red a la que pertenece el equipo.
- **Bits de hosts:** Son los bits que distinguen a un equipo de otro dentro de una red. Los bits de red siempre están a la izquierda y los de host a la derecha, veamos un ejemplo sencillo:

Bits de Red	**Bits de Host**
10010110 11010110 10001101	11000101
150.214.141.	197

Para continuar con el ejemplo, diremos también que esta máquina pertenece a la red 150.214.141.0 y que su máscara de red es 255.255.255.0. A continuación encontraremos el mismo numero en formato binario.

10010110	**11010110**	**10001101**	**11000101**
11111111	11111111	11111111	00000000

La máscara de red es un número con el formato de una dirección IP que nos sirve para distinguir cuando una máquina determinada pertenece a una subred dada, con lo que podemos averiguar si dos máquinas están o no en la misma subred IP. En formato binario todas las máscaras de red tienen los 1 agrupados a la izquierda y los 0 a la derecha.

Para llegar a comprender como funciona todo esto presentaremos un ejercicio práctico.

Ejercicio 1

Sea la dirección de una subred 150.214.141.0, con una máscara de red 255.255.255.0

Comprobar cuales de estas direcciones pertenecen a dicha red:

150.214.141.32

150.214.141.138

150.214.142.23

Paso 1: Para ver si son o no direcciones validas de dicha subred clase C tenemos que descomponerlas a nivel binario:

- 10010110.1101010.10001101.10000000

150.214.141.138 10010110.1101010.10001101.10001010

- 10010110.1101010.10001110.00010111
- 11111111.1111111.11111111.00000000
- 10010110.1101010.10001101.00000000

Paso 2: Una vez tenemos todos los datos a binario pasamos a recordar el operador lógico AND o multiplicación:

Valor A	**Valor B**	**Resultado**
0	0	0
0	1	0
1	0	0
1	1	1

Vamos a explicar como hace la comprobación el equipo conectado a una red local.

Primero comprueba la dirección IP con su máscara de red, para ello hace un AND bit a bit de todos los dígitos:

150.214.141.32 10010110.1101010.10001101.10000000

- 11111111.1111111.11111111.00000000

150.214.**141**.0 10010110.1101010.10001101.00000000

Luego hace la misma operación con la dirección IP destino.

150.214.141.138 10010110.1101010.10001101.10001010

- 11111111.1111111.11111111.00000000

150.214.**141**.0 10010110.1101010.10001101.00000000

El resultado que obtenemos ambas veces es la dirección de red, esto nos indica que los dos equipos están dentro de la misma red.

Paso3: vamos ha hacerlo con la otra dirección IP.

- 10010110.1101010.10001110.00010111
- 11111111.1111111.11111111.00000000

- 10010110.1101010.10001110.00000000

Como vemos este resultado nos indica que dicho equipo no pertenece a la red sino que es de otra red en este caso la red sería 150.214.142.0.

- CLASES DE RED

Para una mejor organización en el reparto de rangos las redes se han agrupado en cuatro clases, de manera que según el tamaño de la red se optará por un tipo u otro.

La clase A contiene 7 bits para direcciones de red, con lo que permite tener hasta 128 redes, con 16.777.216 computadores cada una. Las direcciones estarán comprendidas entre 0.0.0.0. y 127.255.255.255., y la mascara de subred sera 255.0.0.0.

Las direcciones de **CLASE A** corresponden a redes que pueden direccionar hasta 16.777.214 máquinas cada una.

Las direcciones de red de clase A tienen siempre el primer bit a 0.

0 + Red (7 bits) + Máquina (24 bits)

Solo existen 124 direcciones de red de clase A.

Ejemplo:

	Red	**Máquina**		
Binario	0 0001010	00001111	00010000	00001011
Decimal	10	15	16	11

Rangos (notación decimal):

1.xxx.xxx.xxx − 126.xxx.xxx.xxx

Las direcciones de red de **CLASE B** permiten direccionar 65.534 máquinas cada una.

Los dos primeros bits de una dirección de red de clase B son siempre 01.

01 + Red (14 bits) + Máquina (16 bits)

Existen 16.382 direcciones de red de clase B.

Ejemplo:

	Red		**Máquina**	
Binario	01 000001	00001010	00000010	00000011
Decimal	129	10	2	3

Las direcciones de **CLASE C** permiten direccionar 254 máquinas.

Las direcciones de clase C empiezan con los bits 110

110 + Red (21 bits) + Máquina (8 bits)

Existen 2.097.152 direcciones de red de clase C.

Ejemplo:

	Red			**Máquina**
Binario	110 01010	00001111	00010111	00001011
Decimal	202	15	23	11

Las direcciones de **CLASE D** son un grupo especial que se utiliza para dirigirse a grupos de máquinas. Estas direcciones son muy poco utilizadas. Los cuatro primeros bits de una dirección de clase D son 1110.

Direcciones de red reservadas

Existen una serie de direcciones IP con significados especiales.

- Direcciones de subredes reservadas:

000.xxx.xxx.xxx (1)

127.xxx.xxx.xxx (reservada como la propia máquina)

128.000.xxx.xxx (1)

191.255.xxx.xxx (2)

192.168.xxx.xxx (reservada para intranets)

223.255.255.xxx (2)

- Direcciones de máquinas reservadas:

xxx.000.000.000 (1)

xxx.255.255.255 (2)

xxx.xxx.000.000 (1)

xxx.xxx.255.255 (2)

xxx.xxx.xxx.000 (1)

xxx.xxx.xxx.255 (2)

- Se utilizan para identificar a la red.
- Se usa para enmascarar.

ANTECEDENTES IP VERSION 6

La red Internet, basada en un diseño de los años 80, ha experimentado un crecimiento sin parangón en la historia de las telecomunicaciones tanto en número de usuarios conectados como en aplicaciones y servicios disponibles. Para remediar estos males, los cuerpos técnicos de la Internet impulsaron un debate bajo el lema de IP Next Generation (IPng) que ha culminado con la especificación de un nuevo protocolo IP, sucesor del actual IPv4, y conocido formalmente como la versión 6 del Protocolo Internet o IPv6.

EL PROBLEMA DE LA ASIGNACIÓN DE DIRECCIONES

A la hora de diseñar un método de asignación de direcciones en los albores de la Internet, cuando estaba conectada apenas una docena de centros, se pensó en un esquema basado en el tamaño de las organizaciones y de ahí nació el modelo de clases en la que sólo se daba cabida a tres tipos de prefijo de longitud predeterminada según fuera una gran organización (clase A, prefijo 8 bits), de tamaño mediano (clase B, prefijo 16 bits) o pequeño (clase C, prefijo 24 bits). La asignación de direcciones comenzó a hacerse de manera centralizada por un único centro de registro (SRI−NIC) satisfaciendo casi todas las solicitudes sin necesidad de mayor trámite. Este modelo de asignación de direcciones, cuando la Internet comenzó a crecer de forma espectacular, trajo algunas de estas consecuencias:

Mal aprovechamiento del espacio de direcciones. Cada centro tendía a pedir una clase superior a la requerida, normalmente una clase B en vez de una o varias clases C, por puro optimismo en el crecimiento propio o por simple vanidad.

Peligro de agotamiento de las direcciones de clase B. Las más solicitadas debido a la escasez de posibilidades de elección. La alerta sonó cuando se había agotado el 30% de esta clase y la demanda crecía exponencialmente.

Síntomas de saturación en los routers de los backbones. Al imponerse restricciones severas en la asignación de clases B, las peticiones de múltiples clases C se hicieron masivas, lo que hizo que aumentara de forma explosiva el número de prefijos que los routers habían de mantener en sus tablas, llegándose a alcanzar los límites físicos impuestos por la capacidad de memoria y de proceso.

Por tanto nos encontramos ante un doble problema: agotamiento de direcciones y colapso de routers debido a la explosión de rutas. En una situación en la que la población conectada a la red se duplicaba (en términos de equipos y redes conectadas) en períodos que oscilaban en torno a los 6 meses había que tomar medidas urgentes, y he aquí algunas de las que se tomaron:

Imposición de políticas restrictivas de asignación de direcciones por parte de los centros de registros (ya descentralizados del primitivo NIC), como ya se ha apuntado antes.

Modificación de los protocolos exteriores de encaminamiento para soportar prefijos de red variables. Este método se conoce como CIDR (Classless Inter−Domain Routing) y consiste en la agregación de prefijos que son adyacentes para dar lugar a prefijos menores (y por tanto más generales), con lo que se reducía el número de entradas en las tablas de los routers. Por ejemplo, el RIPE−NCC ha asignado a RedIRIS el bloque 193.144.0.0/15 (131.072 direcciones) para delegar entre sus miembros, anunciándose todo el bloque como un único prefijo.

Iniciación de la asignación, según el modelo CIDR o sin−clase, de partes del espacio de direcciones que estaban reservadas, que suponen aproximadamente 1/4 del total del espacio asignable. Estas direcciones se asignarán en bloques de prefijo variable.

Para entender bien el problema hay que tener en cuenta que el período de tiempo en el que los fabricantes duplican la capacidad de proceso de sus equipos y la de sus memorias es de aproximadamente dos años. La capacidad de los routers que deben mantener en sus tablas una información completa o full−routing sobre la

topología de la Internet (equipos conectados a los backbones principales o de dominios conectados a múltiples proveedores −multi−homed) se habría hoy día superado, con el colapso consiguiente de la Internet, si CIDR no hubiese sido puesto en funcionamiento a primeros de 1994. Téngase en cuenta que al escribir esto hay más de 60.000 redes conectadas mientras que los equipos que soportan full−routing manejan del orden de los 30.000 prefijos, estando el límite de tecnología actual en torno a los 40.000 prefijos. Como dato ejemplificador, RedIRIS cuenta en su dominio interno con más de 650 redes pero sólo anuncia al exterior 32 prefijos, en su mayoría clases B históricas, con lo que se consigue una agregación óptima.

En cualquier caso, hay que entender que tanto CIDR como las políticas restrictivas de asignación de direcciones son sólo medidas temporales, dirigidas a afrontar problemas concretos y que no resuelven (en algunos casos hasta agravan) los problemas crónicos detectados en la Internet en gran parte debidos a su tremendo éxito. Así, se han llegado a plantear iniciativas como la devolución de direcciones, la obligatoriedad de cambiar de direcciones al cambiar de proveedor (en un mundo en el que los operadores telefónicos están considerando introducir mecanismos para que esto no ocurra con el número de teléfono cuando se cambie de compaqma), la asignación dinámica de direcciones, el uso de traductores de direcciones (NAT) que transformen un espacio privado de direcciones en otro perteneciente al proveedor, o incluso el cobrar una cantidad elevada por cada prefijo (no perteneciente al espacio del proveedor) que un cliente desee que su proveedor anuncie.

- Otros puntos débiles

De forma recurrente vemos como se achaca a la Internet el ser un medio de comunicación inseguro. Este es un tema con muchas aristas y que debe ser examinado en cada una de sus partes. Dado el carácter puramente académico de la Internet en el comienzo de su andadura, los asuntos relativos a la seguridad fueron, como desgraciadamente suele ocurrir en la práctica, relegados a posterior estudio hasta que los primeros ataques globales hacen sonar la alarma y empieza a producirse un notable esfuerzo en incorporar mecanismos de seguridad a las aplicaciones existentes.

Sin embargo, el problema de seguridad en el nivel de red sigue sin ser tenido en cuenta y comienza a producirse una serie de ataques cada vez más sofisticados y basados en la suplantación de la identidad de máquinas conectadas a la red, dando la posibilidad de violar un acceso prohibido o dando la posibilidad de escudriñar (o desviar) la información a intrusos. Como respuesta surgen mecanismos de barrera como los cortafuegos, pero los protocolos siguen sin incorporar medidas específicas de seguridad.

Pero esto es sólo una parte del problema. La seguridad integral comprende servicios tanto de confidencialidad como de autentificación, integridad y no rechazo para los que se requieren técnicas criptográficas que están sujetas a diferentes normativas de exportación y uso en determinados países, lo que hace complicado su uso generalizado en un medio que se tiene por libre (en cuanto a la naturaleza de la información intercambiada y su formato) y homogéneo (en cuanto al tipo de protocolos/aplicaciones empleados). Se corre el peligro de fracturar la Internet en zonas donde se puedan intercambiar información de forma segura y otras en que no, bien por considerarse tecnología de uso militar, bien por el derecho que se guardan algunos gobiernos a poder intervenir −e interpretar− las comunicaciones de sus ciudadanos.

En otro orden de cosas, estamos asistiendo al nacimiento de servicios de transmisión de información en tiempo real dentro de la Internet. Ejemplos de ello son las aplicaciones para comunicaciones de voz a través de la red y el Mbone, red virtual superpuesta a la Internet, basada en el concepto de IP Multicast [4]. Un defecto claro de IPv4 es la falta de caracterización de los distintos flujos de información que viajan por la red, dando la misma consideración a un tráfico que podría considerarse como de relleno como las NetNews, sujeto a la redundancia de un mecanismo corrector de transporte, que a una transmisión de voz en tiempo real en la que la pérdida de un número significativo de paquetes puede alterar o incluso imposibilitar la interpretación de la información. El advenimiento de este tipo de servicios en la era de las autopistas de la información presenta una clara limitación al uso de la Internet tal y como la concebimos actualmente en contraposición a otro tipo

de tecnologías orientadas a la conexión como ATM que parecen más adecuadas para los servicios en tiempo real.

Los problemas mencionados anteriormente han sido tenidos en cuenta por la comunidad Internet desde que se empezaron a predecir sus consecuencias (en mayor o menor grado de pesimismo catastrofista) lo que motivó que sus técnicos elaboraran una serie de propuestas conducentes a la creación de un nuevo protocolo para la red Internet, conocido como IP Next Generation (IPng). A finales de 1994 El IESG (Internet Engineering Steering Group), después de examinar las propuestas finales y en base a unos criterios que habían sido elaborados con anterioridad, emitió una recomendación para IPng que posteriormente se publicaría como RFC 1752 con la categoría de Proposed Standard. Dicha recomendación está siendo desarrollada actualmente por los grupos de trabajo del IETF (Internet Engineering Task Force).

En esta recomendación se asigna para IPng el número de versión 6 y pasa a denominarse formalmente como IPv6 . La decisión del IETF tiene como aspecto más importante la elección de SIPP (Simple IP Protocol Plus) como base para la elaboración de IPv6 con aspectos de otros contendientes, en particular de TUBA (TCP & UDP with Bigger Addresses) del que se toma el modelo de transición, uno de los aspectos más importantes recogidos entre los criterios de selección.

DIRECCIONES IP VERSIÓN 6

Formato de la cabecera.

Esta cabecera ocupa el doble que la versión 4, pero se ha simplificado omitiendo algunos campos y haciendo que otros sean opcionales. De esta manera, los routers no tienen que procesar tanta información. Los campos son los siguientes:

- Versión: Este campo ocupa 4 bits, y contiene el numero de versión del IP, en este caso 6.
- Prioridad: Ocupa 4 bits, y indica la importancia del paquete que se esta enviando.
- Etiqueta de Flujo: Ocupa 24 bits. Indica que el paquete requiere un tratamiento especial por parte de los routers que lo soporten.
- Longitud: Ocupa 16 bits. Indica la longitud en bytes de los datos del mensaje
- Siguiente Cabecera: Ocupa 8 bits e indica a que protocolo corresponde la cabecera que esta a continuación de la actual.
- Tiempo de vida: Ocupa 8 bits y tiene la misma función que el la versión 4.
- Dirección de origen: Ocupa 128 bits (16 octetos), y es el numero de dirección del origen.
- Dirección de Destino: Ocupa 128 bits (16 octetos). Es él numero de dirección del destino.

El cambio más significativo en las direcciones ha sido, que ahora, se refieren a un interfaz y no a un nodo, aunque como cada interfaz pertenece a un nodo, es posible referirse a estos mediante su interfaz.

El numero de direcciones diferentes se ha multiplicado de una manera exagerada. Teóricamente, es posible tener 2128 direcciones diferentes. Este numero quiere decir que se podrían llegar a tener mas de 665.000 trillones de direcciones por metro cuadrado, aunque si siguieran una jerarquía, este numero decrece hasta 1564 direcciones por metro cuadrado en el peor caso o tres trillones siendo optimistas.

En el IPv6 existen tres tipos básicos de direcciones:

Direcciones unicast: Están dirigidas a un único interfaz en la red. Actualmente se dividen en varios grupos, y existe un grupo especial que facilita la compatibilidad con las direcciones de la versión 4.

La dirección de destino especifica una sola computadora(anfitrión o ruteador); el datagrama deberá rutearse hacia el destino a lo largo de la trayectoria más corta. Para asignar direcciones unicast a equipos se dispone de más de 3.750 millones de direcciones (0.0.0.0−223.255.255.255) que se agrupan de forma topológica en forma de parte de red (los bits más significativos o más a la izquierda), que es común a todos los miembros de la unidad topológica pudiendo ser ésta una red local, una organización o un proveedor y parte local (los bits menos significativos) que es diferente para cada ente individual.

Direcciones anycast: Identifican a un conjunto de interfaces de red. El paquete se enviara a cualquier interfaz que forme parte del conjunto. En realidad son direcciones unicast que se encuentran asignadas a varios interfaces.

Direcciones multicast: Identifican a un conjunto de interfaces de la red, de manera que cada paquete es enviado a cada uno de ellos individualmente. El destino es un conjunto de computadoras, posiblemente en múltiples localidades. Una copia del datagrama deberá entregarse a cada miembro del grupo que emplee hardware de multicast o de difusión si están disponibles.

Direcciones Broadcast: El destino es un conjunto de computadoras en el que todas comparten un solo prefijo de dirección , el datagrama deberá rutearse hacia el grupo a través de la trayectoria más corta y después, entregarse exactamente a un miembro del grupo.

Las direcciones de broadcast no existen en IPv6. Son casos particulares de direcciones multicast. Estas últimas incorporan un campo de ámbito, en sustitución del parámetro TTL usado en la actualidad para determinar el rango de actuación de una sesión multicast.

Las cabeceras de los paquetes han sido simplificadas en IPv6 eliminando los campos no utilizados y añadiendo el concepto de cabeceras de extensión. Estas permiten seleccionar facilidades especiales de encaminamiento, fragmentación y seguridad así como el manejo de opciones, que han sido eliminadas de la cabecera IPv6. Cada cabecera incluye un campo que define el tipo de cabecera que le sigue a continuación, hasta llegar a la de transporte, con lo que se agiliza el proceso de los paquetes.

En IPv6 la fragmentación/ensamblado de paquetes es una tarea de los sistemas finales con lo que de nuevo se facilita la vida a los routers para que se entreguen a su misión primordial, encaminar paquetes. La unidad máxima de transmisión (MTU) de un enlace es ahora como mínimo de 576 octetos (68 en IPv4).

El encaminamiento propuesto permitirá la selección de proveedor por parte del originador así como la movilidad mediante el empleo de cabeceras de extensión de encaminamiento en la que se especifique un camino elegido (que será recorrido a la inversa al regreso) mediante direcciones unicast o anycast.

La transmisión de información en tiempo real se podrá realizar mediante el empleo de dos campos en la cabecera IPv6. La prioridad, que distingue los diferentes tipos de datagramas según la clase de servicio y la etiqueta de flujo, que permite diferenciar y asignar distintos estados a distintos flujos originados por la misma fuente.

Por fin, la seguridad en el nivel de red será una realidad mediante el empleo de cabeceras de extensión de autentificación, que proporciona servicios de verificación de identidad e integridad y de encapsulado de seguridad que proporciona servicios de confidencialidad. En el primer caso no se plantean problemas de exportación de tecnología por tratarse de un procedimiento de verificación (se cifra una función del contenido,

pero no el contenido en sí) mientras que en el segundo caso todos los malos presagios mencionados en el capítulo anterior salen a relucir. Más sorprendente es aún el hecho de que, de acuerdo con las especificaciones, todo producto que pretenda ser conforme a IPv6 ha de incluir necesariamente ambos mecanismos de seguridad a pesar de los impedimentos expuestos.

CONSIDERACIONES Y VENTAJAS ADICIONALES

En IPv6 el método propuesto se basa primordialmente en la coexistencia de ambos protocolos. Los nuevos sistemas que vayan incorporando IPv6 (computadores y routers) deberán mantener asimismo la plena capacidad de procesar paquetes IPv4.

Para conectar las islas IPv6 que irán emergiendo mediante la infraestructura Internet actual se emplearán técnicas de encapsulado (túneles IPv6) en los datagramas IPv4 de forma similar a como funciona en la actualidad el Mbone. A medida que los routers vayan incorporando IPv6, los túneles se irán desmantelando para dar paso a una infraestructura ya basada en IPv6.

Respecto a las aplicaciones actuales, la migración a IPv6 requiere que todas las referencias a direcciones de 32 bits sean sustituidas por las nuevas de 128. Desgraciadamente eso supone cambiar prácticamente todas la aplicaciones existentes. Además, un nuevo tipo de registro deberá ser definido en el DNS para realizar la transformación de los nombres de dominio actuales (que no requieren cambio) en direcciones de 128 bits. Este nuevo registro es el AAAA y la traducción inversa de direcciones a nombres se realizará dentro de la nueva zona ip6.int dispuesta a tal efecto.

Otras ventajas del nuevo IP son el aumento de los recursos de seguridad para los datos que viajan por Internet, mayor calidad de soporte de aplicaciones, comunicaciones en tiempo real y mejor rendimiento del routing.

Posibilidades de autenticación y de confidencialidad. IPv6 define extensiones que permiten la autenticación de los usuarios y la integridad de los datos mediante herramientas de criptografía.

Posibilidades de autoconfiguración. IPv6 contiene varias formas de autoconfiguración como la configuración "Plug and Play" de direcciones de nodos sobre una red aislada gracias a las características ofrecidas por DHCP.

Posibilidades para el "Source Route". IPng tiene una función extendida de Source Routing gracias a SRDP (Source Demand Routing Protocol) para difundir el routing a rutas interdominio e intradominio.

Un nuevo mecanismo en el IPv6 soporta reservación de recursos y permite a un ruteador asociar cada datagrama con una asignación de recursos dados. La atracción subyacente, un flujo, consiste en una trayectoria a través de una red de redes a lo largo de la cual ruteadores intermedios garantizan una calidad de servicio específica.

La autoconfiguración de direcciones es una característica que permite a un host configurar una o más direcciones por interface automáticamente. El propósito de la autoconfiguración es permitir a un host operar en modo "plug & play", esto es, permitir a una máquina ser conectada en la red y que inmediatamente esté lista para usarse sin necesidad de intervención manual. La autoconfiguración es un elemento importante en la escalabilidad de Internet debido sobre todo a sus facilidades en el proceso de traer nuevos usuarios a la red, ya que resulta impráctico para todos y cada uno de los hosts el requerir la configuración del sistema antes de que éste sea utilizado, además, la mayoría de los usuarios no saben lo suficiente o no tienen el deseo de llevar a cabo las tareas de configurar su sistema.

Las direcciones requieren ser configuradas cada vez que una interface es inicializada, y tal vez se requiera que sea reconfigurada por otros motivos, por ejemplo si un host va a ser movido a otra subred, etc.

Para ser útil en varios ambientes de red, la autoconfiguración debe tener ciertas características:

Debería soportar redes simples, sin enrutadores y sin servidores, así como topologías más complejas.

Debería soportar diferentes niveles e control administrativo del sistema.

IP Versión 6: Compatibilidad con IP versión 4

Como ya se comento anteriormente, IP versión 6 tiene la gran ventaja de que es compatible con su anterior versión de 32 bits, lo que le permite coexistir en la misma red. Las implementaciones de este nuevo protocolo empiezan a estar disponibles, y gracias a su compatibilidad permiten a los administradores de redes y directores de sistemas ir realizando las mejoras necesarias en sus equipos de forma temporal, teniendo en cuenta sus posibilidades y sin importar el tiempo empleado.

Además, IP versión 6 puede funcionar de forma concurrente en la misma maquina con IP versión 4, salvo que se configure para trabajar en modo único. Además, un ordenador con IP versión 6 puede comunicarse con otro con la versión 4 sin que este ultimo note la diferencia de protocolos.

También IP versión 6 permite que los paquetes puedan ser "tuneleados" a través de una red existente con el IP versión 4, característica que

permite a los administradores del sistema renovar gradualmente sus equipos para acogerse al nuevo protocolo.

CONCLUSIONES

En caso de que la nueva versión de IP logra cumplir con la mayoría de las demandas, presentes y futuras, de las redes modernas, mantiene una total compatibilidad con la base actualmente instalada, al tiempo que proporciona una ruta de migración fácil y poco costosa, no cabe duda que será un contrincante muy importante en la arena de los protocolos de red, sobretodo por mantener una Internet libre de estándares propietarios.

Con el tiempo, IPv6 llegará a nuestras empresas. Por tanto, debemos estar seguros de entender qué es IPv6 para poder aplicar correctamente esta tecnología en nuestras redes.