ANEXOS

1 Origen del Protocolo IPv6

Protocolo de Internet versión 6 (IPv6), también llamado IP next generation (IPng), es la nueva versión del protocolo IP, por lo que reemplaza a la versión 4. Se establece versión 6, debido a que se le asignó versión 5, al protocolo experimental denominado Internet Stream (STD-2), el cual nunca fue un sucesor de IPv4 [11].

Se establecieron diversas propuestas antes de definir al protocolo IPv6. De acuerdo a la RFC 1752, se definieron tres propuestas: Simple Internet Protocol Plus - SIPP, TCP and UDP with Bigger Addresses – TUBA y Common Architecture for the Internet – CATNIP, de las cuales se consideraron principalmente las características de SIPP y TUBA [101].

Finalmente, IPv6 se describe con la publicación de la RFC 1883 "Internet Protocol, Version 6 (IPv6) Specification", publicada en 1995 [4]. Posteriormente se publica, en 1998, la RFC 2460, dejando obsoleto a la RFC 1883 [4].

2 Características del Protocolo IPv6

La característica principal del protocolo IPv6 es el incremento del tamaño de la dirección IP de 32 bits (IPv4) a 128 bits, alcanzado un total de direcciones IP teórico de 2^{128} o 340 sextillones de direcciones aproximadamente, logrando de esta manera tener un gran número de direcciones IP disponibles para el crecimiento futuro de la Internet [1] [4].

Otras principales características de la versión 6 del protocolo IP se describen a continuación [1] [12]:

- **Simplificación del formato de cabecera:** IPv6 considera en su cabecera 8 campos, con una longitud fija de 40 Bytes. Esto ha permitido mejorar el tiempo de procesamiento de la cabecera IPv6 en el proceso de encaminamiento [1] [12].
- **Soporte mejorado para las extensiones y opciones:** IPv6 considera diversas opciones de tratamiento del paquete en las denominadas "Cabeceras de extensión", las cuales son enviadas solo si son necesarias [4]. Esto permite un procesamiento de la cabecera más eficiente, insertando funcionalidades adicionales y flexibilidad del protocolo para nuevas tecnologías [12] [4].
- **Capacidad de etiquetado de flujo:** Para el tratamiento especial del paquete, IPv6 agrega el campo denominado "Etiqueta de flujo (Flow Label)" [1]. El cual permite al origen etiquetar el paquete para que este reciba un tratamiento especial durante su encaminamiento [12]. Generalmente hacer usado por tráfico que requiere calidad de servicio, como las transmisiones en tiempo real (audio y video) [1] [12].
- **Capacidades de autenticación y privacidad:** IPv6 permite agregar funcionalidades de encriptación y autenticación con la finalidad de garantizar la integridad y confidencialidad de los paquetes [1] [12].

- **Conexión de extremo a extremo:** IPv6 elimina el concepto de la traducción de direcciones (NAT), permitiendo la comunicación entre el origen y destino de forma directa.
- **Autoconfiguración:** IPv6 considera diversos mecanismos que permiten la autoconfiguración de los parámetros de red de los host cuando estos son conectados a la red. La autoconfiguración simplifica el despliegue del protocolo y mejora la administración del recurso IP.

En la Figura 1, se muestra a detalle el formato de la cabecera IPv6 [12].

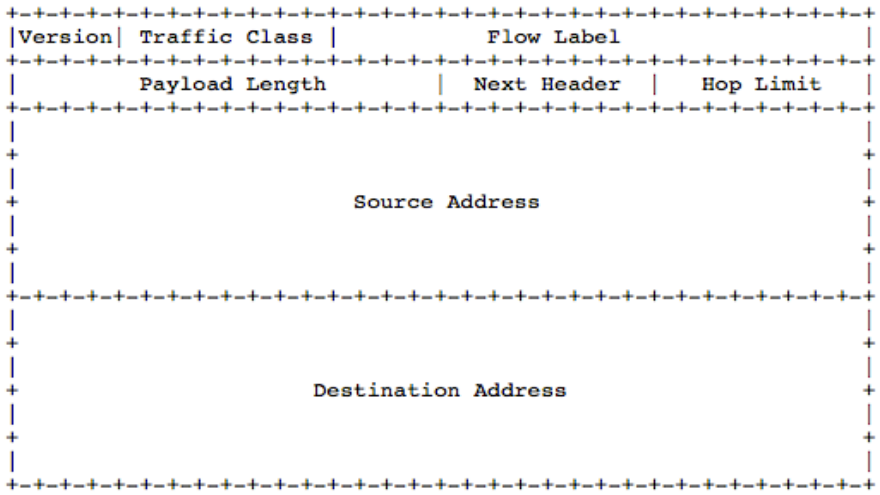

Figura 1 – Cabecera del Protocolo IPv6

Fuente: RFC 2460 [12]

A continuación se describe las funciones de cada campo:

- **Versión (4 bits):** Establece la versión del protocolo. Tiene asignado el valor 0110 en binario (6 en decimal) [12].
- **Clase de tráfico o prioridad (8 bits):** Este campo reemplaza al campo ToS (Type of Service) descrito en IPv4 [13] [4]. El funcionamiento a detalle está definido en la RFC 2474 [13] [4]. De manera general este campo define la prioridad del paquete respecto a otros del mismo origen [12]. Ante una congestión, se elimina el paquete con menor prioridad [1]. Este campo divide el tráfico en dos categorías: tráfico con control de congestión y tráfico sin control de congestión [1]. Básicamente, estas dos categorías, se diferencian en la capacidad de adaptación o de la aceptación de ciertos paquetes a tráficos lentos, en los cuales es aceptable el retraso, desorden o pérdida de los paquetes [1]. Tráficos en tiempo real, que transportan paquetes de voz y/o video, son considerados en la categoría de "tráfico sin control de congestión" [1]. En la Tabla 2, se muestran algunos valores.

Tabla 1 Prioridades para congestión - Control de Tráfico

Prioridad	Significado
0	No specific traffic
1	Background data
2	Unattended data traffic
3	Reserved
4	Attended bulk data traffic
5	Reserved
6	Interactive traffic
7	Control traffic

Fuente: TCP/IP Protocol Suite – 3rd ed. [1]

- **Etiqueta de flujo (20 bits):** Este campo permite establecer un tratamiento especial, por parte de los enrutadores, a un flujo de paquetes que comparten las mismas características (dirección origen y destino, puerto origen y destino, e incluyendo las cabeceras de extensión de ser el caso) [4] [12]. Esto permite acelerar el procesamiento de enrutamiento, ya que no vuelve a procesar la cabecera del resto de paquetes que tengan la misma etiqueta de flujo, evitando realizar nuevamente el proceso de enrutamiento y determinación de ruta [1] [4]. La dirección origen y la etiqueta de flujo identifican de forma exclusiva al flujo de paquetes [1]. La etiqueta de flujo recibe un valor aleatorio entre 00001 a FFFFF [4]. Sin embargo a la fecha de escrito esta tesis, el uso de este campo es todavía considerado como experimental, la IETF ha publicado la RFC 6294 y RFC 7098, para impulsar su utilización [4].
- **Longitud de la carga útil (16 bits):** Este campo establece el valor de la longitud de las cabeceras de extensión que acompañan a la cabecera IPv6 más los datos encapsulados de nivel superior [1], [4], [12]. El valor máximo que se establece es de 65,536 bytes, esto debido al tamaño de 16 bits de este campo [4]. IPv6 tiene la opción de enviar paquetes grandes denominados "Jumbograms", y puede ser habilitado cuando los host soporten tramas grandes (mayores a 65,536 bytes) [4].
- **Cabecera siguiente (8 bits):** Este campo establece el valor que define al tipo de cabecera que acompaña a la cabecera IPv6 [1] [12] [4]. Este valor puede indicar una cabecera de capa superior como TCP (Valor=6) ó UDP (valor=17) u otros; pero si la cabecera IPv6 usa las cabeceras de extensión, este campo definirá el valor según corresponda a la cabecera de extensión que acompaña a IPv6 [4] [12]. Los diversos valores están establecidos por la IANA y pueden ser consultados en la referencia [14]. En la Tabla 2 se muestra alguno de los valores:

Tabla 2 Código del Campo "Cabecera Siguiente"

Código	Cabecera Siguiente
0	Hop-by-hop option
2	ICMP
6	TCP
17	UDP
43	Source routing
44	Fragmentation
50	Encrypted security payload
51	Authentication
59	Null (No next header)
60	Destination option

Fuente: TCP/IP Protocol Suite – 3rd ed. [1]

- **Límite de saltos (8 bits):** Este campo establece el máximo número de saltos (256 saltos) de recorrido de un paquete durante su transmisión [4] [12]. Por cada nodo que reenvía el paquete se disminuye en 1 el valor máximo [4] [12]. Si un enrutador recibe un paquete, y este al reenviarlo disminuye en 0 el valor, el paquete es descartado automáticamente [4] [12]. Al ocurrir este descarte, el enrutador envía un mensaje de error ICMPv6 "Limite de salto en transmisión" al remitente [4].
- **Dirección Origen y Destino (128 bits cada uno):** Estos dos campos definen la dirección del protocolo de internet versión 6 de origen y destino [4] [12]. Durante la transmisión del paquete, desde el origen al destino, el campo no se modifica o altera [1].

  La nueva estructura de IPv6, establece el concepto de "cabeceras de extensión", la cual considera algunas de las funciones establecidas en el campo "Opciones" de IPv4. Estas cabeceras son insertadas a continuación de la cabecera IPv6, pero solo si son establecidas por el remitente. El máximo número de cabeceras de extensión son seis (06) cabeceras, las cuales son procesadas en los extremos (Origen y Destino), a excepción de la cabecera "Salto a Salto", la cual es procesada en cada salto del paquete. Esta nueva estructura permite simplificar el procesamiento de la cabecera IPv6.

  El análisis detallado de las "cabeceras de extensión" no es materia de la presente tesis; sin embargo describiremos, de manera general, cada una de estas cabeceras de extensión:

- **Cabecera opciones de salto a salto:** Esta cabecera se utiliza para llevar información opcional de enrutamiento específico de salto a salto, el cual debe ser examinado por cada nodo que intervenga en el proceso de comunicación entre el emisor (Origen) y el receptor (Destino) [4] [12]. Se identifica a esta cabecera, cuando el valor del campo "Cabecera Siguiente", de la cabecera precedente, tiene el valor de 0 [4]. La cabecera de "Opciones de Salto a Salto", comprende tres (03) campos: Cabecera Siguiente, Longitud de Cabecera de Extensión y el campo Opciones (Figura 2) [12].

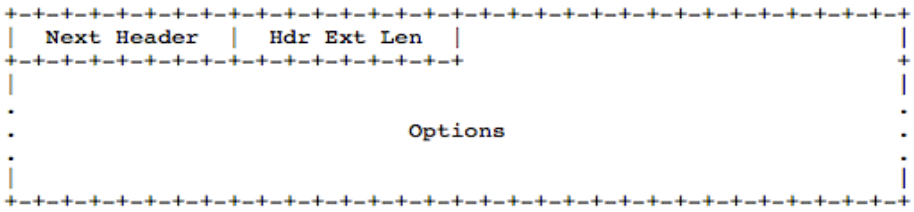

Figura 2 Formato de cabecera "Opciones de Salto a Salto"

Fuente: RFC 2460 [12]

El campo "Cabecera Siguiente" de tamaño de 8 bits, indica el valor del tipo de cabecera que sigue inmediatamente a esta cabecera; el campo "Longitud de Cabecera de Extensión", de 8 bits de tamaño, indica la longitud de esta cabecera; y el campo "Opciones", el cual es un campo de longitud variable, que define el uso de diversas opciones como el uso de paquetes de tamaño grandes denominados "Jumbograms", el cual permite enviar paquetes mayor a 65,536 bytes, pero no mayor a 4,294'967,296 bytes, ya que tiene un tamaño de 32 bits (en la RFC 2675 se describe el uso de Jumbograms) [4] [12]. En el campo "Opciones" se establecen diversas alertas para el procesamiento del paquete por parte de los nodos que lo procesen, estas alertas han sido definidas por la IETF en la RFC 6398 [4].

- **Cabecera de enrutamiento:** Esta cabecera se utiliza para que un origen IPv6 establezca una lista de uno o más nodos intermedios a ser visitados en el camino hacia el destino de un paquete [12]. Esta cabecera es identificada con el valor 43, el cual es establecido en el campo "Cabecera Siguiente" de la cabecera precedente [4] [12]. Esta cabecera, comprende 5 campos: Cabecera Siguiente, Longitud de Cabecera de Extensión, Tipo de Enrutamiento, Segmentos Dejados y Datos Específicos del Tipo (Figura 3) [4] [12].

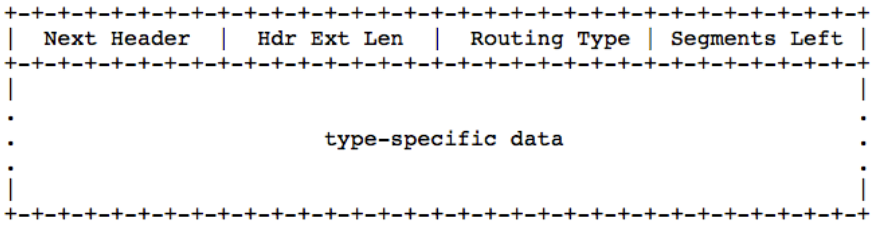

Figura 3 Formato de Cabecera "Enrutamiento"
Fuente: RFC 2460 [12]

El campo “Cabecera Siguiente” y “Longitud de Cabecera de Extensión” tienen un tamaño de 8 bits, cada uno. Estos campos cumplen las mismas funciones que las descritas en la cabecera de “Opciones de Salto a Salto” [4] [12]. El campo “Tipo de Enrutamiento”, de un tamaño de 8 bits, se encuentra especificada en la RFC 5095 [4]. El campo “Segmentos Dejados”, de un tamaño de 8 bits, indica el número de nodos restantes antes de que el paquete alcance el destino final [4] [12]. Finalmente el campo “Datos Específicos del Tipo”, es de longitud variable múltiplo de 8 bytes [4] [12].

- **Cabecera de fragmento:** Esta cabecera tiene un tamaño fijo de 8 bytes (64 bits) [4] [12]. Su función principal es la de fragmentar el paquete, de acuerdo al MTU máximo soportado por el camino que utilizará hacia su destino [4] [12]. Esta función es similar a la fragmentación realizada en IPv4; pero, IPv6 solo fragmenta el paquete en el origen y no en cada enrutador que atraviesa hasta su destino [4]. Esta cabecera es identificada con el valor 44, el cual es establecido en el campo “Cabecera Siguiente” de la cabecera precedente [4] [12]. Esta cabecera, comprende 6 campos: Los campos “Cabecera Siguiente” y “Reservado”, de tamaño de 8 bits cada uno; el campo “Desplazamiento del Fragmento” de tamaño de 13 bits; el campo “Reservado” de tamaño de 2 bits; el campo “M-flag” de 1 bit de tamaño y el campo “Identificación” con un tamaño de 32 bits (Figura 4) [4] [12].

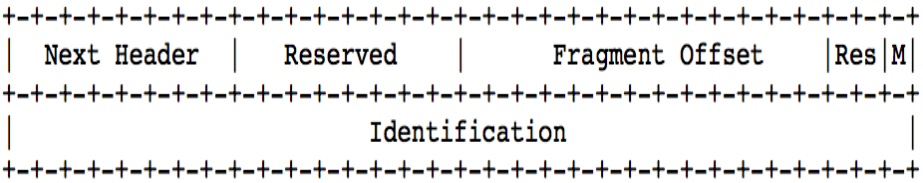

Figura 4 Formato de Cabecera "Fragmento"
Fuente: RFC 2460 [12]

- **Cabecera de opciones de destino:** Esta cabecera de longitud variable, se encarga básicamente de transportar información que se requiere ser analizada por el destino. Esta cabecera puede aparecer hasta dos veces en un paquete IPv6, cuando se inserta

antes de la cabecera de extensión “Enrutamiento”, tendrá información a ser examinada por los enrutadores; y cuando se inserta antes de la cabecera de los datos encapsulados de la capa superior, tendrá información a ser examinada solo por el enrutador final. Esta cabecera es identificada con el valor 60, el cual es establecido en el campo “Cabecera Siguiente” de la cabecera precedente [4] [12]. Esta cabecera, comprende 3 campos: “Cabecera Siguiente” y “Longitud de Cabecera de Extensión”, de tamaño de 8 bits cada una, y el campo “Opciones” de longitud variable (Figura 5) [4] [12].

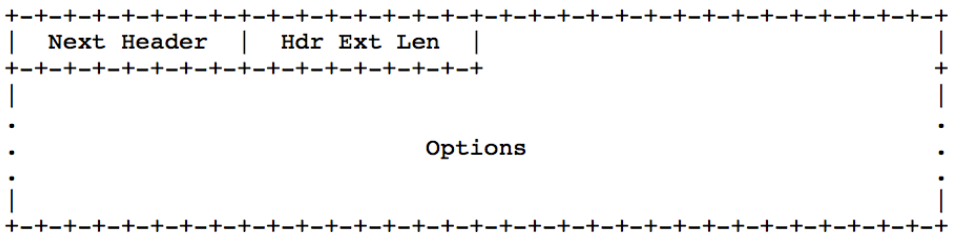

Figura 5 Formato de Cabecera "Opciones de Destino"

Fuente: RFC 2460 [12]

El campo “Opciones”, puede ser utilizado por diversas aplicaciones como IPv6 en las comunicaciones móviles, establecimiento de túneles en IPv6 descrito en la RFC 2473, entre otras [4]. La IANA compila las diversas aplicaciones que a la fecha se tienen para este campo, esta información puede ser consultada mediante la referencia [15].

- **Cabecera de autenticación:** Este campo proporciona integridad y autenticación de extremo a extremo durante el transporte del paquete IP, pero no provee la confidencialidad [4] [16]. Esta cabecera es identificada con el valor 51, el cual es establecido en el campo “Cabecera Siguiente” de la cabecera precedente [4] [16]. La cabecera soporta diversos mecanismos de autenticación los cuales se detallan en la RFC 4302 [4]. La estructura de esta cabecera considera 6 campos: “Cabecera Siguiente” y “Longitud de Cabecera de Extensión”, de 8 bits cada una; el campo “Reservado” de tamaño de 16 bits; los campos “Indexación de Parámetros de Seguridad” y “Secuencia de Número de Campo”, cada una de 32 bits de tamaño; y el campo “Comprobación de Integridad de Valor” de longitud variable (Figura 6) [4] [16].

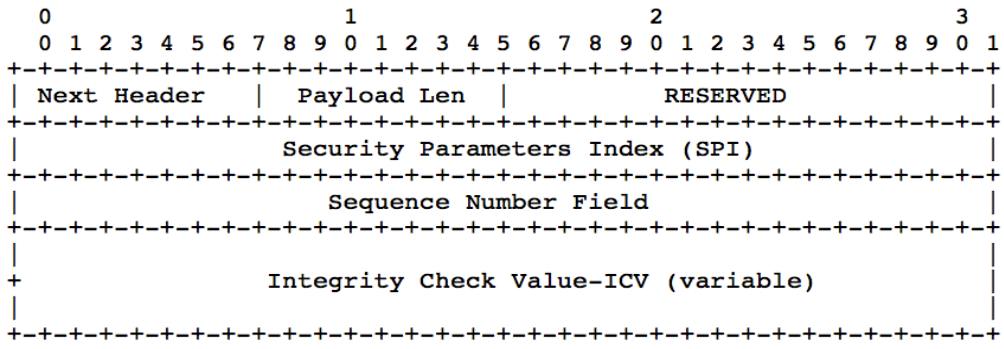

Figura 6 Formato de Cabecera "Autenticación"
Fuente: RFC 4302 [16]

- **Cabecera de seguridad del encapsulado de la carga útil:** Esta cabecera proporciona confidencialidad, integridad sin conexión, autenticación del origen de datos, anti-replay y la confidencialidad del flujo de tráfico de extremo a extremo durante el transporte del paquete IP [4] [17]. Esta cabecera se usa previa negociación entre los organismos que participen de la comunicación. Esta cabecera es identificada con el valor 50, el cual es establecido en el campo "Cabecera Siguiente" de la cabecera precedente [4] [17]. Esta cabecera es de longitud variable conformada por 4 campos en la cabecera: "Indexación de Parámetros de Seguridad" y "Secuencia de Número de Campo", con un tamaño de 32 bits cada una; el campo "Datos de Carga Útil (Payload Data)" y el campo "Comprobación de Integridad de Valor de Longitud", ambos de longitud variable. Esta cabecera considera 3 campos que son colocados en la parte de la cola: los campos "Longitud de Relleno", "Cabecera Siguiente (ambos de tamaño de 8 bits) y el campo "Opciones de Relleno (Padding)" de hasta 255 bytes de tamaño (Figura 7) [4] [17].

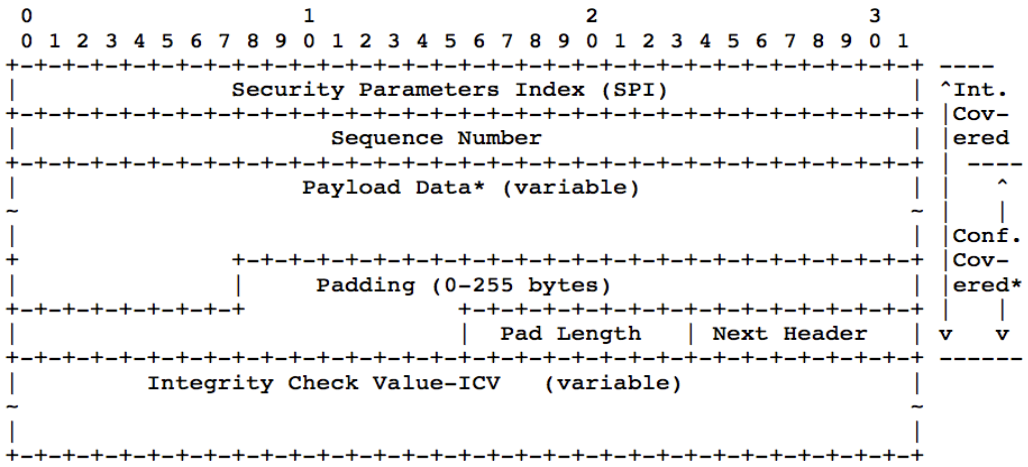

Figura 7 Formato de Cabecera "Seguridad de Encapsulado de la Carga Útil"

Fuente: RFC 4303 [17]

3 Direccionamiento Lógico en IPv6

La dirección IPv6 está conformada por 128 bits, su representación se realiza en notación hexadecimal con dos puntos, que se divide en 8 grupos de 16 bits o 4 dígitos en notación hexadecimal [1].

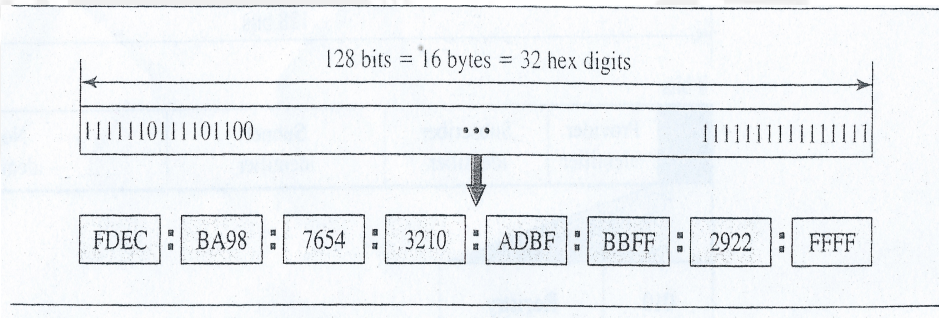

Figura 8– Dirección IPv6

Fuente: TCP/IP Protocol Suite – 3rd ed. [1]

IPv6 utiliza una representación con prefijo para identificar la subred o un tipo de dirección específica [18]. Esta representación es similar a la representación utilizada por CIDR en IPv4 [4] [18]. La longitud de prefijo se escribe en notación decimal, y este, especifica cuantos bits de izquierda a derecha debe considerarse como subred o un tipo de dirección [4] [18]. Por ejemplo, la dirección IPv6 2001:db8::/32, tiene como valor de prefijo 32, este valor nos indica que el prefijo está conformado por los 32 primeros bits (de izquierda a derecha) y el resto de bits (96 bits) nos permitirá crear sub-redes o asignar direcciones IPv6 a los host. La IETF especifica la notación por prefijo en la RFC 4291 [4].

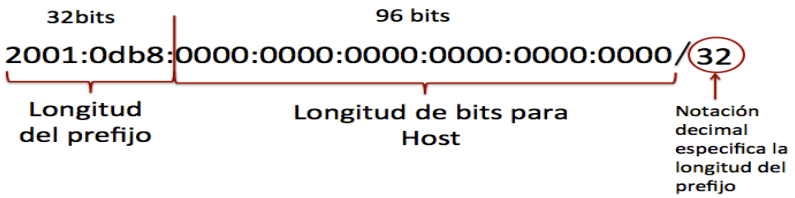

Figura 9 – Estructura de la dirección IPv6

Fuente: RFC 4291 [18]

La estructura de una dirección IPv6 es extensa, exactamente 32 dígitos hexadecimales; por consiguiente, con la finalidad de hacer más fácil su administración, la IETF, ha publicado la RFC 5952, en la que se describen diversas recomendaciones para la representación abreviada de una dirección IPv6 [4] [19]. Algunas de estas recomendaciones son [4] [19]:

- Los ceros iniciales deben ser suprimidos (de izquierda a derecha). (ver Tabla 3)
- Un único campo de 16 bits, en donde todos sean ceros, debe estar representado por un cero y no por un doble dos puntos (::). (ver Tabla 3)
- Utilizar doble dos puntos cuando se tengan dos o más grupo de 16 bits de forma consecutiva (::). (ver Tabla 3)
- Siempre acortar el mayor número de ceros. (ver Tabla 3)
- Si dos bloques de cero no consecutivos son largos, abrevie el primero. (ver Tabla 3)
- Utilizar minúsculas para representar a, b, c, d, e, f. (ver Tabla 3)

Tabla 3 – Ejemplos de abreviación de direcciones IPv6

Fuente: Elaboración propia

Dirección en formato normal	Abreviación correcta	Abreviación incorrecta
2001:0db8:0000:0000:06c0:0000:0000:0000	2001:db8::6c0:0000:0000:0000	2001:db8::6c::
2001:0db8:0000:6500:0000:0000:0000:0010	2001:db8:0:6500::10	2001:Db8::65::1

Es importante considerar todas las recomendaciones descritas en la RFC 5952, para tener una sólida administración del espacio de direcciones. Adicionalmente podemos usar "[ ]" para indicar un puerto como por ejemplo: http://[2001:db8:0:6500::10]:8080.

Las direcciones IPv6 se clasifican en tres tipos, los cuales están descritos en la RFC 4291: Unicast. Anycast y Multicast. A continuación describimos cada una de estas:

3.1 Unicast

Es una dirección IPv6 que puede ser asignada a una interfaz, el cual le permitirá enviar y recibir datos [4] [18] [20]. Existen diversos tipos de direcciones unicast, entre las principales se tiene: Global Unicast, Unique Local y la Link-Local [18].

- ***Las direcciones Global Unicast***, se identifican por sus 3 primeros bits (de izquierda a derecha) que están asignados con los valores 001 en su primer cuarteto (Nibble), esta viene a ser representado en su notación hexadecimal con prefijo 2000::/3 o 3000::/3 [4] [20]. Este tipo de direcciones es asignada por la IANA a los RIR. Las direcciones Global Unicast son exclusivas globalmente, permitiendo a los nodos comunicarse a nivel de Internet [4] [20], cumpliendo un propósito similar al de las direcciones IPv4 públicas [4] [20]. La siguiente figura muestra el formato de este tipo de dirección unicast [4] [20].

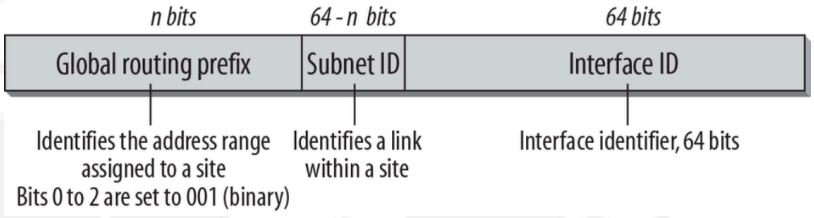

Figura 10 – Formato dirección Unicast global

Fuente: IPv6 Essentials [4]

- ***Las direcciones Unique-Local,*** se identifica con el prefijo de fc00::/7 y se encuentra detallada en la RFC 4193 [4] [20]. Este bloque de direcciones es asignada a nivel local y de uso privado por parte de las organizaciones, no siendo reconocida para su enrutamiento a través de Internet [4] [20]. Su propósito es similar a las direcciones IPv4 privadas descritas en la RFC 1918. La siguiente figura muestra su formato [4]:

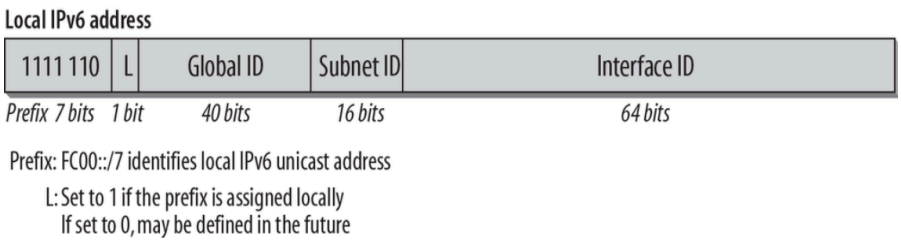

Figura 11 – Formato dirección Unicast local

Fuente: IPv6 Essentials [4]

- ***Las direcciones unicast Link-Local,*** se identifica con el prefijo fe80::/10 y se encuentra definido en la RFC 4291 [4] [18] [20]. Este tipo de direcciones es

generado automáticamente por los host, el cual utiliza los diez primero bits del número hexadecimal fe80, 54 ceros binarios adicionales y los últimos 64 bits que son el ID de interfaz de host, con formato EUI-64 [4] [20]. Su propósito es la de enviar paquetes a través de un mismo segmento de red y son utilizados por el Neighbor Discovery Protocol (NDP) y/o DHCPv6 [37]. Este tipo de direcciones nunca son reenviadas por los router a otras subredes o redes [4] [20].

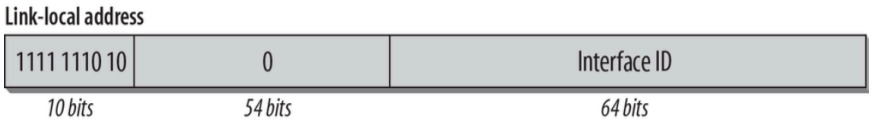

Figura 12 – Formato dirección Unicast de enlace
Fuente: IPv6 Essentials [4]

Según los diferentes subtipos de direcciones unicast, se puede observar, en su formato, el campo "Interface ID", a este campo se le asigna cualquier valor, siempre y cuando no exista otra interfaz de la misma subred que tenga asignado el mismo valor. En la RFC 4291, se especifica un método de asignación del valor en este campo, en base a la dirección MAC de la interfaz. Este método, llamado EUI-64, es usado para establecer el valor de la dirección unicast Link-Local, y su procedimiento consiste en insertar entre el ID compañía y el ID extensión de la dirección física (MAC) el valor fffe. A este procedimiento, también se realiza la modificación del séptimo bit (de izquierda a derecha), este bit es denominado como "bit universal/local" (U/L), cuando el valor del bit esta en cero, significa que es una dirección MAC administrada de forma universal, y cuando tiene establecido el valor 1, significa que la dirección MAC es administrada de forma local [18].

3.2 Anycast

Esta dirección es asignada a múltiples interfaces. Cuando el paquete es enviado, solo la interfaz mas próxima al origen recibe el paquete [4] [18] [20]. Las direcciones anycast son extraídas del rango de direcciones unicast, por lo que no son sintácticamente reconocidas [4]. Este tipo de dirección no nace con IPv6, su desarrollo viene desde 1993, con la publicación de la RFC 1546, en donde se especifica su uso experimental en redes IPv4 [4]. Cada interfaz que forma parte de un grupo anycast, debe tener configurado una dirección anycast que sea reconocido por los enrutadores intermedios, solo el nodo con la interfaz mas cercana al emisor recibirá el paquete [4], la cercanía (distancia) lo determina el protocolo de enrutamiento que se utilice.

La RFC 2526, especifica las direcciones anycast reservadas [21], en esta RFC se describe las siguientes direcciones como reservadas:

Decimal	Hexadecimal	Description
127	7F	Reserved
126	7E	Mobile IPv6 Home-Agents anycast
0-125	00-7D	Reserved

Figura 13 – Direcciones Anycast reservadas

Fuente: RFC 2526 [21]

La RFC 7094, especifica su uso e implementación en las redes IPv6 a mas detalle [4].

3.3 Multicast

Este tipo es similar al tipo anycast; pero, en este tipo, todas las interfaces del grupo reciben el paquete [4] [18] [20]. El prefijo multicast es ff00::/8 [4] [20]. Cuando un paquete es enviado a una dirección multicast, este es enviado a todo el grupo multicast [4] [20]. El emisor no tiene que enviar el paquete de manera individual a cada receptor que forma parte del grupo; ya que solo se genera un único paquete de multicast, el cual es enviado a todos los miembros del grupo, lo que reduce el número de paquetes generados significativamente en el origen [4]. El formato de la dirección multicast se muestra en la siguiente figura [4]:

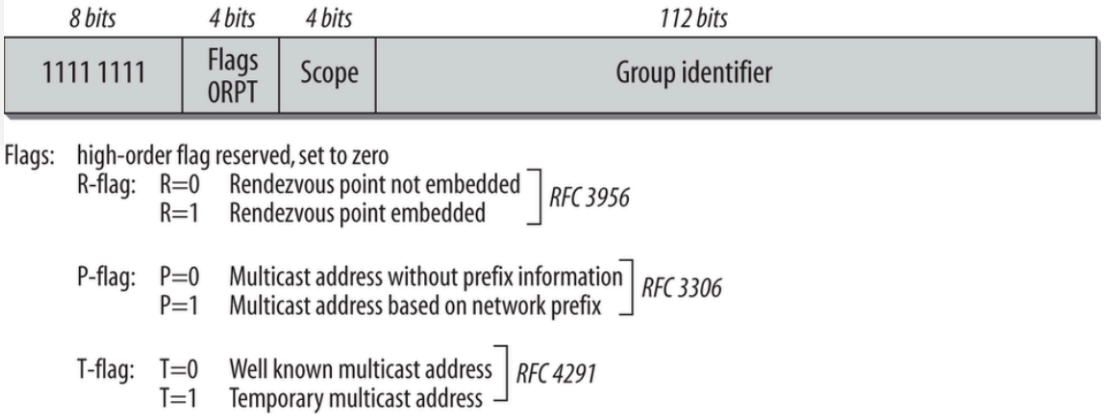

Figura 14 – Formato dirección multicast

Fuente: IPv6 Essentials [4]

Los 8 primeros bits son ceros, lo cual permite identificar una dirección multicast [4] [18]. Los siguientes 4 bits, define el campo flag, el cual establece que el primer bit, de este cuarteto, es cero, ya que esta reservado para su uso futuro [4] [18]. El segundo bit, indica si esta dirección es considerada un punto de encuentro para manejar múltiples grupos (la RFC 3956 especifica el concepto de punto de encuentro denominado “Rendezvous Point”) [4]. El tercer bit, se utiliza en un formato ampliado, y este especifica si la dirección de multicast se

basa en el prefijo de red o no (la RFC 3306 especifica este concepto) [4]. Por último, el cuarto bit, indica si la dirección multicast es permanente o temporal [4].

El campo scope, permite definir el alcance del paquete multicast en su recorrido [4] [18]. Un valor de 2, que en formato hexadecimal seria ff02, tiene un alcance de enlace local y solo será distribuido a nivel local [4]. Un valor de 5, ff05, tiene un alcance de site-local, solo será distribuido hasta la frontera del sitio [4]. Un valor de "e", ff0e, tiene alcance global. Estos valores son especificados en al RFC 4291 y en la RFC 4007 [4].

Los 112 bits restantes, establece la identificación del grupo de multicast. Su utilización se especifica en la RFC 3307 [4] [18].

En la Tabla 4 se describe alguna de las direcciones multicast reservadas publicadas por la IANA:

Tabla 4 – Protocolos de enrutamiento actualizados

Dirección	Descripción
Node-Local Scope	
ff01::1	All-nodes address
ff01::2	All-routers address
ff01::fb	mDNSv6
Link-Local Scope	
Ff02::4	DVMRP routers
Ff02::5	OSPFIGP
Ff02::9	RIP routers
Ff02::a	EIGRP routers
Ff02::b	Mobile agents
Ff02::16	All MLDVv2-capable routers
Ff02::1:2	All-dhcp-agents
Site-Local Scope	
Ff05::fb	mDNSv6
Ff05::1:3	All-dhcp-servers

Fuente: IANA [38]

3.4 Direcciones Reservadas

Estas direcciones son designadas para usos específicos, las cuales se listan a continuación [37]:

Tabla 5 – Direcciones IPv6 Reservadas

Reservado para:	Prefijo
Loopback	::1/128
Documentación	2001:db8::/32
Default Gateway	::/0
No especificada	::/128
Mecanismo de transición	Teredo: 2001::/32 6to4: 2002::/32

Fuente: ISOC - Argentina [37]

4 Enrutamiento y Determinación de la Ruta en IPv6

El procedimiento de enrutamiento IPv6, al igual que en IPv4, basa su funcionamiento en los campos dirección origen y destino de la cabecera IP, manteniendo la misma lógica de enrutamiento estático (manualmente) y dinámico de su predecesor [4] [20].

Sin embargo, para la determinación de la ruta, utilizando la nueva estructura de la cabecera IPv6, los protocolos de enrutamiento dinámico han sido actualizados. Esta actualización, considera tanto los protocolos que operan dentro de un sistema autónomo y entre estos. En la siguiente Tabla muestra la actualización de estos protocolos [4] [20]:

Tabla 6 – Protocolos de enrutamiento actualizados

Protocolo de enrutamiento	RFC
RIP de nueva generación (RIPng)	2080
OSPFv3	2740/5340
BGP4	2545/4760
EIGRPv6	Privado
IS-IS	5308

Fuente: IPv6 Essentials [4] – CCNA ICDN2 [20]

5 Protocolos de Soporte de IPv6

5.1 Autoconfiguración

Para la configuración de los parámetros de red existen dos opciones: manual o autoconfiguración. En IPv6 la autoconfiguración tiene dos métodos, las cual describiremos a continuación:

- **StateLess Address AutoConfiguration – SLAAC**

  Este método basa su configuración en la utilización de mensajes ICMPv6 enviados entre el router y el host solicitante. Los mensajes ICMPv6 utilizados son:

  - RS (Router Solicitation) con valor en el campo tipo de 133 en el mensaje ICMPv6 y
  - RA (Router Advertisement) con valor en el campo tipo de 134 en el mensaje ICMPv6.

  El host luego de generar su dirección Link-Local IPv6, envía el mensaje RS a la dirección multicast ff02::2 conocida a nivel enlace local. El mensaje RS es escuchado por el router perteneciente al enlace local, el cual envía el mensaje RA con los parámetros de configuración: Prefijo de red y DNS. El host solicitante utiliza estos parámetros para configurar su interfaz de red, utilizando el prefijo recibido para crear su dirección IPv6 global, configura la puerta de enlace en base a la dirección origen del mensaje RA y luego establece los parámetros de DNS.

  Actualmente, en la práctica, este método no puede auto-configurar el parámetro de DNS, para lo cual debe soportarse utilizando el método por DHCPv6 o DHCPv4, este último si es que es un entorno doble pila.

  El mensaje RA, está conformada por 9 campos: Type (1 Byte), Code (1 Byte), Checksum (2 Bytes), Current Hop Limit (1 Byte), flags (1 Byte), Router Lifetime (2 Bytes), Reachable Time (4 Bytes), Retrans Time (4 Bytes) y Option (Variable). Las variables M y O del campo flag, define el método de configuración, si el flag M=0 y O=1, se utilizará el método SLAAC para configurar la dirección IPv6 y DHCPv6 para configurar DNS y otros parámetros. En la siguiente Tabla se muestra las posibles combinaciones para determinar el método de autoconfiguración a ser utilizado.

Tabla 7 – Configuración de los flags M y O

M	O	Método de Configuración	Comentarios
0	0	SLAAC/SLAAC	No es posible en la práctica la implementación total de SLAAC
0	1	SLAAC/DHCPv6	Actualmente puede ser implementado con DHCPv6; sin embargo también puede usarse la configuración de DNS y otros parámetros con IPv4, solo si se tiene un entorno doble pila.
1	0	DHCPv6/SLAAC	No es posible en la práctica la implementación de SLAAC para la configuración de DNS y otros parámetros.
1	1	DHCPv6/ DHCPv6	DHCPv6 realiza la configuración total de los parámetros de red, a excepción de la puerta de enlace, el cual es configurado a partir de la dirección origen del mensaje RA.

Fuente: IPv6 Essentials [4]

- **DHCPv6**

  Se encuentra definido en la RFC 3315, este protocolo se actualizo de la versión 4 a la versión 6, con la finalidad de dar el soporte necesario al protocolo IPv6 para la autoconfiguración de los parámetros de red. Al igual que su predecesor su objetivo es asignar direcciones IP en una arquitectura cliente/servidor. Sin embargo, DHCPv6 no mantiene ninguna compatibilidad con DHCPv4 [4].

  Este protocolo tiene las siguientes características [4] [33]:

  - Mas control de la red sobre las asignaciones.
  - Mayor amplitud en la configuración de los servicios de red.
  - Utiliza direcciones reservadas multicast en su proceso de asociación. Estas direcciones son: ff02::1:2 (All_DHCP_Relay_Agents_and_Servers) y ff05::1:3 (All_DHCP_Servers).
  - Utiliza direcciones unicast cuando se establece la comunicación.
  - El servidor DHCP no necesariamente debe estar en la subred, para lo cual utiliza agentes de retransmisión.
  - Emplea IPSec para IPv6 para los mensajes enviados entre servidores y agentes de retransmisión.

- Utiliza método de autenticación de repeticiones para prevenir ataques a sobrecarga de autenticación.
- Cuando el cliente solicita autenticación, utiliza un mecanismo llamado mecanismo de autenticación retardada, en donde se utiliza el algoritmo HMAC (keyed-Hash Message Authentication Code) y la función MD5 para la generación de claves.
- Se utilizan los siguientes mensajes en el proceso de autoconfiguración: SOLICIT, ADVERTISE, REQUEST, REPLY.
- Los clientes usan el puerto UDP 546 y los servidores/retrasmisores utilizan el puerto UDP 547.
- No proporciona información de la puerta de enlace.
- Utiliza DUID (DHCP Unique ID) para la identificación de los clientes.
- DHCPv6 permite la delegación de prefijos, esto permite enviar la información del prefijo hacia los routers que tienen habilitado DHCPv6 como Cliente. Este funcionalidad es generalmente usado por ISP para la configuración de sus routers en el lado del cliente.

DHCPv6 tiene dos opciones de configuración: Stateless DHCPv6, esto utilizado cuando DHCPv6 se utiliza para configurar otros parámetros, como el DNS, y se usa el método de autoconfiguración SLAAC para configurar el IP. La otra opción se denomina Statefull DHCPv6, con el cual se utiliza solo DHCPv6 para configurar todos los parámetros de red[4] [33].

La opción de autoconfiguración a ser utilizada, es definida de acuerdo a los valores M y O del campo flag del mensaje RA, que es enviado por el router en respuesta de un mensaje RS del host solicitante. La configuración de estos valores se detallan en la Tabla 7.

5.2 DNSv6

Domain Name Service – DNS, es un protocolo de la capa de aplicación. En el mundo IPv4, su función principal es traducir las direcciones IP en nombres de dominio. En un mundo IPv6, donde la dirección IP tiene una longitud mayor, la implementación de este protocolo (DNS) toma mayor importancia [4].

La IETF, publica las RFC 1886 y la RFC 3152, para establecer los alcances técnicos de las modificaciones del protocolo DNS para su funcionamiento con el protocolo IPv6 [4] [34]. Finalmente, la IETF, publica la RFC 3596, que combina la RFC 1886 y 3152 [34]. La RFC 3596, no establece cambios en la estructura de la cabecera del protocolo DNS, básicamente define las siguientes extensiones [34]:

- Define un registro de recursos para el mapeo del nombre de dominio para la dirección IPv6.

- Se define un domino que permita apoyar a las operaciones de búsqueda.
- Se redefine el procesamiento de búsqueda para que soporte ambos protocolos, IPv4 e IPv6.

Específicamente la RFC 3596, define el registro de tipo AAAA o quad-A. Los tipos de registro NS y PTR se mantienen sin cambios, solo se ajustaron al nuevo formato de la dirección IPv6 [4]. Asimismo, se establece el cambio de dominio para el mapeo inverso de direcciones denominado IP6.INT (definido en la RFC 1886 y eliminado con la RFC 4159) por IP6.ARPA [4] [34]. En la siguiente figura se observa la estructura de la resolución del dominio de una dirección IPv6 [4]:

```
moon.universe.com.    IN    AAAA    2001:db8:1:2:3:4:567:89ab
b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.8.b.d.0.1.0.0.2.IP6.ARPA.
IN  PTR    moon.universe.com.
```

Figura 15 – resolución de dominio IPv6

Fuente: IPv6 Essentials [4]

5.3 ICMPv6

Internet Control Message Protocol versión 6– ICMPv6, descrito en la RFC 4681, es el protocolo de soporte de IP para la gestión de mensajes informativos, diagnóstico y de fallos que puedan presentarse en el proceso de comunicación entre los nodos que intervengan [4] [35].

Se amplia las funcionalidades, en comparación a su versión 4 para el protocolo IPv4. Este protocolo se encuentra descrito en la RFC 4443. Entre las características importantes podemos mencionar lo siguiente [4] [35]:

- ICMPv6 considera las funciones de multicast, definidas en el protocolo IGMP utilizada en la versión IPv4.
- ICMPv6, introduce el concepto de Multicast Listener Discovery – MLD, el cual se utiliza para la gestión de Multicast, existiendo dos versiones MLDv1 y MLDv2, diferenciados por el soporte de origen-especifico de Multicast en la versión MLDv2.
- Se introduce el concepto Neighbor Discovery – ND, el cual realiza las funciones que se realizaban en IPv4 como: ARP/RARP, ICMPv4 router discovery e ICMPv4 redirect. ND, soluciona diversos problemas dentro de un segmento de red, como: descubrimiento de routers, descubrimientos de prefijos, descubrimiento de parámetros, autoconfiguración de direcciones, resolución de direcciones (ARP), determinación del próximo salto, detección de vecinos

inalcanzables, detección de direcciones duplicadas (Duplicate Address Detection – DAD) y el redireccionamiento. Para realizar estas funciones utiliza principalmente los siguientes mensajes:

- NS (Neighbor Solicitation): Para resolver direcciones MAC o comprobar si puede ser alcanzado un nodo en la red.
- NA (Neighbor Advertisement): Se origina como respuesta a un mensaje NS o difundir información.
- RS (Router Solicitation): Se envía al levantar la interfaz de red.
- RA (Router Advertisement): Se genera en respuesta a un RS par informar los parámetros.

- Descubrimiento de MTU o Path MTU Discovery, el cual descubre de una manera proactiva el tamaño del MTU a ser usado en el proceso de transmisión.
- Establece una seudo-cabecera para el cálculo de suma de comprobación.
- Utiliza IPsec como mecanismo de seguridad para autenticación y encriptación.
- Se definen nuevos mensajes para simplificar la re-numeración de las redes y la actualización de la información entre los diferentes nodos que participan en el proceso de comunicación.

ICMPv6 tiene la siguiente formato [35]:

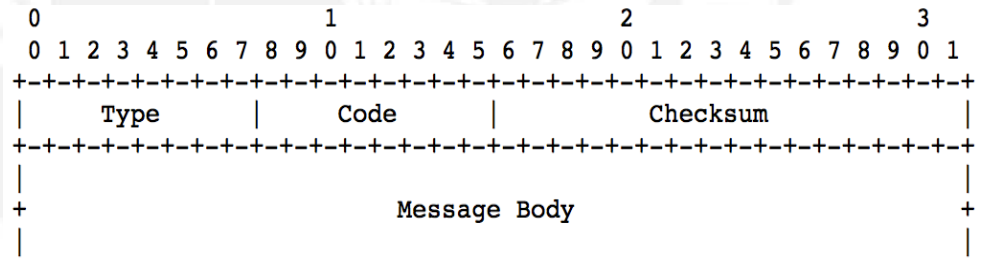

Figura 16 – Formato protocolo ICMPv6

Fuente: IETF RFC 4443[35]

- **El campo tipo (Type),** de tamaño de 8 bits, indica el tipo de mensaje, los cuales pueden ser: mensajes de error (destino inaccesible, paquete demasiado grande, tiempo excedido, problemas de parámetros, entre otros) o mensajes informativos (Echo Request, Echo Reply, Multicast Listener Query/Report/Done, Router Solicitation, entre otros) [4] [35]. Estos mensajes se encuentra definidos en la RFC 4443 [4].
- **El campo código (Code),** de tamaño de 8 bits, depende del tipo de mensaje y permite dar mayor detalle del mensaje. Estos mensajes se encuentran definidos en la RFC 4443 [4] [35].

- **El campo suma de comprobación (Checksum),** de tamaño de 16 bits, permite detectar errores en los datos de la cabecera ICMPv6 y en partes de la cabecera IPv6 [4] [35]. En el cálculo se incluye una seudo-cabecera, la cual esta descrita en la RFC 2460 [4] [35].
- **El campo cuerpo del mensaje (Message Body),** de longitud variable, de acuerdo al valor definido en los campos tipo y código, este campo llevará varios datos [4] [35]. El tamaño máximo de una cabecera ICMPv6 es de 1280 Bytes, por lo que este campo no deberá exceder este tamaño [4] [35].

Cuando se envía una cabecera ICMPv6, este se ubica después de todas las cabeceras de extensión que haya generado el protocolo IPv6. La cabecera ICMPv6 es identificada con el valor 58, en el campo "Next Header" de la cabecera precedente.

6 Mecanismos de transición

Desde la publicación del protocolo IPv6, se han creado diversas técnicas para realizar la migración de las redes basadas en IPv4 hacia el nuevo protocolo, ya que su incompatibilidad (IPv4/IPv6) dificulta este proceso de transición [37]. Cada uno presenta ciertas ventajas y desventajas, las cuales deben ser analizadas por las empresas y seleccionar aquella que se adecúe más a su entorno de red [4] [37].

Los mecanismos de transición podemos agruparlos en tres categorías o estrategias que se han definido hasta la actualidad: Pila Doble (Dual-Stack), Túneles/Encapsulamiento (Tunneling/Encapsulation) y Traducción (Translation) [4] [22].

Durante todo este tiempo algunos de los mecanismos de transición han quedado obsoletos, ya que se presenta un escenario diferente al inicial. Según la publicación, realizada por la Internet Society – Capitulo de Argentina (ISOC-AR) [37], señala que los mecanismos de transición tradicionales fueron creados basados en la disponibilidad de direcciones IPv4 y que los nuevos mecanismos son diseñados para un escenario en el que ya no se cuenta o existe un agotamiento inminente de las direcciones IPv4 [37].

6.1.1 Doble Pila (Dual Stack)

Unas de las primeras técnicas descrita en la RFC 4213. Este mecanismo de transición soporta ambas versiones del protocolo IP (IPv4/IPv6) [4] [22]. Para su implementación se tiene que configurar todos los nodos con ambas pilas de protocolos (IPv4/IPv6), soportando direccionamiento (estático, DHCPv4, SLAAC o DHCPv6) y los protocolos de enrutamiento especificadas para cada versión (OSPFv3, RIPng, BGP4, IS-IS, entre otros) [4]. Su funcionamiento tiene dos escenarios posibles, el primero, cuando recibe un protocolo con IPv4, los nodos activan el soporte de IPv4; segundo, cuando los nodos reciben IPv6, los

nodos activan el soporte de IPv6 [4], [22]. Los nodos pueden tener activado el soporte de ambas pilas de protocolos o solo uno de ellos [4] [22].

Para la resolución de nombres y de direcciones IP, ambas versiones utilizan un servidor DNS [1] [4]. Este servidor debe ser capaz de soportar ambos protocolos, por lo que la lógica de su configuración es muy importante [4]. Cuando se tiene tráfico IPv4, se utiliza las funcionalidades del servidor DNS, que actualmente usamos; y cuando se genera tráfico IPv6, se implementa el concepto de DNS AAAA, el cual es descrito en el Numeral 5.2 [4].

En un escenario doble pila, se da preferencia por defecto al protocolo IPv6. Sin embargo, este escenario genera un problema, ya que al realizar la conexión utilizando IPv6, puede darse el caso que debido a un problema de conexión o configuración, IPv6 no responda, lo cual después de varios intentos, se procede a realizar los intentos con el protocolo IPv4. Este retraso en la verificación de la respuesta de conexión con IPv6 genera una mala experiencia en el usuario. La IETF, con la finalidad de mejorar este procedimiento de verificación, publica la RFC 6555, en el cual, se desarrolla el algoritmo llamado "happy eyeballs", el cual nace para mejorar el proceso de conexión. Básicamente happy eyeballs al momento de realizar la conexión, realiza el intento de conexión utilizando ambos protocolos en paralelo (IPv6/IPv4), de tal manera que si IPv6 no responde, se procede inmediatamente a conectar con IPv4 [4].

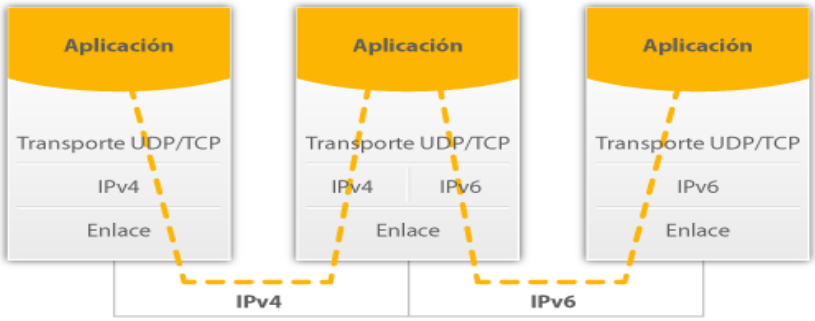

Figura 17 – Dual Stack o Doble Pila

Fuente: LACNIC [22]

En la siguiente Tabla se identifica algunas ventajas y desventajas de esta técnica:

Tabla 8 – Ventajas/Desventajas Doble Pila

Ventajas	- Ejecución de protocolos IPv4/IPv6 en modo nativo. - Rápida migración a IPv6. - No se crean túneles ni traducciones. - Proporciona un mejor rendimiento, escalabilidad y eficiencia. - No se necesita hacer el diseño de una nueva red. - No se necesita hacer pruebas. - No se necesita hacer un despliegue temporal.
Desventajas	- Mayor uso de recursos de hardware. - Doble gestión y seguridad. - Dos escenarios DNS. - Requiere una actualización de todos los nodos de la red. - Mantenimiento de grandes tablas de enrutamiento. - La detección y resolución de problemas es muy complejo. - Alto costo de implementación. - Requiere de una gran cantidad de direcciones IPv4

Fuente: IPv6 Essentials [4] – ISOC Argentina [37] – RFC4213 [39]

6.1.2 Túneles/Encapsulamiento (Tunneling/Encapsulation)

Descrito en la RFC 4213, las técnicas que se agrupan en este mecanismo de transición parten del principio de establecer un túnel virtual de comunicación entre dos redes IPv6 a través de una red con IPv4 [4] [23].

La red IPv6 envía un paquete con el formato IPv6 hasta su enrutador de borde, este enrutador encapsula el protocolo IPv6 en una cabecera IPv4 con valor de campo de protocolo 41 [4] [23], el cual indica que esta encapsulando un paquete IPv6. Cuando el paquete es encapsulado por el protocolo IPv4, es importante verificar los valores configurados del MTU (Maximum Transfer Unit) y del MRU (Maximum Receive Unit), y la conversión de los mensajes ICMPv4/ICMPv6, la RFC 4213 describe las consideraciones a tener en cuenta con estos parámetros [39]. Cuando la trama llega a su destino, el enrutador de borde del destino, basado en la información del valor del campo protocolo (Valor 41 para IPv6), extrae la cabecera IPv6 y envía el paquete al host destino [4] [39].

La RFC 4213, establece 4 caminos para establecer un túnel [39]:

- **Router-to-Router:** Se establece el túnel entre el enrutador de salida y el de la red de destino final.
- **Host-to-Router:** Se establece el túnel entre el host emisor hasta el enrutador de destino final.
- **Host-to-Host:** Se establece el túnel en el segmento completo, del emisor al destino final.
- **Router-to-Host:** Se establece el túnel entre el enrutador de salida y el host de destino final.

De acuerdo a la configuración, se pude diferenciar dos tipo de túneles: manual y automático [4] [39]. Los túneles configurados manualmente, necesitan que se realice la configuración manual entre los nodos participantes, configurando el encapsulamiento del protocolo IPv6 en el protocolo IPv4, en el nodo emisor, y su proceso inverso respectivo en el receptor [4] [39]. La configuración automática de túneles, se realiza utilizando diversas técnicas de túneles, algunas de ellas son identificadas por sus dirección unicast, las cuales son direcciones especiales designadas por la IETF [4].

Las técnicas manuales conocidas son 6in4 y Generic Routing Encapsulation – GRE, esta última descrita en las RFC 2784 y 2890. GRE posee su propio encabezado para encapsular el protocolo IPv6 u otros protocolos [4] [37] [40]. El encabezado del protocolo GRE es encapsulado por el protocolo IPv4, y se identifica con el valor 47 en el campo "Protocolo" de esta cabecera [37]. Su diseño permite enviar más de 2 cabeceras simultáneamente en una comunicación, lo cual es perfecto para entornos multiprotocolo, como el protocolo de enrutamiento IS-IS [37]. Sus principales desventajas son, que no puede atravesar entornos NAT y el doble encapsulado que se realiza; por lo que se recomienda su implementación a nivel de proveedores de servicio [4] [37].

En relación a las técnicas automáticas, se han creado diversas técnicas durante todo este tiempo, algunas de las cuales ya no son recomendadas para realizar un despliegue en ambientes empresariales o de proveedor de servicios y solo se consideran para un contexto académico o de pruebas [4] [37].

Las técnicas de túnel automático Tunnel Brokers y Teredo son algunos de los mecanismos que no se recomienda implementar en este tipo de ambientes [4] [37]. La técnica 6to4 (descrito en la RFC 3056, 3068 y 6343) no se recomienda su implementación por los problemas de asimetría y control que presenta, por lo que, se crea una extensión llamada IPv6 Rapid Deployment – 6rd, en la cual se resuelven estos problemas [4] [37].

A continuación describiremos algunas de las principales técnicas de túneles automáticos recomendadas para ambientes empresariales o para proveedores de servicio [37].

- **6 Rapid Deployment – 6rd:** Esta técnica hereda muchas de las características de la técnica 6to4, corrigiendo aquellos problemas identificados en su antecesor. 6rd considera dos elementos principales: el Router 6rd en el lado del cliente o CE (Client Edge) y el Border Relay 6rd - BR 6rd (o conocido como Relay Router en la técnica 6to4) [45]. Una de las principales diferencias es que el BR 6rd se encuentra gestionado por el proveedor de servicios de Internet, lo cual permite tener control del retorno del paquete y la simetría de los túneles [37]. Otra diferencia importante es la dirección IPv6, mientras que en 6to4 se usa un dirección estándar, 2002:DirecciónIPv4::/48, en esta técnica el proveedor de servicio de Internet puede asignar su propia nomenclatura de dirección y prefijo, manteniendo la siguiente estructura:

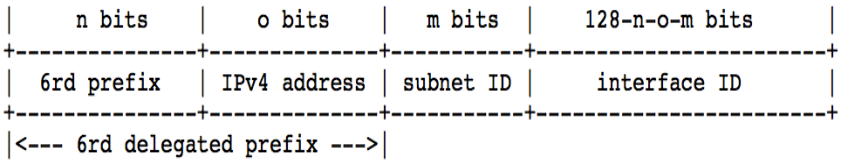

Figura 18 – 6rd

Fuente: RFC 5969 [45]

En la siguiente Tabla se identifica algunas ventajas y desventajas de esta técnica:

Tabla 9 – Ventajas/Desventajas 6rd

Ventajas	- Control y gestión del BR 6rd. - Encaminado simétrico. - Mejora la QoS y la seguridad. - Rápido y fácil despliegue. - Los Router 6rd y BR 6rd tienen conectividad nativa IPv4/IPv6. - Utiliza IPv4 privadas, siempre y cuando sean únicas.
Desventajas	- Requiere el uso de IPv4 público. - Técnica temporal. - Encapsulamiento de la cabecera IPv6. - Requiere de una gran cantidad de direcciones IPv4.

Fuente: IPv6 Essentials [4] – ISOC Argentina [37] – RFC 5569 [45]

La implementación de esta técnica es recomendada también para entornos empresariales que tengan una infraestructura a nivel WAN con IPv4 y sedes que estén iniciando un despliegue de IPv6 nativo.

- **IPv6 Provider Edge Router - 6PE / IPv6 VPN Provider Edge Router - 6VPE:** Ambas técnicas han sido diseñadas específicamente para redes en donde se tenga una infraestructura MPLS sobre IPv4 [4], [37]. Se establece sesiones utilizando el protocolo Multiprotocol Border Gateway Protocol (MP-BGP), el cual permite establecer el túnel entre los routers conocidos como PE (Provider Edge router) que quieren comunicarse a través de la infraestructura core de MPLS [4] [37] [41] [42] [43]. Los equipos de core de esta red MPLS, tanto software o hardware, no necesitan configurarse o actualizarse [4] [37]. Las red core MPLS nunca se da cuenta si esta transmitiendo paquetes IPv6, ya que su enrutamiento es en base a etiquetas [37]. Solo los routers PE pueden requerir de alguna actualización de software, dependiendo de la antigüedad del equipo [4] [37]. La principal diferencia de ambas técnicas radica en el tipo de servicio final que se quiere implementar en los routers CE (Customer Edge router), si solo se quiere dar acceso a Internet en los CE, la técnica 6PE es la recomendada y si se quiere establecer conexión entre múltiples CEs, creándose múltiples tablas de enrutamiento lógicas a través del core MPLS, la técnica 6VPE es la recomendada [4] [37]. Estas técnicas se encuentran descritas a mayor detalle en la RFC 4798 (6PE) y en la RFC 4659 (6VPE).

  En la siguiente Tabla se identifica algunas ventajas y desventajas de esta técnica:

Tabla 10 – Ventajas/Desventajas 6PE/6VPE

Ventajas	- Soportada por múltiples fabricantes. - Tecnología madura para redes que utilizan MPLS en su core. - No se tiene que realizar ningún cambio en los equipos de core (Ninguna configuración y ninguna actualización). - Rápido despliegue.
Desventajas	- En la red MPLS, los routers Providers (P) no pueden enviar mensajes ICMP. - Encapsulamiento del protocolo IPv6.

Fuente: IPv6 Essentials [4] – ISOC Argentina [37] – CISCO [41] – RFC 4798 [42]- RFC 4659 [43]

Estas técnicas, de acuerdo al tipo de servicio (solo acceso a Internet o comunicación entre diversos sitios a través de la red MPLS) que se quiere implementar, son consideradas por la mayoría de los proveedores de servicio de Internet en escenarios MPLS, tanto para aquellos que ya tienen una red desplegada o para aquellos que piensen desplegar una red MPLS [4] [37]. En

ambientes empresariales que tengan su propia infraestructura de red MPLS también es recomendable el uso de esta técnica. Es importante mencionar que a la fecha de escrito este documento, no existe una red MPLS sobre IPv6 nativo, solo a nivel de los routers de borde o routers PE [37].

6.1.3 Traducción (Translation)

Esta técnica permite traducir direcciones IPv6 en direcciones IPv4 y viceversa. Las RFC 6145 y su actualización RFC 6791, describe el proceso de traducción de las cabeceras IP e ICMP y las RFCs 6052 y 6144 describen el proceso de traducción a nivel de prefijos, consideraciones técnicas para los modos de configuración llamados con o sin estado (Stateful o Stateless) y los 8 escenarios para realizar la traducción entre IPv4/IPv6 [4].

El escenario en el que una red IPv4 inicie el proceso de comunicación hacia una red IPv6, utilizando alguna técnica de traducción, la red IPv4 deberá utilizar doble pila (IPv4/IPv6) desde el host que quiera comunicarse, esto de acuerdo a lo indicado en la RFC 4966.

Las traducciones sin estado, conocidas como Stateless IP/ICMP Translation – SIIT, basan su traducción mediante un algoritmo de mapeo que le permite identificar un subconjunto de direcciones IPv4 pre-definidas [4] [46].

El modo de configuración con estado o Stateful, basa su traducción en una tabla de mapeo, en el cual obtiene las direcciones IPv4 traducidas, lo cual permite un correcto retorno de los paquetes [4] [46].

Las cabeceras de capa superior, TCP o UDP, no son modificadas cuando se realiza la traducción; sin embargo, se realiza un checksum a la cabecera UDP, ya que este procedimiento es requerido por el protocolo IPv6 [4]. Este procedimiento de checksum también es requerido para los mensajes traducidos de ICMPv4 [4].

Las opciones de IPv4, las cabeceras de enrutamiento, salto a salto y opciones de destino no son traducidos [4]. Asimismo, el tráfico multicast no puede ser traducido, ya que las direcciones IPv4 no están relacionadas con las direcciones IPv6 multicast [4].

La RFC 6144, considera a este tipo de mecanismos de transición como aquella que nos permitiría establecer una mejor estrategia a mediano plazo en el proceso de transición al protocolo IPv6 en nuestras redes.

Existen diversas técnicas que se basan en este concepto, de las cuales mencionaremos aquellas que están diseñadas para ambientes empresariales o para proveedores de servicio de Internet.

- **NAT64/DNS64:** Las técnicas Stateful NAT64 (RFC 6146) y DNS64 (RFC 6147) son técnicas que se implementan de manera conjunta. Stateful NAT64 se encarga del proceso de traducción de cabeceras IPv6 a IPv4 o viceversa (Solo traduce unicast TCP, UDP e ICMP). DNS64, funciona de forma recursiva, realizando la

resolución de dominio AAAA (quad-a) y en caso sea una dirección IPv4 no conocida reenvía la consulta a otro servidor DNS hasta obtener la dirección IPv4 pública, creando un registro falso AAAA en su base datos, para lo cual utiliza el prefijo conocido 64:ff9b::<dirección IPv4 pública>/96, de tal manera DNS64 envía este registro AAAA asociado al prefijo conocido falso al cliente IPv6 que lo solicito y este creerá que puede acceder utilizando IPv6 [47] [48].

En relación al prefijo conocido, la RFC 6052 define diversas formas de uso de un prefijo, el mas usado es el prefijo citado 64:ff9b::/96 para Stateful NAT64. Este prefijo considera los 96 primeros bits para red o subred y 32 bits para host, estos 32 bits corresponden a la dirección IPv4 de la dirección original en la red IPv4 con la que se quiere establecer la comunicación. Este prefijo permite a Stateful NAT64 traducir la dirección.

En la siguiente Tabla se identifica algunas ventajas y desventajas de esta técnica:

Tabla 11 – Ventajas/Desventajas NAT64/DNS64

Ventajas	- Soportada por múltiples fabricantes. - Los host finales con IPv6 pueden acceder a contenido en IPv4, si es que el contenido es compatible con IPv6. - Rápida migración a IPv6. - Utiliza una sola traducción en comparación con otras técnicas.
Desventajas	- Al ser Stateful es complejo y requiere un consumo alto de recursos (procesamiento y memoria). - Al proporcionar un uso compartido de las direcciones IPv4, lo limita en su capacidad (65,535 conexiones TCP de origen) conexiones. - Si las aplicaciones finales no soportan IPv6 este método no aplica. - No establece una conectividad de extremo a extremo. - Solo funciona con nombre de dominio – DNS.

Fuente: IPv6 Essentials [4] - ISOC Argentina [37]

Esta técnica es recomendada para ISP o grandes corporaciones que tengan múltiples sucursales.

- **464XLAT:** Esta técnica se puede considerar con fines prácticos como una mejora del Stateful NAT64/DNS64, ya que permite acceder a aplicaciones finales que no soportan IPv6 [4] [49]. Se utiliza Stateful NAT64 y SIIT (doble traducción), no se utiliza DNS64. Para que esto sea posible 464XLAT, realiza una traducción adicional, específicamente SIIT, lo cual permite agregar direcciones privadas IPv4 a los nodos finales [4] [49]. La traducción SIIT, toma el nombre de CLAT (Customer-side Translator), el cual se ubica en la frontera de la red IPv6 del lado del cliente con la del proveedor [4] [37] [49]. La traducción stateful NAT64, se denomina PLAT (Provider-side Translator), el cual se ubica en la frontera del ISP hacia Internet (IPv4 e IPv6). Al realizar la doble traducción se evidencia el problema de conectividad de extremo a extremo, aunque en una menor intensidad, debido a que la traducción Stateless (SIIT) no quiebra una traducción 1:1 [4] [37] [49].

  464XLAT, utiliza como formato de direcciones descrito en la RFC 6052, en el cual la dirección IPv4 esta embebida en la dirección IPv6 [4]. El CLAT utiliza direcciones IPv6 con prefijo /64 [4] [49].

  Esta técnica esta descrita en la RFC 6877 y es relativamente nueva; por lo que no es soportado por múltiples fabricantes. Se recomienda su implementación en los proveedores de servicio de Internet móvil [37] [49].
- **DS - LITE (Dual Stack Lite):** Esta técnica de manera similar a 464XLAT, soluciona el problema de acceder a aplicaciones que no soporten IPv6 por parte del usuario final, sin hacer doble traducción; sin embargo mantiene el problema de la conexión de extremo a extremo por la traducción que realiza [37].

  Esta técnica inserta dos componentes: el ATFR (Address Family Transition Router) y el B4 (Basic Bridge BroadBand). El router B4 se ubica en el lado del cliente y el AFTR se ubica en la frontera del ISP hacia la Internet IPv4 [4] [50]. Los host que atraviesan el B4 tiene una configuración doble pila IPv6/IPv4 [4] [50]. Cuando un host quiere comunicarse utilizando IPv6 este será enviado a través de toda la red IPv6 nativa, sin ser encapsulada o traducida; en cambio, cuando un host quiere comunicarse a una red IPv4, el host utiliza su dirección IPv4 privada el cual es encapsulado en el router B4 en una dirección IPv6 hacia el AFTR, quien tiene asignado un conjunto de direcciones IPv4 públicas para acceder al Internet IPv4 [4] [50]. El AFTR utiliza Stateful NAT para comunicar a los host de la red IPv6 hacia una red IPv4 [4] [50].

  DS-Lite es considerado como una técnica madura, por lo que esta soportada por múltiples fabricantes y está diseñado para un contexto en el cual existe un agotamiento de direcciones IPv4.

DS-Lite se encuentra definida en la RFC 6333 y las consideraciones para su despliegue en la RFC 6908.

Esta técnica es recomendada para cualquier tipo de ISP y grandes corporación que tengan múltiples sucursales [37].

- **MAP – Mapping of Address ad Port:** Esta técnica a la fecha de escrito este documento, se encuentra todavía a nivel de borrador. En el cual la IETF ha definido dos tipos, el MAP – E, en la cual se usaría el encapsulamiento a través de un túnel y el MAP – T, el cual estaría basado en traducción del protocolo IP.

  MAP, al igual que DS-Lite o 464XLAT, entrega un dirección privada IPv4 a los host finales [37]. La técnica MAP-E, crea un túnel desde la frontera con el cliente (MAP CE) hasta otro router ubicado en la zona del ISP, llamado Border Relay (MAP BR) [37] [52]. Su funcionamiento es similar al DS-Lite. Asimismo, MAP-T, utiliza los mismos componentes presentes en MAP-E, pero el MAP CE y el MAP BR, realizan traducción del protocolo respectivamente, y su funcionamiento es similar al 464XLAT [37] [53].

  La diferencia principal radica en que MAP, implementa en el MAP BR, un algoritmo de asignación de puertos para cada MAP CE, este algoritmo es llamado Port-Set ID [4] [52] [53]. Asimismo, se introduce el concepto de A+P (Address Plus Port) descrita en la RFC 6346, para el uso compartido de direcciones IPv4 [37] [52] [53]. Esto permite el uso de técnicas para establecer comunicaciones de extremo a extremo, ya que no se usa un NAT stateful en el lado del ISP [37].

  De acuerdo a la descripción de MAP, en sus dos tipo, estos permiten mejorar de forma significativa la transición al protocolo IPv6, en un contexto en el cual las direcciones IPv4 están agotadas; sin embargo, siendo todavía un borrador de estándar, es importante esperar su publicación final para su análisis a detalle.

6.1.4 Comparativo de las técnicas de transición

De acuerdo al marco conceptual de las técnicas de los mecanismos de transición descritos se hace el siguiente análisis comparativo a nivel de consumo de recursos y costo:

Tabla 12 – Comparativo técnicas de transición

Mecanismo de Transición	Tipo	% de consumo de recursos (Procesamiento y memoria)	Costo Operativo	Complejidad
Dual Stack	Doble Pila	Alto	Alto	Bajo
6PE	Túnel automático	Mediano	Mediano	Mediano
6VPE	Túnel automático	Mediano	Mediano	Mediano
6rd	Túnel automático	Mediano	Mediano	Mediano
NAT64/DNS64	Traducción	Alto	Alto	Alto
464XLAT	Traducción	Mediano	Bajo	Alto
DS-Lite	Traducción & Túnel	Alto	Bajo	Alto
MAP	Traducción & Túnel Automático	Bajo	Bajo	Alto

Fuente: Elaboración propia

7 Administración del recurso IP

La distribución del espacio de los recursos de numeración a nivel mundial sigue un esquema jerárquico. El espacio de direcciones IP es administrado por la Internet Assigned Numbers Authority – IANA, el cual es un departamento de la Internet Corporation or Assigned Names and Numbers – ICANN.

La IANA es la encargada de distribuir y asignar el espacio de direcciones IP a los cinco (05) Regional Internet Registry – RIR existentes a nivel mundial (APNIC, RIPE NCC, ARIN, LACNIC y AfriNIC). Asimismo, se encarga de la administración de la resolución de nombres de dominio, sistemas autónomos y mantener actualizados el sistema de numeración de los protocolos.

En Latinoamérica y parte del Caribe, el organismo encargado de cumplir las funciones del IANA es el RIR llamado Latin America and Caribbean Network Information Centre, conocido por sus siglas en ingles como LACNIC. Este organismo, es el encargado de asignar y distribuir los recursos de Internet a los registros nacionales (NIR – National Internet Register), y estos a su vez, a los LIR (Local Internet Register) o ISP - Internet Service Provider con presencia nacional. A nivel de LACNIC solo existen 2 NIR en Brasil y México. Finalmente, los ISPs de acuerdo a sus políticas técnicas y comerciales hacen entrega de estos

recursos IP al usuario final. En la siguiente figura, podemos observar esta estructura jerárquica:

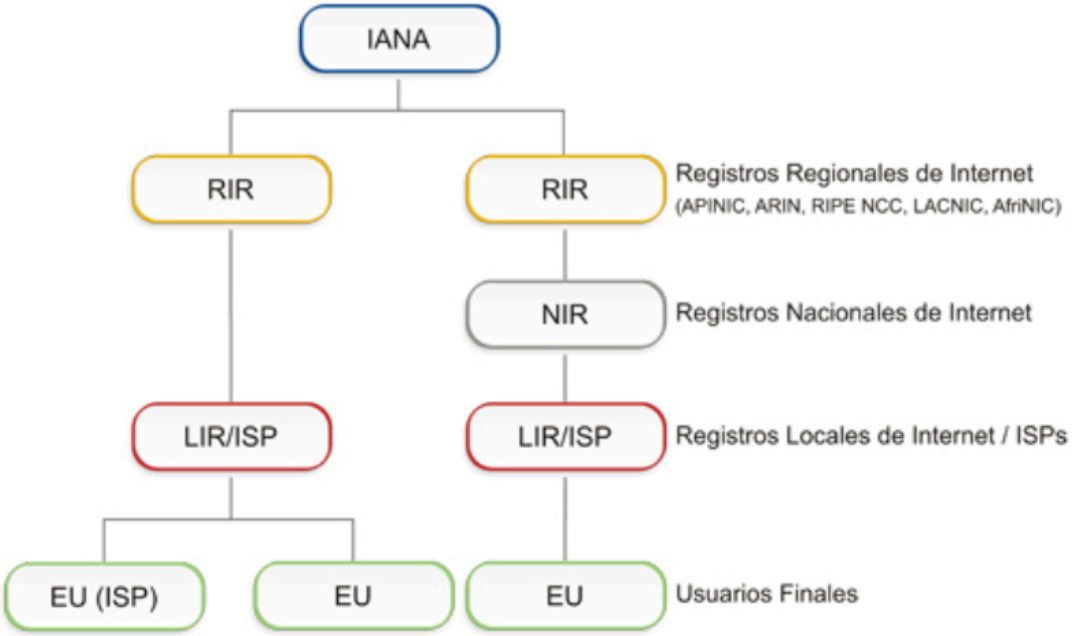

Figura 19 – Estructura administración del recurso IP

Fuente: LACNIC

Los ISPs locales o empresas (públicas o privadas) pueden realizar sus procesos de solicitud directamente a su RIR o NIR.

7.1 Estado de la Asignación de IPv6

La IANA del total de espacio de dirección IPv6, selecciono el prefijo /3 iniciando con los bits 001. La IANA divide este espacio en 512 partes con prefijo /12, de los cuales 5 se asignaron a los RIRs, de acuerdo a la siguiente Tabla:

Tabla 13 – Distribución de prefijos IPv6 a nivel de RIR

Nº	Regionals Internet Registries – RIR's	Direcciones IPv6
1	APNIC (Asia/Pacifico)	2c00:0000::/12
2	ARIN (América del Norte y parte del Caribe)	2400:0000::/12
3	AfriNIC (África y parte del océano indico)	2600:0000::/12
4	LACNIC (América Latina y parte del Caribe)	2800:0000::/12
5	RIPE NCC (Europa, centro y medio de Asia)	2a00:0000::/12

Fuente: www.nro.net [3]

Los RIR generalmente asignan un prefijo /32 a los LIR o ISP que lo soliciten y estos entregan a sus clientes por lo general un prefijo /64.

En el Perú ha Diciembre del 2015 se tiene la siguiente asignación de prefijos IPv6 realizadas por LACNIC:

Tabla 14 – Asignación Prefijo IPv6 Perú

Nº	Empresa	Prefijo
1	BT LATAM PERU S.A.C.	2001:1300::/32
2	AMERICATEL PERU S.A.	2001:1380::/32
3	Telefónica del Perú S.A.A.	2001:1388::/32
4	Red Académica Peruana-RAAP	2001:13a0:: /32
5	Universidad Ricardo Palma	2800:18:: /32
6	OPTICAL TECHNOLOGIES S.A.C.	2800:120:: /32
7	América Móvil Perú S.A.C.	2800:200:: /32
8	América Móvil Perú S.A.C.	2800:4b0:: /32
9	INTERNEXA PERU S.A	2800:650:: /32
10	Yachay Telecomunicaciones	2800:690:: /32
11	VIETTEL PERÚ S.A.C.	2800:cc0:: /32
12	NAP Perú	2801:1c:2000::/48
13	Red Científica Peruana	2801:150::/32
14	COLINANET SRL.	2803:500::/32
15	Media Networks Latin America SAC	2803:f00:: /32
16	O3B LIMITED	2803:1280:: /32
17	ENSATEL E.I.R.L.	2803:1880:: /32
18	EMAX	2803:2100:: /32
19	MEDIA COMMERCE PERÚ S.A.C	2803:2480:: /32
20	ECONOCABLE MEDIA SAC	2803:2500:: /32
21	Moche Inversiones S.A.	2803:3300:: /32
22	UNIFIED GROUP ONLINE EIRL	2803:3580:: /32
23	GLG PERU SAC	2803:4480:: /32
24	MOVILMAX TELECOM S.A.	2803:4780:: /32
25	Olo del Perú S.A.C	2803:4800:: /32
26	NEWCOM PERU	2803:6500:: /32
27	NEXTEL DEL PERU S.A.	2803:7180:: /32
28	DIRECTV PERU S.R.L	2803:7b80:: /32
29	ARBITRARE SOLUCIONES LEGALES Y ARBITRALES S.A.C	2803:ab80:: /32

30	NETLINE PERU SA	2803:c200:: /32
31	EMPRESA DE TELECOMUNICACIONES MULTIMEDIA ALFA	2803:d680:: /32
32	AMITEL PERU TELECOMUNICACIONES SAC	2803:e500:: /32
33	Conexia SRL	2803:ed00:: /32
34	NOCPERU-LATIN TECHNOLOGIES	2803:f080:: /32
35	CONVERGIA PERU S.A.	2803:fe80:: /32

Fuente: LACNIC [102]

MECANISMO DE TRANSICION PREFERIDO

FINALIDAD

La incompatibilidad del protocolo IPv4 con su sucesor el protocolo IPv6 ha sido claramente evidenciado desde la publicación de la RFC 1883, por lo que la IETF ha definido 3 estrategias de transición: IPv6 nativo, túneles y traducción. Realizando diversas investigaciones para definir técnicas que permitan comunicar a ambos mundos (IPv4/IPv6), ya que el proceso de transición hacia el nuevo protocolo no es inmediato y su coexistencia de ambos protocolos es importante para el éxito de la adopción.

Los mecanismos de transición IPv6 tiene como finalidad interconectar una red IPv6 hacia otra red IPv6 a través de una red IPv4, lo que nos indica que son destinadas para usos a nivel WAN o Internet. La comunicación de una red IPv4 a una red IPv6 es considerada como una mala práctica y no existe implementaciones o estrategias para este escenario, siendo declaro obsoleto su desarrollo por la RFC4966.

MECANISMOS DE TRANSICION

En la siguiente Tabla se ha evaluado las técnicas de transición mas conocidas, valorando sus características de acuerdo al % de consumo de recursos, costos operativos que implican su implementación y complejidad técnica.

Tabla 1 – Comparativo de Técnicas de Transición

Estrategias de Transición	Mecanismo de Transición (Técnicas)	Tipo	% de consumo de recursos (Procesamiento y memoria)	Costo Operativo	Complejidad
IPv6 nativo	Dual Stack	Doble Pila	Alto	Alto	Bajo
Túneles	6PE	Túnel automático	Mediano	Mediano	Mediano
Túneles	6VPE	Túnel automático	Mediano	Mediano	Mediano
Túneles	6rd	Túnel automático	Mediano	Mediano	Mediano
Traducción	NAT64/DNS64	Traducción	Alto	Alto	Alto
Traducción	464XLAT	Traducción	Mediano	Bajo	Alto
Traducción	DS-Lite	Traducción & Túnel	Alto	Bajo	Alto
Traducción	MAP	Traducción & Túnel Automático	Bajo	Bajo	Alto

Fuente: Elaboración propia

MEJORES PRACTICAS

De acuerdo a la publicación "IPv6 Best Practices" realizada por la EU-China FIRE, en Marzo del 2015, se establece diversas técnicas de transición como no recomendadas. Estas son: 6over4, 6to4, 6RD, ISATAP, TEREDO, TSP (Tunnel Setup Protocol) Sock64 y TRT (Transport Relay Translation) [99].

En el documento publicado por el gobierno de España, denominado "Guía para la Incorporación de IPv6 como Requisito para la Compra Pública", se recomienda que los ISP no deben de utilizar mecanismos de túneles internamente en la red [75].

ALCANCE DE IMPLEMENTACION

La implementación de los mecanismos de transición están asociados directamente a los ISP, por lo que las instituciones públicas no deberían de entrar en detalles técnicos sobre la implementación de estos mecanismos, pero si conocerlos y saber las ventajas y desventajas que cada uno puedo ofrecer.

MECANISMO PREFERIDO

Las instituciones públicas, no deberían de especificar el mecanismo de transición al ISP que proporcionará el servicio de acceso a Internet o interconexión entre sus dependencias. Esta deberá de exigir que el ISP permita cursar ambos tipos de protocolos (IPv4/IPv6) tanto para la entrada y salida desde la frontera del router instalado en el cuarto de entrada de servicios o centro de datos de la institución pública.

EL fabricante de equipamiento de redes, CISCO, ha definido un modelo de encuesta para ser realizado a los ISP cuando se solicita el requerimiento de servicios de conectividad con IPv6, el cual se considera tenerlo en cuenta. Esta encuesta se puede ubicar en la referencia [76].

BUENAS PRACTICAS PARA ELABORACION DEL PLAN DE DIRECCIONAMIENTO IPv6

MOTIVACION

Una de las principales tareas en el proceso de transición es la elaboración del Plan de Direccionamiento IPv6, el cual permitirá seleccionar el prefijo IPv6 necesario, su distribución y administración en las redes de las Instituciones Públicas, considerando las necesidades actuales y requerimientos futuros.

En ese sentido, se elabora el siguiente documento con la finalidad de exponer las mejores prácticas para la elaboración del Plan de Direccionamiento.

OBJETIVOS

El Plan de direccionamiento IPv6 deberá tener en cuenta los siguientes objetivos principales:

- Estimar la cantidad de direcciones IPv6 en la red.
- Asignación de los prefijos a las redes y subredes identificadas considerando crecimiento a futuro.

RECOMENDACIONES PARA EL PLAN DE DIRECCIONAMIENTO

Anteriormente, se estableció que para las redes de tipo corporativo se asignaran prefijos /48, /64 y /128, lo cual ha quedado obsoleto por la publicación de la RFC 6177, en la cual se recomienda que la selección del prefijo debe responder al tamaño y necesidad de la Empresa.

En ese sentido, existen diversos factores a tener en cuenta para determinar el prefijo IPv6 necesario, por lo que cada Institución Pública deberá de evaluar estos para su dimensionamiento.

Las siguiente recomendaciones han sido recopiladas de las publicaciones realizadas por el LACNIC [37] [59]:

- En caso que las institución públicas tengan varias sucursales deberán de asignar al menos un prefijo /48 para cada una.
- La asignación de prefijos pequeños puede incrementar el costo de administración y de volver a enumerar las redes ante un crecimiento futuro.
- Separar un prefijo para la numeración de los componentes y sistemas de toda la infraestructura tecnológica que pueda configurarse con una IP.
- Los prefijos deberán ser diferentes para la infraestructura tecnológica privada y públicas, con la finalidad de crear listas de acceso.
- Prefijos diferentes para enlaces punto a punto y servicios como DNS, correo, etc.

- Redes en las que se implementará IPv6
- Número y tipo de servicios ofrecidos
- Distribución geográfica de la red
- Estimación de direcciones necesarias para uso interno
- Criterios de asignación de prefijos a cada tipo de usuario y red
- Número estimado de usuarios de cada tipo de servicios y de cada zona geográfica.
- Topología de la red, protocolo de routing y consideraciones de seguridad

OBTENCION DE LA DIRECCION IPv6

La nueva versión del protocolo define diversos tipos de direcciones como Unicast, Anycast y Multicast y a su vez sub-tipos como la Global Unicast Address (GUA), Unique Local Address (ULA), Link Local, entre otras. La dirección IPv6 a solicitar es del tipo Unicast, específicamente las direcciones tipo GUA.

Para las instituciones públicas existen dos formas de obtener una dirección IPv6. La primera considera realizar el requerimiento directamente al RIR regional, en nuestro caso el LACNIC, quien puede asignar un prefijo /48 o la máxima de /32. Los requisitos para la solicitud del prefijo son [114]:

- Anunciar en el sistema de rutas inter-dominio de Internet el bloque asignado con la mínima desagregación que le sea posible.
- Proveer información detallada mostrando como el bloque solicitado será utilizado dentro de tres, seis y doce meses.
- Entregar una descripción detallada de la topología de la red.
- Realizar una descripción detallada de los planes de enrutamiento, incluyendo los protocolos a ser usados.

La solicitud del prefijo al LACNIC es en línea y puede ser accedido a través de la siguiente referencia [114]. La instituciones públicas que se orienten por este medio, es importante que tengan en cuenta las siguientes consideraciones previo requerimiento de la dirección IPv6:

- Validar con el ISP contratado si los equipos de router aceptan la versión 6 del protocolo IP, y
- Conocer si el ISP contratado esta en la capacidad de enrutar este protocolo a través de su red.

La segunda forma de obtener una dirección IPv6 es a través del ISP, para lo cual se tiene que establecer una relación contractual previamente. Generalmente deberá de solicitarse en los términos de referencia para la contratación de los servicios de acceso a Internet.

Los principales ISP a nivel de Perú ya tienen asignado direcciones IPv6, los cuales se detallan en la siguiente Tabla:

Tabla 1 – Asignación Prefijo IPv6 Perú

Nº	ISP	Prefijo
1	BT LATAM PERU S.A.C.	2001:1300::/32
2	AMERICATEL PERU S.A.	2001:1380::/32
3	Telefónica del Perú S.A.A.	2001:1388::/32
4	Red Académica Peruana-RAAP	2001:13a0:: /32
5	Universidad Ricardo Palma	2800:18:: /32
6	OPTICAL TECHNOLOGIES S.A.C.	2800:120:: /32
7	América Móvil Perú S.A.C.	2800:200:: /32
8	América Móvil Perú S.A.C.	2800:4b0:: /32
9	INTERNEXA PERU S.A	2800:650:: /32
10	Yachay Telecomunicaciones	2800:690:: /32
11	VIETTEL PERÚ S.A.C.	2800:cc0:: /32
12	NAP Perú	2801:1c:2000::/48
13	Red Científica Peruana	2801:150::/32
14	COLINANET SRL.	2803:500::/32
15	Media Networks Latin America SAC	2803:f00:: /32
16	O3B LIMITED	2803:1280:: /32
17	ENSATEL E.I.R.L.	2803:1880:: /32
18	EMAX	2803:2100:: /32
19	MEDIA COMMERCE PERÚ S.A.C	2803:2480:: /32
20	ECONOCABLE MEDIA SAC	2803:2500:: /32
21	Moche Inversiones S.A.	2803:3300:: /32
22	UNIFIED GROUP ONLINE EIRL	2803:3580:: /32
23	GLG PERU SAC	2803:4480:: /32
24	MOVILMAX TELECOM S.A.	2803:4780:: /32
25	Olo del Perú S.A.C	2803:4800:: /32
26	NEWCOM PERU	2803:6500:: /32
27	NEXTEL DEL PERU S.A.	2803:7180:: /32
28	DIRECTV PERU S.R.L	2803:7b80:: /32
29	ARBITRARE SOLUCIONES LEGALES Y ARBITRALES S.A.C	2803:ab80:: /32
30	NETLINE PERU SA	2803:c200:: /32

31	EMPRESA DE TELECOMUNICACIONES MULTIMEDIA ALFA	2803:d680:: /32
32	AMITEL PERU TELECOMUNICACIONES SAC	2803:e500:: /32
33	Conexia SRL	2803:ed00:: /32
34	NOCPERU-LATIN TECHNOLOGIES	2803:f080:: /32
35	CONVERGIA PERU S.A.	2803:fe80:: /32

Fuente: LACNIC [102]

ASIGNACION DE DIRECCIONES IPv6

Finalizado el proceso de definir el prefijo a ser adquirido, es necesario realizar las asignaciones de los sub-prefijos a los diferentes componentes y sistemas de la infraestructura tecnológica, para lo cual se propone tener en cuenta 4 formas recomendados por el LACNIC para su asignación:

- **Consecutiva:** Esta forma considera ir asignando de manera consecutiva en orden creciente los prefijos a los diferentes componentes o sistemas de la red identificados. Al utilizar esta forma no se deja espacio entre los prefijos asignados y no hay posibilidad de aumentar el tamaño de los prefijos asignados.
- **Distancia potencia de dos:** Esta forma consiste en dejar prefijos libres contiguos con una distancia de potencia de dos. Al dejar prefijos libres permitirá un crecimiento a futuro.
- **Método Flexible:** Definido en la RFC 3531, esta forma, establece que la asignación de los prefijos es a partir de los bits centrales de acuerdo al prefijo asignado, posponiendo al máximo la asignación de los bits cercanos al prefijo asignado.
- **Algoritmo de asignación rápida:** Esta forma, establece que la asignación de los prefijos corresponde al punto medio de los valores posibles de los bits considerados. Inicialmente se toma el menor valor del prefijo, segundo el mayor valor del prefijo, el tercero será el prefijo del punto medio del mayor espacio disponible, este último procedimiento se repite hasta el finalizar la asignación de los prefijos. En la Figura 1, se aclara el orden de asignación descrita.

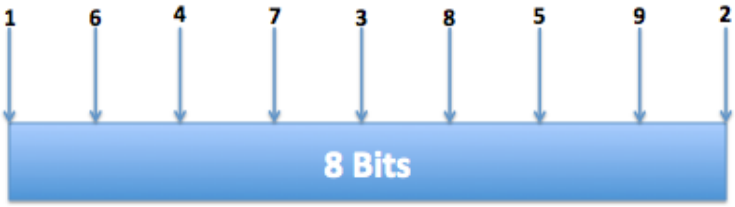

Figura 1– Asignación por el Algoritmo de asignación rápida

Fuente: LACNIC

RECOMENDACIONES DE COMPRA CON IPv6 EN LAS INSTITUCIONES PUBLICAS

MOTIVACION

Una de las principales acciones que están implementado diversos gobiernos como el de Estados Unidos, España, Chile, Colombia, Ecuador y Argentina, países analizados en el Capitulo II de la presente tesis, es la incorporación del requerimiento de IPv6 en las compras públicas en bienes y servicios relacionados a telecomunicaciones y tecnologías de la información.

En ese sentido, el presente documento expone recomendaciones a tener en cuenta para la elaboración de los requerimientos de compras por parte de las instituciones públicas.

MODELOS DE COMPATIBILIDAD

Uno de los principales documentos analizados sobre modelos de compatibilidad, es el realizado por el Gobierno de España, quien elaboró el documento denominado "GUÍA PARA LA INCORPORACIÓN DE IPV6 COMO REQUISITO DE COMPRA PÚBLICA", el cual puede ser accedido mediante la siguiente referencia [75]. Este documento, realiza el análisis de diversos modelos de compatibilidad a tener en cuenta para solicitarlo como requerimiento en las compras públicas.

Los modelos de compatibilidad analizados, en el documento citado previamente, permiten conocer los diversos criterios requeridos para considerar compatible al hardware o software con el nuevo protocolo.

Los modelos analizados son:

- **ISO/IEC 17025:** Esta norma establece los requisitos para los laboratorios de ensayo y calibración. El cumplimiento de esta norma por parte de los laboratorios, garantiza que estos sean técnicamente competentes para realizar diversas pruebas que sean solicitadas [75]. En nuestro caso las de compatibilidad con IPv6.

- **USGv6:** El gobierno de Estados Unidos, ha sido el primero de los países en establecer diversas directivas o normativas tanto técnicas y administrativas, con la finalidad de iniciar una adopción temprana del nuevo protocolo IPv6 en sus redes de gobierno. Como parte de su adopción del protocolo IPv6, ha desarrollado diversos documentos y creado laboratorios que permiten establecer la compatibilidad del protocolo IPv6 con el hardware y software. Estos documentos han sido elaborados por la National Institute of Standards and Technology – NIST, y están agrupados en el USGv6 profile [115]. Uno de los

documentos es la guía para los compradores, llamado USGv6 Buyer's Guide, el cual define un flujo para el proceso de adquisición, el cual se puede observar en la Figura 1.

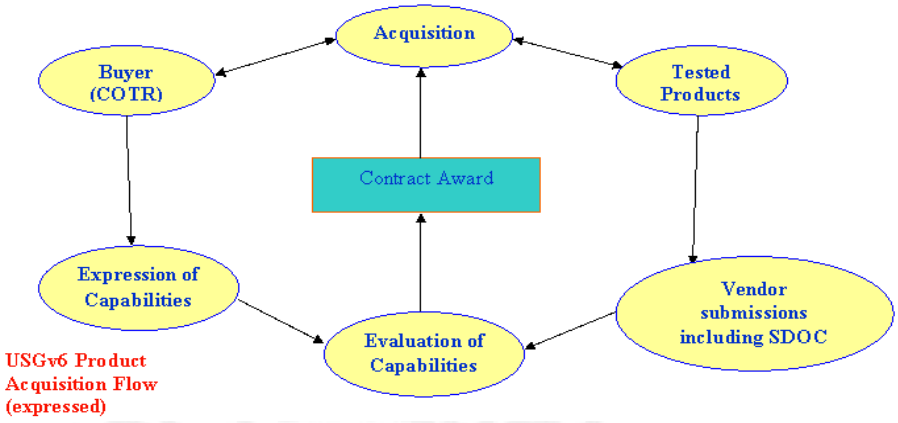

Figura 1 – Flujo para la adquisición de productos

Fuente: NIST [115]

En el flujo se visualiza que uno de los procesos, es la definición de la expresión de las capacidades requeridas. Esto nos indica que los usuarios deben definir las características en base a las funcionalidades requeridas, indicado las RFCs que requieren de un cumplimiento obligatorio por parte de los Proveedores, quienes deberán presentar su cumplimiento a través de laboratorios de pruebas destinadas para este tipo de soluciones.

En ese sentido, Estados Unidos propone una serie de recomendaciones de cumplimiento de RFC en la compra de equipos, clasificando estos en 3 categorías: Host, Router y Network Protection Device. Estas recomendaciones pueden ser accedidas desde la referencia [115] .En resumen los siguientes documentos:

- NIST SP 500-267 USGv6 profile
- USGv6-v1.0 Capabilities Cheklist

- **Programa "IPv6 Ready Logo":** Es un programa internacional de pruebas creado con la finalidad de establecer un conjunto de pruebas sobre la conformidad y compatibilidad de equipos con IPv6 [116]. Los principales objetivos de este programa son [116]:
  - Verificar la implementación del protocolo y validar la interoperabilidad de los productos IPv6.
  - Proporcionar herramientas gratuitas de autopruebas.
  - Proporcionar los laboratorios de pruebas "IPv6 Ready Logo" en todo el mundo para proporcionar asistencia o servicios de pruebas.

Asimismo, este programa, proporciona una base de datos de equipos que han sido probados de los diferentes fabricantes. Esta base de datos puede ser accedido desde la referencia [117]. Los equipos que han sido probados por este programa acceden a diferentes tipo de logotipo de acuerdo a las pruebas realizadas y pueden ser requeridos al momento de realizar el requerimiento de compras.

No es materia de la presente tesis realizar el análisis riguroso de estos modelos; sin embargo se ha descrito los principales criterios y alcances de cada uno de estos modelos, que permita considerar en las recomendaciones de compras públicas a nivel de las instituciones públicas.

RECOMENDACIONES PARA LA COMPRA EN EL ESTADO PERUANO

- En relación al hardware, de acuerdo a los modelos descritos, el RIR RIPE elabora el documento RIPE-554, en el cual se realiza un estudio de compilación de las RFCs de requerimiento obligatorio y opcional en base a los modelos de compatibilidad de IPv6 de la USGv6 y del IPv6 Ready Logo. Es importante considerar el estudio como requerimientos en las compras públicas a nivel Perú. El estudio puede ser accedido desde la siguiente referencia [118].
- Se considera importante que solicitar al proveedor de hardware que las pruebas a los equipos sean realizadas por un laboratorio que cumpla con las norma ISO/IEC 17025 y que esta emita un certificado de la compatibilidad con IPv6, precisando las RFCs con sus respectivas pruebas.
- En relación al software comercial, se deberá solicitar que estos tengan habilitado las características de configuración de todo su arquitectura tanto para IPv4, IPv6 y en doble pila (IPv4/IPv6) y se garantice que todas la funcionalidades requeridas en IPv4 se realicen en IPv6 y doble pila.
- En relación a los sistemas de información o software a medida, que requieran el uso de una dirección IP para su funcionamiento deberán de garantizar el soporte de la pila de protocolos IPv4, IPv6 y doble pila. Se deberá garantizar que todas las funcionalidades estén disponibles indistintamente de la versión del protocolo. Asimismo, se deberá considerar los siguientes estándares de acuerdo a la referencia de la guía de compras del gobierno de España [75]:
  - IEEE Standard 1003.1-2001, basado en la especificación de servicios XNS.
  - RFC3542, Advanced Sockets Application Program Interface (API) for IPv6.
  - RFC4038, Applicacion Aspects of IPv6 Transition.
  - RFC4584, Extension to Sockets API for Mobile IPv6, para algunas aplicaciones móviles de nodos MIPv6.
  - RFC5014, IPv6 Socket API for Source Address Selection.

- RFC3678, Socket Interface Extension for Multicast Source Filtering .
- RFC3986, Uniform Resource Identifiers, sintaxis genérica para la representación de direcciones IPv6 en interfaces de usuario.

- Para validar la compatibilidad de los sistemas de información o software a medida que se adquiere, será necesario contratar una proveedor tercero, él cual realizará las pruebas de manera independiente y validará si el software cumple con lo requerido en relación a la compatibilidad con IPv6. Se recomienda solicitar que la metodología de pruebas sea la Certiv6 creado por el RIR LACNIC.
- Se deberá de solicitar que el proveedor presente una carta del fabricante de hardware y software indicando la compatibilidad con cada uno de los RFCs que la institución pública considere pertinente solicitarlo. Agregado a este documento, una carta de compromiso de la actualización de las RFCs o de versión de software relacionadas a IPv6 durante el periodo de garantía.

METODOLOGIA PARA PRUEBAS DE COMPATIBILIDAD DE IPv6 EN SOFTWARE

MOTIVACION

El software tanto comercial como los sistemas de información que se desarrollan a la medida, que requieran el uso del protocolo IP para su funcionamiento, deberán de pasar por una Fase de pruebas antes de su publicación, de tal manera se garantice su compatibilidad y normal funcionamiento con el nuevo protocolo IPv6.

En ese sentido, en el presente documento se describe la metodología desarrollada por el Centro de Ensayos de Software – CES, el cual es una organización privada del Gobierno de Uruguay. El CES elaboro la metodología de pruebas denominada Certiv6 a solicitud del RIR LACNIC y viene realizando diversas capacitación en pruebas de software en nuestra región.

METODOLOGIA DE PRUEBAS ELABORADO POR EL CES DE URUGUAY

Cem Kaner, define pruebas o testing, como una investigación empírica y técnica orientada a proporcionar información sobre la calidad de un producto de software para un actor o usuario. “Es una actividad cognitiva, no es una actividad mecánica”.

Basados en este concepto, el CES de Uruguay, establece la metodología de pruebas Certiv6, el cual considera 5 etapas que agrupan diversas actividades orientadas a las pruebas del protocolo IPv6. Estas etapas se muestran en la siguiente Figura 1:

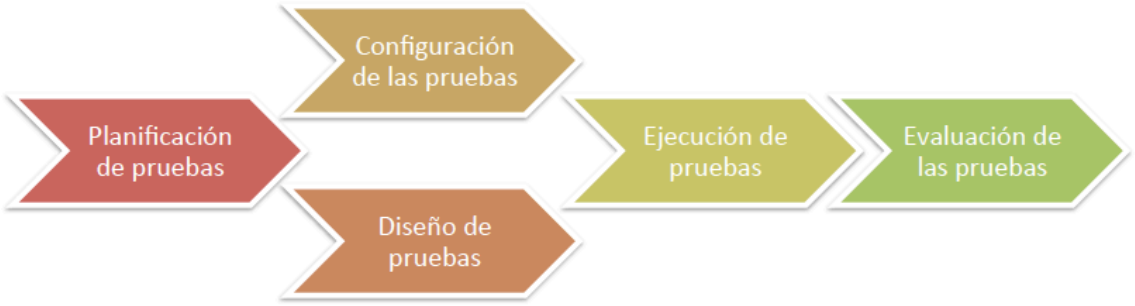

Figura 1 – Etapas de la Metodología Certiv6

Fuente: LACNIC [122]

Se ha definido diversas actividades por cada una de las etapas, las cuales generan diversos documentos necesarios para el ingreso de las etapas siguientes, permitiendo un análisis secuencial. Estas actividades de describen en la Figura 2:

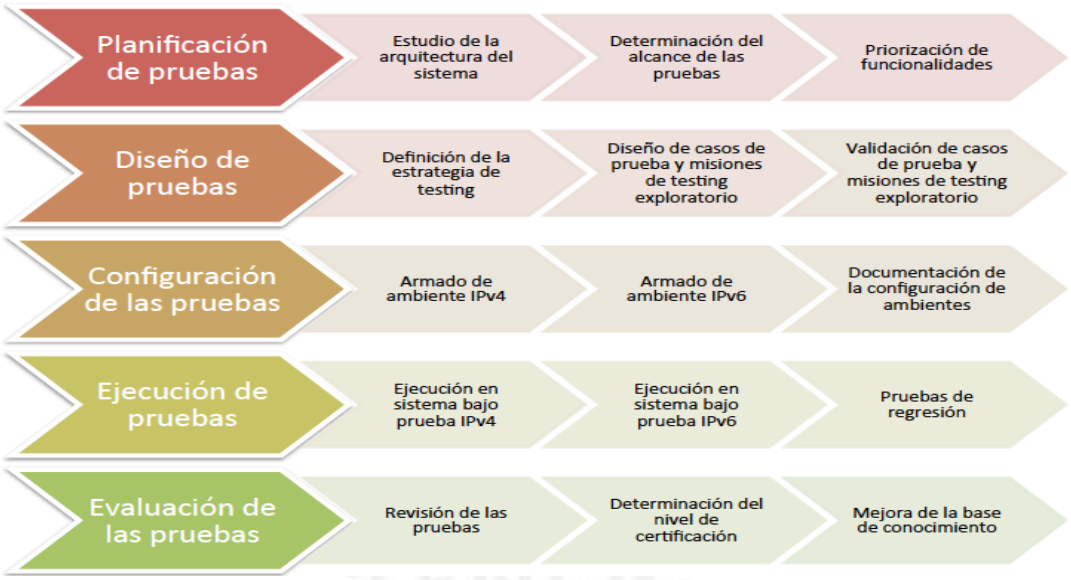

Figura 2 – Actividades por Etapa de la Metodología Certiv6

Fuente: LACNIC [122]

Asimismo, esta metodología recomienda la definición de 3 roles importantes, los cuales deben ser los profesionales principales a considerar para esta etapa de pruebas:

- Lider de Testing
- Tester
- Experto en IPv6

Finalmente, se recomienda que para las compras de software las instituciones públicas deberán de requerir que se realicen las pruebas del software adquirido en base a la metodología Certiv6.