UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

CONFIGURACION DE TUNELES EN EL PROTOCOLO IPv6

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRONICO

PRESENTADO POR:

ANGEL GOOVERT AYALA HERRERA

PROMOCIÓN
2003 - I

LIMA – PERÚ
2006

CONFIGURACION DE TUNELES EN EL PROTOCOLO IPv6

Dedico este trabajo a:

Mis padres,

ANGEL SALOMON AYALA ALLENDE

LUZ OTILIA HERRERA CASTILLO

SUMARIO

Debido a la multitud de nuevas aplicaciones en las que IPv4 (Protocolo Internet versión 4) ha sido utilizado, ha sido necesario crear ¨añadidos¨ al protocolo IPv4, podemos mencionar Calidad de Servicio (QoS), Seguridad (IPsec) y movilidad. El inconveniente más importante de estas aplicaciones de IPv4 es que utilizar cualquiera de ellos es fácil, pero no tanto cuando se pretende usar dos añadidos.

Con los cambios producidos en un corto tiempo se han conectado las PC a LAN (Redes de

Area Local), se han conectado las LAN entre sí, y las WAN (Redes de Area Amplia) y todo ello a menudo se ha conectado con la Internet, el resultado de esta es una Internet muy diversa con millones de usuarios.

Los criterios que se han seguido a lo largo del desarrollo de IPv6 (Protocolo Internet versión 6) han sido fundamentales para obtener un protocolo sencillo.

En este informe se mostrara los diferentes avances que en materia de IPv6 están siendo establecidos, y además como se puede hacer la transición de redes IPv4 a IPv6 para aprovechar los beneficios de IPv6.

INDICE

PROLOGO

El propósito del informe es la transición de redes IPv4 a redes IPv6, para esto es imprensidible que se muestre los diferentes características y beneficios de usar IPv6, formatos de cabecera IPv6, principales protocolos de IPv6, arquitectura de direcciónamiento IPv6. Como apéndice mostrare la implementación de túneles en el protocolo IPv6.

Los protocolos de transición no son fáciles y la transición de IPv4 a IPv6 no es la excepción, dos de las estrategias que se muestran son los protocolos doble pila usando IPv4/IPv6 y los mecanismos de túneles IPv6 sobre IPv4.

CAPITULO I

CARACTERISTICAS Y BENEFICIOS DE USAR IPv6

1.1 Introducción a IPv6

El Protocolo Internet llamado IP versión 4 o IPv4 no ha cambiado de forma significativa desde sus inicios en 1981. IPv4 ha demostrado ser un protocolo robusto y ínteroperable, y ha logrado ampliar un conjunto de redes interconectadas para un uso global del tamaño que Internet tiene en la actualidad. Estas son las virtudes de su diseño inicial.

Podemos mencionar que el diseño inicial no previó las siguientes circunstancias:

El reciente crecimiento exponencial de Internet y el agotamiento inminente del espacio de direcciones IPv4. Las direcciones IPv4 han empezado a escasear relativamente, lo que ha obligado a algunos Proveedores de Servicios de Internet a utilizar un NAT (Traductor de Direcciones de Red) para asignar múltiples direcciones privadas a una única dirección IP pública. Pero los NAT no admiten la seguridad de nivel de red basada en estándares o la asignación correcta de todos los protocolos de nivel superior y se pueden crear problemas al conectar dos Proveedores de Servicios de Internet que utilizan el espacio de direcciones privadas.

El crecimiento de Internet y la capacidad de los enrutadores (Routers) de la red troncal de Internet para mantener tablas de enrutamiento grandes.

La necesidad de mayor compatibilidad con la entrega de datos en tiempo real llamado QoS (Calidad de Servicio) aunque existe en IPv4, se necesita una configuración más sencilla.

La mayoría de las implementaciones actuales de IPv4 se deben configurar manualmente o mediante un protocolo de configuración de direcciones, como el DHCP (Protocolo de Configuración Dinámica de Host).

El requisito de seguridad en el nivel de IP.

1.2 Características IPv6

IPv6 provee los siguientes beneficios a las redes :

- Mayor espacio de direcciones.
- Simplificación del formato de la cabecera.
- Jerarquía en la arquitectura de red para la eficiencia de enrutamiento.
- Soporte para los protocolos de enrutamiento.
- Auto configuración y soporte "Plug and Play".
- Seguridad embebida con implementación IPsec obligatoria.
- Calidad de servicio.

1.2.1 Mayor espacio de direcciones

El tamaño de las direcciones IP cambia de 32 bits a 128 bits, para soportar: más niveles de jerarquías de direcciónamiento y más nodos direcciónables. IPv4 tiene un espacio de direcciones de 32 bits, es decir 2^32 (4.294.967.296). En cambio IPv6 nos ofrece un espacio de 2^128 bits (340.282.366.920.938.463.374.607.431.768.211.456). El formato se muestra en la figura 1.1. Esto permite que cualquier dispositivo electrónico disponga de una dirección IPv6: telefonos celulares, artefactos electrónicos, etc. Con esto ya no es necesaria la implementación de NAT en la red.

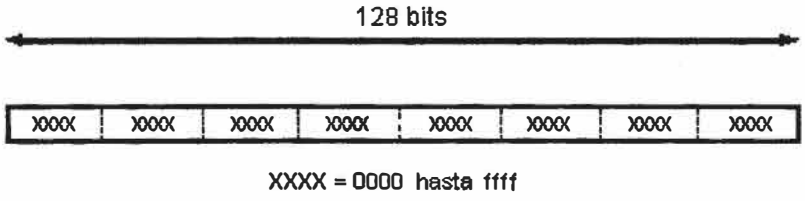


Figura 1.1 : Muestra el formato general de una dirección IPv6

La capacidad de proveer una única dirección para cada dispositivo de red es uno de los beneficios del mayor espacio de direcciones. La cual es especialmente importante para la telefonía residencial IP.

1.2.2 Simplificación de la cabecera

Aunque el incremento en el numero de bits en las direcciones de IPv6 resulta en un incremento en el tamaño de la cabecera de IPv6, el formato de la cabecera IPv6 es más simple que comparado con la cabecera de IPv4. El tamaño básico en la cabecera IPv4 es solo de 20 octetos pero tiene campos para adicionar otras características. La cabecera IPv6 tiene un tamaño fijo de 40 octetos. Aunque en IPv4 los campos de la cabecera 6 de los 12 han sido removidos del IPv6, algunos campos IPv4 han sido llevados al IPv6 modificando sus nombres y algunos de los nuevos campos han sido adicionados para mejorar la eficiencia e introducir nuevas características. Como muestra la figura 1.2, la longitud de cabecera, identificación, indicador, desplazamiento de fragmentación, suma de chequeo y las opciones de relleno han sido removidos de la cabecera IPv6. Todo se hace para procesar rápido la cabecera. También todos los campos en la cabecera IPv6 son de 64 bits, aprovechando la generación actual de los actuales procesadores de 64 bit.

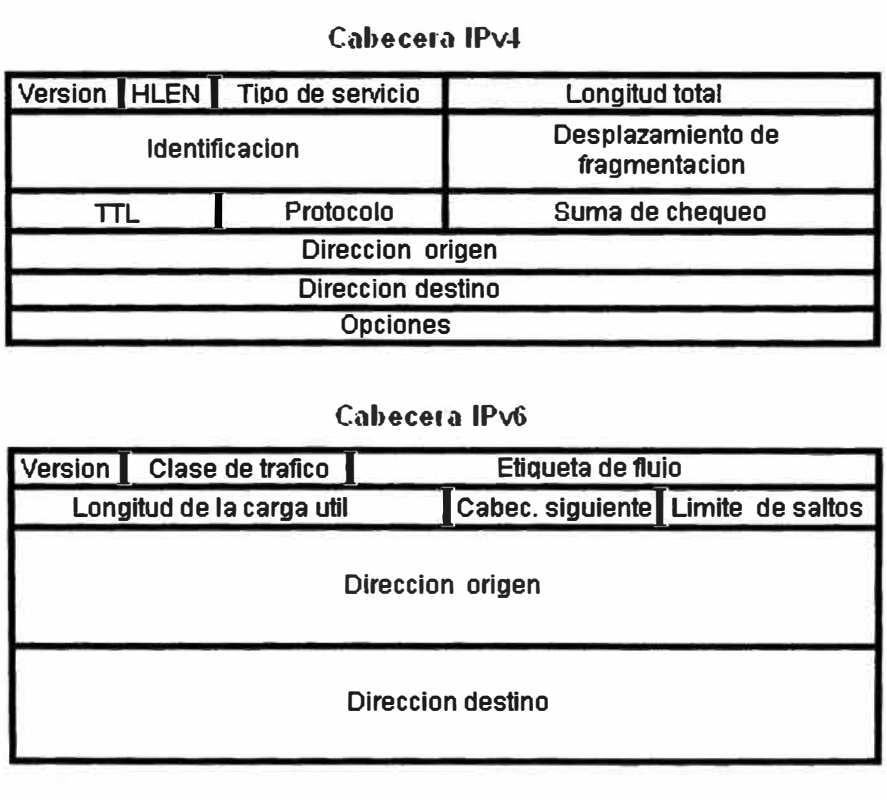


Figura 1.2 : Comparación de cabeceras IPv4 y IPv6

La fragmentación es ahora manejada diferente y no necesita campos en la cabecera básica de IP ya que los enrutadores perdían mucho tiempo recalculando la suma de chequeo cada vez que pasaba por ellos, esto ha sido mejorado en IPv6. En las redes IPv6 la fragmentación es manejada por el dispositivo de origen con la ayuda de MTU (Unidad Máxima de Transmisión). La suma de chequeo ha sido removido de la capa IP porque varias de las tecnologías capas de enlace ya hacen la suma de chequeo, control de error y porque la fiabilidad de la capa de red es muy buena. La suma de chequeo en la cabecera IP fue considerado innecesario y no muy provechoso. Las posiciones de campo de IPv4 están cambiadas en IPv6 y ahora es administrada por una cabecera de extensión. La mayoría de los otros campos fueron cambiados solo ligeramente. Se resalta que un menor numero de campos en la cabecera tendremos un procesamiento más rápido.

1.2.3 Jerarquía en la arquitectura de red para la eficiencia de enrutamiento

La disponibilidad de espacios de direcciones muy largas y prefijos de redes proveen una flexible arquitectura de red, esta flexibilidad permite a una organización usar solo un prefijo de una red entera de la organización. Un espacio de dirección largo permite la asignación de direcciones de bloques largos para Proveer Servicios de Internet (ISP) y a otras organizaciones. Esta locación permite que el ISP agregue prefijos en conjunto a todos sus clientes en un solo prefijo y anunciar este único prefijo a la Internet IPv6. Las largas direcciones IPv6 también habilitan el uso de múltiples niveles de jerarquía dentro de los espacios de direcciones. Cada nivel ayuda en su conjunto al tráfico a ese nivel, y a aumentar la cuota de direcciones en un formato de jerarquía. La implementación de múltiples niveles en la dirección de jerarquía permite flexibilizar las nuevas funciones como en el ámbito de las direcciones. La jerarquía de arquitectura de red de IPv6 permite a las IPS's (Seguridad en Internet Protocolo) usar en su conjunto los prefijos de las redes y proveer un eficiente y escalable enrutamiento. La estructura de dirección de jerarquía esta diseñado para reducir el tamaño de las tablas de enrutamiento de la Internet. Sin un buen plan de dirección de jerarquía, los enrutadores podrían almacenar largas tablas de enrutamiento.

1.2.4 Soporte para protocolos de enrutamiento

Para habilitar el enrutamiento escalable, IPv6 soporta la existencia de Protocolos de Entrada Interior (IGP's) y Protocolos de Puerta Exterior (EGP's). Similar al IPv4, el IPv6 usa la mayor longitud del prefijo para un algoritmo de enrutamiento.

a) Protocolo de Información de Ruteo (RIP)

Uno de los protocolos de enrutamiento más antiguos RIP utiliza algoritmos de vector distancia para calcular sus rutas. El protocolo de la siguiente generación del Protocolo de Información de Ruteo (RIPng) se explica en RFC 2080 (Request for Comments). RIPng para IPv6.

b) Protocolo del Primer Camino más Corto Abierto versión 3 (OSPF)

OSPF propone el uso de rutas más cortas y accesibles mediante la construcción de un mapa de la red y mantenimiento de bases de datos con información sobre sistemas locales y vecinos, de esta manera es capaz de calcular la métrica para cada ruta, entonces se eligen las rutas de encaminamiento más cortas.

c) Protocolo de Entrada de Frontera (BGP) o Borde Multiprotocolo

BGP (Protocolo de Entrada de Frontera) se encarga de mover paquetes de una red a otra pero en algunos casos debe preocuparse de otras cuestiones que no tienen porque estar relacionadas con el objetivo de mover los paquetes de la forma más eficiente posible. Es posible que se deban considerar algunas restricciones relacionadas con cuestiones comerciales o políticas, por ejemplo:

- Una empresa no hace de red de tránsito para los mensajes de la competencia.

1.2.5 Auto configuración y soporte "Plug and Play"

La característica de auto configuración de dirección es construida dentro del protocolo IPv6 para facilitar el intranet de amplia gestión de dirección. La característica de auto configuración habilita el desarrollo de Internet "Plug and Play" de nuevos dispositivos consumidores, tal como teléfonos celulares, dispositivos inalámbricos, aparatos electrodomésticos. Como resultado, los dispositivos de red pueden conectarse a la red sin configuración manual y sin ningún servidor, tal como los servidores DHCP (Protocolo de Configuración Dinámica de Servidores).

1.2.6 Seguridad integrada con implementación IPsec obligatoria

Mientras el uso de IPsec es opcional en IPv4, el IPsec es obligatorio en IPv6 y es parte del juego de protocolos IPv6, además, los implementadores de red pueden habilitar IPsec en todos los nodos IPv6, potencialmente hacer a las redes más seguras. La comunicación privada a través de un medio público como Internet requiere servicios de cifrado que impidan que los datos enviados se puedan ver o modificar durante el tránsito.

El IPv6 provee seguridad a las cabeceras de extensión, hacerlo más fácil para implementar las encriptaciones, autenticaciones y para Redes Privadas Virtuales (VPN's). Porque IPv6 ofrece globalmente direcciones únicas y seguridad. IPv6 puede proveer servicios de seguridad punto a punto tal como el control de acceso, confidencialidad y la integridad de la data sin la necesidad para firewalls adicionales que podrían introducir problemas adicionales, incluyendo la ejecución del cuello de botella.

1.2.7 Calidad de servicio (QoS)

QoS en IPv6 es el mismo que en IPv4, pero en la cabecera de IPv6 tiene un nuevo campo llamado Etiqueta de Flujo el cual puede contener una etiqueta identificando un flujo específico, tal como video o videoconferencia. El nodo fuente genera esta etiqueta de flujo. Teniendo una etiqueta de flujo, esta habilita los dispositivos QoS en el camino para tomar acciones propias basadas en esta etiqueta. Pero, la existencia misma de la etiqueta de flujo no es una característica de QoS.

CAPITULO II

IPv6 FORMATOS DE CABECERA

Las cabeceras de IPv6 son más simples y más eficientes que las cabeceras IPv4. La simplicidad de las cabeceras IPv6 ayuda a reducir los costos de procesamiento.

Los principales cambios entre las dos versiones son los siguientes:

Capacidades de direccionamiento extendida: IPv6 incrementa el tamaño de dirección IP de 32 bits a 128 bits, para dar soporte a mas niveles de direccionamiento jerárquico, un numero mucho mayor de nodos direccionables y una auto configuración mas simple de direcciones.

Simplificación del formato de cabecera: Algunos campos de la cabecera IPv4 se han sacado o se han hecho opcional, para reducir el costo del caso común de proceso de tratamiento de paquete y para limitar el costo del ancho de banda, de la cabecera IPv6.

Soporte mejorado para las extensiones y opciones: Los cambios en la manera en que se codifican las opciones de la cabecera IP permiten un reenvío más eficiente, límites menos rigurosos en la longitud de opciones, y mayor flexibilidad para introducir nuevas opciones en el futuro.

Capacidad de etiquetado de flujo : Una nueva capacidad se agrega para permitir el etiquetado de paquetes que pertenecen a "flujos" de tráfico particulares para lo cuál el remitente solicita tratamiento especial, como la calidad de servicio no estándar o el servicio en "tiempo real".

Capacidades de autenticación y privacidad: Extensiones para utilizar autenticación, integridad de los datos, y (opcional) confidencialidad de los datos, se especifican para el IPv6.

2.1 Campos de cabecera IPv6

La cabecera del paquete básico en IPv6 consiste en 8 campos como se muestra en la figura 2.1

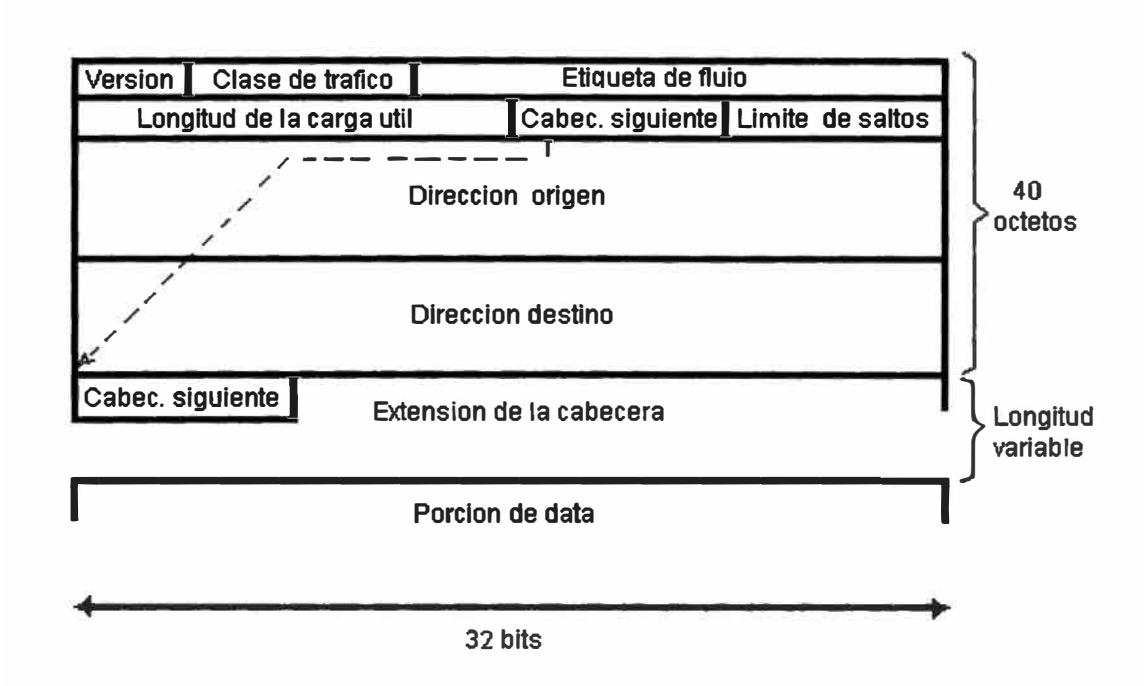


Figura 2.1 : Campos de cabecera IPv6

Descripción de los campos de cabecera IPv6:

Versión : El campo versión de IPv6 consta de 4 bits (6 en binario) y la versión en IPv4 consta de 4 bits (4 en binario).

Clase de trafico : El campo de clase de trafico son 8 bits similar al Tipo de Servicio (ToS) que tenia en IPv4. Las funcionalidades son las mismas en IPv4 y IPv6. Se usa para nodos originadores o enrutadores para que distingan entre diferentes clases o prioridades de paquetes IPv6.

Etiqueta de flujo : Los 20 bits del campo de etiqueta de flujo es un nuevo campo en IPv6. El campo de etiqueta de flujo puede ser usado para etiquetar paquetes de un específico flujo a diferenciar en los paquetes en la capa de red. Por lo tanto, el campo de etiqueta de flujo habilita la identificación de un flujo procesado por los enrutadores en la trayectoria. Con este nivel el enrutador no necesita chequear profundamente el paquete para identificar el flujo, porque la información esta disponible en el paquete de la cabeza IP. La etiqueta de flujo permite aplicaciones en el fin del sistema para diferenciar fácilmente el

trafico en la capa IP, esto provee calidad de servicio, por ejemplo la etiqueta del flujo se utiliza para la calidad de las conexiones del servicio, tales como ésos necesitados por datos en tiempo real (voz y vídeo).

Longitud de la carga util : Similar al campo de la longitud total en IPv4, la longitud de la carga indica la porción total del paquete. Con 16 bits, una carga útil IPv6 de hasta 65.535 octetos puede ser indicada.

Cabecera siguiente : Similar al campo de protocolo en el campo de cabecera IPv4. El valor del nuevo campo de cabecera de IPv6 determina el tipo de información siguiente a la cabecera básica de IPv6. El tipo de información siguiente de la cabecera básica del IPv6 puede ser un paquete de la capa de transporte, como un paquete TCP, UDP o una cabecera de extensión como muestra la figura 2.2. IPv6 usa diferentes enfoques para administrar información opcional en la cabecera. Esto define las cabeceras de extensión que forman una cadena de enlaces de cabeceras juntas por el siguiente campo de cabecera contenida en cada cabecera de extensión. Este mecanismo mejora mas eficientemente el proceso de extensión de cabecera , habilita una rápida velocidad de atención, y deja al enrutador (router) con menos procesamiento de trabajo para cada paquete.

Limite de saltos : Es similar al campo de tiempo de vida en la cabecera de IPv4 el valor del limite de salto especifica el numero máximo de enrutadores que un paquete de IPv6 puede pasar antes de que sea considerado invalido. El campo de limite de saltos de IPv6 contiene 8 bits, cada enrutador decrementa el valor en uno, porque no hay suma de chequeo en IPv6 el enrutador puede decrementar el valor sin necesidad de recalcular la suma de chequeo lo cual ahorra recursos de procesamiento.

Dirección origen: El campo de la dirección origen en IPv6 es similar al campo de dirección origen en la cabecera IPv4 , extensión que contiene en el campo 128 bits en lugar de los 32 bits de dirección origen que tiene en IPv4.

Dirección de destino: El campo de dirección de destino IPv6 es similar al campo de dirección de destino en la cabecera IPv4, extensión que el campo contiene 128 bits de destino en lugar de los 32 bits en IPv4.

2.2 Cabeceras de extensión IPv6

En IPv6, la información de capa Internet opcional se codifica en cabeceras separadas que se pueden colocar entre la cabecera IPv6 y la cabecera de capa superior dentro de un

paquete. Hay limitadas cabeceras de extensión, cada una identificada por un valor de cabecera siguiente distinto. Según muestra la figura 2.2, un paquete IPv6 puede llevar cero, una, o más cabeceras de extensión, cada una identificada por el campo cabecera siguiente de la cabecera precedente.

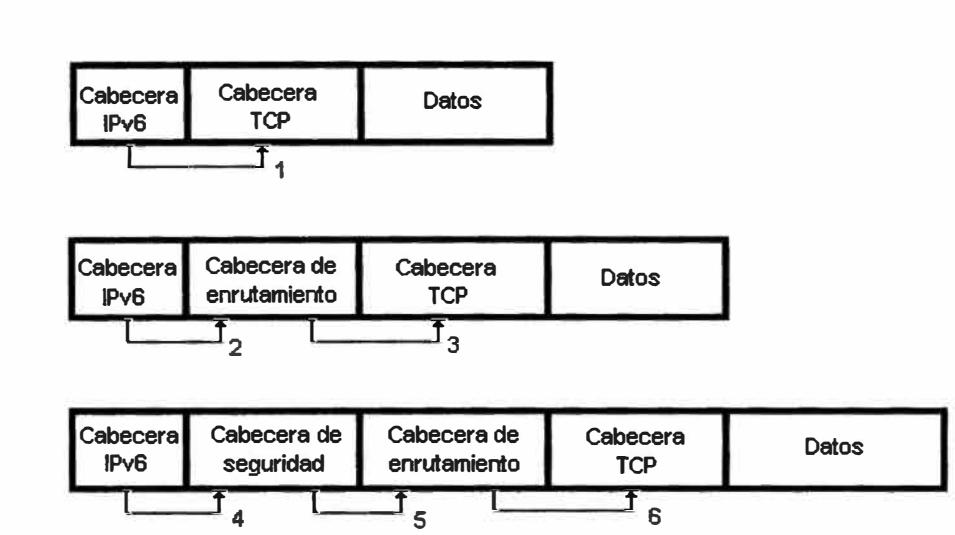


Figura 2.2 : Cabeceras de extensión

La tabla N^{O} 2.1 muestra las cabeceras del paquete IPv6.

TABLA N^{0} 2.1: CABECERAS DEL PAQUETE IPv6

Cabecera siguiente (1)	TCP
Cabecera siguiente (2)	Enrutamiento
Cabecera siguiente (3)	TCP
Cabecera siguiente (4)	Seguridad
Cabecera siguiente (5)	Enrutamiento
Cabecera siguiente (6)	TCP

Pero, las cabeceras de extensión no son examinadas ni procesadas por ningún nodo a lo largo de la ruta de entrega de un paquete, hasta que el paquete alcance el nodo (o cada uno del conjunto de nodos, en el caso de multidifusión) identificado en el campo dirección destino de la cabecera IPv6. Allí, el demultiplexaje normal en el campo cabecera siguiente de la cabecera IPv6 invoca el módulo para procesar la primera cabecera de extensión, o la

cabecera de capa superior si no hay ninguna cabecera de extensión presente. Este contenido y la semántica de cada cabecera de extensión determinan si se procede o no a la cabecera siguiente. Entonces, las cabeceras de extensión se deben procesar estrictamente en el orden que aparecen en el paquete; un receptor no debe, por ejemplo, examinar a través de un paquete buscando un tipo en particular de cabecera de extensión y procesar esa cabecera antes de procesar todas las precedentes.

La excepción mencionada en el párrafo precedente es la cabecera opciones de salto a salto, la cual lleva información que debe ser examinada y procesada por cada nodo a lo largo de la ruta de entrega de un paquete, incluyendo los nodos de origen y de destino. La cabecera opciones de salto a salto, cuando está presente, debe seguir inmediatamente a la cabecera IPv6. Su presencia es indicada por el valor cero en el campo cabecera siguiente de la cabecera IPv6.

Si, como resultado de procesar una cabecera, un nodo necesita proceder a la cabecera siguiente pero el valor cabecera siguiente en la cabecera actual es desconocido por el nodo, debe descartar el paquete y enviar un mensaje ICMP (Protocolo de Control de Mensajes de Internet) de problema de parámetro al origen del paquete, con un valor código ICMP de 1 ("encontrado tipo de cabecera siguiente desconocido") y el campo puntero ICMP conteniendo el desplazamiento del valor desconocido dentro del paquete original. La misma acción se debería tomar si un nodo encuentra un valor cabecera siguiente de cero en cualquier cabecera con excepción de una cabecera IPv6.

Cada cabecera de extensión es un entero múltiplo de 8 octetos de largo, para conservar la alineación de 8 octetos para las cabeceras subsiguientes. Los campos multiocteto dentro de cada cabecera de extensión se alinean en sus límites naturales, es decir, los campos de ancho de n octetos son colocados en un entero múltiplo de n octetos desde el inicio de la cabecera, para n = 1, 2, 4, o 8.

2.2.1 Orden de las cabeceras de extensión

Cuando más de una cabecera de extensión se usa en un mismo paquete, se recomienda que esas cabeceras aparezcan en el siguiente orden:

Cabecera IPv6
Cabecera opciones de salto a salto
Cabecera opciones de destino (*)
Cabecera enrutamiento

- Cabecera fragmento
- Cabecera autenticación (**)
- Cabecera seguridad del encapsulado de la carga util (**)
- Cabecera opciones de destino (***)
- Cabecera de capa superior

* : Para las opciones a ser procesadas por el primer destino que aparece en el campo dirección destino IPv6 más los destinos subsiguientes listados en la cabecera enrutamiento.

** : Recomendaciones adicionales con respecto al orden relativo de las cabeceras autenticación y seguridad del encapsulado de la carga util se dan en la [RFC-2406].

*** : Para las opciones a ser procesadas solo por el destino final del paquete.

Cada cabecera de extensión debe ocurrir solamente una vez, a excepción de la cabecera opciones de destino la cual debe de ocurrir a lo sumo dos veces (una vez antes de una cabecera enrutamiento y la otra vez antes de una cabecera de capa superior).

Si la cabecera de capa superior es otra cabecera IPv6 (en el caso de que el IPv6 sea túnelizado o encapsulado en el IPv6), puede ser seguida por sus propias cabeceras de extensión, las cuales están separadamente sujetas a las mismas recomendaciones de orden. Siempre y cuando se definan otras cabeceras de extensión, sus restricciones de orden concerniente a las cabeceras arriba listadas deben ser especificadas.

Los nodos IPv6 deben aceptar e intentar procesar cabeceras de extensión en cualquier orden y cualquier número de veces que ocurran en un mismo paquete, a excepción de la cabecera opciones de salto a salto la cual está restringida a aparecer sólo inmediatamente después de una cabecera IPv6.

2.2.2 Opciones

Dos de las cabeceras de extensión (la cabecera opciones de salto a salto y la cabecera opciones de destino) llevan un número variable de "opciones" codificadas Tipo-Longitud-Valor (TLV), como muestra la figura 2.3.

Figura 2.3 : Cabecera de extensión

Donde los campos son:

Tipo de opción : Identificador de 8 bits.

Longitud de datos opcionales : Entero sin signo de 8 bits. Longitud del campo datos de la opción de esta opción, en octetos.

Datos de la opción: Campo de longitud variable. Datos específicos del tipo de opción.

Los identificadores tipo de opción se codifican internamente tales que sus 2 bits de más alto orden especifican la acción que se debe tomar si el nodo IPv6 en proceso no reconoce el tipo de opción:

- 00 : No tomar en cuenta esta opción y continuar procesando la cabecera.
- 01 : Descartar el paquete.
- 10 : Descartar el paquete sin tener en cuenta si o no la dirección de destino del paquete fue una dirección multidifusión, enviar un mensaje ICMP con problema de parámetro, código 2, a la dirección origen del paquete señalando el tipo de opción desconocido.
- 11 : Descartar el paquete y, solo si la dirección destino del paquete no fue una dirección multidifusión, enviar un mensaje ICMP problema de parámetro, código 2, a la dirección origen del paquete señalando el tipo de opción desconocido.

El tercer bit de más alto orden del tipo de opción especifica si o no los datos de la opción de esa opción pueden modificar el enrutamiento hacia el destino final del paquete. Cuando una cabecera autenticación está presente en el paquete, para cualquier opción cuyos datos pueden modificar el enrutamiento, su campo entero datos de la opción se debe tratar como octetos de valor cero cuando se calcula o verifica el valor de autenticidad del paquete.

- 0 Los datos de la opción no modifican el enrutamiento.
- 1 Los datos de la opción pueden modificar el enrutamiento.

Los tres bits de alto orden descritos arriba están para ser tratados como parte del tipo de opción, no independientemente del tipo de opción. Es decir, una opción en particular se identifica por un tipo de opción de 8 bits completo, no sólo por los 5 bits de bajo orden de un tipo de opción.

El mismo espacio de enumeración del tipo de opción se usa tanto para la cabecera opciones de salto a salto como para la cabecera opciones de destino. Sin embargo, la

especificación de una opción en particular puede restringir su uso a solamente una de esas dos cabeceras.

Las opciones individuales pueden tener requisitos específicos de alineación, para asegurar que los valores multiocteto dentro de los campos datos de la opción caigan en límites naturales. El requisito de alineación de una opción se especifica usando la notación xn+y, lo que significa que el tipo de opción debe aparecer en un entero múltiplo de ¨x¨ octetos desde el inicio de la cabecera, más ¨y¨ octetos.

Por ejemplo:

- 2n : Significa cualquier desplazamiento de 2 octetos a partir del comienzo de la cabecera.

- 8n+2 : Significa cualquier desplazamiento de 8 octetos a partir del comienzo de la cabecera, mas 2 octetos..

2.2.3 Cabecera opciones de salto a salto

La cabecera opciones de salto a salto se usa para llevar información opcional que debe ser examinada por cada nodo a lo largo de la ruta de entrega de un paquete. La cabecera opciones de salto a salto se identifica por un valor cabecera siguiente de 0 en la cabecera IPv6, como muestra la figura 2.4.

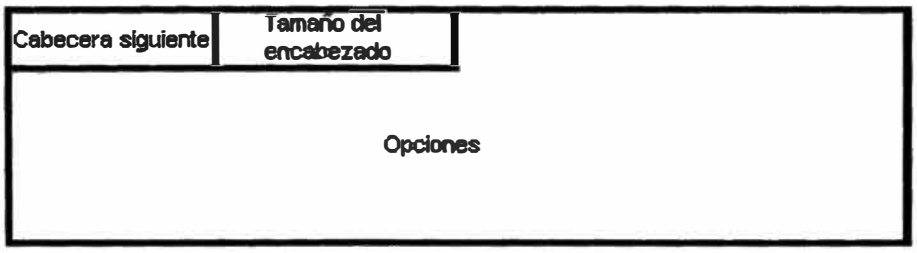


Figura 2.4 : Cabecera Opciones de Salto a Salto

Donde los campos son:

Cabecera siguiente : Campo de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera opciones de salto a salto. Utiliza los mismos valores que el campo protocolo del IPv4.

Tamaño del encabezado : Entero sin signo de 8 bits. Longitud de la cabecera opciones de salto a salto en unidades de 8 octetos, no incluye los primeros 8 octetos.

Opciones : Campo de longitud variable, de longitud tal que la cabecera opciones de salto a salto completa es un entero múltiplo de 8 octetos de largo. Contiene una o más opciones codificadas TLV.

2.2.4 Cabecera enrutamiento

La cabecera enrutamiento es utilizada por un origen IPv6 para listar uno o más nodos intermedio a ser "visitados" en el camino hacia el destino de un paquete. La cabecera enrutamiento se identifica por una cabecera siguiente de valor 43 en la cabecera inmediatamente precedente, como muestra la figura 2.5.

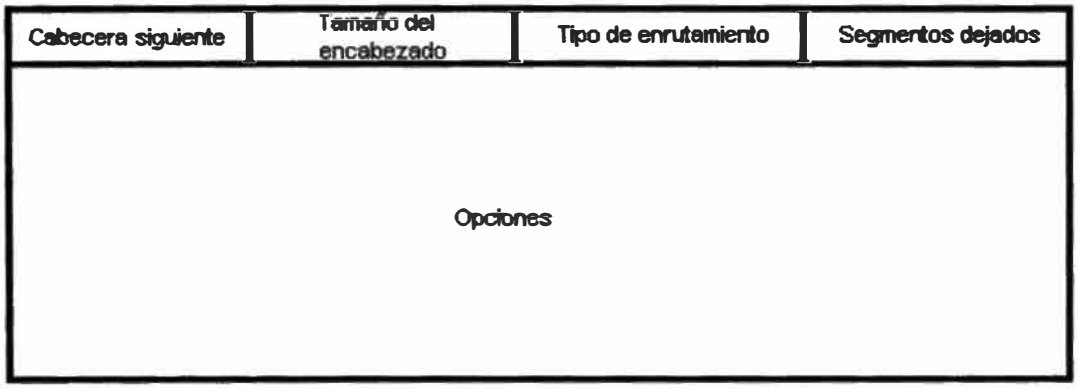


Figura 2.5 : Cabecera de enrutamiento

Donde los campos son:

Cabecera siguiente : Campo de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera enrutamiento. Utiliza los mismos valores que el campo protocolo del IPv4.

Tamaño encabezado : Entero sin signo de 8 bits. Longitud de la cabecera enrutamiento en unidades de 8 octetos, no incluye los primeros 8 octetos.

Tipo de enrutamiento : Identificador de 8 bits de una variante en particular de cabecera enrutamiento.

Segmentos dejados : Entero sin signo de 8 bits. Número de segmentos de ruta restantes, es decir, número de nodos intermedio explícitamente listados aún a ser visitados antes de alcanzar el destino final.

Datos específicos del tipo : Campo de longitud variable, de formato determinado por el tipo de enrutamiento, y de longitud tal que la cabecera enrutamiento completa es un entero múltiplo de 8 octetos de largo.

Si, al procesar un paquete recibido, un nodo encuentra una cabecera enrutamiento con un valor tipo de enrutamiento desconocido, el comportamiento requerido del nodo depende del valor del campo segmentos dejados, como sigue:

- Si segmentos dejados es cero, el nodo debe ignorar la cabecera enrutamiento y proceder a procesar la siguiente cabecera en el paquete, cuyo tipo se identifica por el campo cabecera siguiente en la cabecera enrutamiento.
- Si segmentos dejados no es cero, el nodo debe descartar el paquete y enviar un mensaje ICMP problema de parámetro, código 0, a la dirección origen del paquete, apuntando al tipo de enrutamiento desconocido.

Si, después de procesar una cabecera enrutamiento de un paquete recibido, un nodo intermedio determina que el paquete será remitido hacia un enlace cuya MTU de enlace es menor que el tamaño del paquete, el nodo debe descartar el paquete y enviar un mensaje ICMP paquete demasiado grande a la dirección origen del paquete.

2.2.5 Cabecera fragmentación

La cabecera fragmentación es utilizada por un origen IPv6 para enviar un paquete más grande de lo que cabría en la MTU de la ruta hacia su destino. (Nota: a diferencia del IPv4, la fragmentación en el IPv6 sólo se lleva a cabo por los nodos origen, no por los enrutadores a lo largo de la ruta de entrega de un paquete) La cabecera fragmento se identifica por un valor cabecera siguiente de 44 en la cabecera inmediatamente precedente, como muestra la figura 2.6.

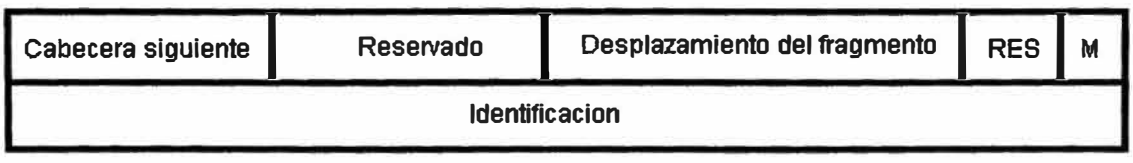


Figura 2.6 : Cabecera fragmento

Donde los campos son:

Cabecera siguiente : Campo de 8 bits. Identifica el tipo de cabecera inicial de la parte fragmentable del paquete original. Usa los mismos valores que el campo protocolo del IPv4

Reservado : Campo reservado de 8 bits. Inicializado a cero para la transmisión; ignorado en la recepción.

Desplazamiento del fragmento : Entero sin signo de 13 bits. El desplazamiento, en unidades de 8 octetos, de los datos que siguen a esta cabecera, relativo al comienzo de la parte fragmentable del paquete original.

Res : Campo reservado de 2 bits. Inicializado a cero para la transmisión; ignorado en la recepción.

Bandera M 1 = más fragmentos;
0 = último fragmento.

Identificación : 32 bits. El nodo origen genera una identificación, este debe ser diferente a otro paquete que fragmentado enviado recientemente.

Para enviar un paquete que es demasiado grande para caber en la MTU de la ruta hacia su destino, un nodo origen puede dividir el paquete en fragmentos y enviar cada fragmento como un paquete separado, para ser reensamblado en el receptor.

El paquete inicial, llamado el "paquete original", está dividido en dos partes, la parte fragmentable y la parte no fragmentable. La parte no fragmentable conciste del encabezado IPv6 y de cualquier encabezado de extensión que deba ser procesado por todos los nodos en la ruta hacia el destino. La parte fragmentable consiste de el resto del paquete, como el resto de encabezados de extensión que sólo deban ser procesados por el destinatario, los encabezados de protocolos superiores más la información.

El paquete original se reensambla únicamente de fragmentos que contengan las mismas direcciones de origen y destino y la misma identificación de fragmento. La parte no fragmentable del paquete reensamblado consiste de todos los encabezados sin incluir el encabezado de fragmentación del primer paquete (el que tiene offset=0). La parte fragmentable del paquete original es armada a partir de los fragmentos que vienen después de cada encabezado de fragmentación en cada paquete, al final después de reensamblar el paquete original no debe estar presente ningún encabezado de fragmentación.

2.2.6 Cabecera opciones de destino

La cabecera opciones de destino es usada para llevar información opcional que necesita ser examinada solamente por el(los) nodo(s) destino del paquete. La cabecera opciones de destino es identificada por un valor cabecera siguiente de 60 en la cabecera inmediatamente precedente, como muestra la siguiente figura 2.7.

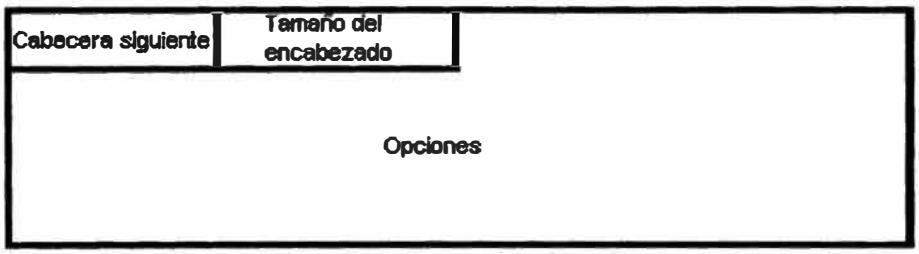


Figura 2.7 : Cabecera opciones de destino

Donde los campos son:

Cabecera siguiente : Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera opciones de destino. Utiliza los mismos valores que el campo protocolo del IPv4.

Tamaño del encabezado : Entero sin signo de 8 bits. Longitud de la cabecera opciones de destino en unidades de 8 octetos, no incluye los primeros 8 octetos.

Opciones : Campo de longitud variable, de longitud tal que la cabecera opciones de destino completa es un entero múltiplo de 8 octetos de largo. Contiene uno o más opciones codificadas TLV.

2.2.7 Cabecera no hay siguiente

El valor 59 en el campo cabecera siguiente de una cabecera IPv6 o de cualquier cabecera de extensión indica que nada hay siguiendo esa cabecera. Si el campo de tamaño del encabezado de IPv6 indica que hay más encabezados después de uno, el cual su campo de encabezado siguiente indica que no hay más, estos deben ser ignorados.

2.3 Cuestiones de tamaño del paquete

El IPv6 requiere que cada enlace en la internet tenga una MTU de 1280 octetos o mayor. En cualquier enlace que no pueda llevarse un paquete de 1280 octetos en un bloque, debe

proporcionarse fragmentación y reensamblaje especifico al enlace en una capa debajo del IPv6.

Los enlaces que tienen una MTU configurable (por ejemplo, enlaces PPP) deben configurarse para tener una MTU de por lo menos 1280 octetos; se recomienda que sean configurados con una MTU de 1500 octetos o mayor, para alojar posibles encapsulaciones (es decir, túnelizar) sin incurrir en la fragmentación de la capa IPv6. De cada enlace al cuál un nodo se conecta directamente, el nodo debe poder aceptar paquetes tan grandes como la MTU de ese enlace.

Con el propósito de enviar un paquete más grande que la MTU de la ruta, un nodo puede utilizar la cabecera fragmentación IPv6 para fragmentar el paquete en el origen y tenerlo reensamblado en el(los) destino(s). Sin embargo, el uso de tal fragmentación se desalienta en cualquier aplicación que pueda ajustar sus paquetes para satisfacer la MTU de la ruta medida (es decir, por debajo de los 1280 octetos).

Un nodo debe poder aceptar un paquete fragmentado que, después del reensamblaje, sea tan grande como de 1500 octetos. Se permite a un nodo aceptar paquetes fragmentados de tal manera que reensamblan a más de 1500 octetos. Un protocolo o aplicación de capa superior que depende de la fragmentación IPv6 para enviar paquetes más grandes que la MTU de una ruta no debe enviar paquetes más grandes que 1500 octetos a menos que tenga la certidumbre que el destino es capaz reensamblar paquetes de esos tamaños tan grandes.

En contestación a un paquete IPv6 que se envía a un destino IPv4 (es decir, un paquete que experimenta la traducción del IPv6 al IPv4), el nodo IPv6 originante puede recibir un mensaje ICMP paquete demasiado grande, reportando de una MTU del salto siguiente menor a 1280. En ese caso, no se exige que el nodo IPv6 reduzca el tamaño de los paquetes subsiguientes a menos de 1280, pero debe incluir una cabecera fragmento en esos paquetes para que el enrutador traductor de IPv6 a IPv4 pueda obtener un valor identificación apropiado para usar en los fragmentos IPv4 resultantes.

CAPITULO III

ARQUITECTURA DE DIRECCIONAMIENTO IPv6

El esquema de direcciónamiento IPv6 ha sido diseñado para proveer compatibilidad e interoperabilidad con la existencia de la arquitectura de red IPv4 y permite la coexistencia de las redes IPv6 con las redes IPv4 existentes. El IPv6 no sólo soluciona el problema de escasez de direcciones IP en IPv4, pero esto también aumenta y mejora algunas de las características salientes de IPv4, el IPv6 aumenta las capacidades de enrutamiento y direccionamiento, mientras se simplifica de la cabecera IP. IPv6 soporta varios tipos de direcciones IP y los más grandes bloques de direcciones para el uso con el enrutamiento multidifusión.

3.1 Formato de dirección IPv6

IPv6 usa los campos de numeración hexadecimal de 16 bits separados por dos punto(:) para representar el formato de dirección IPv6 de 128 bits, haciendo la representación menos pesada. En IPv6 la dirección de 128 bits se divide en limites de 16 bits y cada bloque de 16 bits se convierte a un numero hexadecimal de 4 digitos separados por dos puntos (:). La representación resultante se denomina hexadecimal con dos (:). Aquí esta un ejemplo de una dirección valida IPv6: 21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A. La siguiente seria su dirección en formato binario:

0010000111011010000000001101001100000000000000000010111100111011
0000001010101010000000001111111111111111000101000100111000101101O

Esta dirección de 128 bits se dividen limites de de 16 bits de la manera siguiente:

0010000111011010 0000000011010011 0000000000000000 0010111100111011
0000001010101010 0000000011111111 1111111000101000 1001110001011010

En hexadecimal tenemos la siguiente dirección 21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

3.1.1 Compresión de ceros

Algunas direcciones pueden contener secuencias largas de ceros. Para poder simplificar la representación de estas direcciones IPv6, una secuencia contigua de bloques de 16 bits establecidos como 0 en el formato hexadecimal se puede comprimir en :: (denominado dos puntos dobles).

Por ejemplo, la dirección local del vínculo de 2031:0000:130F:0000:0000:09C0:876A:130B se puede comprimir en 2031:0:130F::09C0:876A:130B. La dirección de multidifusión de FF02:0:0:0:0:0:0:2 se puede comprimir en FF02::2. La compresión de ceros sólo se puede utilizar para comprimir una única serie contigua de bloques de 16 bits expresados en notación hexadecimal con dos puntos. La compresión de ceros no se puede utilizar en una parte de un bloque de 16 bits. Por ejemplo, FF02:30:0:0:0:0:0:5 no se puede expresar como FF02:3::5.

Para determinar cuántos bits 0 se representan mediante ::, se puede contar el número de bloques de la dirección comprimida, restar dicho número de 8 y, después, multiplicar el resultado por 16. Por ejemplo, en la dirección FF02::2, hay dos bloques (el bloque FF02 y el bloque 2). El número de bits expresados mediante :: es 96 (96 = (8 - 2) × 16).

Cabe mencionar que la compresión de ceros sólo se puede utilizar una vez en una dirección dada. De lo contrario, no se podría determinar el número de bits 0 que representa cada instancia de dos puntos dobles (::).

3.2 Prefijos IPv6

El prefijo es la parte de la dirección que indica los bits que tienen valores fijos o que son los bits del identificador de red. Los prefijos de las rutas y los identificadores de subred en IPv6 se expresan de la misma forma que la notación enrutamiento entre dominios sin clase de IPv4. Un prefijo IPv6 se escribe con la notación dirección/longitud de prefijo. Por ejemplo, 21DA:D3::/48 es un prefijo de ruta y 21DA:D3:0:2F3B::/64 es un prefijo de subred.

Las implementaciones de IPv4 suelen utilizar una representación decimal con puntos del prefijo de red denominado máscara de subred. En IPv6 no se utiliza una máscara de subred. Sólo se admite notación con longitud de prefijo.

3.3 Direcciones IPv6 de unidifusión (Unicast)

Una dirección de unidifusión identifica una sola interfaz en el ámbito del tipo de dirección de unidifusión. Con la topología adecuada de enrutamiento de unidifusión, los paquetes dirigidos a una dirección de unidifusión se entregan en una única interfaz. Los siguientes tipos de direcciones son direcciones IPv6 de unidifusión:

3.3.1 Direcciones globales de unidifusión

Las direcciones globales de unidifusión, que se identifican mediante el formato de prefijo de 001, estas equivalen a las direcciones IPv4 públicas. Es posible un enrutamiento y tener acceso a ellas globalmente en la red Internet IPv6. Las direcciones globales unidifusión están diseñadas para que produzcan una infraestructura de enrutamiento eficaz. A diferencia de la red Internet actual IPv4, que tiene una mezcla de enrutamiento plano y jerárquico, la red Internet basada en IPv6 se ha diseñado desde la base para admitir direcciónamiento y enrutamiento jerárquico eficaz. La figura 3.1 muestra el formato.

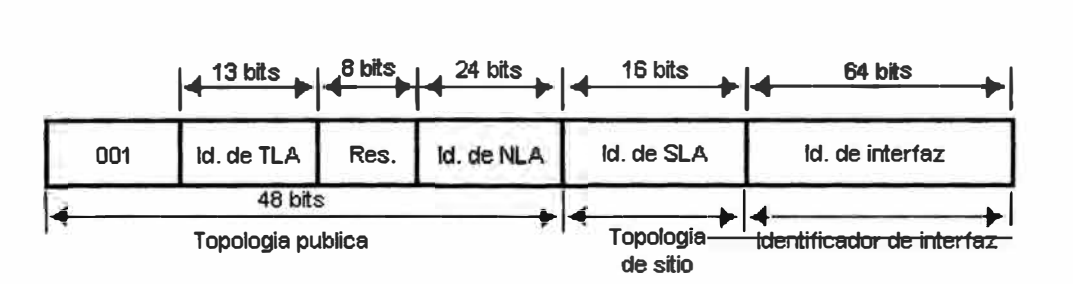


Figura 3.1 : Formato de la dirección global de unidifusión

Los campos de una dirección global de unidifusión son:

Id. de TLA : El tamaño de este campo es de 13 bits. El campo Id. (Identificador) de TLA indica el Identificador de agregación de nivel superior de la dirección. TLA identifica el nivel superior en la jerarquía de enrutamiento, estos son administrados por IANA (Agencia de Asignación de Números Internet).

Res : El tamaño de este campo es de 8 bits. El campo Res está reservado para su uso futuro en la ampliación del tamaño del Id. de TLA.

Id. de NLA : El tamaño de este campo es de 24 bits. El campo Id. de NLA indica el identificador de agregación de siguiente nivel de la dirección. El campo Id. de NLA se

utiliza para identificar un sitio cliente específico. El campo Id. de NLA permite que un ISP cree múltiples niveles de jerarquía de direcciones para organizar el direcciónamiento y enrutamiento, así como para identificar sitios.

Id. de SLA : El tamaño de este campo es de 16 bits. El campo Id. de SLA indica el identificador de agregación de nivel de sitio de la dirección. El campo Id. de SLA sirve para que se identifiquen subredes en el sitio de una organización individual. La organización puede utilizar los 16 bits correspondientes a su sitio para crear 65.536 subredes o múltiples niveles de jerarquía de direcciones y una infraestructura de enrutamiento eficaz.

Id. de interfaz : El tamaño de este campo es de 64 bits. El campo identificador de interfaz indica la interfaz de un nodo en una subred determinada

3.3.2 Direcciones locales del vínculo

Las direcciones locales del vínculo equivalen a las direcciones IPv4 de direcciónamiento IP privado automático. Los nodos utilizan direcciones locales del vínculo, para comunicarse con nodos vecinos que están en el mismo vínculo y se identifican mediante el prefijo de formato 1111 1110 10. El ámbito de una dirección local del vínculo es el vínculo local. Es necesaria una dirección local del vínculo para los procesos de descubrimiento de vecinos y siempre se configura automáticamente, incluso si no hay ninguna otra dirección de unidifusión.

Las direcciones locales del vínculo siempre comienzan por FE80. Con el identificador de interfaz de 64 bits, el prefijo de las direcciones locales del vínculo siempre es FE80::/64. Un enrutador IPv6 nunca reenvía el tráfico local del vínculo fuera del vínculo. Su formato se muestra en la figura 3.2.

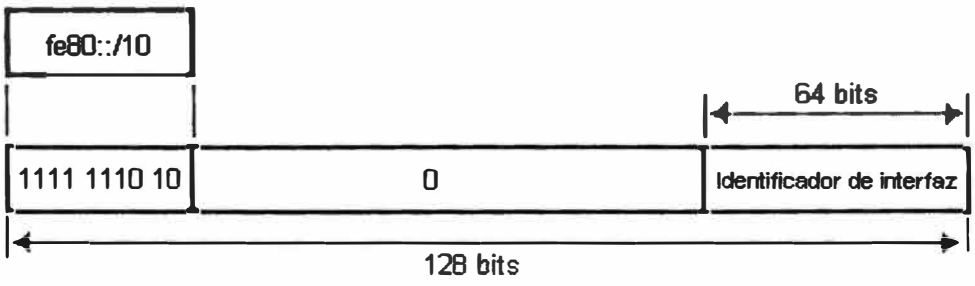


Figura 3.2 : Formato de la dirección locales del vínculo

3.3.3 Direcciones locales del sitio

Las direcciones locales del sitio, que se identifican mediante el prefijo de formato 1111 1110 11, equivalen al espacio de direcciones privadas de IPv4 (10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16). Las direcciones locales del sitio no son accesibles desde otros sitios y los enrutadores no deben reenviar tráfico local del sitio fuera del sitio. Las direcciones locales del sitio se pueden utilizar al mismo tiempo que las direcciones globales de unidifusión. El ámbito de una dirección local del sitio es el sitio (el conjunto de redes de la organización).

Los primeros 48 bits siempre son fijos en las direcciones locales del sitio y comienzan por FEC0::/48. A continuación de los 48 bits fijos hay un identificador de subred de 16 bits (campo Id. de subred) que proporciona 16 bits con los que se pueden crear subredes en la organización. Al disponer de 16 bits, puede haber hasta 65.536 subredes en una estructura de subredes plana o se pueden subdividir los bits de orden superior del campo Id. de subred para crear una infraestructura de enrutamiento jerárquica y agregable. Después del campo Id. de subred está el campo Id. de interfaz de 64 bits que identifica una interfaz específica de una subred.

La dirección global agregable de unidifusión y la dirección local del sitio comparten la misma estructura a partir de los primeros 48 bits de la dirección.

A diferencia de las direcciones locales del vínculo, las direcciones locales del sitio no se configuran automáticamente y se deben asignar mediante procesos de configuración de direcciones. Su formato se muestra en la figura 3.3.

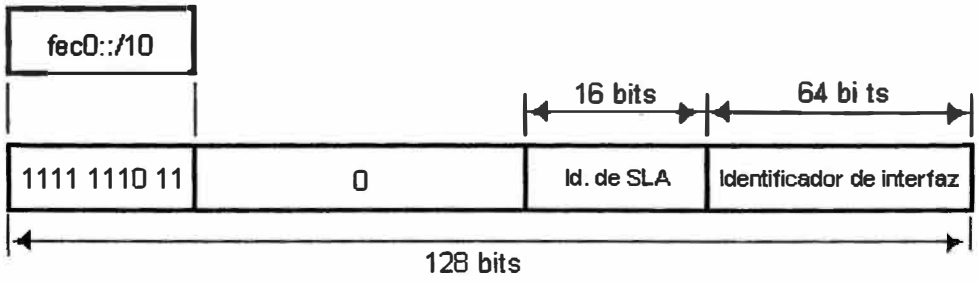


Figura 3.3 : Formato de la dirección local de sitio:

3.3.4 Direcciones especiales

Estas son:

a) Dirección no especificada (::)

La dirección no especificada (0:0:0:0:0:0:0:0 ó ::) sólo se utiliza para indicar la ausencia de dirección. Equivale a la dirección IPv4 no especificada de 0.0.0.0. Por ejemplo cuando se halla en el campo de dirección fuente indica que se trata de un host que esta iniciándose, antes que haya aprendido su propia dirección. La dirección no especificada nunca se asigna a una interfaz ni se utiliza como dirección de destino.

b) Dirección de bucle de retroceso (Loopback) ::1

La dirección de bucle de retroceso (0:0:0:0:0:0:0:1 ó ::1) permite que un nodo se envíe paquetes a sí mismo. Esta dirección nos permite hacer un bucle para verificar la correcta inicialización del protocolo. Equivale a la dirección IPv4 de bucle de retroceso de 127.0.0.1. Los paquetes dirigidos a la dirección de bucle de retroceso nunca se envían en un vínculo ni se reenvían mediante un enrutador IPv6.

3.3.5 Direcciones de compatibilidad

Para facilitar la transición de IPv4 a IPv6 y la coexistencia de ambos tipos de hosts, se han definido las direcciones siguientes:

a) Dirección IPv4-compatible

La dirección IPv4-compatible tiene la forma, 0:0:0:0:0:0:*w.x.y.z* o ::*w.x.y.z* (donde *w.x.y.z* es la representación decimal con puntos de una dirección IPv4 pública), la utilizan los nodos de doble pila que se comunican con IPv6 a través de una infraestructura IPv4. Los nodos doble pila son nodos con protocolos IPv4 e IPv6. Cuando la dirección IPv4-compatible se utiliza como destino IPv6, el tráfico IPv6 se encapsula de forma automática con un encabezado IPv4 y se envía al destino mediante la infraestructura IPv4.

b) Dirección asignada a IPv4

La dirección asignada a IPv4 tiene la forma, 0:0:0:0:0:FFFF:*w.x.y.z* o ::FFFF:*w.x.y.z* se utiliza para representar un nodo solo-IPv4 ante un nodo IPv6. Sólo sirve para la representación interna. Esta dirección nunca se utiliza como dirección de origen o destino

de un paquete IPv6 y además el protocolo IPv6 no admite el uso de direcciones asignadas a IPv4.

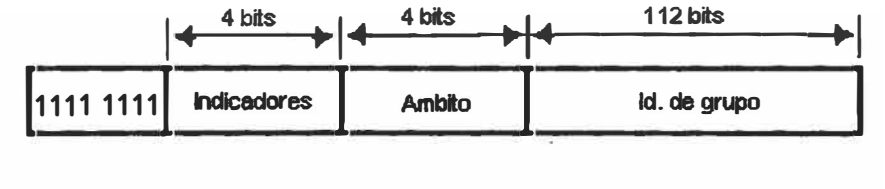
c) Dirección 6to4

La dirección 6to4 se utiliza para la comunicación entre dos nodos que ejecutan IPv4 e IPv6 sobre Internet. La dirección 6to4 se crea mediante la combinación del prefijo 2002::/16 con los 32 bits de la dirección IPv4 pública del nodo, con lo que se forma un prefijo de 48 bits (mas información en el capitulo V).

3.4 Direcciones IPv6 de multidifusión (Multicast)

Una dirección de multidifusión se utiliza para la comunicación de uno a muchos y la entrega en varias interfaces. Las direcciones IPv6 de multidifusión tienen el prefijo de formato de 1111 1111, es decir que una dirección multidifusión IPv6 siempre comienza por FF además las direcciones de multidifusión no se pueden utilizar como direcciones de origen.

En una dirección de multidifusión se identifican varias interfaces, los paquetes dirigidos a una dirección de multidifusión se entregan en todas las interfaces identificadas en ella. Su formato se muestra en la figura 3.4.



La figura 3.4 : Formato de la dirección de multidifusión

La dirección de multidifusión tiene los campos siguientes:

Indicadores : El tamaño de este campo es de 4 bits. El campo indicadores corresponde a los indicadores establecidos en la dirección de multidifusión. El documento RFC 4291 establece cuatro campos estos donde el ultimo indicador es Transitorio (T). El indicador T utiliza el bit de orden inferior del campo Indicadores. Cuando el indicador T

- T = 0 : Especifica que se trata de una dirección de multidifusión asignada de forma conocida por IANA.

- T = 1 : Especifica que la dirección de multidifusión es transitoria, es decir no está asignada de forma conocida por IANA.

Ambito : El tamaño de este campo es de 4 bits. El campo Ámbito indica el ámbito del conjunto de redes IPv6 al que va dirigido el tráfico de multidifusión. Además de la información proporcionada por los protocolos de enrutamiento de multidifusión, los enrutadores utilizan el ámbito de multidifusión para determinar si se puede reenviar el tráfico de multidifusión.

Los ámbitos siguientes están definidos en el documento RFC 4291 como muestra la tabla N^0 3.1.

TABLA N^0 3.1: VALORES DEL CAMPO AMBITO

Valor del campo de ámbito	Ámbito
1	Local del nodo
2	Local del vínculo
5	Local del sitio
8	Local de la organización
E	Global

Id. de grupo : El tamaño de este campo es de 112 bits. El campo Id. de grupo identifica el grupo de multidifusión. Las direcciones de multidifusión en el intervalo de FF01:: a FF0F:: son direcciones conocidas reservadas.

Para identificar todos los nodos de los ámbitos local del nodo y local del vínculo, se han definido las direcciones de multidifusión siguientes:

- FF01::1 (dirección para todos los nodos de ámbito local del nodo)
- FF02::1 (dirección para todos los nodos de ámbito local del vínculo)

Para identificar todos los enrutadores de los ámbitos local del nodo, local del vínculo y local del sitio, se han definido las direcciones de multidifusión siguientes:

- FF01::2 (dirección para todos los enrutadores de ámbito local del nodo)
- FF02::2 (dirección para todos los enrutadores de ámbito local del vínculo)
- FF05::2 (dirección para todos los enrutadores de ámbito local del sitio)

Debido a la forma en que las direcciones IPv6 de multidifusión se asignan a direcciones MAC (Control de Acceso al Medio) de multidifusión de ethernet, se recomienda asignar el Id. de grupo de los 32 bits de orden inferior de la dirección IPv6 de multidifusión y

establecer los restantes bits del Id. de grupo original en 0. Al utilizar sólo los 32 bits de orden inferior del Id. de grupo, cada Id. de grupo se asigna a una única dirección MAC de multidifusión de ethernet.

3.4.1 Dirección de nodo solicitado

La dirección de nodo solicitado facilita la consulta de los nodos de la red durante la resolución de direcciones. En IPv4, la trama solicitud de ARP (Protocolo de Resolución de Direcciones), se envía a la difusión de nivel MAC, con lo que afecta a todos los nodos del segmento de red, incluidos los que no ejecutan IPv4. IPv6 utiliza el mensaje de solicitud de vecino para efectuar la resolución de direcciones. Sin embargo, en lugar de utilizar la dirección para todos los nodos de ámbito local del vínculo como destino del mensaje de solicitud de vecino, que afectaría a todos los nodos IPv6 del vínculo local, se utiliza la dirección de multidifusión de nodo solicitado.

El resultado de utilizar la dirección de multidifusión de nodo solicitado es que la resolución de direcciones, que suele producirse en un vínculo, no necesita utilizar un mecanismo que afecte a todos los nodos de la red, son muy pocos los nodos que se ven afectados durante la resolución de direcciones. La dirección de multidifusión de nodo solicitado consta del prefijo FF02::1:FF00:0/104 y los últimos 24 bits de la dirección IPv6 que se esté resolviendo.

3.5 Direcciones IPv6 de difusión por proximidad (Anycast)

Cuando una dirección de unidifusión es asignada a más de una interfaz se convierte en una dirección de difusión por proximidad. Con la topología de enrutamiento adecuada, los paquetes dirigidos a una dirección de difusión por proximidad se entregan en una sola interfaz esta es la interfaz más próxima identificada en la dirección. Dicha interfaz se define como la más próxima en términos de distancia de enrutamiento. Una dirección de difusión por proximidad se utiliza para la comunicación de uno a uno de muchos y la entrega en una sola interfaz.

Para facilitar la entrega en el miembro más próximo del grupo de difusión por proximidad, la infraestructura de enrutamiento debe conocer las interfaces que tienen asignadas direcciones de difusión por proximidad y su distancia en términos de métrica de enrutamiento. Por el momento, las direcciones de difusión por proximidad sólo se utilizan

como direcciones de destino y sólo se asignan a enrutadores. Las direcciones de difusión por proximidad se asignan desde el espacio de direcciones de unidifusión.

3.6 Direcciones para hosts y enrutadores

Un host IPv4 con un solo adaptador de red tiene generalmente una única dirección IPv4 asignada al adaptador. Sin embargo, un host IPv6 suele tener varias direcciones IPv6, aunque sólo tenga una interfaz.

TABLA N^0 3.2: CUADRO DE DIRECCIONES

TIPO	DIRECCIÓN	DESCRIPCION
Host	Unidifusión	- Una dirección local del vínculo para cada interfaz - Direcciones de unidifusión para cada interfaz (que puede ser una dirección local del sitio y una o varias direcciones globales) - La dirección de bucle de retroceso (::1) para la interfaz de bucle de retroceso
	Multidifusión	- La dirección para todos los nodos de ámbito local del nodo (FF01::1) - La dirección para todos los nodos de ámbito local del vínculo (FF02::1) - La dirección de nodo solicitado de cada dirección de unidifusión en cada interfaz - Las direcciones de multidifusión de los grupos unidos a cada interfaz
Enrutador	Unidifusión	- Una dirección local del vínculo para cada interfaz - Direcciones de unidifusión para cada interfaz (que puede ser una dirección local del sitio y una o varias direcciones globales) - La dirección de bucle de retroceso (::1) para la interfaz de bucle de retroceso
	Difusión por Proximidad	- Una dirección de difusión por proximidad de un enrutador de subred para cada subred - Direcciones de difusión por proximidad adicionales
	Multidifusión	- La dirección para todos los nodos de ámbito local del nodo (FF01::1) - La dirección para todos los enrutadores de ámbito local del nodo (FF01::2) - La dirección para todos los enrutadores de ámbito local del vínculo (FF02::2) - La dirección para todos los enrutadores de ámbito local del sitio (FF05::2) - La dirección de nodo solicitado de cada dirección de unidifusión en cada interfaz - Las direcciones de los grupos unidos a cada interfaz

3.7 Identificadores de interfaz de IPv6

Los últimos 64 bits de una dirección IPv6 corresponden al identificador de la interfaz, que es único para el prefijo de 64 bits de la dirección IPv6. En la actualidad tenemos los siguientes identificadores de interfaz:

- En el documento RFC 3041 describe un identificador de interfaz generado aleatoriamente que cambia al cabo de un tiempo.
- En el documento RFC 4291 describe que todas las direcciones de unidifusión que utilicen los prefijos del 001 al 111 deben utilizar también un identificador de interfaz de 64 bits derivado de la dirección EUI-64 (identificador unico extendido).
- Un identificador de interfaz configurado manualmente.

3.7.1 Identificadores de interfaz basados en direcciones EUI-64

El IEEE (Instituto de Ingeniería Eléctrica y Electrónica) define la dirección EUI-64 de 64 bits. Las direcciones EUI-64 se asignan a un adaptador de red o se derivan de las direcciones IEEE 802.

a) Direcciones IEEE 802

Los identificadores de interfaz tradicionales para los adaptadores de red utilizan una dirección de 48 bits que se llama dirección IEEE 802. Esta dirección consta de un Id. de compañía (también llamado Id. de fabricante) de 24 bits y un Id. de extensión (también llamado Id. de tarjeta) de 24 bits. La combinación del Id. de compañía, que se asigna de forma única a cada fabricante de adaptadores de red, y el Id. de tarjeta, que se asigna de forma única a cada adaptador de red en el momento del ensamblaje, genera una dirección única global de 48 bits. Esta dirección de 48 bits también se denomina dirección física, de hardware o de control de acceso a medios (MAC). Su formato se muestra en la figura 3.5.

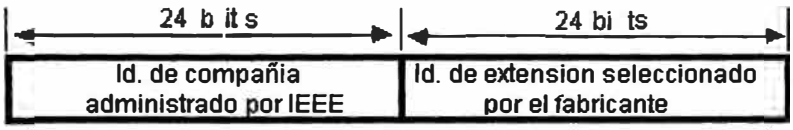


Figura 3.5 : Formato de la dirección de IEEE 802

b) Direcciones IEEE EUI-64

La dirección IEEE EUI-64 representa un nuevo estándar para el direcciónamiento de interfaces de red. El Id. de compañía sigue teniendo 24 bits de longitud, pero el Id. de extensión tiene 40 bits, por lo que se crea un espacio de direcciones mucho mayor para los fabricantes de adaptadores de red. Su formato se muestra en la figura 3.6.

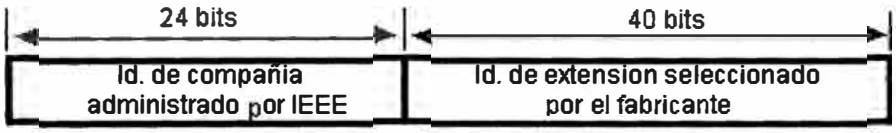


Figura 3.6 : Formato de la dirección de IEEE EUI-64

c) Asignación de direcciones IEEE 802 a direcciones EUI-64

Para crear una dirección EUI-64 a partir de una dirección IEEE 802, los 16 bits de 11111111 11111110 (0xFFFE) se insertan en la dirección IEEE 802 entre el Id. de compañía y el Id. de extensión. La figura 3.7 muestra la conversión de una dirección IEEE 802 en una dirección EUI-64.

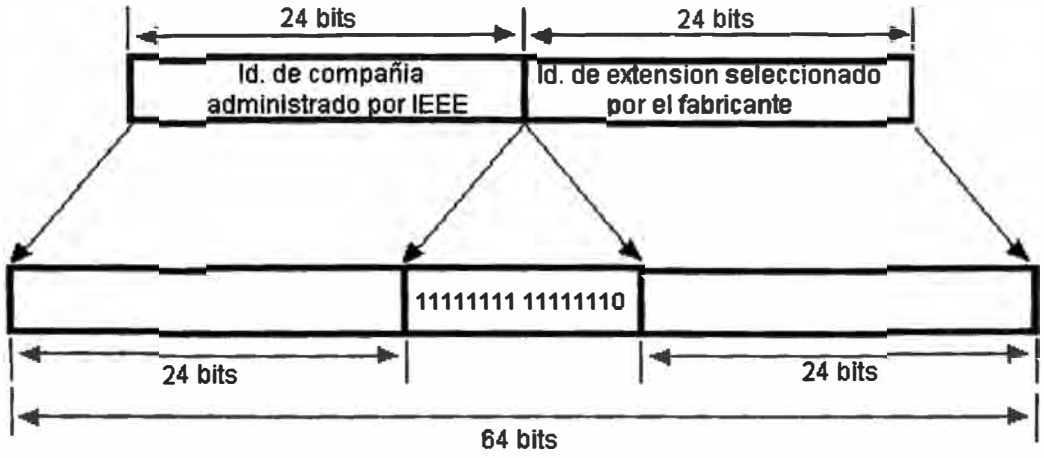


Figura 3.7 : Formato de la dirección IEEE 802 en una dirección EUI-64.

d) Asignación de direcciones EUI-64 a identificadores de interfaz IPv6

Para obtener el identificador de interfaz de 64 bits para las direcciones IPv6 de unidifusión, se complementa el septimo bit de la dirección EUI-64 (si es 1, se establece en 0; y si es 0, se establece en 1).

CAPITULO IV

PROTOCOLOS DE CONTROL IPv6

4.1 Protocolo de mensajes de control de Internet para IPv6 (ICMPv6)

El Protocolo de control de mensajes Internet para IPv6 es un estándar de IPv6 necesario que está definido en el documento RFC 2463. Con ICMPv6, los hosts y los enrutadores que se comunican mediante IPv6 pueden informar de errores y enviar mensajes de eco simples.

El formato genérico de los mensajes ICMPv6 lo muestra la figura 3.1.

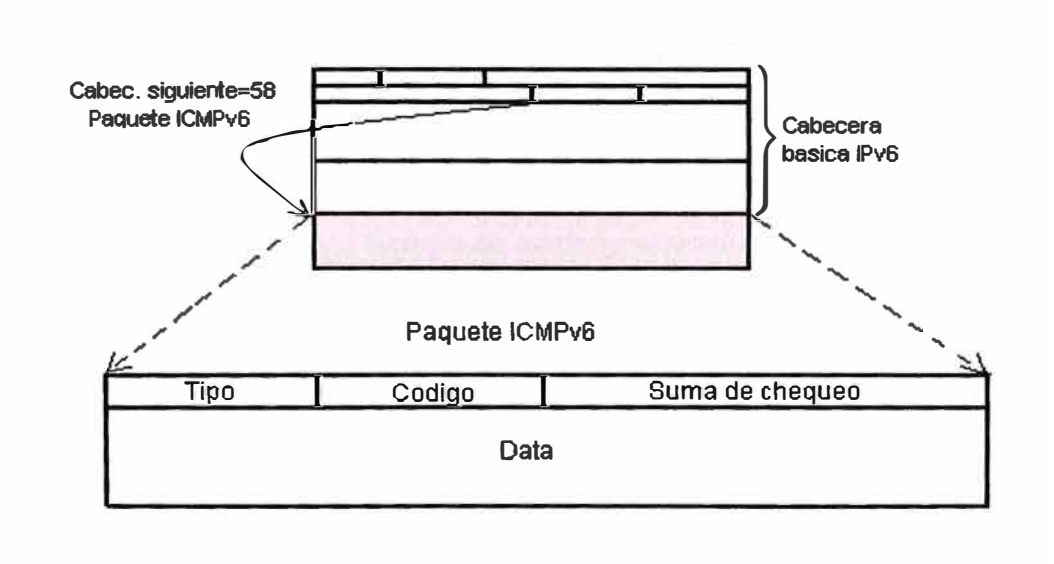


Figura 4.1 : Formato del encabezado ICMPv6

Donde

Tipo : El campo tipo indica el tipo de mensaje y su valor determina el formato del resto de la cabecera.

Código: El campo código depende del tipo de mensaje y se emplea para crear un nivel adicional de jerarquía para la clasificación del mensaje.

Suma de chequeo : El campo suma de chequeo nos permite detectar errores en el mensaje IPv6.

Los mensajes ICMPv6 se agrupan en dos tipos o clases: mensajes de error y mensajes informativos. Los mensajes de error tiene cero en el bit de mayor peso en el campo ¨tipo¨, por lo que sus valores se oscilan entre 0 y 127. Los valores de los mensajes informativos oscilan entre 128 y 255. Los principales mensajes se muestran la tabla N^0 4.1.

TABLA N^0 4.1: PRINCIPALES MENSAJES EN ICMPv6

Mensajes de error ICMPv6		
Tipo	Descripción y Códigos	
1	Destino no alcanzable	
	Código	Descripción
	0	Sin ruta hacia el destino
	1	Comunicación prohibida administrativamente
	2	Sin asignar
	3	Dirección no alcanzable
	4	Puerto no alcanzable
2	Paquete demasiado grande	
3	Tiempo excedido	
	Código	Descripción
	0	Limites de saltos excedido
	1	Tiempo de desfragmentación excedido
4	Problema de parámetros	
	Código	Descripción
	0	Campo erróneo en cabecera
	1	Tipo de ¨cabecera siguiente¨ desconocida
	2	Opción IPv6 desconocida
Mensajes informativos ICMPv6		
Tipo	Descripción	
128	Solicitud de eco	
129	Respuesta de eco	

El protocolo ICMPv6 proporciona también un marco de trabajo para los protocolos siguientes:

- Descubrimiento de escucha de multidifusión (MLD)
- Descubrimiento de vecinos (ND)

4.2 Descubrimiento de escucha de multidifusión (MLD)

El uso de la multidifusión en redes IP está definido como estándar TCP/IP en RFC 1112, IGMP. En el documento RFC se definen las extensiones de direcciones y hosts para la forma en que los hosts IP admiten la multidifusión. Los mismos conceptos que se desarrollaron originalmente para la versión actual de IP, denominada IP versión 4 (IPv4), se aplican también a IPv6.

¿Qué es la multidifusión?

El tráfico de multidifusión se envía a una única dirección, pero se procesa en múltiples hosts. La multidifusión es similar a la suscripción a una revista. Al igual que sólo los suscriptores reciben la revista cuando se publica, sólo los equipos host que pertenecen al grupo de multidifusión reciben y procesan el tráfico enviado a la dirección reservada del grupo. El conjunto de hosts que atienden en una dirección de multidifusión específica se denomina grupo de multidifusión.

Otros aspectos importantes de la multidifusión son los siguientes:

- La pertenencia a grupos es dinámica, lo que permite a los hosts unirse al grupo o abandonarlo en cualquier momento.
- La unión a grupos de multidifusión se realiza mediante el envío de mensajes de pertenencia a grupos. En IPv6, los mensajes MLD se utilizan para determinar la pertenencia a grupos en un segmento de red, denominado también vínculo o subred
- Los grupos no tienen límite de tamaño y los miembros pueden estar repartidos en diversos segmentos de red (si los enrutadores de conexión admiten el reenvío del tráfico de multidifusión y la información de pertenencia a grupos)
- Un host puede enviar tráfico a la dirección del grupo aunque no pertenezca al grupo correspondiente

4.2.1 Direcciónamiento de multidifusión IPv6

Las direcciones IPv6 de multidifusión son reservadas y se asignan a partir del prefijo de formato 1111 1111 (0xFF). En la tabla N^0 4.2 se incluye una lista parcial de direcciones

IPv6 de multidifusión que están reservadas para multidifusión IPv6 y están registradas por IANA.

TABLA N^0 4.2 : PRINCIPAL LISTA DE DIRECCIONES MULTIDIFUSION

Dirección IPv6 de multidifusión	Descripción
FF02::1	La dirección para todos los nodos utilizada para llegar a todos los nodos del mismo vínculo.
FF02::2	La dirección para todos los enrutadores utilizada para llegar a todos los enrutadores del mismo vínculo.
FF02::4	La dirección para todos los enrutadores de Protocolo DVMRP (Protocolo de Enrutamiento Multidifusión de Vectores Distancia) utilizada para llegar a todos los enrutadores de multidifusión DVMRP del mismo vínculo.
FF02::5	La dirección para todos los enrutadores de OSPF (Abrir Primero la Trayectoria más Corta) utilizada para llegar a todos los enrutadores OSPF del mismo vínculo.
FF02::6	La dirección para todos los enrutadores designados OSPF utilizada para llegar a todos los enrutadores designados OSPF del mismo vínculo.
FF02::1:FF*XX:XXXX*	La dirección de nodo solicitado utilizada en el proceso de resolución de direcciones para resolver la dirección IPv6 de un nodo local del vínculo en su dirección de nivel de vínculo. Los últimos 24 bits (*XX:XXXX*) de la dirección de nodo solicitado son los últimos 24 bits de una dirección IPv6 de unidifusión.

4.2.2 Mensajes MLD

MLD se utiliza para intercambiar información acerca del estado de pertenencia entre los enrutadores IPv6 que admiten la multidifusión y los miembros de grupos de multidifusión en un segmento de red. Los hosts miembros individuales informan acerca de la pertenencia de hosts al grupo de multidifusión y los enrutadores de multidifusión sondean periódicamente el estado de la pertenencia. MLD está definido en el documento RFC 2710. Los tipos de mensajes MLD se describen en la tabla N^0 4.3.

TABLA N^0 4.3: TIPOS DE MENSAJES MLD

Tipo de mensaje MLD	Descripción
Consulta de escucha de multidifusión	Un enrutador de multidifusión envía este mensaje para sondear un segmento de red en busca de los miembros del grupo. Las consultas pueden ser generales (solicitan la pertenencia a todos los grupos) o específicas (solicitan la pertenencia a un grupo específico).
Informe de escucha multidifusión	Un host envía este mensaje cuando se une a un grupo de multidifusión o como respuesta a una consulta de escucha de multidifusión MLD enviada por un enrutador
Escucha de multidifusión terminada	Un host envía este mensaje cuando al abandonar un grupo de hosts podría ser el último miembro de ese grupo en el segmento de red.

4.3 Descubrimiento de vecinos (ND)

El descubrimiento de vecinos de IPv6 es un conjunto de mensajes y procesos que determinan las relaciones entre nodos vecinos. El descubrimiento de vecinos reemplaza al protocolo ARP, el descubrimiento de enrutadores del ICMP y la redirección ICMP, que se utilizan en IPv4, y proporciona funciones adicionales. Descubrimiento de vecinos está definido en el documento RFC 2461, descubrimiento de vecinos para IP versión 6 (IPv6).

Los hosts utilizan el descubrimiento de vecinos para efectuar las funciones siguientes:

- Descubrir enrutadores vecinos.
- Descubrir direcciones, prefijos de direcciones y otros parámetros de configuración

Los enrutadores utilizan el descubrimiento de vecinos para efectuar las funciones siguientes:

- Anunciar su presencia, los parámetros de configuración de host y los prefijos en vínculo.
- informar a los hosts acerca de la mejor dirección de salto siguiente para reenviar los paquetes dirigidos a un destino determinado.

Los nodos utilizan el descubrimiento de vecinos para efectuar las funciones siguientes:

- Resolver la dirección de nivel de vínculo de un nodo vecino al que se reenvía un paquete IPv6 y determinar cuándo ha cambiado la dirección de nivel de vínculo de un nodo vecino.
- Determinar si los paquetes IPv6 se pueden enviar a y recibir de un vecino.

En la tabla N^0 4.4: se muestran y describen los procesos de descubrimiento de vecinos.

TABLA N^0 4.4: PROCESOS DE DESCUBRIMIENTO DE VECINOS

Proceso	Descripción
Descubrimiento de enrutadores	El proceso mediante el cual un host descubre los enrutadores locales de un vínculo conectado y configura automáticamente un enrutador predeterminado (equivalente a una puerta de enlace predeterminada en IPv4).
Descubrimiento de prefijos	El proceso mediante el cual un host descubre los prefijos de red para los destinos locales.
Descubrimiento de parámetros	El proceso mediante el cual un host descubre parámetros operativos adicionales, que incluyen la Unidad Máxima de Transmisión del vínculo y el límite de saltos predeterminado para los paquetes salientes.
Configuración automática de direcciones	El proceso de configuración de direcciones IP para las interfaces en presencia o en ausencia de un servidor de configuración de direcciones.
Resolución de direcciones	El proceso mediante el cual un nodo resuelve la dirección IPv6 de un nodo vecino en su dirección de nivel de vínculo (equivalente a ARP en IPv4).
Determinación de salto siguiente	El proceso mediante el cual un nodo determina la dirección IPv6 del vecino al que se reenvía un paquete en función de la dirección de destino. La dirección de reenvío o de salto siguiente es la dirección de destino del paquete que se envía o la dirección de un enrutador vecino.

CAPITULO V

MECANISMOS DE TRANSICION

Los protocolos de transición no son fáciles y la transición de IPv4 a IPv6 no es la excepción, los protocolos de transición son utilizados en los nodos de una red y enrutadores. Sin embargo esto puede darse a una pequeña o mediana organización, cuando la red es grande se torna dificultosa.

Los diseñadores de redes recomiendan utilizar IPv6 primero en los bordes de la red para luego mover hacia el núcleo para reducir el costo y los impactos operacionales de la integración. Las estrategias utilizadas en IPv6 en los bordes de la red implican llevar trafico IPv6 en redes IPv4, permitiendo aislar redes con dominios IPv6 para comunicar a las otras redes que están en transición. También es posible ejecutar IPv4 y IPv6 en la red, en los bordes a través de la red, o para traducción entre IPv4 y IPv6 para permitir las comunicaciones entre hosts en un determinado protocolo. Varias técnicas permiten a las redes ser mejoradas y IPv6 se desarrolla poco a poco para no interrumpir los servicios IPv4.

RFC 4213 define los siguientes tipos de nodos:

- **Nodo solo-IPv4**

  Es un nodo que tiene solo direcciones IPv4. Este nodo no soporta direcciones IPv6. Muchos de los host y enrutadores instalados hoy en día son nodos solo-IPv4.

- **Nodo solo-IPv6**

  Es un nodo que tienes solo direcciones IPv6. Este nodo se puede comunicar con otros nodos y aplicaciones IPv6. Este tipo de nodo no es muy común hoy en día.

- **Nodo IPv6/IPv4**

  Es un nodo que tiene implementado IPv4 y IPv6. En este tipo de nodo se habilita IPv6 solo si tiene una interfase configurada IPv6. También se le conoce como doble pila.

Nodo IPv4

Es un nodo que tiene implementado IPv4 (este puede enviar y recibir paquetes IPv4). Un nodo puede ser solo-IPv4 o un nodo IPv6/IPv4.

Nodo IPv6

Es un nodo que tiene implementado IPv6 (este puede enviar y recibir paquetes IPv6). Un nodo puede ser solo-IPv6 o un nodo IPv6/IPv4.

Dos de las estrategias para utilizar en IPv6 son las siguientes:

- **Utilización IPv6 sobre red doble pila**

Esta técnica permite aplicaciones tanto al IPv4 como IPv6 para coexistir en una capa IP dual. Todos los enrutadores o una porción de ellos las redes necesitan ser mejorados para soportar doble pila (es decir Nodo IPv6/IPv4), con la comunicación IPv4 usando el protocolo pila IPv4 y la comunicación IPv6 usando la pila IPv6.

- **Utilización IPv6 sobre túneles IPv4**

Estos túneles encapsulan el trafico IPv6 en paquetes IPv4 y son ante todo para la comunicación entre sitios aislados IPv6 o conexión remota de redes IPv6 sobre una red IPv4. Las técnicas incluyen usar los túneles de configuraciones manuales, túneles de encapsulación de enrutadores Genéricos (GRE), mecanismos de túneles automáticos como 6to4, túneles teredo.

5.1 Mecanismos de protocolo doble pila usando IPv4/IPv6

La red de Doble pila es una estrategia básica para enrutamiento de IPv4 y IPv6 y requiere mecanismos de redes como enrutadores y hosts ejecutando ambas en protocolos pilas IPv4 y IPv6. Los dispositivos de doble pila permite aplicaciones de migración de IPv4 y IPv6. Estas aplicaciones no están mejoradas para soportar solo pila IPv6, además esta puede coexistir con aplicaciones mejoradas en los mismos dispositivos.

El dispositivo tendrá una dirección en cada pila, se pueden utilizar direcciones IPv6 o IPv4 relacionadas o no y se pueden utilizar mecanismos manuales o automáticos para la asignación de direcciones (cada una correspondiente al protocolo en cuestión).

Como muestra la figura 5.1, nuevas y mejores aplicaciones se hacen a los protocolos pila IPv4 y IPv6.

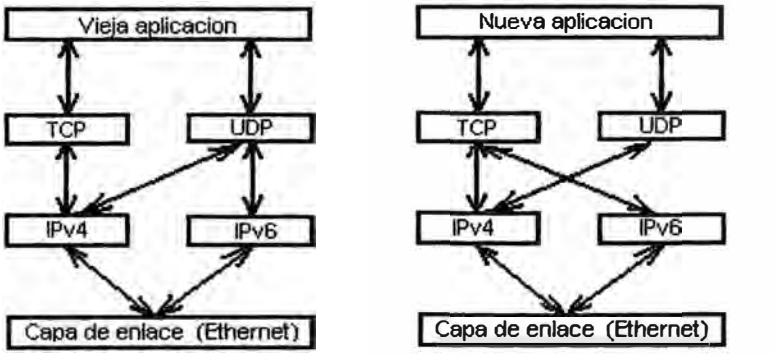


Figura 5.1: Doble pila IPv4/IPv6

Una nueva interfase de Aplicación-Programación (API) ha sido definida para soportar a ambas direcciones y requerimientos del Servidor de Nombres de Dominio (DNS) que es el protocolo de resolución de nombres para redes TCP/IP, como Internet. DNS aloja la información que permite a los equipos cliente resolver nombres DNS alfanuméricos fáciles de recordar para las direcciones IP que los equipos utilizan para comunicarse entre sí. Una API puede ser mejorada a una nueva API y aun usarse en el protocolo pila IPv4.

Las aplicaciones se optan entre los protocolos IPv4 o IPv6 basados en la dirección de búsqueda, ambas las direcciones IPv4 y IPv6 puede ser regresadas del DNS, con la aplicación correcta escogida basada en el tipo de trafico IP y los requerimientos particulares de la comunicación.

Una aplicación que soporta protocolos doble pila requieren que esté disponible la dirección del nombre del host (por ejemplo www.a.com) de destino del DNS. DNS responde todas las direcciones disponibles (ambas direcciones IPv4 y IPv6). La aplicación escoge una dirección (en muchos de los casos escoge direcciones IPv6 por defecto) y conecta el nodo fuente de el destino usando el protocolo doble pila. Como se muestra en la figura 5.2.

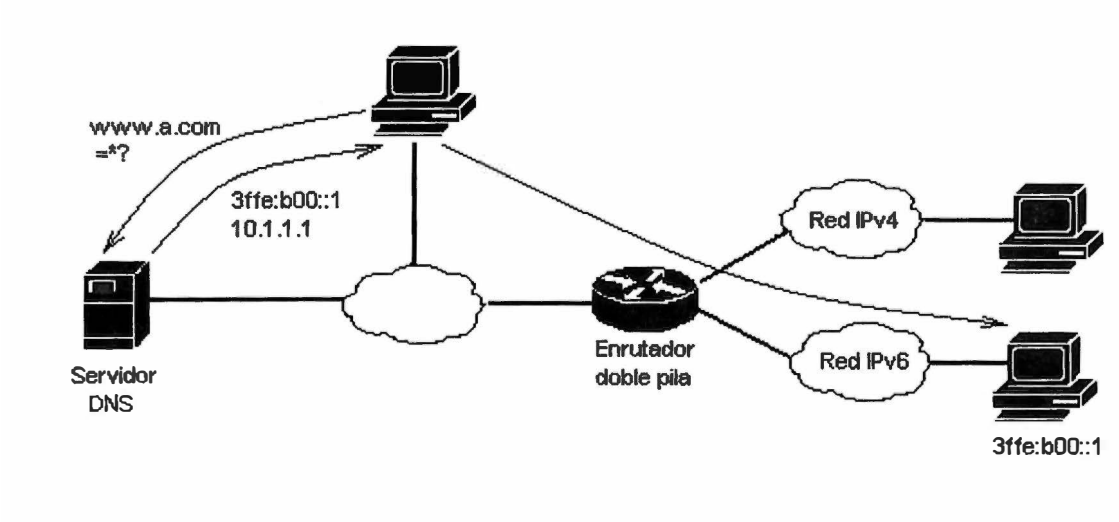


Figura 5.2 : Servidor DNS con doble pila IPv4/IPv6

5.1.1 Utilización de redes IPv6 usando doble pila

Con la utilización de redes doble pila, todos los enrutadores en la red necesitan ser mejorados para poder ser doble pila. La comunicación IPv4 usa el protocolo pila IPv4, los enrutadores aprenden a través protocolos específicos IPv4 y la comunicación IPv6 usa la pila IPv6 con enrutadores que aprenden a través de específicos protocolos de enrutamiento IPv6.

Las aplicaciones que se escogen entre usar IPv4 o IPv6 están basados en la respuesta del DNS, con la correcta dirección basada en el tipo de trafico IP y los requerimientos particulares de la comunicación.

El camino mas lógico y evidente de transición es el uso simultaneo de ambos protocolos, en pilas separadas. De esta forma un dispositivo con ambas pilas pueden recibir y enviar trafico a nodos que solo soportan uno de los dos protocolos (nodo solo IPv4 o nodo solo IPv6).

Hoy los enrutadores doble pila son utilizados para especificas infraestructuras de redes con una mezcla de aplicaciones de redes IPv4 y IPv6, requiriendo ambos protocolos para ser configurado. Sin embargo aparte de la necesidad obvia de mejorar los enrutadores de la red, hay limitaciones para esto, como son que los dispositivos en la red sean doble pila, estos requieren gestión de los protocolos de enrutamiento IPv4 y IPv6, además los enrutadores deberían ser configurados con suficiente memoria para ambas tablas de enrutamiento.

5.2 Mecanismos túneles IPv6 sobre IPv4

El trafico IPv6 encapsulado en paquetes IPv4 también pueden ser enviados sobre una red IPv4, permiten aislar los dispositivos IPv6 para comunicar sin la necesidad de mejorar la infraestructura IPv4 que existe entre ellos. El túnel es una de las estrategias para mejorar los servicios durante el periodo de coexistencia IPv4 y IPv6. La figura 5.3 muestra el uso de túneles IPv6 sobre IPv4.

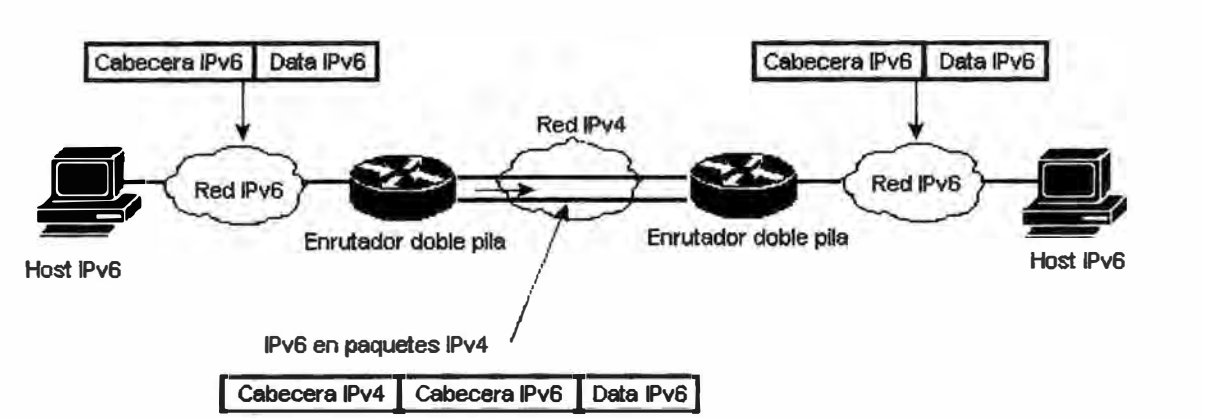


Figura 5.3 : Túneles IPv6 sobre IPv4

Por ejemplo los túneles proporcionan los servicios que ofrecen enlaces punto a punto IPv6 sin mayor dificultades por la infraestructura existente, sin alterar los servicios IPv4 y permiten a las empresas aislar dominios IPv6 sobre infraestructuras existentes IPv4 o conectar redes remotas IPv6..

5.2.1 Requerimientos de túneles

Todos los mecanismos de túneles requieren que los puntos finales ejecuten con protocolos pila IPv4 y IPv6, los puntos finales deberán tener el modo doble pila. Los enrutadores doble pila deberán soportar simultáneamente protocolos IPv4/IPv6 y de esta manera pueden interactuar directamente con los dispositivos en IPv4 y IPv6.

5.2.2 Túneles y seguridad:

Es posible proteger el trafico IPv6 sobre IPv4 usando IPSec IPv4, aplicando mapas de criptologia a ambas interfaces de los túneles para encriptar a la salida del trafico y a la otra interfase física para la decriptacion del trafico, porque si se protege los túneles haríamos que afecte negativamente a la performance de la red. Las consideraciones de diseño deberían balancear las perdidas de performance contra la seguridad que puede ser alcanzada por cuidadosas configuraciones de red.

5.2.3 Configuración de túneles

RFC 4213 defines las siguientes configuraciones de túneles entre nodos IPv6/IPv4 sobre una infraestructura IPv4:

- Enrutador a enrutador
- Host a enrutador o enrutador a host
- Host a host

a) Enrutador a enrutador

En la configuración de túnel enrutador a enrutador, dos enrutadores IPv6/IPv4 se conectan con dos infraestructuras IPv6 o IPv4 sobre una infraestructura o red IPv4. Los puntos finales del túnel abarcan un camino lógico entre la fuente y el destino. El túnel IPv6 sobre IPv4 entre dos enrutadores se representa como un único salto. Los enrutadores entre cada punto de la infraestructura IPv4 o IPv6 salen por un enrutador de frontera IPv6/IPv4. Para cada enrutador IPv6/IPv4, hay una interfase de túnel representando por el túnel IPv6 sobre IPv4 y rutas que usan la interfase del túnel., como se muestra en la figura 5.4.

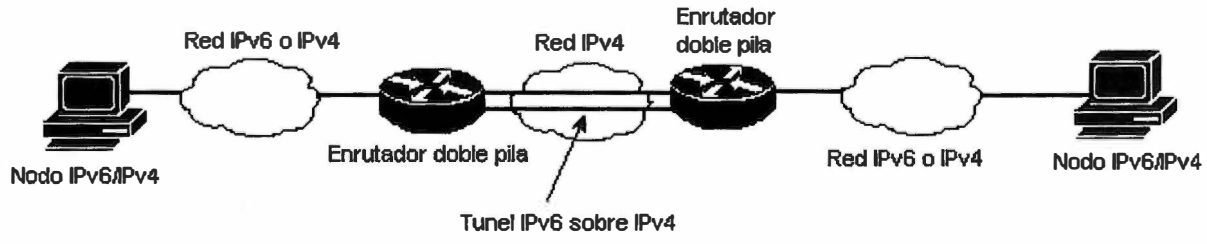


Figura 5.4 : Túnel enrutador enrutador

Ejemplos de configuración de túneles son:

- Un nodo IPv6 a través de un túnel de infraestructura IPv4 para alcanzar la Internet IPv6.
- Comunicación de dos enrutadores IPv6 a través de túnel por la Internet IPv4.
- Un enrutador 6to4 a través de un túnel IPv4 para alcanzar otro enrutador 6to4 o enrutador de retransmisión 6to4.

b) Host a enrutador o enrutador a host

En la configuración de túneles Host a Enrutador, un nodo IPv6/IPv4 que reside en una infraestructura IPv4, crea un túnel IPv6 sobre IPv4 para alcanzar a un enrutador IPv6/IPv4. Los puntos finales del túnel abarcan el primer segmento del camino entre el nodo fuente y el nodo destino. El paquete IPv6 sobre túnel IPv4 entre el nodo IPv6/IPv4 y el enrutador IPv6/IPv4 se representa como un único salto.

En un nodo IPv6/IPv4, hay una interfase de túnel representando por el túnel IPv6 sobre IPv4 que es creada y una ruta (típicamente una ruta por defecto) es agregada usando la interfase del túnel. El nodo IPv6/IPv4 envía paquetes basados en rutas coherentes con la dirección del enrutador IPv6/IPv4 como se muestra en la figura 5.5.

En la configuración de túneles enrutador a host, un enrutador IPv6/IPv4 crea un túnel IPv6 sobre IPv4 a través de una infraestructura IPv4 para alcanzar un nodo IPv6/IPv4. Los puntos finales del túnel abarcan el último segmento del camino entre el nodo origen y el nodo destino. El túnel IPv6 sobre IPv4 entre el enrutador IPv6/IPv4 y el nodo IPv6/IPv4 se representa como un único salto.

En el enrutador IPv6/IPv4, una interfase IPv6 sobre túnel IPv4 es creado y una ruta (típicamente una ruta subnet) es agregada usando la interfase del túnel. El enrutador IPv6/IPv4 envía paquetes basados en rutas subnet, interfase del túnel y la dirección destino del nodo IPv6/IPv4.

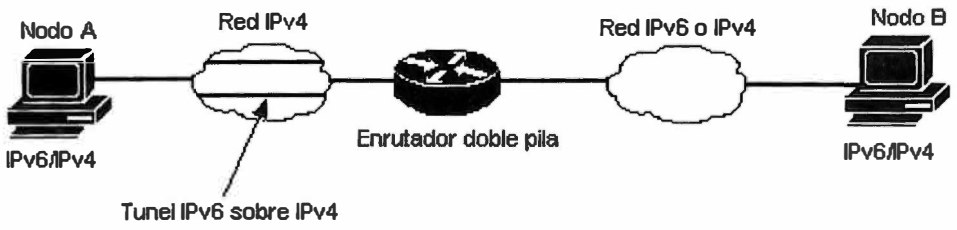


Figura 5.5 : Túnel host - enrutador

Ejemplos de configuración de túneles host a enrutador o enrutador a host son:

Un host IPv6/IPv4 a través de un túnel de infraestructura IPv4 para alcanzar la Internet IPv6.

Un host ISATAP a través de una red IPv4 o un enrutador ISATAP para alcanzar internet IPv4, otra red IPv4 o una red IPv6.

Un enrutador ISATAP a través de una red IPv4 para alcanzar un host ISATAP.

c) Host a host

En la configuración de túneles host a host, un nodo IPv6/IPv4 que reside en una infraestructura IPv4 crea un túnel IPv6 sobre IPv4 para alcanzar otro nodo IPv6/IPv4 que residen en un misma infraestructura IPv4. Los puntos finales del túnel abarcan el camino entero entre los nodos fuente y destino. Los túneles IPv6 sobre IPv4 entre nodos IPv6/IPv4 se representan como un único salto.

En cada nodo IPv6/IPv4 una interfase representando IPv6 sobre túneles IPv4 es creada, los enrutadores podrán estar presentes para indicar que el nodo destino esta en la misma subnet lógica definida por la infraestructura IPv4 como se muestra en la figura 5.6.

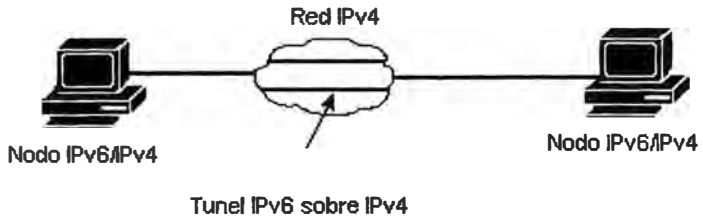


Figura 5.6: Túnel host a host

Ejemplos de configuración de túneles Host a Host son:

Hosts IPv6/IPv4 que usan direcciones ISATAP través de un túnel de infraestructura IPv4

Hosts IPv6/IPv4 que usan direcciones IPv4-compatibles a través de un túnel de infraestructura IPv4

5.3 Tipos de túneles

Los túneles proporcionan un mecanismo para utilizar infraestructuras IPv4 mientras la red IPv6 esta siendo implantada. Este mecanismo consiste en enviar datagramas IPv6 encapsulados en paquetes IPv4.

No todas las estrategias de transición son aplicables en todas las situaciones y en todas las redes, muchos de las personas podrán estar interesados en específicos túneles IPv6 sobre redes existentes de IPv4. Se definen los siguientes tipos de túneles:

Configurados

Automáticos

5.3.1 Túneles configurados

Un túnel configurado requiere configuración manual de los puntos finales del túnel. En un túnel configurado la dirección de los puntos finales del túnel IPv4 no provienen de direcciones que están codificadas en la fuente IPv6 o del destino de la dirección, estas son independientes.

Típicamente las configuraciones enrutador a enrutador son manualmente configuradas. La configuración de la interfase del túnel, consiste de las direcciones IPv4 del punto final del

túnel, esta deberá ser manualmente especificado junto con rutas estáticas que usan la interfase del túnel.

El uso primario de una configuración de túnel es proveer estables y seguras conexiones para comunicaciones regulares entre 2 enrutadores de borde o entre un host IP6/IPv4 y un enrutador de frontera, o para una conexión remota de redes IPv6. Los enrutadores de frontera, los nodos IPv6/IPv4 se usan como puntos finales (deberán ser doble pila). Los túneles manuales son usados entre 2 puntos y requieren configuración para ambos, la dirección fuente y la dirección de destino del túnel.

Como otros mecanismos de túneles la Traslación de Direcciones de la Red (NAT) no es permitido a lo largo de el camino del túnel. La figura 5.7 muestra la configuración de un túnel manual.

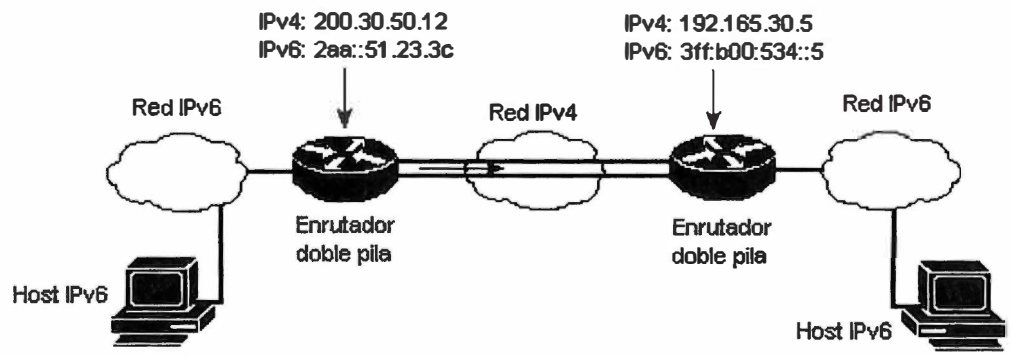


Figura 5.7 : Configuración de un túnel manual

Una dirección IPv6 se configura manualmente en una interfaz del túnel, y las direcciones manualmente configuradas IPv4 se asignan a la fuente del túnel y a al destino del túnel. El host IPv6/IPv4 o el enrutador IPv6/IPv4 en cada extremo de un túnel configurado debe soportar los protocolos IPv4 y IPv6. Los túneles manualmente configurados se pueden configurar entre los enrutadores IPv6/IPv4 de frontera o entre un enrutador IPv6/IPv4 de frontera y un host IPv6/IPv4. Un ejemplo de túnel configurado es el túnel GRE.

a) Túneles IPv6 sobre IPv4 GRE

Túneles IPv6 sobre IPv4 GRE usa el estándar de la técnica de túneles GRE esta es diseñado para mejorar los servicios necesarios para implementar cualquier encapsulacion estándar punto a punto. Como un túnel de configuración manual estos túneles están

enlazados entre dos puntos, con un túnel separado para cada enlace. Los túneles GRE no están vinculados a un especifico protocolo de transporte, pero en este caso llevan trafico IPv6 como un protocolo pasajero sobre GRE.

Similar a los tunes manuales, los túneles GRE son usados entre dos puntos y requieren configuración de ambas direcciones origen y el destino del túnel. Los enrutadores IPv6/IPv4 de frontera y los hosts IPv6/IPv4 son usualmente usados como los puntos finales del túnel.

Porque los Protocolos de Enrutamiento Integrados IS-IS se ejecutan a través de la capa enlace de datos del modelo OSI, otras técnicas de enrutamiento no pueden ser usadas en GRE, los paquetes IPv6 sobre túneles IPv4 GRE usan el estándar de las técnicas de túneles que es diseñado para mejorar los servicios necesarios para implementar cualquier combinación estándar de encapsulación punto a punto, la figura 5.8 muestra como un paquete IPv6 es llevado a través de un túnel GRE.

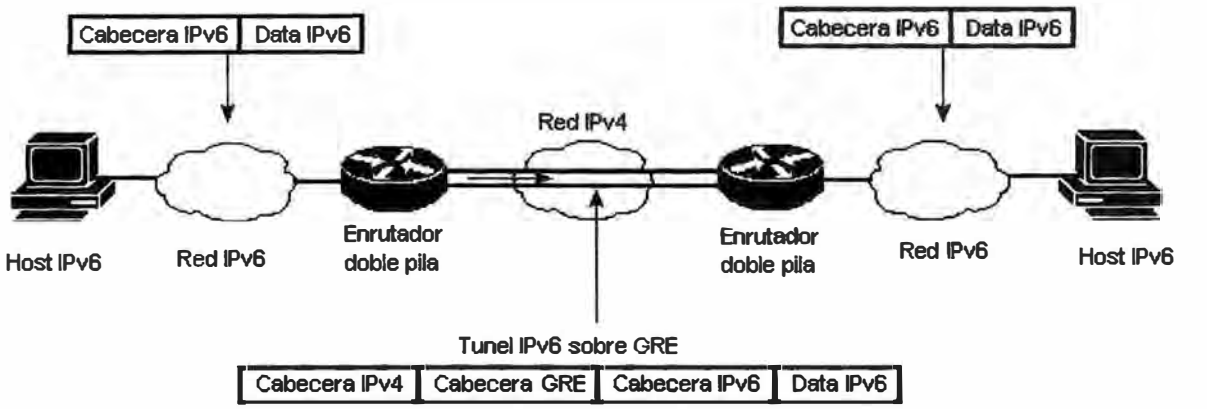


Figura 5.8 : IPv6 sobre túneles GRE

Como con los túneles manualmente configurados, se configuran las direcciones IPv4 y IPv6 del enrutador IPv6/IPv4 en la interfase del túnel GRE y se identifica los puntos de entrada y salida (origen y destino), usando direcciones IPv4.

Porque cada túnel GRE es independientemente administrado, la mayoría de los puntos finales en los túneles que se tiene, son administrados por un nivel superior. Como otros

mecanismos de túneles la traslación de direcciones de la red (NAT) no es permitido a lo largo del camino del túnel.

5.3.2 Túneles Automáticos

Un túnel automático es aquel que no requiere configuración manual. Los puntos finales son determinados haciendo uso lógico de las interfaces, rutas, el origen y el destino de las direcciones IPv6. Podemos mencionar algunos túneles automáticos:

Túneles automáticos IPv4-compatible
Túneles automáticos 6to4
Túneles ISATAP
Túneles Teredo
Túneles 6over4

a) Túneles automáticos IPv4-compatible

Los Túneles automáticos IPv4-compatible es un mecanismo de IPv6 sobre IPv4, la cual usa una dirección compatible IPv4-IPv6. Una dirección compatible IPv4-IPv6 es la concatenación de ceros a la izquierda, 96 bits y una dirección IPv4 incrustada en los últimos 32 bits, 0:0:0:0:0:0:w.x.y.z (donde w.x.y.z es la representación decimal de la dirección publica IPv4).

Por ejemplo, ::192.168.99.1 es una dirección compatible IPv4

Aunque un túnel automático puede ser configurado entre hosts IPv6/IPv4, enrutadores IPv6/IPv4 o un enrutador IPv6/IPv4 de borde y hosts IPv6/IPv4, los túneles automáticos compatibles IPv4 tienen que ser utilizados para establecer comunicación entre los enrutadores.

A diferencia de los túneles configurados manualmente la técnica de los túneles automáticos IPv4-compatible construye túneles con puntos remotos. Las configuraciones manuales de los puntos finales no es requerido para el túnel origen y el túnel destino ya que son automáticamente determinados por las direcciones IPv4. Los túneles automáticos son establecidos y desmontados tanto como dure la comunicación.

Este es el camino más fácil para crear túneles, sin embargo el túnel automático IPv4-compatible no muy escalable para interconectar redes, porque cada host requiere una dirección IPv4 eliminando la ventaja del espacio de la dirección grande en IPv6.

Los túneles automático IPv4-compatible son reemplazados por el mecanismo de túneles automáticos 6to4.

b) Túneles automáticos 6to4

6to4 es una dirección asignada y un túnel de tecnología automática enrutador a enrutador. El servicio 6to4 permite que los sitios y hosts habilitados para IPv6 se comuniquen mediante direcciones IPv6 de unidifusión a través de Internet. Los sitios y hosts IPv6 pueden utilizar su prefijo de dirección 6to4 e Internet para comunicarse sin necesidad de obtener un prefijo de dirección global IPv6 de un proveedor de servicios Internet y conectarse a la red Internet IPv6. Un túneles automático 6to4 permiten aislar dominios IPv6 para ser conectados sobre una red IPv4 y permitir conexiones con remotas redes IPv6. El desarrollo de túneles 6to4 es para interconectar múltiples sitios IPv6, cada una de las cuales tiene por lo menos una mínima conexión a una porción de la red IPv4. Esta red IPv4 podría ser la internet global o podría ser una dirección de una red corporativa. 6to4 usa el prefijo global:

2002:WWXX:YYZZ::/48

en cual WWXX:YYZZ::/48 es la representación hexadecimal de una dirección IPv4 publica (w.x.y.z) asignada a un sitio o host. La dirección completa 6to4 es:

2002:WWXX:YYZZ:subnetID:interfaceID

6to4 se describe en RFC 3056 la cual define los siguientes terminos:

Host 6to4

Un host IPv6 que es configurado con la menor dirección 6to4 (una dirección global con prefijo 2002::/16). Estos hosts no requieren ninguna configuración manual y crean direcciones 6to4 usando mecanismos de autoconfiguración de dirección estándar .

Enrutador 6to4

Un enrutador IPv6/IPv4 que soporta el uso de interfase de túnel 6to4 es usado para remitir direcciones de trafico 6to4 entre hosts 6to4 dentro de un sitio y otros enrutadores 6to4 o enrutadores de retransmisión 6to4 en una red internet IPv4. Los enrutadores 6to4 requieren procesamiento adicional lógico para una correcta encapsulación y desencapsulacion y podría requerir adicional configuración manual.

Enrutador de retransmisión 6to4

Enrutador IPv4/IPv6 que reenvía tráfico que utiliza direcciones 6to4, tanto entre enrutadores 6to4 en Internet como entre hosts en Internet IPv6.Este tipo enrutador

IPv6/IPv4 remite direcciones 6to4 entre enrutadores 6to4 en la Internet. Estos enrutadores de retransmisión mejoran un servicio de enrutamiento entre los dominios nativos IPv6, donde un protocolo de enrutamiento es esperado para ser ejecutado.

6to4 habilita los enrutadores de borde para enviar paquetes a cualquier destino con 2002::/16 de prefijo. Sin embargo otros destinos de IPv6 son inalcanzables a menos de que un enrutador de borde 6to4 sea especificado como retransmisión 6to4.

La figura 5.9 muestra el uso de un enrutadores de retransmisión 6to4 para interconectar 6to4 y dominios IPv6 nativos.

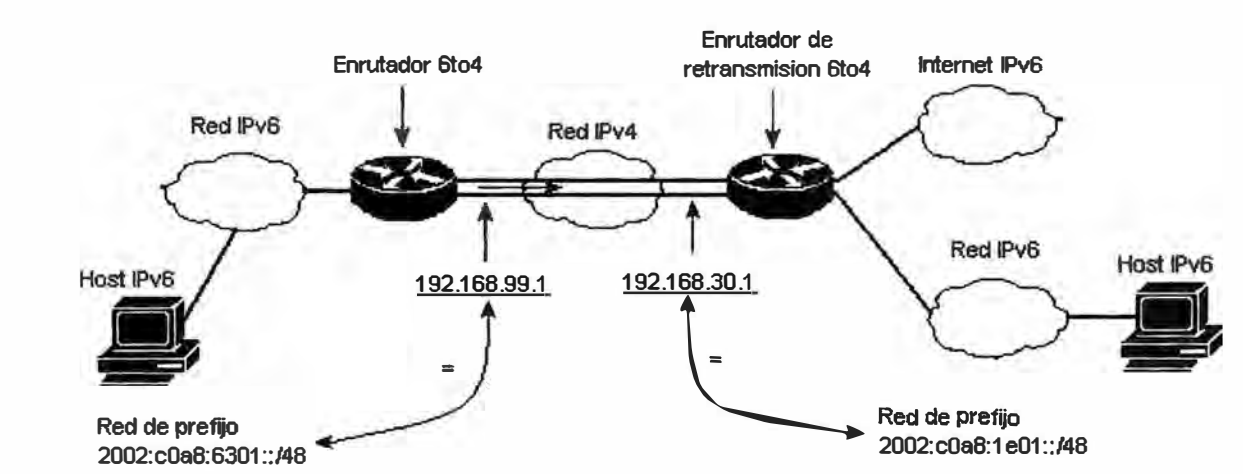


Figura 5.9: Enrutador de retransmisión 6to4

Los tipos de comunicación posible son:

- Un host 6to4 puede comunicarse con otros hosts 6to4 en el mismo sitio. Este tipo de comunicación esta disponible usando la infraestructura de ruteo IPv6 .
- Un host 6to4 puede comunicarse con host 6to4 en otros sitios a través de la Internet IPv4. Este tipo de comunicación se produce cuando un host 6to4 reenvía al enrutador 6to4 del sitio local el tráfico IPv6 que está destinado a un host 6to4 de otro sitio. El enrutador 6to4 del sitio local encapsula el tráfico IPv6 con un encabezado IPv4 y lo envía al enrutador 6to4 del sitio de destino en Internet. El enrutador 6to4 del sitio de destino quita el encabezado IPv4 y reenvía el paquete IPv6 al host 6to4 correcto, para lo que utiliza la infraestructura de enrutamiento IPv6 del sitio de destino.

Un host 6to4 puede comunicarse con otros hosts en la Internet IPv6 Este tipo de comunicación se produce cuando un host 6to4 reenvía al enrutador 6to4 del sitio local el tráfico IPv6 que está destinado a un host de Internet IPv6. El enrutador 6to4 del sitio local encapsula el tráfico IPv6 con un encabezado IPv4 y lo envía a un enrutador de retransmisión 6to4 que está conectado a la red Internet IPv4 y la red Internet IPv6. El enrutador de retransmisión 6to4 quita el encabezado IPv4 y reenvía el paquete IPv6 al host de Internet IPv6 apropiado mediante la infraestructura de enrutamiento IPv6 de la red Internet IPv6.

c) Túneles ISATAP (Protocolo de Direccionamiento Automático de Túnel Dentro de un Sitio)

ISATAP es un mecanismo de asignación de direcciones y túnel para la comunicación entre nodos IPv4 e IPv6 en un sitio IPv4. Los hosts ISATAP no requieren configuración manual para crear direcciones ISATAP estas usan mecanismos de autoconfiguracion estándar de direcciones.

Las direcciones ISATAP emplean el identificador de interfase local ::0:5EFE:w.x.y.z, en el cual w.x.y.z es cualquier dirección de unidifusión IPv4, la cual incluye direcciones privadas y publicas.

La parte 0:5EFE está formada por la combinación del identificador de la unidad organizativa asignado por IANA (00-00-5E) y un tipo que indica una dirección IPv4 incrustada (FE).

La parte *w.x.y.z* es una dirección IPv4 de unidifusión que incluye direcciones públicas y privadas.

El identificador de interfase ISATAP puede ser combinada con prefijos de 64 bit que son validos para direcciones de unidifusión IPv6. Estas incluyen los prefijos de direcciones locales de red (FE80::/64) y prefijos globales (incluidos prefijos 6to4).

Al igual que las direcciones IPv4 compatibles , las direcciones 6over4 y las direcciones 6to4, las direcciones ISATAP contienen una dirección IPv4 incrustada que se utiliza para determinar las direcciones IPv4 de origen o destino en el encabezado IPv4 cuando se envía tráfico IPv6 con direcciones ISATAP a través de una red IPv4.

Como ejemplo podemos mencionar que de forma predeterminada, el protocolo IPv6 para la familia Windows Server 2003 y Windows XP configura automáticamente la dirección ISATAP FE80::5EFE:*w.x.y.z* en la interfaz de túnel automático para cada dirección IPv4

asignada al nodo. Esta dirección ISATAP local del vínculo permite que dos hosts se comuniquen a través de una red IPv4 mediante sus direcciones ISATAP respectivas.

Un enrutador ISATAP es un enrutador IPv6 que efectúa:

- Remite paquetes entre hosts ISATAP en una subnet lógica (en una red IPv4) y a hosts en otras subnets. Las otras subnets pueden ser otras redes IPv4 (como una porción de red o la internet IPv4) o subnets nativas en IPv6 (como una red IPv6 o internet IPv6).
- El enrutador actúa en forma predeterminada para host ISATAP.
- Prefijos de direcciones de anuncio para identificar una subnet en el cual los hosts ISATAP usan los prefijos de direcciones para configurar direcciones globales ISATAP.

La figura 5.10 muestra un túnel ISATAP.

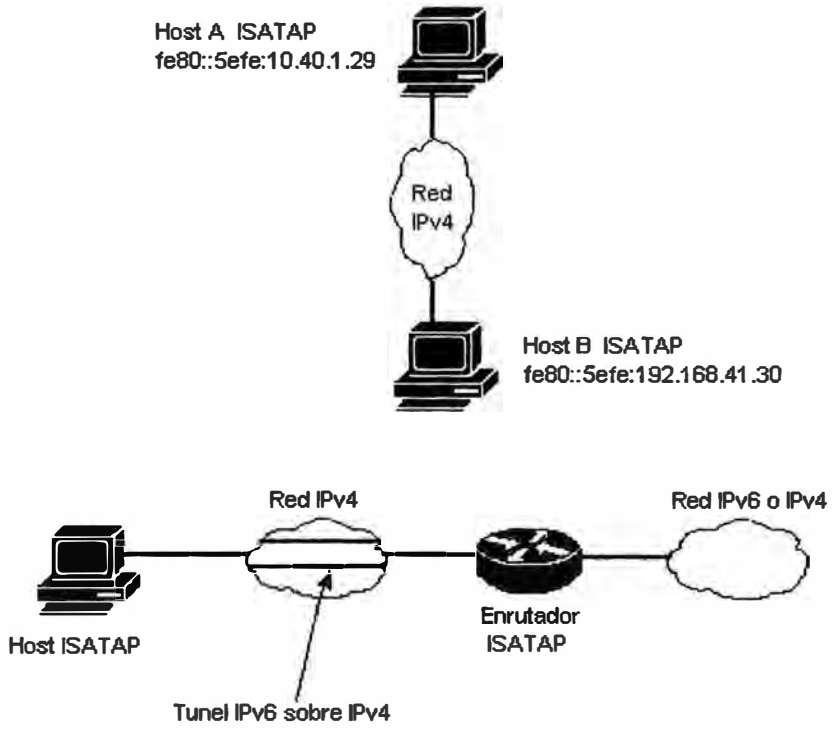


Figura 5.10 : Túnel ISATAP

Cuando un host ISATAP recibe un anuncio del enrutador ISATAP, una ruta predeterminada (::/0) es agregada usando la interfase de túnel automático. Cuando tiene paquetes destinados a sitios fuera de la subnet estas son enviados con direcciones IPv4

dadas por el enrutador ISATAP correspondiente al enrutador de interfase ISATAP de la subnet.

d) Túnel Teredo

Teredo, también conocido como Traducción de direcciones de Red Transversal IPv4 (NAT-T), provee asignación de direcciones y tunelizacion automática host-host para conectividad de unidifusión IPv6 a través de internet IPv4 cuando hosts IPv6/IPv4 están localizados detrás de uno o múltiples NATs IPv4. Para atravesar NATs IPv4, los paquetes son enviados como mensajes de Protocolo Datagrama de Usuario (UDP).

6to4 proporciona una función similar al teredo, sin embargo los enrutadores 6to4 son requeridos en los dispositivos de frontera que son conectados a internet. Los enrutadores 6to4 no son generalmente soportados por NATs IPv4. Incluso si el NAT fuera 6to4 habilitado, 6to4 podría no trabajar para configuraciones en el cual hay múltiples configuraciones NATs entre un sitio y la internet.

Teredo resuelve el tema de la falta de funcionalidad de 6to4 en los NATs por la túnelizacion de los paquetes IPv6 entre los hosts dentro de los sitios. En contraste 6to4 usa la tunelizacion de los dispositivos de frontera. La tunelizacion de los hosts presentan otros temas para los NATs por ejemplo: Los paquetes IPv6 son encapsulados en IPv4 y son enviados colocando 41 en el campo de protocolo de la cabecera IPv4. Muchos NATs solo traducen trafico TCP o UDP y deben ser manualmente configurados para traducir otros protocolos o instalar un editor NAT, esto quiere decir que no todos los NATs pueden encapsular IPv6 en IPv4. Por tanto los paquetes IPv6 son encapsulados en un mensaje UDP IPv4, conteniendo cabeceras IPv4 y UDP. Los mensajes UDP pueden ser traducidos por la mayoría de NATs.

Teredo esta diseñado como último recurso de transición para IPv6. Si conectividad nativa IPv6, 6to4 o ISATAP esta presente entre los nodos, teredo no es usado. Como cada vez mas los NATs son mejorados para soportar 6to4 y conectividad IPv6 teredo cada vez es menos usado.

Los componentes de teredo son los siguientes:

Cliente Teredo

Un nodo IPv6/IPv4 que soporta la interfase de túnel teredo a través de paquetes son tunelizados a otro cliente teredo o nodos en Internet IPv6.

- **Servidor Teredo**

  Un nodo IPv6/IPv4 que esta conectado a Internet IPv6 y Internet IPv4. El papel del servidor Teredo es asistir la configuración inicial de los clientes Teredo y de esta forma facilitar la comunicación inicial entre los diferentes clientes Teredo o entre clientes Teredo y hosts IPv6.

- **Retransmisión Teredo**

  Un enrutador IPv6/IPv4 puede remitir paquetes entre clientes Teredo en la Internet IPv4 y host en IPv6 en la Internet IPv6.

- **Retransmisión para host especifico Teredo**

  Un nodo IPv6/IPv4 que tiene una interfase y conectividad en Internet IPv4, Internet IPv6 y puede comunicar directamente con clientes Teredo sobre Internet IPv4, sin la necesidad de un retransmisor intermedio teredo. La conectividad en la Internet IPv4 ocurre sin la necesidad de un retransmisor intermedio Teredo. La conectividad en la Internet IPv4 puede lograrse con direcciones publicas o privadas y un NAT vecino. La conectividad para la Internet IPv6 puede ser a través de una conexión directa a Internet IPv6 por medio de tecnologías como 6to4.

Dirección Teredo

La dirección teredo lo muestra la figura 5.11.

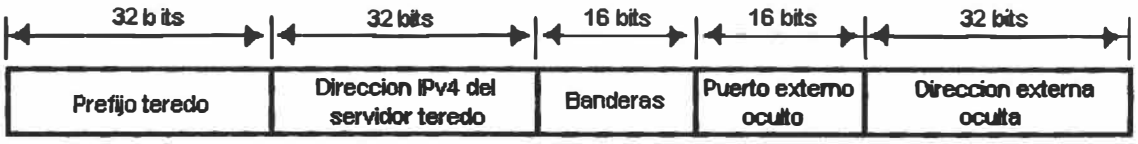


Figura 5.11 : Dirección teredo

Una dirección teredo consiste en lo siguiente:

Prefijo Teredo : Los primeros 32 bits son para el prefijo Teredo, la cual es la misma de la dirección Teredo. La IANA todavía no define este prefijo, sin embargo el prefijo 3FFE:831F::/32 es usado por Microsoft para implementaciones teredo.

Dirección IPv4 de servidor Teredo : Los siguientes 32 bits contienen la dirección publica IPv4 del servidor Teredo que ayuda en la configuración de esta dirección Teredo.

Banderas : Los siguientes 16 bits son reservados para banderas Teredo.
Puerto externo oculto : Los siguientes 16 bits almacenan una versión oculta del puerto externo UDP que corresponde a todo el trafico Teredo para este cliente Teredo.
Dirección externa oculta : Los siguientes 32 bits almacenan una versión oculta de la dirección externa IPv4 que corresponde a todo el trafico Teredo para este cliente Teredo.

e) Túneles 6over4

También conocido como túnel multidifusión IPv4, es un túnel de tecnología automática host a host, host a enrutador y enrutador a host que es usado para proveer conectividad multidifusión y unidifusión IPv6 entre nodos IPv6 a través de una Intranet IPv4. Los hosts 6over4 usan un prefijo de 64 bit para direcciones unidifusión y la identificación de interfase usan ::WWXX:YYZZ, donde WWXX:YYZZ es la representación hexadecimal del la dirección IPv4 (w.x.y.z) asignada al host. Por defecto hosts 6over4 automáticamente configuran la dirección local de red FE80::WWXX:YYZZ en cada interfase 6over4.
6over4 trata una infraestructura como una sola red con capacidades multidifusión. Esto significa que el proceso de descubrimiento vecino (como descubrimientos de direcciones y enrutadores) trabajan como ellos en la capa física de la red con capacidades multidifusión. Para emular capacidades multidifusión en la red , la infraestructura IPv4 debe estar habilitar multidifusión, como muestra la figura 5.12.

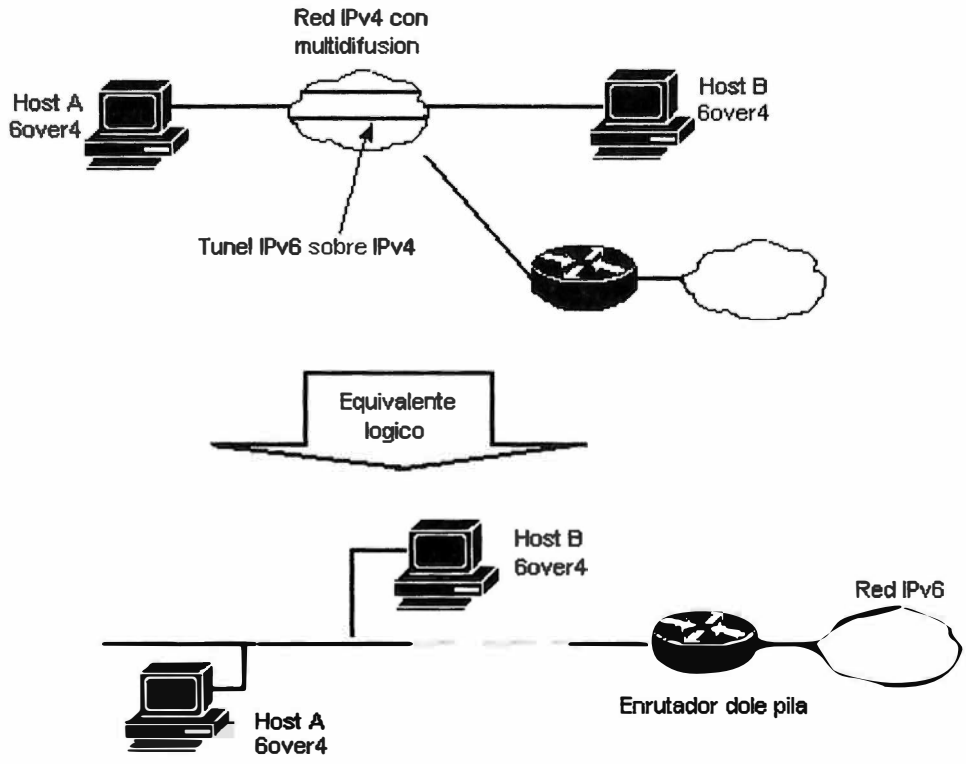


Figura 5.12: Túnel 6over4

Para facilitar las comunicaciones de multidifusión IPv6 sobre una infraestructura habilitada multidifusión IPv4, RFC 2529 define las siguientes traducciones para mapear una dirección multidifusión IPv6 a una dirección multidifusión IPv4:

239.192.[segundo al ultimo byte de la dirección IPv6].[ultimo byte de la dirección IPv6]

Los siguientes ejemplos son mapeados por direcciones multidifusión IPv6:

- FF02::1 (red local alcanza a todos los hosts por direcciones multidifusión) es mapeado a 239.192.0.1
- FF02::2 (red local alcanza a todos los enrutadores por direcciones multidifusión) es mapeado a 239.192.0.2
- FF02::1:FF28:9C5A (ejemplo de nodo requerido por dirección multidifusión) es mapeado a 239.192.156.90

Cuando 6over4 es habilitado, las capas IPv4 usan mensajes IGMP para informar a enrutadores locales de su interés en recibir trafico multidifusión IPv4 que se esta enviado a direcciones multidifusión mapeadas IPv4.

Por ejemplo cuando un host 1 (con una dirección publica IPv4 de 157.60.91.123 y su red local correspondiente con dirección 6over4 de FE80::9D3C:5B7B) envía trafico al host 2

(con una dirección publica IPv4 de 131.107.210.49 y su red local correspondiente con dirección 6over4 de FE80::836B:D231), se obtienen las direcciones IPv4 y IPv6 que están en la tabla N^0 5.1.

TABLA N^0 5.1 : EJEMPLO DE DIRECCIONES 6OVER4

Campo	Valor
Dirección fuente IPv6	FE80::9D3C:5B7B
Dirección destino IPv6	FE80::836B:D231
Dirección fuente IPv4	157.60.91.123
Dirección destino IPv4	131.107.210.49

CONCLUSIONES

1. El camino de IPv4 a IPv6 es una cuestión de transición y de integración, los dispositivos de las redes actuales pueden ser de doble pila y podrán cumplir las especificaciones de IPv6, sin por ello dejar de ser valido el IPv4.
2. Al ser IPsec obligatorio en todos los nodos IPv6, cuando se establece una sesión IPv6 siempre es posible disponer de una conexión segura extremo a extremo, como la autenticación de la comunicación y el cifrado de los datos para protegerlos de otros terminales esto posibilita las transacciones seguras en la red.
3. IPv6 es apropiado para enfrentar los problemas de escalamiento, provee mecanismos flexibles para la transición de la red actual Internet y fue diseñado para manejar los nuevos mercados tales como entretenimiento en redes, dispositivos de control.
4. IPv6 esta proyectada para trabajar en redes de alta velocidad y a la vez ser eficiente en redes actuales.
5. IPv6 soporta gran cantidad de direcciones jerárquicas que permiten a la Internet seguir creciendo y proveerla de nuevas capacidades de enrutamiento eficientes. Incluye soporte para aplicaciones en tiempo real, selección de proveedores, seguridad.
6. De todos los túneles que se investigo el mejor es el túnel ISATAP debido a su eficiencia para interconectar varias redes IPv6.
7. Al ser encapsulado el paquete IPv6 en IPv4 pierde las ventajas que ofrece IPv6.
8. Cuando se ejecuta el túnel en una red privada (no Internet) es muy confiable.
9. Los túneles utilizan un MTU de 1280 Bytes, que es el doble de la carga mas eficiente de IPv4, por consiguiente no es muy eficiente.

ANEXO A

IMPLEMENTACION DE TÚNELES EN EL PROTOCOLO IPv6

Este anexo describe cómo configurar las técnicas de hacer un túnel usadas por el software IOS del Cisco para apoyar la transición de redes de IPv4 a las redes integradas de IPv4/IPv6. El túnel encapsula los paquetes IPv6 en los paquetes IPv4 y utiliza la red IPv4 como mecanismo de capa de red.

1.1 Operación del software Cisco IOS

1.1.1 Funciones del software Cisco IOS

Al igual que un computador, un enrutador o switch no puede funcionar sin un sistema operativo. Cisco ha denominado a su sistema operativo el Sistema operativo de internetworking Cisco o Cisco IOS. Sin un sistema operativo el hardware no puede hacer ninguna función. El Cisco IOS brinda los siguientes servicios de red:

Funciones básicas de enrutamiento y conmutación

Acceso confiable y seguro a los recursos de la red

Escalabilidad de la red

1.1.2 Interfaz de usuario del enrutador

El software Cisco IOS usa una Interfaz de Línea de Comando (CLI) como entorno de consola tradicional. El IOS es de tecnología medular de Cisco. Sus detalles de operación puede variar según los distintos dispositivos de red.

Se puede acceder a este entorno a través de varios métodos. Una de las formas de acceder a la CLI es a través de una sesión de consola. La consola usa una conexión serial directa, de baja velocidad, desde un computador o terminal a la conexión de consola del enrutador. Otra manera de iniciar una sesión CLI es mediante una conexión de acceso telefónico , con un modem conectado al puerto AUX del enrutador. Ninguno de estos métodos requiere que el enrutador tenga configurado algún servicio de red. Otro de los métodos para iniciar una sesión CLI es establecer una conexión Telnet con el enrutador . Para establecer una sesión Telnet al enrutador , se debe configurar por lo menos una

interfaz con una dirección IP y configurar las conexiones y contraseñas de las sesiones de terminal virtual.

1.1.3 Modos de interfaz de usuario

La Interfaz de Línea de Comando (CLI) de Cisco es una estructura jerárquica. Esta estructura requiere el ingreso a distintos modos para realizar tareas particulares. Por ejemplo para configurar una interfaz del enrutador, el usuario debe ingresar al modo de configuración de interfaces. Desde el modo de configuración de interfaces, todo cambio de configuración que se realice tendrá efecto únicamente en esa interfaz en particular. Al ingresar a cada uno de estos modos específicos, la petición de entrada del enrutador cambia para señalar el modo de configuración en uso y solo acepta los comandos que son adecuados para este modo.

El IOS suministra un servicio de interprete de comandos , denominado comando ejecutivo (EXEC). Luego de ingresar un comando, el EXEC lo valida y lo ejecuta.

Como característica de seguridad, el software Cisco divide las sesiones EXEC en dos niveles de acceso. Estos niveles son el modo EXEC usuario y el modo EXEC privilegiado. El modo EXEC privilegiado también se le denomina modo enable. Las siguientes son las características resaltantes del modo EXEC usuario y el modo EXEC privilegiado:

El modo EXEC usuario permite solo una cantidad limitada de comandos de monitoreo básicos . A menudo se le describe como un modo ¨de visualización solamente¨. El nivel EXEC usuario no permite ningún comando que pueda cambiar la configuración del enrutador. El modo EXEC usuario se puede reconocer por la petición de entrada : ¨>¨

El modo EXEC privilegiado da acceso a todos los comandos del enrutador . Se puede configurar este modo para que solicite una contraseña del usuario antes de dar acceso. Para mayor protección, también se puede configurar para que solicite una ID (identificación) de usuario . Esto permite que solo los usuarios autorizados puedan ingresar al enrutador . Los comandos de configuración y administración requieren que el administrador de red se encuentre en el nivel EXEC privilegiado. Para ingresar al modo de configuración global y a todos los demás modos específicos, es necesario encontrarse en el modo EXEC privilegiado. El modo EXEC privilegiado puede reconocer por la petición de entrada ¨#¨

Para ingresar al nivel EXEC privilegiado desde el nivel EXEC usuario se ejecuta el comando enable con la petición de entrada ">" en la pantalla . Si se ha configurado una contraseña el enrutador la solicitara. Por razones de seguridad los dispositivos de red Cisco no muestran la contraseña al ser introducida. Una vez que se ha introducido la contraseña correcta, la petición de entrada del enrutador cambia a "#" lo que indica que el usuario se encuentra ahora en el nivel EXEC privilegiado. Si se introduce un signo de interrogacion (?) en el nivel EXEC privilegiado.

1.1.4 Operación del software Cisco IOS

Los dispositivos que usan el Cisco IOS tiene tres entornos o modos de operación distintos

- Monitor de la ROM
- ROM de arranque
- Cisco IOS

Los comandos inicio del enrutador generalmente se cargan en la RAM y ellos activan uno de estos entornos de operación . El registro de configuración puede ser utilizado por el administrador del sistema para controlar el modo de inicio por defecto del enrutador.

2.1 Prerrequisitos para implementar túneles en IPv6

La tabla identifica los requisitos mínimos.

Tabla de requisitos mínimos (software IOS CISCO)

Característica	REQUISITOS MINIMOS IOS CISCO
Túneles automáticos 6to4	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T, 12.4, 12.4(2)T, 12.2(27)SBC
Túneles compatibles automáticos IPv4	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T, 12.4, 12.4(2)T, 12.2(27)SBC
Túneles manualmente configurados IPv6	12.2(2)T, 12.0(21)ST, 12.0(23)S, 12.2(14)S, 12.3, 12.3(2)T, 12.4, 12.4(2)T, 12.2(27)SBC
Túneles GRE IPv6 sobre IPv4	12.2(2)T, 12.0(21)ST, 12.0(22)S, 12.2(14)S, 12.3, 12.3(2)T, 12.4, 12.4(2)T, 12.2(27)SBC
Túneles ISATAP	12.2(14)S, 12.3(2)T, 12.4, 12.4(2)T, 12.2(27)SBC
Túneles IPv4 sobre IPv6	12.3(7)T, 12.4, 12.4(2)T
Túneles IPv6 sobre IPv6	12.3(7)T, 12.4, 12.4(2)T

2.1.1 Configuración de parámetros por tipo de túnel

La tabla identifica los parámetros por tipo de túnel

Tabla de configuración de parámetros:

Tipo de Túnel	parámetros de configuración del enrutador			
	Modo del Túnel	**Inicio del Túnel**	**Destino del Túnel**	**Prefijo de la Interfase o Dirección**
Manual	IPv6ip	Una dirección IPv4, o una referencia para una interfase en la cual IPv4 esta configurado.	Una dirección IPv4.	Una dirección IPv6
GRE/IPv4	GRE IP		Una dirección IPv4.	Una dirección IPv6
IPv4-compatible	IPv6ip auto-tunnel		No necesario. Estos son tipos de túneles punto multipunto. El destino de la dirección es calculado en una base de paquetes, del destino IPv6	No necesario. La interfase de la dirección es generada como *::tunnel-source*/96.
6to4	IPv6ip 6to4			Una dirección IPv6. El prefijo debe estar incrustado en la dirección de inicio del túnel IPv4.
ISATAP	IPv6ip isatap			Un prefijo IPv6 modificado con formato eui-64 . La dirección IPv6 es generada del prefijo y el inicio de la dirección del túnel IPv4 .

3.1 Como implementar túneles en IPv6

En esta parte se explica como implementar los túneles para IPv6:

- Túneles de configuración Manual
- Túneles de configuración GRE IPv6
- Túneles de configuración 6 to 4
- Túneles de configuración IPv4 compatible con IPv6
- Túneles de configuración ISATAP

3.1.1 Túneles de configuración Manual

Con los túneles manualmente configurados IPv6, una dirección IPv6 se configura en un interfaz del túnel, y las direcciones manualmente configuradas IPv4 se asignan a la inicio del túnel y al destinó del túnel. El host o el enrutador en cada extremo de un túnel configurado debe soportar las pilas del protocolo IPv4 e IPv6.

Pasos

1. enable
2. configure terminal
3. interface tunnel *numero de tunnel*
4. IPv6 address *IPv6-prefix/prefix-longitud* [eui-64]
5. tunnel source {*ip-address* | *interface-type interface-number*}
6. tunnel destination *ip-address*
7. tunnel mode IPv6ip

Pasos Detallados

	Comando	Propósito
Step 1	**enable** Ejemplo: Enrutador> enable	Habilitar modo priviligiado EXEC
Step 2	**configure terminal** Ejemplo: Enrutador# configure terminal	Entra modo de configuración global .
Step 3	**interface tunnel** tunnel-number Ejemplo: Enrutador(config)# interface tunnel 0	Especifica una interfaz y un número del túnel, y entra en modo de la configuración de la interfaz.
Step 4	**IPv6 address** IPv6-prefix/prefix-length [eui-64] Ejemplo: Enrutador(config-if)# IPv6 address 3ffe:b00:c18:1::3/127	Especifica la red IPv6 asignada a la interfaz IPv6 y permite que procese en la interfaz. Nota: Refiere a la conectividad básica de configuración para el módulo IPv6
Step 5	**tunnel source** {ip-address | interface-type interface-number} Ejemplo: Enrutador(config-if)# tunnel source ethernet 0	Especifica la dirección del inicio IPv4 o el tipo y el número del interfaz de la fuente para el interfaz del túnel - Si se especifica un interfaz, el interfaz se debe configurar con una dirección IPv4.
Step 6	**tunnel destination ip-address** Ejemplo: Enrutador(config-if)# tunnel destination 192.168.30.1	Especifica la dirección del destino IPv4 o el host name para el interfaz del túnel.
Step 7	**tunnel mode IPv6ip** Ejemplo: Enrutador(config-if)# tunnel mode IPv6ip	Especifica un tunel manual IPv6.

3.1.2 Túneles de configuración GRE IPv6

Este ejemplo explica cómo configurar un túnel de GRE en una red IPv6. Los túneles de GRE se pueden configurar para funcionar sobre una capa de red IPv6 y para transportar los paquetes IPv6 en los túneles IPv6 y los paquetes IPv4 en los túneles IPv6.

Pasos

1. enable
2. configure terminal
3. interface tunnel *tunnel-number*
4. IPv6 address *IPv6-prefix/prefix-length* [eui-64]
5. tunnel source {*ip-address* | *IPv6-address* | *interface-type interface-number*}
6. tunnel destination {*host-name* | *ip-address* | *IPv6-address*}
7. tunnel mode {aurp | cayman | dvmrp | eon | gre | gre multipoint | gre IPv6 | ipip [decapsulate-any] | iptalk | IPv6 | mpls | nos}

Pasos Detallados

	Comando	Propósito
Step 1	**enable** Ejemplo: Enrutador> enable	Habilitar modo priviligiado EXEC
Step 2	**configure terminal** Example: Enrutador# configure terminal	Entra modo de configuración global.
Step 3	**interface tunnel** *tunnel-number* Ejemplo: Enrutador(config)# interface tunnel 0	Especifica una interfaz y un número del túnel, y entra en modo de la configuración de la interfaz.
Step 4	**IPv6 address** *IPv6-prefix/prefix-length* **[eui-64]** Ejemplo: Enrutador(config-if)# IPv6 address 3ffe:b00:c18:1::3/127	Especifica la red IPv6 asignada a la interfaz IPv6 y permite que procese en la interfaz. Nota: Refiere a la conectividad básica de configuración para el módulo IPv6

Step 5	**tunnel source** {*ip-address* | *IPv6-address* | *interface-type interface-number*} Ejemplo: Enrutador(config-if)# tunnel source ethernet 0	Especifica la dirección del inicio IPv4 o el tipo y el número del interfaz de la fuente para el interfaz del túnel. - Si se especifica un interfaz, el interfaz se debe configurar con una dirección IPv4.
Step 6	**tunnel destination** {*host-name* | *ip-address* | *IPv6-address*} Ejemplo: Enrutador(config-if)# tunnel destination 192.168.30.1	Especifica la dirección del destino IPv4 o el host name para el interfaz del túnel.
Step 7	**tunnel mode {aurp | cayman | dvmrp | eon | gre | gre multipoint | gre IPv6 | ipip [decapsulate-any] | iptalk | IPv6 | mpls | nos}** Ejemplo: Enrutador(config-if)# tunnel mode gre IPv6	Especifica el túnel GRE IPv6 .

3.1.3 Túneles de configuración 6to4

Pasos

1. enable
2. configure terminal
3. interface tunnel *tunnel-number*
4. IPv6 address *IPv6-prefix/prefix-length* [eui-64]
5. tunnel source {*ip-address* | *interface-type interface-number*}
6. tunnel mode IPv6ip 6to4
7. exit
8. IPv6 route *IPv6-prefix/prefix-length* tunnel *tunnel-number*

Pasos Detallados

	Comando	Proposito
Step 1	**enable** Ejemplo: Enrutador> enable	Habilitar modo priviligiado EXEC
Step 2	**configure terminal** Ejemplo: Enrutador# configure terminal	Entra modo de configuración global
Step 3	**interface tunnel** tunnel-number Ejemplo: Enrutador(config)# interface tunnel 0	Especifica un número y una interfase del túnel. Entra al modo de configuración de la interfase.
Step 4	**IPv6 address** IPv6-prefix/prefix-length **[eui-64]** Ejemplo: Enrutador(config-if)# IPv6 address 2002:c0a8:6301:1::1/64	Especifica la dirección asignada IPv6 para la interfase y habilita el procesamiento en la interfase IPv6. - Los 32 bits siguientes al prefijo inicial 2002::/16 corresponden a una dirección IPv4 asignada al inicio del túnel. Nota: Refiere a la conectividad básica de configuración para el módulo IPv6.
Step 5	**tunnel source** {ip-address | interface-type interface-number} Ejemplo: Enrutador(config-if)# tunnel source ethernet 0	Especifica el tipo de interfase de inicio y el numero para la interfase del túnel. Nota: El tipo de interface y el numero especificado en el comando de tunnel source debe ser configurado con una dirección IPv4.
Step 6	**tunnel mode IPv6ip 6to4** Ejemplo: Enrutador(config-if)# tunnel mode IPv6ip 6to4	Especifica un tunel de revestimiento IPv6 usando direcciones 6to4.
Step 7	**exit** Ejemplo: Enrutador(config-if)# exit	El modo de configuración de interfase exits retorna al enrutador al modo de configuración global.
Step 8	**IPv6 route** IPv6-prefix/prefix-length tunnel tunnel-number Ejemplo: Enrutador(config)# IPv6 route 2002::/16 tunnel 0	Configura una ruta estatica para IPv6 6to4 de prefijo 2002::/16 para la interfase de tunel especificada. Nota: Cuando se configura un tunel de recubrimiento 6to4, se debera configurar una ruta estática para IPv6 6to4 de prefijo 2002::/16 para la interfase del túnel 6to4. - El numero de túnel especificado en el comando de ruta IPv6 debe ser el mismo numero especificado en el comando de interfase tunnel

3.1.4 Túneles de configuración IPv4 compatible con IPv6

PASOS

1. enable
2. configure terminal
3. interface tunnel *tunnel-number*
4. tunnel source {*ip-address* | *interface-type interface-number*}
5 tunnel mode IPv6ip auto-tunnel

Pasos Detallados

	Comando	Proposito
Step 1	**enable** Ejemplo: Enrutador> enable	Habilitar modo priviligiado EXEC
Step 2	**configure terminal** Ejemplo: Enrutador# configure terminal	Entra modo de configuración global
Step 3	**interface tunnel** tunnel-number Ejemplo: Enrutador(config)# interface tunnel 0	Especifica un numero y una interfase del tunel. Entra al modo de configuración de la interfase.
Step 4	**tunnel source** {ip-address | interface-type interface-number} Ejemplo: Enrutador(config-if)# tunnel source ethernet 0	Especifica el tipo de inicio de interfase y el numero de interfase de tunel.. Nota: El tipo de interfase y el numero especificado en el comando tunnel source esta configurado con una dirección IPv4 solamente.
Step 5	**tunnel mode IPv6ip auto-tunnel** Ejemplo: Enrutador(config-if)# tunnel mode IPv6ip auto-tunnel	Especifica un tunel compatible IPv4 usando direcciones IPv4 compatible con IPv6

3.1.5 Túneles de configuración ISATAP

PASOS

1. enable
2. configure terminal
3. interface tunnel *tunnel-number*
4. IPv6 address *IPv6-prefix/prefix-length* [eui-64]
5. no IPv6 nd suppress-ra
6. tunnel source {*ip-address* | *interface-type interface-number*}
7. tunnel mode IPv6ip isatap

Pasos Detallados

	Comando	Proposito
Step 1	**enable** Ejemplo: Enrutador> enable	Habilitar modo priviligiado EXEC
Step 2	**configure terminal** Ejemplo: Enrutador# configure terminal	Entra modo de configuración global.
Step 3	**interface tunnel** *tunnel-number* Ejemplo: Enrutador(config)# interface tunnel 1	Especifica un numero y una interfase del tunel. Entra al modo de configuración de la interfase.
Step 4	**IPv6 address** *IPv6-prefix/prefix-length* [eui-64] Ejemplo: Enrutador(config-if)# IPv6 address 2001:0DB8:6301::/64 eui-64	Especifica la dirección IPv6 asignada a la interfase y habilita el procesamiento en la interfase IPv6. Nota: Refiere a la conectividad básica de configuración para el módulo IPv6
Step 5	**no IPv6 nd suppress-ra** Ejemplo: Enrutador(config-if)# no IPv6 nd suppress-ra	El envio de los enrutador de anuncio IPv6 esta desabilitado por defecto en las interfaces del tunel. Este comando re hablita los envios al enrutador de anuncio IPv6 para permitir al cliente autoconfiguracion.

Step 6	**tunnel source** {*ip-address* | *interface-type interface-number*} Ejemplo: Enrutador(config-if)# tunnel source ethernet 1/0/1	Especifica el tipo de inicio de interfase y numero para la interfase del túnel. Nota: El tipo de interfase y numero especificado en el commando tunnel source debe ser configurado con una dirección IPv4
Step 7	**tunnel mode IPv6ip isatap** Ejemplo: Enrutador(config-if)# tunnel mode IPv6ip isatap	Especifica un recubrimiento de túnel IPv6 usando direcciones ISATAP.

3.2 Ejemplos de Configuración de Túneles en IPv6

- Ejemplo : Túneles de configuración Manual
- Ejemplo: Túneles de configuración GRE IPv6
- Ejemplo: Túneles de configuración 6 a 4
- Ejemplo: Túneles de configuración IPv4 compatible con IPv6
- Ejemplo: Túneles de configuración ISATAP

3.2.1 Ejemplo : Túneles de configuración Manual

El ejemplo siguiente configura un túnel manual IPv6 entre el enrutador A y el enrutador B. En el ejemplo, la interfaz 0 del túnel para un enrutador A y un enrutador B se configura manualmente con una dirección global IPv6. El inicio del túnel y las direcciones de destinó también se configuran manualmente.

Configuracion del enrutador A

```
interface ethernet 0
 ip address 192.168.99.1 255.255.255.0
interface tunnel 0
 IPv6 address 3ffe:b00:c18:1::3/127
 tunnel source ethernet 0
 tunnel destination 192.168.30.1
 tunnel mode IPv6ip
```

Configuracion del enrutador B

```
interface ethernet 0
 ip address 192.168.30.1 255.255.255.0
interface tunnel 0
 IPv6 address 3ffe:b00:c18:1::2/127
 tunnel source ethernet 0
 tunnel destination 192.168.99.1
 tunnel mode IPv6ip
```

3.2.2 Ejemplo: Túneles de configuración GRE IPv6

El ejemplo siguiente configura el túnel GRE un tráfico de funcionamiento IS-IS e IPv6 entre el enrutador A y el enrutador B

Configuracion del enrutador A

```
IPv6 unicast-routing
clns routing
!
interface tunnel 0
 no ip address
 IPv6 address 2001:0DB8:1111:2222::1/64
 IPv6 enrutador isis
 tunnel source Ethernet 0/0
 tunnel destination 10.0.0.2
 tunnel mode gre IPv6
!
interface Ethernet0/0
 ip address 10.0.0.1 255.255.255.0
!
enrutador isis
 net 49.0000.0000.000a.00
```

Configuracion del enrutador B

```
IPv6 unicast-routing
clns routing
!
interface tunnel 0
 no ip address
 IPv6 address 2001:0DB8:1111:2222::2/64
 IPv6 enrutador isis
 tunnel source Ethernet 0/0
 tunnel destination 10.0.0.1
 tunnel mode gre IPv6
!
interface Ethernet0/0
 ip address 10.0.0.2 255.255.255.0
!
enrutador isis
 net 49.0000.0000.000b.00
 address-family IPv6
 redistribute static
 exit-address-family
```

a) Cuando la dirección del tunel de destino es para IPv6

El ejemplo siguiente demuestra cómo configurar la dirección de destinó del túnel para hacer un túnel de GRE de los paquetes IPv6.

```
Enrutador(config)# interface Tunnel0
Enrutador(config-if)# no ip address
Enrutador(config-if)# IPv6 enrutador isis
Enrutador(config-if)# tunnel source Ethernet 0/0
Enrutador(config-if)# tunnel destination 2001:0DB8:1111:2222::1/64
Enrutador(config-if)# tunnel mode gre IPv6
Enrutador(config-if)# exit
!
```

```
Enrutador(config)# interface Ethernet0/0
Enrutador(config-if)# ip address 10.0.0.1 255.255.255.0
Enrutador(config-if)# exit
!
Enrutador(config)# IPv6 unicast-routing
Enrutador(config)# enrutador isis
Enrutador(config)# net 49.0000.0000.000a.00
```

b) Configuración Ctunnels en modo GRE para llevar paquetes IPv6 en CLNS:

El ejemplo siguiente configura de GRE CTunnel un tráfico de funcionamiento IS-IS e IPv6 entre el enrutador A y el enrutador B en una red de CLNS. El comando del GRE del modo ctunnel permite el hacer un túnel entre la red Cisco y los otros dispositivos de una red y lleva el tráfico IPv4 e IPv6. Este se encuentra en la RFC 3147

Configuracion del enrutador A

```
IPv6 unicast-routing
clns routing
interface ctunnel 102
 IPv6 address 2001:0DB8:1111:2222::1/64
 ctunnel destination 49.0001.2222.2222.2222.00
 ctunnel mode gre
interface Ethernet0/1
 clns enrutador isis
enrutador isis
 net 49.0001.1111.1111.1111.00
```

Configuracion del enrutador B

```
IPv6 unicast-routing
clns routing
interface ctunnel 201
 IPv6 address 2001:0DB8:1111:2222::2/64
 ctunnel destination 49.0001.1111.1111.1111.00
```

```
 ctunnel mode gre
interface Ethernet0/1
 clns enrutador isis
enrutador isis
 net 49.0001.2222.2222.2222.00
```

Para apagar el modo de GRE y para restaurar el CTunnel los enrutadores cisco lo encapsulan por defecto entre los puntos finales del equipò cisco ,utilice el comando del modo del ctunnel de no comando del Cisco del modo del ctunnel. El ejemplo siguiente demuestra la misma configuración modificada al tráfico IPv4 del transporte.

3.2.3 Ejemplo: Túneles de configuración 6to4

El ejemplo siguiente configura un túnel 6to4 en un enrutador de frontera en una red aislada IPv6. La dirección IPv4 es 192.168.99.1, que traduce al prefijo IPv6 de 2002:c0a8:6301::/48. El prefijo IPv6 es 2002:c0a8:6301::/64 para el interfaz del túnel: 2002:c0a8:6301:1::/64 para la primera red IPv6, y 2002:c0a8:6301:2::/64 para la segunda red IPv6. La ruta estática se asegura de que cualquier otro tráfico para IPv6 el prefijo 2002::/16 esté ordenado hacer un túnel el interfaz 0 para hacer un túnel automático.

```
interface Ethernet0
 description IPv4 uplink
 ip address 192.168.99.1 255.255.255.0
!
interface Ethernet1
 description IPv6 local network 1
 IPv6 address 2002:c0a8:6301:1::1/64
!
interface Ethernet2
 description IPv6 local network 2
 IPv6 address 2002:c0a8:6301:2::1/64
!
interface Tunnel0
 description IPv6 uplink
```

```
 no ip address
 IPv6 address 2002:c0a8:6301::1/64
 tunnel source Ethernet 0
 tunnel mode IPv6ip 6to4
!
IPv6 route 2002::/16 tunnel 0
```

3.2.4 Ejemplo: Túneles de configuración IPv4 compatible con IPv6

El ejemplo siguiente configura un túnel de IPv4-compatible IPv6 que permita que el Border Gateway Protocol (BGP) funcione entre un número de enrutadores sin tener que configurar un acoplamiento de túneles manuales. Cada enrutador tiene un solo túnel de IPv4-compatible, y las sesiones múltiples pueden funcionar sobre cada túnel, una del BGP a cada vecino. El interfaz 0 de Ethernet se utiliza como la fuente del túnel. El destinación del túnel es determinada automáticamente por la dirección IPv4 en los 32 bits de orden inferior de una dirección de IPv4-compatible IPv6. Específicamente, IPv6 el prefijo 0:0:0:0:0:0 se concatena a una dirección IPv4 (en el formato 0:0:0:0:0:0:A.B.C.D o::A.B.C.D) crear la dirección de IPv4-compatible IPv6. El interfaz 0 de Ethernet se configura con una dirección global IPv6 y una dirección IPv4 (el interfaz apoya las pilas del protocolo IPv6 e IPv4).

El BGP multiprotocol se utiliza en el ejemplo para intercambiar la información de la escalabilidad IPv6 por la dirección 10.67.0.2. La dirección IPv4 del interfaz 0 de Ethernet se utiliza en los 32 digitos de orden inferior de una dirección de IPv4-compatible IPv6 y también se utiliza el siguiente-salto. Usar una dirección de IPv4-compatible IPv6 para el vecino del BGP permite que la sesión del BGP IPv6 sea transportada automáticamente sobre un túnel de IPv4-compatible.

```
interface tunnel 0
 tunnel source Ethernet 0
 tunnel mode IPv6ip auto-tunnel
interface ethernet 0
 ip address 10.27.0.1 255.255.255.0
 IPv6 address 3000:2222::1/64
enrutador bgp 65000
 no synchronization
```

```
 no bgp default ipv4-unicast
 neighbor ::10.67.0.2 remote-as 65002

address-family IPv6
 neighbor ::10.67.0.2 activate
 neighbor ::10.67.0.2 next-hop-self
 network 2001:2222:d00d:b10b::/64
```

3.2.5 Ejemplo: Túneles de configuración ISATAP

El ejemplo siguiente muestra la fuente del túnel definida en Ethernet 0 y el comando del modo del túnel usado para configurar el túnel de ISATAP. Los anuncios del enrutador permiten la autoconfiguración del cliente.

```
IPv6 unicast-routing
interface tunnel 1
 tunnel source ethernet 0
 tunnel mode IPv6ip isatap
 IPv6 address 2001:0DB8::/64 eui-64
 no IPv6 nd suppress-ra
 exit
```

BIBLIOGRAFIA

1. Feit, Sidnie, "Arquitectura TCP/IP, Protocolos e Implementacion", Lima, 1998
2. CISCO, "The ABCs of IP versión 6", www.cisco/go/abc
3. S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, 1998
4. Microsoft Corporation, "Introduccion a IPv6", "www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/892c53fa-cf13-43d7-8086-11ab9ac1f0e8.mspx?mfr=true", 2005
5. A. Conta, S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 2463, 1998
6. B. Haberman, D. Thaler, "Unicast-Prefix-based IPv6 Multicast Addresses", RFC 3306, 2002
7. R. Hinden, S. Deering, E. Nordmark, "IPv6 Global Unicast Address Format", RFC 3587, 2003
8. S. Deering, W. Fenner, B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, 1999
9. T. Narten, E. Nordmark, W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6) ", RFC 2461, 1998
10. Microsoft Corporation, "IPv6 Transition Technologies" , www.microsoft.com/technet/itsolutions/network/ipv6/ipv6coexist.mspx, 2003
11. E. Nordmark, R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, 2005
12. CISCO, "Configuracion de Routers", Cisco-Ccna Modulo II, 2003
13. CISCO, "Implementing Tunneling for IPv6", http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/sa_tunv6.htm, 2005