Artículo Científico

https://doi.org/10.52428/20758944.v10i30.747

COMUNICACIÓN ENTRE USUARIOS IPV6 EN UNA RED IPV4

COMMUNICATION BETWEEN USERS IN A IPV4 IPV6 NETWORK

Marlon David González Ramírez (1)
Guadalupe Cristina Balderas Cortez (2)

RESUMEN

El presente artículo, muestra una configuración para la comunicación entre usuarios que utilicen el protocolo de Internet (IP) en sus versiones 4 y 6, utilizando el método de Túnel Manual 6to4 simulado en GNS3. Debido a que IPv6 es un protocolo no popular pero necesario, es importante dar a conocer sus atributos ya que en la actualidad la cantidad de usuarios que utilizan un identificador IPv4 para conectarse a Internet ha sido sobrepasada.

El segmento de direcciones que es administrado por IANA se ha agotado y se tiene la necesidad de recurrir a estas técnicas de traducción hasta que se obtenga una comunicación nativa entre IPv6, es por ello que es indispensable conocer los métodos de coexistencia entre estos dos protocolos, este método presentado ayuda para la integración y mejoras en el rendimiento de Internet comunicando usuarios IPv6 sobre la red IPv4.

Palabras clave: IPv6. Protocolo. Direcciones. Anycast. Multicast. Unicast. Seguridad.

ABSTRACT

This article shows a configuration for communication between users who use the Internet Protocol (IP) versions 4 and 6; using the method of tunnel Manual 6to4 simulated in GNS3. Since IPv6 is an unpopular but necessary protocol, it is important to make their attributes, as nowadays the quantity of users which use an IPv4 identifier to connect to the Internet has been exceeded.

The segment address that is managed by IANA is exhausted and has the need for these translation techniques until a native communication between IPv6 is obtained, which is why it is essential to know the methods of coexistence between these two protocols, therefore this presented method supports for Internet integration and performance improvements, communicating users to IPv6 on the IPv4 network.

Keywords: IPv6. Protocol. Directions. Anycast. Multicast. Unicast. Security.

INTRODUCCIÓN

El protocolo IPv6 es un protocolo que se ha desarro-

1. M.Sc. Redes de Computadoras, Desarrollador de aplicaciones en Windows y plataformas libres,Ingeniero en Sistemas Computacionales
Docente-Investigador, CIDETEC-Depto de Posgrado. México D.F.
Ponente del Primer Congreso Internacional de Informática y Electrónica- Universidad del Valle Cochabamba 2013.
dgonzalezr@ipn.mx
2. Ingeniera en Comunicaciones y Electrónica
Investigadora, CIDETEC-Depto de Posgrado. México D.F.
cristina.balderas85@gmail.com

Páginas 48 a 53
Fecha de recepción: 06/12/13
Fecha de aprobación: 21/01/14

llado desde los 90s, con la finalidad de que su versión 4 dejara de ser útil. En estos momentos, la versión 4 no ha dejado de ser útil, pero ha dejado de ofertar direcciones para los usuarios que desean integrarse a Internet.

Una de las medidas para seguir usando el protocolo IPv4 es aplicar servicios como lo es el NAT, que por medio de una dirección válida para Internet, un conjunto de usuarios con direcciones privadas ingresan a la red, e implementando mecanismos de administración, se eficiente el manejo del recurso.

Sin embargo, llegará el momento de desplazar el IPv4 y se debe acoplar simultáneamente su versión 6, manejando mecanismos de integración deseables para cada tipo de red.

1. PROTOCOLOS DE INTERNET

IPv6 es una versión más del Protocolo de Internet, definido en el RFC 2460 y está desarrollado para subsanar las carencias de disposición de conexión a Internet que el protocolo IPv4 (RFC 791) cuenta.

IPv4 es un protocolo de uso común que permite a los usuarios de redes divergentes, comunicarse entre sí, sin embargo, aunque consta de cuatro octetos en formato binario o decimal (según su aplicación) y una longitud de 232 (4,294,967,296), no todas las combinaciones de direcciones IP se asignan a los usuarios, ya que tienen una tarea específica. Considerando que los usuarios actuales que acceden a Internet no requieren sólo de una dirección, sino de más debido a que ellos cuentan con más de un dispositivo al cual se le asignará una dirección para su conexión y comunicación.

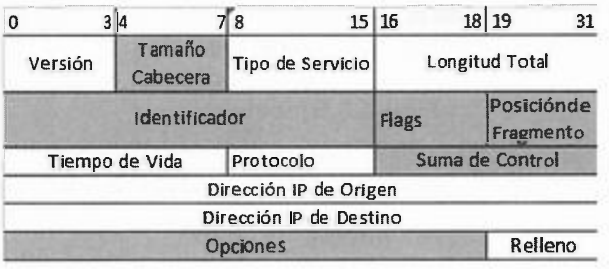
El caso del protocolo IPv6 ofrece una longitud de 2128, es decir, una composición de 340,282,366,920,938, 463,463,374,607,431,768,211,456. Usando esta longitud, IPv6 subsana la carencia de oferta de direcciones que se pueden otorgar a los usuarios que desean ingresar a redes, aspecto que IPv4, dejó de ofrecer desde hace algún tiempo.

La representación de las direcciones IPv6 divide la dirección en ocho grupos de 16 bits, separados mediante ":", representados con dígitos hexadecimales. Ejemplo: 2001 :0db8:85a3:0000:0000:8a2e:0370:7334. IPv6 incrementa el tamaño de la dirección IP de 32 bits a 128 bits para así soportar más niveles en la jerarquía de direccionamiento y un número mayor de host a direccionar. El diseño de este protocolo, adiciona múltiples beneficios en seguridad, manejo de calidad de servicio, una mayor capacidad de transmisión y mejora la facilidad de administración, entre otras cosas, características que IPv4 no tiene (1).

1.1.FORMATOS DE CABECERA DE PROTOCOLOS DEINTERNET

El encabezado de IPv6 es más sencillo que el de IPv4 del cual se eliminaron 6 campos: Longitud de encabezado, Identificación, Banderas, Desplazamiento por fragmentación, Suma de verificación de encabezado, Opciones y Relleno. Al pasar de un encabezado de IPv4 con longitud variable a IPv6 con menos campos y longitud fija se obtiene una reducción en procesos de los routers al momento de enviar los paquetes de IPv6, para mejor claridad ver Figura 1 y Figura 2 respectivamente.

Figura 1 Cabecera IPv4.



Fuente: (1), 2013.

Figura 2 Cabecera IPv6

Fuente: (1), 2013

Un atributo destacable es que esta versión agrega seguridad (IPsec), estandarizado por el Grupo Especial sobre Ingeniería de Internet que provee las funciones de:

- Limita el acceso solo a usuarios autorizados.
- Certifica la autenticación de la persona que envía los datos.
- Encripta los datos transmitidos a través de la red.
- Asegura la integridad de los datos.

• Invalida la repetición de sesiones, para evitar que no sean repetidas por usuarios maliciosos.

Los protocolos que respaldan el funcionamiento de IPSec son: la Autenticación de Encabezado (Autentication Header, AH) y la Carga de Seguridad Encapsulada (Encapsulated Security Payload, ESP). Al estar incluidos en cada implementación de IPv6 se provee mayor seguridad ya que IPSec está presente en todos los nodos de la red (2).

1.2. TIPOS DE DIRECCIONAMIENTO IPV6

IPv6 está definido por 3 tipos de direcciones:

• Unicast: Para enviar a una sola interfaz; actualmente existen dos tipos de unicast: Global–aggregatable unicast y Link-local unicast. Las direcciones global–aggregatable unicast son adheridas con máscaras de bits contiguos, similares al caso de IPv4, y se le asigna direcciones del tipo 2000::/3 ver Figura 3.

Figura 3 Global Unicast.

Prefijo de Encaminamiento Global	ID dela Subred	ID de la Interfaz

Fuente: (2), 2011

Las direcciones Link-local unicast han sido diseñadas para direccionar un único enlace para propósitos de auto-configuración (mediante identificadores de interfaz), o situaciones en las que no hay routers. Por tanto, los routers no pueden retransmitir ningún paquete con direcciones fuente o destino que sean locales de enlace (su ámbito está limitado a la red local)(3). Tienen el formato ver Figura 4.

Figura 4 Link-local Unicast.

10 bits	54 bits	64 bits
1111111010	0	Identificador de Interfaz

Fuente (2), 2011

• Anycast: Envía tráfico a la interfaz más cercana dentro de un grupo, a su vez que identifica un grupo de interfaces en diferentes dispositivos. Estas direcciones son creadas asignando a más de un dispositivo la misma dirección.

• Multicast: Identifica las interfaces de un mismos grupo. El tráfico enviado al grupo llega a todas interfaces, aun perteneciendo a diferentes grupos. El formato de una dirección multicast se representa en la siguiente Figura 5.

Figura 5 Formato de direcciones multicast.

8 bits	4 bits	4 bits	112 bits
11111111	Flag	Alcance	Identificador del grupo

Fuente: (2), 2011

Con IPv6 es posible atribuir una única interfaz a múltiples direcciones, independientemente de su tipo(4). Así un nodo se puede identificar a través de cualquier dirección de sus interfaces.

• Loopback ::1
• Link Local FE80:...
• Unique local FD07:..
• Global 2001:...

1.3. VENTAJAS Y DESVENTAJAS DE IPV6

Tabla 1 Comparación entre IPv4 e IPv6.

IPv6	IPv4
Direcciones de 128 bits (16 bytes)	Direcciones de 32 bits (4 bytes)
Arquitectura jerárquica Arquitectura plana	Configuración automática Configuración manual
Multicast y anycast	Broadcast
Seguridad obligatoria	Seguridad opcional
Identificación QoS	Sin Identificación QoS

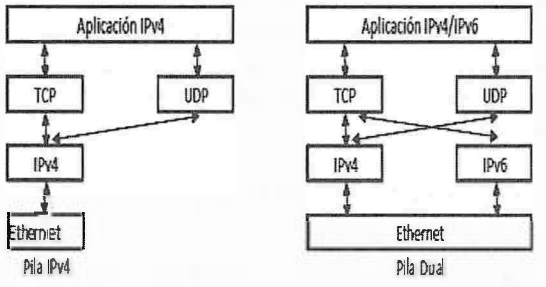
Fuente: (4), 2011

1.4. MÉTODOS DE TRANSICIÓN IPV4 A IPV6

La implementación de IPv6, será de manera gradual, de tal manera que existen mecanismos donde las dos versiones de estos protocolos subsisten, y permiten la comunicación de interfaces en Internet.

• Dual stack. Es posible ejecutar IPv4 e IPv6 (5)a la vez sin comunicación entre ambas versiones, los host y los routers llevan configuraciones a las dos versiones de IP e independientemente utilizan los recursos que desean alcanzar ver Figura 6.

Figura 6. Dual stack

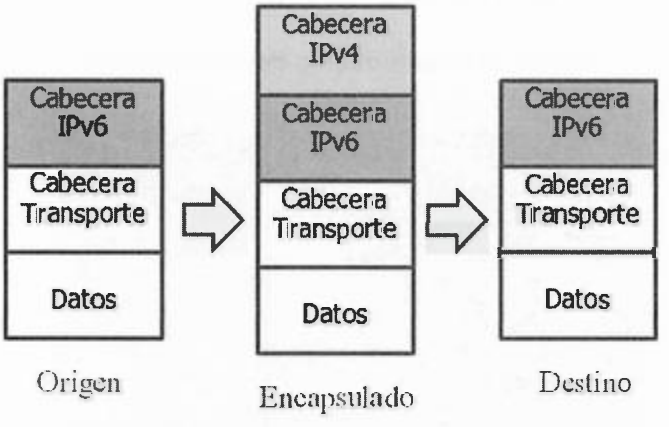


Fuente: (5), 2010

• Tunneling. Se utiliza para redes que solo soportan IPv4. Los routers encapsulan los paquetes IPv6 dentro de paquetes IPv4. El origen de los paquetes IPv4 es el propio router local y el destino será en el extremo del túnel(6). Debido al encapsulado, este sistema incrementa la tasa de transferencia ver Figura 7.

Existen cuatro tipos de túneles: Manual tunnels, 6to4, teredo e ISATAP (Intra-Site Automatic Tunnel Addressing Protocol).

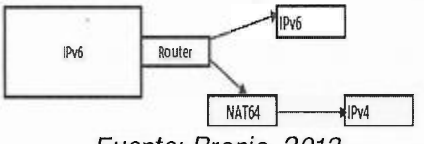
Figura 7 Método de Túnel



Fuente: (6), 2013

• Translation. El método de traducción, convierte las cabeceras de IPv4 a IPv6 y viceversa, sin que los usuarios tengan que comunicarse directamente con protocolos de diferentes versiones.

Figura 8 Método de traducción



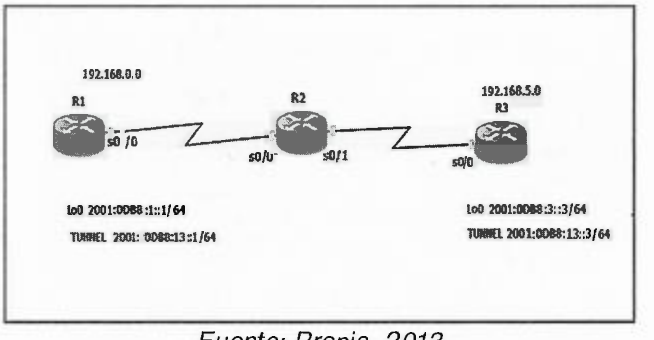
Fuente: Propia, 2013

2. SIMULACIÓN DE UN TUNEL MANUAL

Para la topología de la Figura 9 se muestra la distribución de una red con 3 router de un túnel manual 6to4, conocido como una conexión punto a punto donde se comunican los extremos nombrados islas IPv6 aprovechando la estructura de IPv4, su principal función del túnel manual 6to4 es agregar un encabezado IPv4 a los paquetes IPv6 que se generan en las islas, al final del proceso se realiza el des encapsulamiento para poder leer el tráfico IPv6 nativo generado por las islas por alguno de los host del extremo capaces de soportar tráfico IPv6.

La interfaz loopback simula el tráfico IPv6 nativo para crear un camino para que el tráfico Ipv6 pueda fluir del router R1 al router R3 a través del router R2 teniendo en cuenta que este no tiene soporte ipv6, para poder realizarlo se ha dividido el proceso en las siguientes actividades:

Figura 9 Diagrama simulado en GNS3

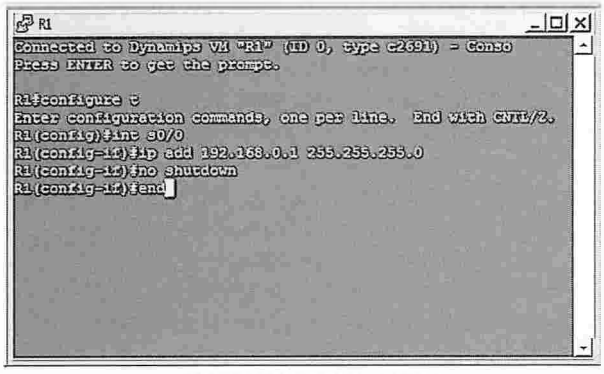


Fuente: Propia, 2013

La configuración consiste en inicializar los routers serie 2460 en el simulador GNS3 (cuentan con los requerimientos mínimos), abriendo una terminal para visualizar el arranque de los sistemas operativos de cada dispositivo iniciando la configuración del R1 con la interfaz puerto serial 0/0 con la dirección pública 192.168.0.1 y máscara 255.255.255.0.

Para el router R2 se debe tener en cuenta que se conecta entre las redes 192.168.0.0 y la red 192.168.5.0, conectada la interfaz serial s0/0 con la dirección lógica 192.168.0.2 y al puerto serial s0/1 192.168.5.1; ambas con una máscara de red 255.255.255.0. El router 3 se configura el puerto serial s0/0 con la dirección lógica 192.168.5.2 y una máscara de red 255.255.255.0, tal y como se muestra en la Figura 10.

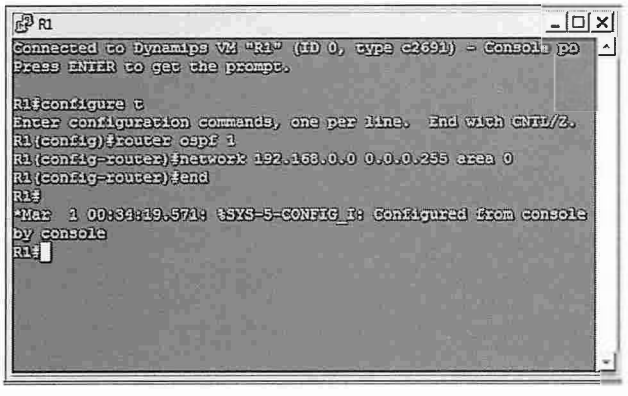
Figura 10 Inicialización se los puertos



Fuente: Propia, 2013

Posterior a la configuración de la interfaz del puerto serial, se prosigue con la configuración del enrutamiento dinámico para IPv4 para que se puedan comunicar entre el R1 y R3 en esta actividad se configura el protocolo OSPF ver Figura 11.

Figura 11 Protocolo de enrutamiento OSPF.



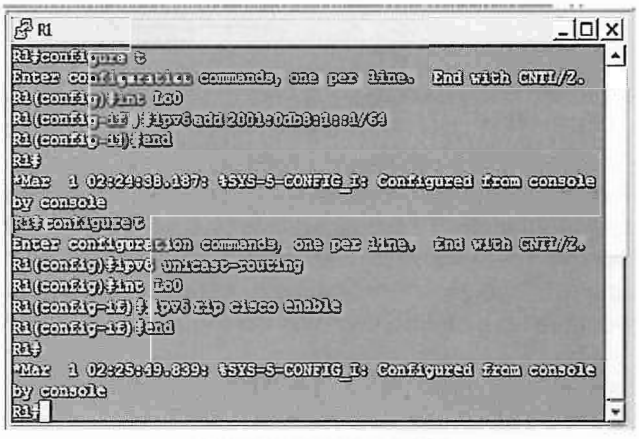
Fuente: Propia, 2013

Las configuraciones de los parámetros IPv6 para el túnel manual se inicia con la configuración de la interfaz loopback, con dirección IPv6, asignando al router R1 2001:DB8:1::1/64 y al router R3 2001:DB8:3::3/64 que simulará el tráfico IPv6 que generan las isla los router R1 y R3.

Posteriormente, se activa el protocolo de enrutamiento para la interfaz loopback en esta actividad el protocolo informa de las islas IPv6.

En la consola se ingresa el comando "ipv6 unicast-routing" que habilita el enrutamiento del tráfico IPv6 en cualquiera de las interfaces del router, en este caso se indica la interfaz loopback, donde se genera el tráfico IPv6, luego se configura el protocolo de enrutamiento RIP NG la sintaxis es "ipv6 rip<nombre del proceso del enrutamiento> enable". Para esta simulación se indica de la siguiente manera: "ipv6 rip cisco enable"; este comando identifica a las redes Ipv6 para que haya comunicación entre las islas IPv6, en la Figura 12 se registran en la consola del router dichos comandos teniendo en cuenta que esta configuración se realiza para los router R1 y R3 donde se encuentran localizadas las islas.

Figura 12 Protocolo de enrutamientro RIP



Fuente: Propia, 2013

En la generación del túnel manual, se observan comandos de la Figura 13.

Figura 13 Configuración del túnel manual

Fuente: Propia, 2013

3. PRUEBAS Y RESULTADOS

Las pruebas de comunicación se realizaron en el siguiente orden:

1. La comunicación entre el R1 S0/0 al R2 S0/0, fue exitosa, utilizando la herramienta ping.

2. La comunicación entre el R1 S0/0 al R2 S0/1, fue

exitosa, utilizando la herramienta ping.

3. La comunicación entre el R1 S0/0 al R3 S0/0, fue exitosa, utilizando la herramienta ping.

Este proceso se realizó también de manera contraria, para cada interfaz de cada router, generando resultados exitosos.

4. CONCLUSIONES

IPv4 es un protocolo que desde sus primeras aplicaciones, no se le visualizaba en desuso, debido a que la demanda de los usuarios que ingresaban a una red era muy baja. En la actualidad, la demanda ha sido sobrepasada, ya que los usuarios de Internet no requieren solamente de una dirección para conectarse, sino de varias, gracias a que cuentan con varios dispositivos con cuales entrar a compartir recursos.

Es importante conocer las deficiencias del protocolo actual IPv4 de Internet, y el valor de difundir los métodos de transición para converger con el protocolo IPv6, mostrando en este caso de estudio, el desarrollo de la configuración del Túnel manual. Es de vital importancia mencionar que la aplicación de los métodos de transición son situacionales, se aplicarán dependiendo los recursos y el tipo de red que se maneja.

Tal y como se observó en las pruebas, se identifica cómo los paquetes Ipv6 generados por las islas, en este caso simulación de la interfaz loopback, pueden transitar por la estructura de la red IPv4.

Es por ello que en este tipo de desarrollos se tenga que configurar a los routers con los parámetros IPv4, y en los dispositivos extremos configurar con la misma importancia los parámetros IPv6, para identificar y desencapsular los paquetes nativos de las islas.

La interfaz del tunnel es prioritaria ya que en este se denomina el origen y el destino del tráfico Ipv6, y si se utiliza un analizador de protocolos se observará el protocolo ICMPv6 se identificaría como a los paquetes generados por la interfaz loopback se le inserta un encabezado de IPv4.

5. AGRADECIMIENTOS

Agradecemos el apoyo al equipo de trabajo de la línea de Redes de Computadoras del CIDETEC, a la DCyC del IPN, así como a la UNIVALLE por su invitación.

6. REFERENCIAS BIBLIOGRÁFICAS

(1). BATIHA, KHALDOUN. Improving IPv6 Addresing types and size. 2013, International Journal of Computer Networks and Communications. https://doi.org/10.5121/ijcnc.2013.5404

(2). MARTÍNEZ, CARLOS. Direccionamiento IPv6. 2011. LACNIC, Santiago de Chile.

(3). XIANHUI CHE, L., DYLAN. IPv6: Current Deployment amd Migration Status. 2010. International Journal of Research and Reviews in Computer Science.

(4). HAMARSHEH, ALA. Configuring host to auto-detect (IPv6, IPv6-inIPv4, or IPv4) Network Connectivity.2011. KSII Transactions on Internet and Information Systems. https://doi.org/10.3837/tiis.2011.07.002

(5). BANSAL, K.L., SINGH, CHAMAN. Dual Stack Implementation of Mobile IPv6 Software Architecture. 2011. International Journal of Computer Applications. https://doi.org/10.5120/3062-4182

(6). JUNYUN WU, CAIYUN XIE. A New Kind of IPv6 Tunnel Desing to Support NAT. 2013. Journal of Theoretical and Applien Information Technology. https://doi.org/10.5121/ijcnc.2013.5404

Fuentes de financiamiento: Esta investigación fue financiada con fondos de los autores.

Declaración de conflicto de intereses: Los autores declaran que no tiene ningún conflicto de interés.

Copyright (c) 2014 Marlon David González Ramirez; Guadalupe Cristina Balderas Cortéz.

Este texto está protegido por una licencia *CreativeCommons 4.0*.

Usted es libre para Compartir —copiar y redistribuir el material en cualquier medio o formato— y Adaptar el documento —remezclar, transformar y crear a partir del material— para cualquier propósito, incluso para fines comerciales, siempre que cumpla la condición de:

Atribución: Usted debe dar crédito a la obra original de manera adecuada, proporcionar un enlace a la licencia, e indicar si se han realizado cambios. Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que tiene el apoyo del licenciante o lo recibe por el uso que hace de la obra.

Resumendelicencia - *Textocompletodelalicencia*