Análisis comparativo de los protocolos IPv6 e IPv4

Comparative analysis of IPv6 and IPv4 protocols

Recibido: 15 de julio del 2009
Aprobado: 5 de septiembre del 2009

Ingrid Paola Solano Benítez*
Guefry Agredo Méndez**
Nilsa Milena Agredo Salazar***
Danyeli Cabezas Burbano****
Carlos Iván Uribe Guirales*****

Resumen

La tendencia tecnológica vislumbra un cambio obligado hacia una plataforma IPv6 debido, entre otras razones, a la masificación de Internet como herramienta cotidiana, al surgimiento de nuevas tecnologías y al uso de aplicaciones que requieren un mayor rendimiento del sistema. Como respuesta a dicha tendencia, en el programa de Ingeniería de Sistemas de la Facultad de Ingeniería, en la Universidad Cooperativa de Colombia, seccional Popayán, se elaboró un trabajo de grado para implementar esta plataforma. El artículo explica en detalle dicha propuesta y presenta la metodología elaborada, los resultados obtenidos y el análisis e interpretación de éstos.

Palabras clave: protocolo IPv6, sistema operativo Linux, Nombre de Dominio de Sistema (DNS), protocolo de transferencia de hipertexto (http), Protocolo de Transferencia de Archivos (FTP).

Abstract

The technological trend glimpses a forced change towards an IPv6 platform, due to, among other reasons, the Internet spread as a daily tool, the emergence of new technologies and the use of applications that require higher system performance. As a response to the pointed trend, at the Program of Systems Engineering from the Faculty of Engineering, at The *"Universidad Cooperativa de Colombia"* –Popayán Satellite Campus, a graduation work to implement this platform was prepared. The article explains the proposal in detail and presents the methodology elaborated, the results obtained and the analysis and interpretation of those.

Keywords: protocol IPv6, Linux Operating System, Domain Name System (DNS), hypertext transfer protocol (http), File Transfer Protocol (FTP).

* Magíster en Computación, Especialista en Redes y Servicios Telemáticos, coordinadora de Investigaciones de la Facultad de Ingeniería, Universidad Cooperativa de Colombia, seccional Popayán, asesora del proyecto presentado en este artículo, correo electrónico: isolano@uccpopayan.edu.co

** Magíster en Ingeniería Electrónica y Telecomunicaciones, Especialista en Redes y Servicios Telemáticos, docente de la Universidad Cooperativa de Colombia, seccional Popayán, asesor del proyecto presentado en este artículo, correo electrónico: gagredo@gmail.com

*** Ingeniera de Sistemas de la Universidad Cooperativa de Colombia, seccional Popayán, desarrolladora del proyecto presentado en este artículo, correo electrónico: milena540@hotmail.com

**** Ingeniera de Sistemas de la Universidad Cooperativa de Colombia, seccional Popayán, desarrolladora del proyecto presentado en este artículo, correo electrónico: dani123191@hotmail.com

***** Ingeniero de Sistemas de la Universidad Cooperativa de Colombia, seccional Popayán, desarrollador del proyecto presentado en este artículo, correo electrónico: calilleri2000@yahoo.com

Introducción

Un cambio tecnológico altamente significativo lo constituyó la introducción de IPv6, inclusive desde la aparición de la web. Esta tecnología hace presencia en un momento en que se hace crítica su llegada, especialmente en las economías en transición, por el hecho del agotamiento del espacio de direcciones IPv4 que contempla 3,4 billones de direcciones sobre una base de 32 bits. Como se está en una fase de transición porque IPv6 no puede ingresarse al uso de una forma instantánea ya que el actual Internet funciona sobre la base de IPv4, es necesario contar con un esquema de transición. IPv6 comienza a ser una realidad en Japón y Corea a partir de julio del 2004, y en el 2007 se realizan pruebas en Europa y Estados Unidos.

Ya que la infraestructura de la Red Académica de la Universidad Cooperativa de Colombia, Popayán, se soporta en el protocolo IPv4, eventualmente es posible que se requiera el paso a IPv6, al menos para proyectos en el marco de Redes Avanzadas como la Red Universitaria de Popayán (RUP) y la Red Nacional Académica de Tecnología Avanzada (RENATA). Como no se tiene un trabajo previo en el tema, se hace necesario cuanto antes iniciar proyectos de grado como el actual, que dejen una base conceptual sobre el *protocolo*, pero que también vayan más allá con el fin de aportar al conocimiento sobre la implementación de servicios de Internet con IPv6. Se busca generar un curso sobre IPv6 para la plataforma Moodle de la Universidad Cooperativa de Colombia, seccional Popayán, describiendo el *protocolo* IPv6 y su direccionamiento, detallando los requerimientos que las aplicaciones de servicios de Internet deben tener para soportar al protocolo IPv6 frente a las construidas con IPv4. Además, se desea generar un documento de referencia sobre la puesta en funcionamiento para cada uno de los servicios de Internet por trabajar con IPv6 y con IPv4 desde un enfoque comparativo sobre las diferencias y similitudes funcionales y de configuración.

Para alcanzar los objetivos planteados en el anteproyecto, se realizó un trabajo sistemático en el cual, inicialmente, se recopiló y analizó la información relacionada con IPv6, pasando luego a los *servicios* de Internet sobre los protocolos IPv4 e IPv6, seleccionando sus similitudes y diferencias en cuanto a parámetros de configuración. Se llevó a cabo un proceso de apropiación de la tecnología que hasta el momento no se había hecho en la Facultad de Ingeniería de Sistemas de la Universidad Cooperativa de Colombia, seccional Popayán, para tener un punto de partida sobre el cual adherir nuevas capas de conocimiento; se realizó también un estudio enfocado en los factores que influyen sobre las nuevas aplicaciones IPv6. Finalmente, se materializaron los conceptos con la implantación de los servicios tradicionales o canónicos, con base en una selección de herramientas que implementan las nuevas versiones de los protocolos de nivel de aplicación en el sistema operativo Linux.

Marco teórico

Protocolo de Internet versión 6-IPv6

Hacia 1990 las previsiones acerca de que en un futuro no muy lejano las direcciones de protocolo de Internet (IP) podrían agotarse, llevaron al "Grupo de trabajo de ingeniería en Internet" (*Internet Engineering Task Force* [IETF]) a iniciar una serie de acciones encaminadas a obtener un nuevo protocolo IP. Si bien los 32bits en la estructura de las direcciones IPv4 permiten enumerar 4,294,967,296 posibles direcciones, la realidad está muy alejada de estas cifras. La estructura inicial utilizada para la asignación de direcciones con dos niveles —segmento de red, segmento de host— desaprovecha una gran cantidad del espacio de direccionamiento. Esta ineficiencia se ha visto incrementada por la organización en el reparto de rangos de direcciones en las clases A, B, C y D.

Tabla 1. División del rango de direcciones IPv4

Clase	Bits más significativos	Bits segmento de Red	N.º de redes	Bits segmento de Host	N.º de Hosts
A	0	7	124	24	16,777,214
B	01	14	16,382	16	65,534
C	110	21	2,097,152	8	254
D	Las direcciones de clase D son un grupo especial que se utiliza para dirigirse a grupos de hosts. Estas direcciones son muy poco utilizadas. Los cuatro primeros bits de una dirección de clase D son 1110.				

Fuente: los autores

Ante esta situación, en noviembre de 1991 el IETF formó el grupo de trabajo *Routing and Addressing* (ROAD), destinado a estudiar los problemas de enrutamiento y direccionamiento asociados al crecimiento de Internet. Este grupo hizo una serie de propuestas que abarcaban desde soluciones a corto plazo, como el "Enrutamiento entre dominios sin clase" (*Classless Inter-Domain Routing* [CIDR]), hasta la recomendación de una solicitud de propuestas para un nuevo protocolo IP con direcciones de mayor tamaño. Dicha solicitud de propuestas para un protocolo de *próxima generación* se llevó a cabo en julio de 1992 y quedó recogida en el Request for Comments (RFC) 1550. Se recibieron veintiuna propuestas, algunas de ellas procedentes de industrias que se esperaba se convirtieran en importantes mercados para las redes de datos: televisión por cable, la industria de la telefonía móvil y la industria eléctrica. Todas las propuestas recibidas fueron examinadas por el área IPng, grupo creado al efecto por el IETF.

IPng fue diseñado como una evolución de IPv4, pues mantuvo las funciones que eran satisfactorias y eliminó aquellas que no lo eran. La primera versión del IP de *próxima generación* apareció en 1996 bajo el nombre de IPv6. Los principales signos de identidad que le diferencian de su predecesor son:

Direccionamiento y enrutamiento

El tamaño de las direcciones IP pasa de 32 a 128bits. Esto supone un espacio de direccionamiento 296 veces mayor, lo que hace posible una jerarquía de asignación de más niveles y una autoconfiguración más simple de las direcciones. La escalabilidad del enrutamiento multicast se ve mejorada con la adición de un campo scope (ámbito) a las direcciones multicast para limitar el ámbito de un grupo multicast.

Formato simplificado de la cabecera

Algunos campos de la cabecera IPv4 se han eliminado o se han hecho opcionales. De esta forma, se simplifica y agiliza el manejo de los paquetes IPv6 por parte de los enrutadores.

Soporte mejorado de opciones

En IPv6 las opciones se implementan en cabeceras de extensión separadas. Esta organización supone una gran mejora en cuanto al rendimiento de los enrutadores, puesto que en la mayoría de los casos estas opciones no se procesan hasta que el paquete alcance su destino final.

Extensibilidad

Es posible indicar las acciones a realizar por el enrutador en caso de que desconozca alguna opción, codificando dicha información dentro de la propia opción. Ésta es una característica muy importante para hacer posible el desarrollo incremental de nuevas funcionalidades.

Autenticación y privacidad

IPv6 define dos extensiones relacionadas con este tema: el IP Authentication Header (AH) y el IP Encapsulating Security Payload (ESP). El primero de ellos garantiza que se ha realizado la transmisión del mensaje sin errores ni modificaciones. El segundo provee un mecanismo para cifrar la carga útil del paquete o incluso el propio paquete, lo que permite la transmisión de información sensible a salvo de posibles intromisiones.

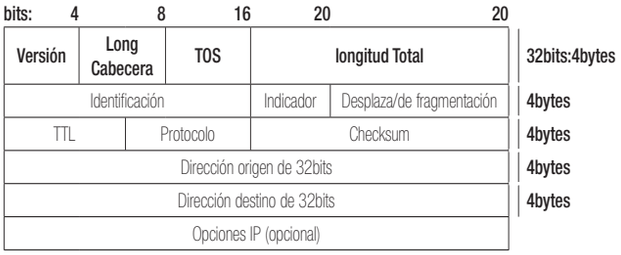
Calidad de servicio

IPv6 implementa el concepto de flujo, es decir, una secuencia de paquetes entre dos nodos para los cuales el nodo origen desea un tratamiento determinado por parte de los enrutadores intermedios. Esto hace que los enrutadores tengan que llevar el control de los flujos y cierta información sobre cómo tratar el paquete, pero también se acelera el tiempo de procesamiento, pues si no fuera así habría que incluir dicha información en alguna extensión que tendría que ser procesada por los enrutadores.

Formato de presentación para una dirección IPv4

La cabecera de un paquete IPv4 es de longitud variable, y se especifica utilizando múltiplos de 32bits. La longitud mínima —sin incluir el campo *opciones*— de la cabecera IPv4 es 20bytes, pero si se agregan *opciones*, la cabecera se extiende en múltiplos de 4bytes hasta 60bytes para transmitir información adicional relacionada con seguridad, enrutamiento de origen, registro de ruta, identificación de flujo o marca de tiempo. Los campos que definen el formato de la cabecera de un paquete IPv4 se ilustran en la tabla 2.

Tabla 2. Descripción de la cabecera de un paquete ipv4



Fuente: los autores

- Versión, *Version* (4bits)
- Longitud de la cabecera, *Header length* (4bits)
- Tipo de servicio, *Type of service* (TOS) (1byte)
- Longitud total, *Total length* (2bytes)
- Identificación, *Identification* (2bytes)
- Indicador, *Flag* (4bits)
- Desplazamiento de fragmentación, *Fragment offset* (12bits)
- Tiempo de vida, *Time to live* "TTL" (1byte)
- Protocolo, *Protocol* (1byte)
- Código de verificación, *Checksum* (2bytes)
- Dirección origen de 32bits (4bytes)
- Dirección destino de 32bits (4bytes)

Formato y contenido de la cabecera de un paquete IPV6

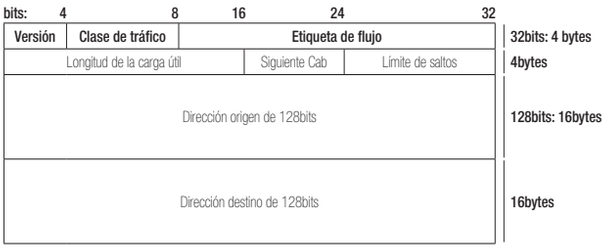
La estructura de la cabecera de un paquete IPV6 es más simple y más eficiente que la estructura de una cabecera IPV4. La longitud de esta cabecera tiene un tamaño fijo de 40bytes y contiene ocho campos, a diferencia de la cabecera de un paquete IPV4 que contiene como mínimo doce campos.

IPV6 ha eliminado cinco campos de la cabecera IPV4. Éstos son:

- Longitud de la cabecera
- Identificación
- Indicador
- Desplazamiento de fragmentación, *Fragment offset*
- Código de verificación, *Checksum*

Los campos que definen el formato de la cabecera de un paquete IPV6 se ilustran en la tabla 3.

Tabla 3. Descripción de la cabecera de un paquete ipv6



Fuente: los autores

- Los campos en la cabecera de un paquete IPV6 son los siguientes:
- Versión (4bits): este campo indica la versión del protocolo IP. En el caso de IPV6, el número de versión es el 6. El número de versión 5 no puede ser usado, debido a que ya ha sido asignado a un protocolo experimental (ST2, RFC1819).
- Clase de tráfico, *Traffic class* (1byte): este campo remplaza el campo *Tipo de servicio* en IPV4 y tiene como función etiquetar paquetes con una clase de tráfico para utilizarse en *Servicios diferenciados*. El RFC 2474, "Definición del Campo de Servicios Diferenciados (DS) en cabeceras IPV4 e IPV6" explica cómo el campo *clase de tráfico* puede ser utilizado.
- Etiqueta de flujo, *Flow label* (20bits): este nuevo campo se utiliza para etiquetar paquetes de un flujo específico y, de este modo, diferenciarlos de otros paquetes en el nivel de red. Con esta etiqueta un enrutador no necesita examinar el interior del paquete para identificar sus características, ya que la información está disponible en la cabecera del paquete IPV6. Los campos *clase de tráfico* y *etiqueta de flujo* son los que permiten una de las características fundamentales e intrínsecas de IPV6: Calidad de Servicio (Quality of service, (QOS), a partir de mecanismos de control de flujo y de asignación de prioridades diferenciadas según el tipo de servicio.
- Longitud de la carga útil, *Payload length* (2bytes): este campo, nombrado en IPV4 como *longitud total*, especifica la longitud de la carga útil (payload) o la longitud de los datos transportados después

de la cabecera básica IPv6. Es de señalar que las cabeceras de *extensión* se consideran parte del payload IPv6. Debido a que el campo *longitud de la carga útil* tiene una longitud de 2bytes, se limita el tamaño del payload IPv6 a 65,536bytes. Sin embargo, IPv6 dispone de la opción *jumbograma*,[1] descrita en el RFC 2675 como "IPv6 jumbograms", la cual soporta, si es necesario, tamaños grandes de payload. Es de anotar que el cálculo del payload en IPv6 es diferente al realizado en IPv4. El campo *longitud total* en IPv4 define la longitud total del paquete, incluidas las partes de cabecera y de datos de usuario.

- Siguiente cabecera, *Next header* (1byte): en IPv4 este campo es conocido como *protocolo*, y es modificado en IPv6 para transportar información opcional que se codifica en cabeceras de *extensión*. Así, el valor del campo *siguiente cabecera* determina el tipo de cabecera de *extensión* que complementa la cabecera básica de un paquete IPv6.
- Límite de saltos, *Hop limit* (1byte): similar al campo *tiempo de vida* en IPv4. El valor del campo *límite de saltos* en IPv6 especifica el número máximo de enrutadores que un paquete puede transitar antes de ser descartado. Disminuye en 1 cada vez que un paquete atraviesa un nodo IPv6. Si llega a 0 se descarta.
- Dirección origen, *Source address* (16bytes): este campo contiene la dirección IP de quien origina el paquete IPv6.
- Dirección destino, *Destination address* (16bytes): este campo contiene la dirección IP del destino del paquete IPv6.

El Sistema de Nombres de Dominio (DNS)

Constituye una base jerárquica de datos distribuida en la cual se almacena información para realizar el mapeo de direcciones IP a nombres de máquina y viceversa, información de enrutamiento para el servicio de correo, y datos utilizados por las diferentes aplicaciones en Internet. Permite que los usuarios localicen determinadas máquinas mediante el nombre asignado por el administrador, liberándolos así de la pesada tarea de recordar la dirección numérica de los recursos de red; además, mantiene direcciones de otros servidores de nombres que puede emplear para actualizar su información.

El DNS almacena la información de acuerdo con una estructura de árbol, y cada nodo de éste, llamado *dominio*, se identifica con una etiqueta; el nombre del dominio de cada nodo es la concatenación de todas las etiquetas utilizadas para marcar la ruta desde el nodo final hasta el nodo raíz que se representa de la forma "." De allí se desprenden todos los dominios primarios que indican el país, región o tipo de organización que utiliza ese nombre. Existen dos tipos de dominios primarios, los genéricos y los geográficos. Los genéricos son conocidos como internacionales u organizacionales, entre los cuales están .org, .net, .edu, .com, .mil, y .gov; los geográficos son organizados por localidades. Así, por ejemplo el dominio uccpopayan.edu.co indica que su ubicación geográfica es Colombia (.co) y el tipo de organización es educativa (.edu).

Secure Shell (ssh)

Es un protocolo basado en la arquitectura cliente/servidor; permite que un usuario se conecte a un host remotamente o ejecute procesos remotos utilizando el puerto 22, que ha sido registrado por Internet Assigned Numbers Authority (IANA) y oficialmente asignado para SSH, en redes que utilizan TCP/IP. A diferencia de los protocolos FTP y TELNET, que también facilitan el acceso remoto, SSH se encarga de encriptar la información de registro, es decir, los datos utilizados para la validación de sesión, reduciendo así los riesgos de seguridad tanto para el sistema cliente como para el sistema remoto, cuando se envía información a través de una red insegura. SSH también es ampliamente utilizado para asegurar el uso de protocolos inseguros.

Las técnicas de cifrado que utiliza SSH para la manipulación de la información permiten asegurar que alguien que no sea un legítimo destinatario acceda a información que no le corresponde, que la información no pueda ser alterada en el tránsito desde el emisor hacia el destinatario, y que tanto el emisor como el receptor puedan confirmar la identidad de la

[1] Jumbograma es una opción que permite que la longitud máxima de los datos transportados por IPv6 (16bits, 65,536bytes) se extienda hasta 64bits. Se prevé su uso especialmente para tráficos multimedia, sobre líneas de banda ancha. Sin embargo, estos paquetes no pueden ser fragmentados.

otra parte involucrada en la comunicación. Estos tipos de cifrado se dividen en dos grupos: los de cifrado simétrico y los de cifrado asimétrico.

La técnica de cifrado simétrico consiste en el uso de una clave que es conocida por el emisor y el receptor involucrados en la comunicación. Cuando el emisor desea enviar un mensaje al receptor utiliza un algoritmo de cifrado simétrico y la clave que tienen en común, generando así el nuevo mensaje que será transmitido. El receptor, al utilizar la clave y el algoritmo inverso utilizado por el emisor, obtiene el mensaje original. El algoritmo de cifrado utilizado debe contar con las técnicas necesarias para garantizar que sea difícil de descifrar; sin embargo, este sistema presenta vulnerabilidades ya que es necesario que ambas partes conozcan la clave.

La técnica de cifrado asimétrico consiste en el uso de dos llaves: una pública y una privada. La clave pública, como su nombre lo indica, se puede hacer pública y se entrega a aquellos receptores que nos vayan a enviar mensajes cifrados; la clave privada se debe mantener en secreto. El emisor tiene dos llaves, por ejemplo JyK, para denotar la pública y la privada respectivamente; cuando éste desea transmitir un mensaje que nadie, excepto el receptor específico debe conocer, con el uso de un algoritmo de cifrado asimétrico y su llave privada, genera un nuevo mensaje ya cifrado y lo transmite. Posteriormente, en el destino, se utiliza un algoritmo de cifrado inverso al que utilizó el emisor y la clave pública del emisor (la cual ha sido enviada al servidor con anterioridad) para obtener el mensaje original. Si bien las dos llaves están fuertemente relacionadas entre sí, no es posible calcular la primera a partir de los datos de la segunda, ni tampoco a partir de los documentos cifrados con la clave privada. Este tipo de cifrado opera de tal forma que la información cifrada con una de las claves sólo puede ser descifrada con la otra; es decir, si un usuario cifra determinada información con su clave privada, cualquier persona que conozca su clave pública podrá descifrarla. Por tanto, si un receptor logra descifrar un mensaje utilizando la llave pública del emisor, puede afirmarse que el mensaje lo generó dicho emisor utilizando su clave privada, validación de la identidad del cliente y servidor.

Servicio web-http

Un servidor web es un programa que implementa el protocolo http (Hypertext Transfer Protocol). Este protocolo está diseñado para transferir lo que se conoce como hipertextos, páginas web o páginas html (Hypertext Markup Language): textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de sonidos.

Un servidor web se encarga de mantenerse a la espera de peticiones http llevadas a cabo por un cliente http, que se suele conocer como navegador. El navegador realiza una petición al servidor y éste le responde con el contenido que el cliente solicita. A modo de ejemplo, al digitar www.ipv6uccpopayan.edu.co en un navegador, éste realiza una petición http al servidor de dicha dirección. El servidor responde al cliente enviando el código html de la página; el cliente, una vez recibido el código, lo interpreta y lo muestra en pantalla. Como se puede apreciar, el cliente es el encargado de interpretar el código html, es decir, de mostrar las fuentes, los colores y la disposición de los textos y objetos de la página; el servidor tan sólo se limita a transferir el código de la página sin llevar a cabo ninguna interpretación de ésta.

Sobre el servicio web clásico se puede disponer de aplicaciones web. Éstas son fragmentos de código que se ejecutan cuando se realizan ciertas peticiones o respuestas http. Hay que distinguir entre:

Aplicaciones en el lado del cliente: el cliente web es el encargado de ejecutarlas en la máquina del usuario. Son las aplicaciones tipo javascript: el servidor proporciona el código de las aplicaciones al cliente y éste, mediante el navegador, las ejecuta. Es necesario, por tanto, que el cliente disponga de un navegador con capacidad para ejecutar aplicaciones (también llamadas scripts). Normalmente, los navegadores permiten ejecutar aplicaciones escritas en lenguaje javascript y java, aunque pueden añadirse más lenguajes mediante el uso de plugins.

Aplicaciones en el lado del servidor: el servidor web ejecuta la aplicación; ésta, una vez ejecutada, genera cierto código html; el servidor toma este código recién creado y lo envía al cliente por medio del protocolo http.

Las aplicaciones de servidor suelen ser la opción por la que se opta en la mayoría de las ocasiones para realizar aplicaciones web, aunque es de notar que las aplicaciones del cliente pueden ser usadas en combinación, para obtener funcionalidades adicionales. La razón es que, al ejecutarse éstas en el servidor y no en la máquina del cliente, éste no necesita ninguna capacidad adicional. Así pues, cualquier cliente dotado de un navegador web básico puede utilizar este tipo de aplicaciones. Algunos lenguajes de este tipo relacionados con las aplicaciones web son: PHP, ASP, Perl, CGI, .NET, JSP (tecnología java).

File Transfer Protocol (FTP)

Es una especificación para el protocolo internet en la cual se definen los métodos por los cuales es posible intercambiar archivos entre estaciones de trabajo a través de Internet. Este protocolo es ampliamente utilizado para la transferencia de archivos alojados en páginas web y para descargar programas y otro tipo de archivos desde los servidores FTP hacia las estaciones de trabajo destino. Es posible copiar, borrar, actualizar, mover y renombrar los archivos alojados en el servidor FTP, desde el mismo servidor o desde un cliente FTP. Los objetivos principales del protocolo FTP son:

- Promocionar el uso compartido de archivos (programas o datos).
- Incentivar el uso indirecto o implícito (a través de programas) de servidores remotos.
- Hacer transparente al usuario las variaciones entre la forma de almacenar archivos en diferentes computadores.
- Transferir datos fiable y eficientemente.

Este protocolo se basa en el esquema cliente/servidor. El cliente FTP se conecta a un servidor FTP (que es la máquina remota) y, una vez establecida la conexión, se inicia una sesión entre las dos máquinas basada en peticiones, respuestas y transmisión de información mediante un canal de datos creado para tal fin. Las peticiones realizadas por el cliente se denominan comandos FTP.

Para la transferencia de archivos mediante el protocolo FTP se utilizan dos tipos de conexiones, la conexión de control y la conexión de datos. La conexión de control sirve para enviar subcomandos desde el cliente al servidor y recibir las correspondientes respuestas a esos subcomandos. La conexión de datos es utilizada para transferir los archivos que el cliente haya solicitado. Conectividad TCP/IP, existencia de un servidor FTP configurado apropiadamente, tener el nombre de host del sistema remoto y contar con nombre de usuario y contraseña en el sistema remoto; los anteriores son los elementos necesarios en el establecimiento de una sesión FTP.

Para que un usuario pueda conectarse con un servidor FTP es necesario tener un usuario (login) y una contraseña (password), debido a que los servidores controlan el acceso de los usuarios a su sistema de carpetas, pero en los casos en los cuales los servidores FTP contienen información que puede ser vista por cualquier tipo de usuario. Es posible utilizar una forma de acceso no autentificada, es decir que no utiliza contraseñas, denominada usuario anonymous. Existen tres tipos de usuarios FTP:

- Usuario anónimo: puede acceder a los archivos del servidor, sin importar si se encuentra registrado en él, cualquiera que esté conectado a Internet puede establecer una conexión y realizar transferencia de archivos, del tipo servidor-cliente. Está específicamente orientado para trabajar con archivos de contenido variado (fotos, texto, software) y la transferencia se puede realizar entre computadores con distintos sistemas operativos y entre distintas redes. Sus privilegios son restringidos.
- Usuario autenticado: necesita un nombre de usuario y una contraseña para acceder al servidor y poder enviar o recibir archivos desde y hacia los directorios del servidor y convertirlos en públicos o privados.
- Usuario embebido: forma parte del usuario anónimo; las descargas de archivos se realizan desde enlaces predispuestos en páginas web, y es la forma de acceso a servidores FTP más popular hoy en día.

Servicio de correo electrónico

El correo electrónico es sin duda uno de los servicios más utilizados y de mayor importancia en Internet actualmente. No sólo por los millones de usuarios que diariamente utilizan este servicio, sino también

porque en muchos casos, por medio del correo electrónico, los usuarios hacen sus primeros acercamientos a esta tecnología; además, actualmente es requisito poseer un correo electrónico para poder acceder a otros servicios.

Por tanto, se hace totalmente indispensable en Internet IPv6 que este servicio se encuentre plenamente disponible a los usuarios; de esta manera se podrá asegurar una penetración más eficaz entre los clientes finales, ya que es imposible pensar en captar usuarios para la nueva red sin ofrecer uno de los pilares sobre los que se cimienta la actual demanda de Internet.

El servicio de correo electrónico inicialmente se soportaba solamente con el "protocolo simple de transporte de correo" (*Simple Mail Transport Protocol* [SMTP]) porque para hacer uso del servicio tenía que iniciarse sesión remota en un servidor y por medio de comandos como "mail" o por aplicaciones como "pine" o "mutt" que ofrecían una interfaz mediada por menús, se realizaba el envío o lectura de correo. Sin embargo, con la llegada de los computadores personales (Personal Computers [PC]) y, en especial, por la aparición de los entornos gráficos como los de Microsoft Windows, surgieron aplicaciones como Outlook de MS Office, Thunderbird de Mozilla y Eudora que permitieron al usuario administrar su correo de manera remota y gráfica, pero para que esto fuera posible se necesitó desarrollar los protocolos *Post Office Protocol* (POP) e *Internet Messages Access Protocol* (IMAP).

Protocolo simple de transferencia de correo (SMTP)

Es uno de los IP diseñados para transferir correos electrónicos de manera confiable y eficiente. La idea que subyace a SMTP es bastante sencilla: un usuario o una aplicación redacta un mensaje que contiene la dirección de correo electrónico del destinatario (por ejemplo, "jperez@uccpopayan.edu.co") junto con el asunto y el contenido del mensaje. La entrega del mensaje se inicia al transferir el mensaje a un servidor SMTP dedicado, basándose en el nombre de dominio de la dirección de correo electrónico del destinatario, el servidor SMTP inicia la comunicación con un servidor de nombres de dominio (DNS), que busca y devuelve el nombre de host del servidor SMTP de destino para ese dominio.

Por último, el servidor SMTP de origen se comunica directamente con el servidor SMTP de destino a través del puerto 25 del protocolo TCP. Si el nombre de usuario de la dirección de correo electrónico del destinatario coincide con una de las cuentas de usuario autorizadas en el servidor de destino, el mensaje original se transferirá a dicho servidor, esperando que el destinatario recoja el mensaje mediante un programa cliente.

En caso de que el servidor SMTP de origen no pueda comunicarse directamente con el servidor de destino, el protocolo SMTP dispone de mecanismos para transferir mensajes a través de uno o varios servidores SMTP intermedios de retransmisión. Un servidor de retransmisión recibirá el mensaje original e intentará entregarlo al servidor de destino o redirigirlo a otro servidor de retransmisión. Este proceso se repetirá hasta que se entregue el mensaje o hasta que transcurra un periodo de espera designado.

Propuesta metodológica

Dada la naturaleza del proyecto, para el logro de los objetivos planteados se trabajó con un modelo en fases inspirado en la metodología secuencial o en cascada: así, se organizó en fases y tuvo que haberse cumplido cada una para poder pasar a la siguiente. Adicionalmente, como este trabajo no es un desarrollo software, las fases se han adaptado para dar coherencia a la labor realizada. Las fases se describen a continuación:

Fases del proyecto

Fase de recolección y análisis de la información

- Recolección de información: consiste en realizar una revisión bibliográfica de revistas, libros, material de Internet y otros para obtener información necesaria para el trabajo.
- Análisis y clasificación de la información: se realiza un análisis crítico de la información obtenida durante el proceso de recolección de modo que se tenga en cuenta la confiabilidad, calidad y coherencia de los datos.

Fase de desarrollo

- Aseguramiento de los elementos para la puesta en funcionamiento de los servicios de Internet y

la autoconfiguración con IPv6 y equivalente con IPv4, en el ámbito de un laboratorio en una sala de cómputo de la Universidad Cooperativa de Colombia, seccional Popayán.
- Puesta en funcionamiento de los servicios de Internet con IPv6 e IPv4 y análisis de similitudes y diferencias.
- Adquisición de los elementos para generar un curso sobre el protocolo IPv6 y el direccionamiento con un enfoque comparativo frente a IPv4 para la plataforma Moodle de la Universidad Cooperativa de Colombia, seccional Popayán.

Fase integración

- Elaboración del documento final y anexos: se hace una recopilación en escrito y en medio digital de los resultados del desarrollo del proyecto para su divulgación.
- Resultados y sustentación final del proyecto.

Resultados

Análisis e Interpretación

Después del desarrollo del presente trabajo de grado, se analizó e interpretó que:

1. Para las aplicaciones fue necesario agregar nuevos elementos que permitieran a los programas que implementan servidores interactuar con IPv6.
2. La configuración de los servicios tratados, en general, no cambia notoriamente entre lo que debe hacerse para IPv4 y lo que debe hacerse para IPv6. A continuación se hace un listado resumido:

   a. Servicio DNS: éste es el servicio que más cambios presenta para IPv6; en las zonas directas aparecen los registros AAAA y los DNAME siendo equivalente a los A y CNAME de IPv6. En cuanto a la zona inversa, lo diferente es el uso de las direcciones que son más "largas" en IPv6 respecto a IPv4. Es fundamental activar la opción listen-on-v6 para que el servidor active el soporte para IPv6 y es clave que este servicio esté funcionando para soportar el funcionamiento de los demás, porque los clientes en general hacen uso de conexiones a los servidores por los nombres y no por las direcciones IPs.
   b. Servicio SSH: para este servicio el proceso de configuración es el mismo y ya viene listo para soportar conexiones tanto con IPv6 como con IPv4; solamente se debe revisar que no se haya puesto a escuchar solamente por una de las dos con la directiva *listen*. Desde la perspectiva de los clientes, cuando se hace la conexión con SSH para IPv6 debe activarse la opción que lo indica, por ejemplo, si es por comandos, agregarse el parámetro -6 para indicarlo.
   c. Servicio http: el proceso de configuración es el mismo y ya viene listo para soportar IPv6 e IPv4. Desde la perspectiva de los clientes cambia la situación cuando se hace la conexión por la IP, teniendo que colocar entre corchetes las direcciones para conexiones por IPv6.
   d. Servicio FTP: en este caso, aunque el servidor soporta trabajar con IPv6 e IPv4, no soporta hacerlo al tiempo con una sola instancia como lo hace SSH y FTP. El cuidado entonces es que para implementación dual debe hacer con múltiples instancias. Para el uso de clientes, es necesario trabajar soportado en el DNS.
   e. Servicio de correo electrónico: el proceso de configuración es el mismo, debe activarse la opción que permite que el servidor *sendmail* acepte conexiones por IPv6 y por IPv4 y tenerse un cuidado especial con la interacción con el servicios DNS dado que ahora se necesita la zona para IPv6 donde el registro MX resuelva adecuadamente el servidor.
   f. Para el caso del ejemplo se trabajó con apolo.ipv6uccpopayan.edu.co, así que era necesario en el DNS la existencia del registro @ IN MX 10 apolo.ipv6uccpopayan.edu.co para que se tuvieran conexiones por IPv6. En cuanto a POP3 e IMAP, el servidor Dovecot trae el soporte para trabajo dual, dependiendo nuevamente del DNS y la dirección que utilice el cliente para conectarse.

3. Las aplicaciones que vienen con Linux en la actualidad están listas para trabajar en modo dual; es necesario, entonces, trabajar en cuanto a capacitación para cuando sea necesario el cambio a IPv6. El presente trabajo es un buen referente para aportar en este proceso.

4. Aunque los servidores en su mayoría traen el soporte para IPv6, no viene por defecto activo para todos; debe tenerse en cuenta esto porque no se puede generalizar. A muchos se les tuvo que activar la capacidad con las directivas respectivas en el archivo de configuración. Una forma de establecer si el servicio ya quedó listo para funcionar para IPv6 es ejecutar el comando netstat -tan y revisar que los puertos de los servicios aparezcan con [puerto].

Conclusiones

Respecto a los servicios

- Los registros AAAA se constituyen en la mejor alternativa al momento de implantar un DNS IPv6, debido a la similitud que en formato y funcionamiento tienen con los registros A, abonando así la ventaja de experiencia operativa que con estos últimos se ha obtenido desde la definición del Sistema de Nombres de Dominio.
  Por otro lado, cabe destacar las características adicionales que ofrecen los registros A6 y DNAME en un entorno en el cual una renumeración pueda significar un proceso laborioso dada la cantidad de hosts y servidores que formen parte de la red, o en organizaciones que trabajen con topologías multiproveedor, donde un cambio en un DNS de alto nivel dentro de la jerarquía pueda significar cambios traumáticos en los niveles más bajos de ésta. El estado de dichos registros es actualmente experimental, sin embargo, vale la pena seguir estudiándolos para abarcar todo el potencial que éstos pueden llegar a brindar al desarrollar mecanismos que permitan enlazar las diferentes respuestas provenientes de registros A6.
- Durante el periodo de transición IPv4 a IPv6 es importante contar con servidores de nombres de dominio *dual-stack* para garantizar la conectividad entre escenarios de redes heterogéneas IPv4-IPv6. La tendencia Dual-Stack se observó a lo largo de todo el proyecto, al verificar esta condición en un sin número de servidores DNS externos.
- El buen funcionamiento de todos los servicios de Internet dependen de una óptima configuración del Servidor de Nombres de Dominio.
- La autoconfiguración es una característica fundamental en el protocolo IPv6, y su implantación resulta definitiva para el desarrollo de esta tecnología; existen múltiples metodologías para asignar parámetros de autoconfiguración a un nodo cliente (Stateful, Staeless, combinación).
- La autoconfiguración libera al usuario de la tarea de configurar los parámetros de la red para obtener conectividad y minimiza los posibles errores de direcciones duplicadas al utilizar un algoritmo creado para tal fin.
- Utilizando la autoconfiguración sin control de estado, es posible que cualquier dispositivo que se conecte a la red tenga una dirección IPv6 válida, lo cual podría disminuir el nivel de seguridad en una red, dado el bajo nivel de control en la asignación de las direcciones a usuarios anónimos.
- El correo electrónico funciona óptimamente en un ambiente dual-stack, siempre y cuando se sigan los lineamientos propuestos en este documento. Un servidor de correo dual-stack está en capacidad de enviar y recibir desde y hacia MTA IPv6 puros y MTA IPv4.
- Los nuevos comandos adicionados a las especificaciones FTP para dar soporte al protocolo IPv6 le imprimen flexibilidad, dado que es posible utilizarlos indistintamente del protocolo IP gracias al formato que manejan.

Respecto al software que implementa los protocolos del nivel de aplicación

- El desarrollo de las aplicaciones IPv6 requiere consideraciones especiales, dado que el Application Programming Interface (API) de comunicaciones para el desarrollo cambia para soportar el protocolo IPv6; sin embargo, la mejor opción es construir aplicaciones independientes al protocolo sobre el cual van a trabajar.
- Teniendo en cuenta los lineamientos para la construcción de aplicaciones orientadas hacia IPv6 es posible desarrollar software que explote las características principales que este nuevo protocolo ofrece.
- A diferencia de Linux, los sistemas operativos como Windows 2000, XP, Server 2003 e Inclusive Server 2008 y Vista no cuentan con los

mecanismos apropiados para configurar un equipo que sirva como cliente de un servidor DNS con IPv6, pues gráficamente se aceptan direcciones sólo de 32 bits y mediante consola aparentemente se pueden agregar los de 128 bits, más sin embargo su funcionamiento no es el esperado para Windows 2000 y XP, ya que no fueron diseñados para soportar este protocolo.

- Existe gran cantidad de aplicaciones que implementan este protocolo, aunque es de notar que la mayoría son producidas para el sistema operativo Linux, entre los que se encuentran no sólo paquetes fundamentales como los de servicios canónicos, sino también de aplicaciones multimedia como videoconferencia, chat, y otros servicios de valor agregado, lo cual muestra el auge y el momento clave por el que se está atravesando.
- Existen mecanismos de coexistencia entre aplicaciones que manejan diferentes pilas de protocolos que pueden ser de gran utilidad en el periodo de transición.
- Gracias a los esfuerzos de las empresas productoras y desarrolladores de software de comunicaciones, la transición para la UCC no debería suponer un gran trauma, dado que la mayoría de las aplicaciones utilizadas cuentan con soporte IPv6.

Recomendaciones

- Se recomienda la conformación de un grupo institucional que propenda por darle continuidad a la investigación sobre el protocolo IPv6 en la Universidad Cooperativa de Colombia, seccional Popayán, utilizando como herramienta base la conjunción de todo el conocimiento adquirido en cada una de las entidades investigadoras que en torno a esta temática han aportado en la Universidad.
- Sería conveniente hacer una implementación real de los servicios tratados en este trabajo de grado, en equipos que ofrezcan la capacidad técnica para brindar soporte de dichos servicios a toda la comunidad universitaria, dado que actualmente todos ellos se encuentran alojados en un mismo equipo.
- El desarrollo de este proyecto de grado deja abierta la posibilidad de futuros trabajos relacionados con esta tecnología, enfocados en el análisis e implementación de servicios que exploten las nuevas características que brinda el protocolo IPv6, como: servicios de tiempo real, calidad de servicio y Mobile IPv6, al igual que el desarrollo de herramientas propietarias para que, de esta manera, la tecnología no sea solamente adquirida, sino que también sea generada.
- Debido a que en RENATA existe un grupo de trabajo alrededor de IPv6 que tiene como objetivo coordinar esfuerzos para lograr una eficaz y pronta adopción del protocolo IPv6, es de gran importancia el acercamiento de la Universidad Cooperativa de Colombia, seccional Popayán, a este grupo de trabajo para intercambiar experiencias e impulsar a nivel nacional la adopción de esta tecnología.

Referencias

Arroyo, R. (2008, agosto), "La lenta adopción de IPV6 [en línea]", en *La actualidad tecnológica al minuto*, disponible en: http://www.vnunet.es/es/vnunet/report/2008/08/22la_lenta_adopcion_de_ipv6, recuperado: 10 de octubre del 2008.

Carrasco, S. (2008, 5 de junio), "IPV6: ¿Qué está retrasando su implantación? ¿Qué ventajas supone?" [en línea], en *Derecho y Nuevas Tecnologías*, disponible en: http://www.derechonntt.com/?p=142, recuperado: 15 de septiembre del 2008.

Castro, E. (s.f.), "Porting applications to IPv6 How To" [en línea], disponible en: http://jungla.dit.upm.es/~ecastro/IPv6-web/ipv6.html, recuperado: agosto del 2008.

Delgado, R. (2004, octubre), "Nuevo Internet (IPV6). Implicaciones en economía emergentes" [en línea], *Info Citel,* núm. 4, disponible en: http://www.oas.org/en/citel/infocitel/2004/octubre/internetv6_e.asp, recuperado: 20 de agosto del 2008.

Larrabeiti, D. et ál. (2008, octubre), "Redes activas con IPV6, [en línea]", en *Revista Net Work World*, disponible en: http://www.idg.es/comunicaciones/articulo.asp?id=117863, recuperado: 10 de noviembre del 2008.

Nuñez, J. (s.f.), "Descripción del servicio DNS" [en línea], disponible en: http://es.tldp.org/htmls/manuales.html, recuperado: 10 de septiembre del 2008.

Palet, J. (2008, octubre), "¿Por qué es importante su implementación?" [en línea]", en *Portal IPv6 Lacnic*, disponible en: http://portalipv6.lacnic.net/es/ipv6/novedades/por-qu-es-importante-su-implementaci-n, recuperado: 15 de noviembre del 2008.

Renata (2008, agosto), "Implementación de ipv6 en Renata" [en línea], *Comunicaciones Renata*, disponible en: http://www.renata.edu.co/ipv6.html?start=2, recuperado: 20 de septiembre del 2008.

Rocha, M. C. (s.f.), "Nuevo portal IPv6" [en línea], en *Lacnic News*, vol. 2, núm. 5, disponible en: http://www.lacnic.net/sp/sobre-lacnic/newsletter/005/ipv6_nuevo_portal.html, recuperado: 13 de agosto del 2008.

Royce, W. (s.f.), "Modelo lineal secuencial" [en línea], disponible en: http://members.fortunecity.es/odi39/modelo.htm, recuperado: 22 de septiembre.

Secretaría de Agricultura, Ganadería, Desarrollo Rural, Pesca y Alimentación (Sagarpa). (2008), "Metodología de evaluación" [en línea], disponible en: http://www.ruta.org/documentos_no_indexados/tallerSAGARPA/22oct2008/metodologiadeevaluacion.pdf, recuperado: 22 de octubre del 2008.

Smaldone, J. (s.f.), "Introducción a Secure Shell, versión 0.20" [en línea], disponible en: http://es.tldp.org/htmls/tutoriales.html, recuperado: diciembre del 2008.