Tecnura
ISSN: 0123-921X
tecnura@udistrital.edu.co
Universidad Distrital Francisco José de Caldas
Colombia

Guevara Peña, Alexis
Nivel de desempeño en redes IPv4 con respecto a redes IPv6 con MPLS y RSVP
Tecnura, vol. 15, núm. 28, enero-junio, 2011, pp. 123-133
Universidad Distrital Francisco José de Caldas
Bogotá, Colombia

Nivel de desempeño en redes IPv4 con respecto a redes IPv6 con MPLS y RSVP

Level network performance with respect to IPv4 IPv6 networks with MPLS and RSVP

Alexis Guevara Peña
Ingeniero Electrónico. Estudiante de la Maestría en Ciencias de la Información y las Comunicaciones de la Universidad Distrital Francisco José de Caldas. Bogotá, Colombia. aguevarap@correo.udistrital.edu.co

Clasificación del artículo: revisión (Recreaciones)

Fecha de recepción: agosto 16 de 2010 Fecha de aceptación: noviembre 23 de 2010

Palabras clave: Ingeniería de Tráfico, IPv4, IPv6, MPLS, RSVP.

Key words: Traffic Engineering, IPv4,IPv6, MPLS, RSVP.

Resumen

Este documento contiene información pertinente sobre el estado del arte de la Ingeniería de Tráfico (TE) MPLS (Multiprotocol Label Switching) y RSVP (Resource Reservation Protocol); también es importante como caso de estudio y porque da a conocer las técnicas utilizadas bajo la nueva versión de IPV6, en comparación con la versión IPV4. El objetivo es que sirva como marco de referencia para el estudio de la TE basada en la nueva versión de IPV6, específicamente en redes MPLS y RSVP, teniendo en cuenta las consideraciones pertinentes a la hora de tomar decisiones con respecto a la estabilidad del *backbone* y siendo la clave para proveedores de servicios de Internet que recientemente han estabilizado su infraestructura con IPV4.

Abstract

This paper contains relevant information of the state of art of traffic engineering, MPLS (Multiprotocol Lable Switching) and RSVP (Resource Reservation Protocol), as a case study and the techniques used under the new version of IPV6, against IPV4 version. The paper is intended to serve as a framework for the study of Engineering Traffic Based on the new version of IPV6, specifically MPLS and RSVP, taking into account relevant considerations necessary when making decisions regarding the stability of the Backbone remains the key to Internet service providers that have recently stabilized its IPv4 infrastructure.

* * *

1. Introducción

El aumento exponencial de número de equipos, la cantidad de tráfico generado y el número de enlaces son buenos indicadores para mostrar el impresionante crecimiento de Internet; por otra parte, se espera que éste ofrezca nuevos servicios de telecomunicaciones que requieran nodos de conmutación de alta velocidad y que, además, garanticen la Calidad de Servicio (QoS) [1][2].

Actualmente, Internet ofrece un servicio *best-effort* sin garantía de QoS, por lo que se han diseñados varios protocolos con el fin de proporcionar un servicio adecuado y con requerimientos temporales pare el tráfico [3][4].

RSVP (Resourse Reservation Protocol) es un protocolo de señalización que provee reserva de recursos de red siendo un modelo de servicios integrados para flujos individuales y agregados [5] [6]. En cada nodo, la reserva de ancho de banda se mantiene mediante un algoritmo de planificación de servicios como el WFQ (Weighted Fair Queueing) [7]. Fundamentalmente, los servicios integrados se dividen en dos tipos: garantía del servicio [8][9] y carga controlada [10]. La garantía del servicio es lo más parecido a una emulación de circuito virtual, limitando el retardo extremo a extremo, debido a encolamientos y asegurando la disponibilidad del ancho de banda durante la transmisión. Por otra parte, el servicio de carga controlada ofrece una QoS parecida a la que ofrece el *best-effort* en una red, pero no asegura ningún tipo de límite en los retardos de extremo a extremo.

Los servicios diferenciados [11][12][13] fueron propuestos por la IETF (Internet Engineering Task Force) para resolver los problemas de escalabilidad, proporcionando un método simple de priorizar el tráfico usando etiquetas cortas. Éstos tienen la ventaja de mover la complejidad hacia los extremos de la red. De esta forma, los paquetes de datos se pueden etiquetar y agregar a los *routers* de los extremos, basándose en los perfiles de tráfico. Posteriormente, los *routers* de la red troncal pueden transportar paquetes de acuerdo a las etiquetas sin la necesidad de examinar con detalle las cabeceras individuales de los paquetes [14][15][16].

MPLS (Multi Protocol Label Switching) [17] es una técnica de transporte basada en el intercambio de etiquetas y facilita la introducción de TE [8]. Las redes con Ingeniería de Tráfico pueden garantizar ancho de banda para varios flujos de tráfico, lo cual es una condición necesaria para poder proveer Calidad de Servicio en redes. La QoS es la denominación común que se le da a los mecanismos de Calidad de Servicio aplicados en el ámbito de las redes de datos. Éstos permiten manipular características específicas del tráfico en la red, de manera que se satisfagan las necesidades de servicio de ciertas aplicaciones y usuarios, sujetas a las políticas de calidad definidas para dicha red [13].

La Ingeniería de Tráfico es una disciplina de la Ingeniería de Redes, dirigida a optimizar el rendimiento de las redes en operación; abarca la aplicación de tecnología y principios científicos para la medida, modelaje, caracterización y control de tráfico de Internet [11] [14]; incluye la aplicación de conocimientos y de técnicas para lograr objetivos de desempeño específicos, tales como la optimización del uso de los recursos de la red mediante el apoyo provisto por herramientas para la medición/planificación de la capacidad y la distribución del tráfico, y el suministro de funciones para recuperación rápida en caso de fallas de un nodo o enlace en la red [18][19] [20].

Las causas de congestión de una red pueden deberse a la insuficiencia de recursos (por ejemplo, capacidad de los enlaces IPv4) y la utilización ineficiente de los recursos debido al mapeado del tráfico [17]. En el primer caso, con ampliar la capacidad de

los canales se podría resolver el problema; en el segundo caso, se puede solucionar utilizando de manera integral IPv6, diseñado por Steve Deering de Xerox PARC y Craig Mudge, éste está destinado a sustituir al estándar IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India y otros países asiáticos densamente poblados.

El nuevo estándar mejoraría el servicio globalmente; por ejemplo, proporcionando a futuro celdas telefónicas y dispositivos móviles con sus direcciones propias y permanentes. Actualmente, se calcula que las dos terceras partes de las direcciones que ofrece IPv4 ya están asignadas.

La adopción de IPv6 ha sido frenada por la Traducción de Direcciones de Red (NAT), que alivia parcialmente el problema de la falta de direcciones IP. Pero NAT hace difícil o imposible el uso de algunas aplicaciones P2P, como la Voz sobre IP (VoIP) y juegos multiusuario. Además, NAT rompe con la idea originaria de que en Internet todos pueden conectarse con todos.

Actualmente, IPv6 cuenta con un pequeño porcentaje de las direcciones públicas de Internet que todavía están dominadas por IPv4. El gran catalizador de IPv6 es la capacidad de ofrecer nuevos servicios, como la movilidad, QoS, privacidad, etcétera.

2. Ingeniería de Tráfico

La TE abarca la optimización del desempeño de redes en operación [14] [18]. En la práctica, TE significa asignar y distribuir flujos de tráfico IP en la topología física existente de la manera más efectiva posible para cumplir con objetivos operacionales deseados. Los objetivos de optimización pueden ser logrados a través de la gestión de capacidad y recursos, y de tráfico [17].

La gestión de capacidad incluye planificación de capacidad, control de enrutamiento y gestión de recursos. Los recursos de red de particular interés incluyen ancho de banda, espacio en *buffer* y recursos computacionales. [17] La gestión de tráfico incluye funciones de control de tráfico nodal, tales como condicionamiento del tráfico, gestión de colas y servicio de colas (*scheduling*) y otras funciones que regulan el flujo de tráfico a través de la red o arbitran el acceso a los recursos de la red [19].

El proceso de Ingeniería de Tráfico contempla la intervención de un Ingeniero de Tráfico que puede ser una persona o un autómata (sistema de gestión, etc.)[20]. Éste formula una política de control, observa el estado de la red a través del sistema de monitoreo, caracteriza el tráfico y aplica acciones de control para llevar la red al estado deseado de acuerdo con la política de control [19]. Esto puede ser reactivamente, realizar acciones en respuesta al estado actual de la red, o proactivamente, usando técnicas que le permitan predecir el estado de la red y así aplicar acciones para evitar los estados futuros indeseables [21].

Lo ideal es que las acciones de control involucren la modificación de parámetros de gestión de tráfico, de parámetros asociados con el enrutamiento y/o de atributos y restricciones asociados con recursos [20]. El nivel de intervención manual, involucrado en el proceso de TE, debería ser minimizado en lo posible. Esto se puede lograr automatizando aspectos de las acciones de control descritas anteriormente, de manera distribuida y escalable, mediante un sistema de gestión, aunque esto no es sencillo de realizar [18].

3. Multiprotocol Label Switching (MPLS)

La IETF creó el grupo de trabajo MPLS en 1997, para estandarizar el paradigma de conmutación por etiqueta que integra la conmutación de capa 2 con el enrutamiento de capa 3, como funcionalidad para el núcleo de una red [14]. En MPLS el dispositivo que

integra las funciones de enrutamiento y conmutación se denomina Label Switched Router (LSR). Una característica clave de esta tecnología es la separación de los componentes de control y envío en un LSR.

Los LSR construyen y mantienen tablas de reenvío, basándose en la información de control que pueden recibir a través de los protocolos de enrutamiento y de distribución de etiquetas. La separación de los componentes de control y de envío permite que cada componente se desarrolle y modifique independientemente [22]. A diferencia del caso de los dispositivos de enrutamiento (coincidencia con el prefijo más largo), en MPLS el proceso de envío se simplifica, haciendo un indexado directo en una tabla de reenvío. Ese comportamiento se consigue utilizando una etiqueta corta de longitud fija que identifica un circuito virtual entre dos LSR vecinos, por lo que su significado es local y no global, como en el caso de una dirección IP.

MPLS se diseñó para usarse sobre cualquier medio y encapsulación de capa 2 [14]. Para los protocolos de capa 2 que no soportan etiquetas, como es el caso de PPP o Ethernet, sumado a que la mayoría de las encapsulaciones de capa 2 están basadas en tramas, MPLS inserta la etiqueta de 32 bits entre las cabeceras de capa 2 y capa 3, lo que se denomina Frame-Mode MPLS. ATM es un caso especial donde las celdas de longitud fija no permiten la inserción de una etiqueta en cada paquete. En este caso, MPLS codifica la etiqueta local en el valor de los campos VPI/VCI (Virtual Path Identifier/Virtual Channel Identifier) de la cabecera ATM, lo que se denomina Cell-Mode MPLS.

La esencia de la funcionalidad de MPLS es que el tráfico es agrupado en Clases Equivalentes de Envío (FEC). Un grupo de paquetes que reciben el mismo tratamiento de envío pertenecen a la misma FEC [11]. La asignación de etiquetas se refiere al proceso de asignar una etiqueta y asociarla a una FEC [14]. La asignación de etiquetas se puede realizar por tráfico de control (por topología o por solicitud) o por tráfico de datos (por tráfico).

3.1. Funcionamiento

Una red MPLS consiste en un grupo de nodos (LSR) capaces de conmutar y enrutar paquetes basados en una etiqueta añadida a cada uno [16]. Las etiquetas definen un flujo de paquetes entre dos puntos finales o, en el caso de *multicast*, entre un punto terminal fuente y un grupo de puntos terminales destino [12]. Para cada flujo de tráfico distinto, denominado FEC, se define un canal específico en la red; por esta razón, MPLS está orientada a conexión. Con cada FEC se asocia la caracterización de un tráfico que define los requerimientos de QoS para ese flujo [8].

El LSR no necesita examinar o procesar el encabezado IP sino simplemente reenviar cada paquete basado en el valor de la etiqueta, por esta razón el proceso de reenvío es más simple que en IP. En el momento de que un determinado flujo de tráfico ingresa a un dominio MPLS, éste debe ser asignado a una FEC. Para el enrutamiento y entrega de paquetes en una FEC, debe establecerse previamente un Label Switched Path (LSP), el cual debe satisfacer ciertos parámetros de QoS, cuyos parámetros determinan cuántos recursos se van a comprometer para ese camino (ancho de banda) y qué políticas de puesta en cola y de descarte se van a establecer en cada LSR para esta FEC [14]. Con el fin de ejecutar estas tareas se utilizan dos protocolos para intercambiar la información necesaria entre *routers*:

a) Protocolos de Enrutamiento Interior (IGP), tal como OSPF o IS-IS, que permiten intercambiar información de enrutamiento y de la topología de la red [8].

b) Un protocolo de señalización cuyas funciones son coordinar la distribución de etiquetas, prevenir lazos, crear LSP bajo enrutamiento explícito, reservar ancho de banda y aplicar Clase de Servicio (DiffServ) [16].

Los protocolos de señalización actualmente utilizados en MPLS son: Label Distribution Protocol (LDP), Resource Reservation Protocol-Tunnelling Extensions (RSVP-TE), Border Gateway Protocol-Traffic Engineering (BGP4-TE), Constraint Based Routing-LDP (CR-LDP) [23].

Un paquete entra al dominio MPLS a través de un Edge LSR (E-LSR) de ingreso, el cual procesa el paquete para determinar los servicios de red que requiere, definiendo su QoS [14]. El E-LSR asigna el paquete a una FEC particular, agrega la etiqueta apropiada al paquete y lo reenvía. Si aún no existe un LSP para esa FEC, el E-LSR debe cooperar con los otros LSR para definir el nuevo LSP. Dentro del dominio MPLS, cada LSR al recibir un paquete etiquetado, remueve la etiqueta entrante, inserta la etiqueta saliente y envía el paquete hacia el próximo LSR a lo largo del LSP. El E-LSR de salida remueve la etiqueta, lee la cabecera del paquete IP y reenvía el paquete a su destino final [23].

En el dominio MPLS, el plano de control mantiene el contenido de la tabla de reenvío por etiquetas o Label Forwarding Information Base (LFIB) [16]. El plano de reenvío es el encargado de reenviar los paquetes etiquetados y está basado en la dirección destino o las etiquetas; es un simple mecanismo de reenvío y es independiente de los protocolos de enrutamiento y de intercambio de etiquetas. La LFIB es la utilizada para reenviar los paquetes basado en las etiquetas.

La FEC para un paquete puede ser determinada por una o cierta cantidad de parámetros, entre los cuales se encuentran: las direcciones IP de *host* origen o destino, las direcciones IP de red origen o destino, números de puerto origen o destino, ID (Identificador) del protocolo IP, Código de Servicios Diferenciados (Differentiated Services Codepoint), Etiqueta de flujo IPv6 [11]. En un LSR, para una FEC dada, puede definirse un Per Hop Behavior (PHB), éste define la prioridad de encolamiento de los paquetes, así como la política de descarte.

Los paquetes enviados entre los mismos puntos finales pueden pertenecer a diferentes FECs [17]. De allí, los paquetes pueden ser etiquetados de forma diferente, experimentar un PHB diferente en cada LSR y seguir otros caminos a través de la red.

MPLS ofrece reserva de recursos, tolerancia a fallos y optimización de recursos durante la transmisión [20] [24]. La combinación de MPLS y Servicios Diferenciados e Ingeniería de Tráfico (DiffServ-TE) reúne sus ventajas para proporcionar QoS mientras se optimiza la utilización de recursos de la red [20]. Entre las características de MPLS para proporcionar TE están: establecimiento de rutas explícitas (caminos físicos a nivel LSPs), generación de estadísticas de uso LSPs, información que podría utilizarse para planificación y optimización de la red, flexibilidad en la administración de la red y se puede usar enrutamiento restringido [14].

El Ruteo Basado en Restricciones, Constraint Based Routing (CBR), busca caminos entre puntos de la red que satisfagan un conjunto de restricciones explícitas. Éstas pueden ser, por ejemplo, que las pérdidas sean menores que un cierto valor y/o que el retardo extremo a extremo sea menor que 100 ms y/o que exista un ancho de banda mínimo. Sin embargo, se ha observado [17] que el CBR, para casi cualquier problema real, es un problema NP-completo. Por esta razón, se han propuesto múltiples algoritmos heurísticos subóptimos para realizar CBR [15].

El balanceo de carga (*load balancing*) plantea el problema de dividir el tráfico de un agregado de flujos entre diversos caminos basados en algún criterio de optimización de la red [15] [23].

4. Protocolos de Internet: IPv4 vs. IPv6

El siguiente Cuadro resume las principales características funcionales comparativas entre los protocolos IPv4 e IPv6.

Tabla 1. Resumen comparativo entre los protocolos de Internet IPv4 e IPv6.

Protocolo IPv4	Protocolo IPv6
Espacio de direcciones de 32 bits, es decir $2^{32} \sim 4.2x10^9$ direcciones IP posibles. Espacio de direcciones de 128 bits, es decir 2128 ~ .4x1034 direcciones IP posibles.	Espacio de direcciones de 128 bits, es decir $2^{128} \sim 3.4x10^{34}$ direcciones IP posibles.
Configuración Manual o Dinámica (DHCP).	Configuración "Plug & Play", Manual o Dinámica (DHCPv6).
Políticas de calidad de servicio se realizan a través del campo Tipo de Servicio (ToS) del paquete IP.	Políticas de Calidad de Servicio se realizan a través de los campos Etiqueta de Flujo y Clase de Tráfico.
Seguridad es algo opcional, a través del parche IPSec.	Seguridad extremo-a- extremo implementada en forma nativa.
Protocolo no escalable.	Protocolo escalable.

Dentro de las características funcionales de IPv6, podemos mencionar que el encabezado de un paquete presenta un diseño más simple que en el caso de IPv4. Además de definirse un largo encabezado fijo, el número de campos se ha reducido. [24].

4.1. Mecanismo de transición: IPv4 a IPv6

La situación que implica migrar a IPv6 la Internet actual, que está basada en IPv4, ha sido abordada a través de diversos mecanismos de transición. El RFC 2893 [25] describe dos aproximaciones, que pueden usarse separadas o en conjunto, para integrar gradualmente *hosts* y *routers* IPv6 dentro de un mundo IPv4: *Double-Stack* y *Tunnelin*g.

El primer mecanismo, *Double-Stack*, se ve conceptualizado en el modelo TCP/IP de la Figura 1, en donde los nodos IPv6 tienen además una completa implementación de IPv4.

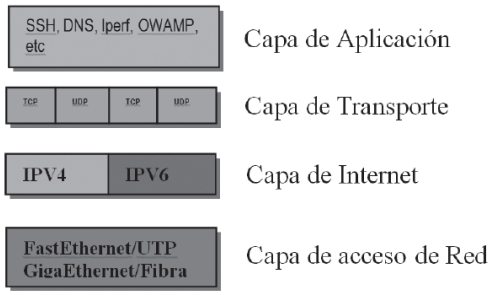

Figura 1. Modelo TCP/IP Double-Stack.

El segundo mecanismo, es conocido como *tunneling* o tunelización. En éste, dos *routers* IPv6 que están interconectados a través de *routers* IPv4, se comunican entre sí utilizando paquetes IPv6 a través del establecimiento de un túnel entre ambos. El conjunto de *routers* IPv4 intermedios pasan a ser parte del túnel.

5. Resource Reservation Protocol (RSVP)

RSVP se ha diseñado [28] [29] para permitir a los emisores, receptores y *routers* de las sesiones de comunicación (tanto *multicast* como *unicast*) comunicarse con el resto para establecer una ruta que pueda soportar la calidad de servicio requerida. Ésta viene especificada en un *flowspec*.

RSVP identifica una sesión por medio de una dirección de destino, un tipo de protocolo de transporte y un número de puerto de destino. RSVP no es un protocolo de encaminamiento, se usa exclusivamente para reservar recursos a través de la ruta que se establezca por cualquiera de los protocolos de niveles inferiores.

Existe un *draft* del protocolo del IETF [29]. Además hay un proyecto para una nueva versión del protocolo RSVP2 de la *University of Southern California/ Information Sciences Institute*, [30] al igual que varias implementaciones [31] de libre distribución para Linux, FreeBSD, etcétera.

Aunque RSVP en principio sólo era un protocolo de reserva de recursos, se describen las especificaciones de flujos utilizadas en una implementación [26] [27] de este protocolo, así como su control de admisión.

Éste incorpora un protocolo de mensajes con refresco periódico para mantener un estado de los *router*es intermedios para proporcionar fiabilidad y seguridad. Para ello, cada entrada en el *router* tiene un contador asociado que cuando llega a cero se elimina la conexión. Para que esto no ocurra, las rutas activas tienen que recibir un refresco por medio del mensaje *Path* a intervalos regulares. Este período debe ser bastante menor que el tiempo de los contadores de limpieza para que no produzcan desconexiones innecesarias.

Aparte de la eliminación de las rutas de forma automática, RSVP incluye el mensaje *PathTear* para eliminar la ruta de forma activa.

5.1. Mensajes de establecimiento de ruta

Los mensajes primarios usados por RSVP son el mensaje *Path*, que tiene su origen en el emisor y el mensaje Resv, que inicia en el receptor.

- Mensaje *Path*: lo primero que realiza es verificar el estado del encaminamiento inverso a través de la ruta y, como segunda medida, proporciona a los receptores información sobre las características del tráfico a enviar y de la ruta para que se puedan hacer las peticiones de reserva adecuadas [32] [33].

- Mensaje Resv: realiza las peticiones de reserva a los *routers* a lo largo del árbol de distribución entre receptores y emisores.

Los mensajes viajan o son transportados dentro del datagramas IP usando el protocolo número 46 (en otros sistema se tendrá que utilizar UDP).Éstos se envían de vuelta por la ruta que ha recorrido. Por cada *router* que pasa de vuelta, los mensajes se pueden fusionar con otros mensajes Resv con la misma interfaz, de acuerdo a una serie de reglas que dependen del estilo de reserva, obteniendo un nuevo *Flowspec* y *Filterspec*. Cada *router* realiza, además, las siguientes acciones:

- El *Flowspec* se pasa al módulo de control del tráfico que aplica el control de admisión para determinar si la reserva se acepta.

- Si la reserva es denegada, se envía un mensaje ResvErr.

- Si la reserva es aceptada, el estado de las reservas se actualiza de acuerdo con los parámetros, *Filterspec* y *Flowspec*. La reserva puede ser mezclada con otras reservas, teniendo en cuenta y estableciendo el tipo de reserva realizada con el fin de crear un nuevo mensaje de ésta [37] [38][39].

5.2. Término slack

El receptor genera un Rspec en el mensaje Rserv, es allí cuando se incluye el término *slack*, *S(ms),* el cual inicialmente arranca en cero. *S* establece el límite del retraso el cual estará por debajo que puede ser necesario para activar la aplicación, al asumir que cada equipo enrutador, reserva un ancho de banda, determinado *R*. Lo que permite este término es mantener,de una manera más flexible, la comunicación de los *routers* en el momento de realizar sus diferentes reservas locales [42][44].

5.3. Tipos de encaminamiento para RSVP

Como hemos visto, el protocolo RSVP no es un protocolo de encaminamiento. Se debe dar a conocer los problemas que se presentan con el protocolo de encaminamiento que podrían resolverse mediante el uso de redes neuronales y lógica difusa [43][45] [46][47], se destacan los siguientes:

1. Establecer y verificar una ruta que pueda soportar la reserva de recursos.

2. Encontrar la mejor ruta que tenga la capacidad suficiente y disponible para un nuevo flujo de datos. Existen dos formas diferentes de encontrar esta ruta; una es la posible modificación de los protocolos de encaminamiento y gestionarlos de acuerdo a un mecanismo de control de tráfico. Alternativamente, el protocolo de encaminamiento podría ser rediseñado para proporcionar múltiples rutas alternativas y al realizar la reserva, éste podría intentarlo con cada una de las rutas [48].

3. Adaptarse a un fallo de ruta. Cuando un nodo falla, el encaminamiento adaptativo encontrará una ruta alternativa. El refresco periódico de RSVP automáticamente hará una reserva en la nueva ruta. Pero la nueva reserva puede fallar si no cuenta con capacidad suficiente la nueva ruta; creándose así un problema de dimensionamiento y calidad de la red, el cual no puede ser solucionado por los protocolos de encaminamiento o reserva [49].

4. Adaptarse a un cambio de ruta (sin fallo). Los cambios de ruta pueden ocurrir sin que se produzcan fallos; aunque RSVP podría adaptarse al fallo de ruta y usar la técnica de reparación descrita en el punto anterior, esta solución podría afectar la QoS. Esto podría ocasionar que si el control de admisión falla en la nueva ruta, el usuario observaría una degradación del servicio, debido a que la ruta original se encuentra aún funcional. Con el fin de evitar este problema, se recomienda realizar un mecanismo de fijado de rutas (*route pinning*) donde las rutas se mantienen fijas mientras sean viables [50].

RSVP es diseñado con el fin de que cualquier protocolo de encaminamiento que se encuentre disponible pueda trabajar sin modificación alguna.

6. Conclusiones

Los avances tecnológicos, acompañados QoS, requieren en este momento de grandes recursos a nivel de equipos y software especializado, con el fin de que Internet ofrezca un servicio más óptimo y puedan correr las diferentes aplicaciones requeridas por los usuarios, como Internet móvil, video, etcétera.

Es allí donde el estudio de los diferentes protocolos propuestos y la transición de IPV4 a IPV6 requieren de la convivencia y de la implementación incremental de garantías de QoS sobre redes IP. Su diseño está orientado a permitir el establecimiento de garantías para las diferentes aplicaciones, especialmente las de tiempo real, que serán cada vez más demandantes de recursos de red con calidad de servicio.

El protocolo RSVP usa una etiqueta de flujo con el fin de ofrecer mayor QoS bajo redes IPV6. También, se clasifican los flujos de datos que pueden circular por Internet según sus requerimientos en cuanto a reserva de recursos, de lo cual debe surgir un método eficiente para minimizar el costo de la transmisión de los datos, reduciendo la cantidad de información enviada mediante la reserva de recursos.

Referencias bibliográficas

[1] The Network Simulator – ns2, 2010 [En línea]. Disponible en: http://www.isi.edu/nsnam/ns/

[2] M. Hamdi, N. Mckeown "Scalable High – Speed Switches/Routers with QoS Support", *IEEE Comunications Magazine*, p. 61, diciembre 2000.

[3] Stardust. Com. White Paper – QoS Protocols & Architectures. [En línea]. Disponible en: http://www.gosforum.com

[4] F. Cerdan, J. Malgosa-Sanahuja, J. García-Haro, F. Burrull, F. Monzo-Sánchez, "Quality of service for TCP/IP traffic: an overview", *Proms 2000*. Poland: Cracow, octubre 2000.

[5] P. White, "RSVP and Integrate Services in the Internet: A Tutorial*", IEEE Comunications Magazine*, mayo 1997.

[6] R. Branden, E. L. Zhang, S. Berson, S. Herzog, S. Jamin, "Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification", *Request for Comments 2205. IETF*, septiembre 1997.

[7] A. Demers, S. Keshav, S. Shenker, "Analysis and Simulation of a Fair Queuing Algorithm", In *Internetworking: Research and Experience*, pp. 3-26, octubre 1999.

[8] M. Kodialam, T.Lacksham, "Minimum interference routing with applications to MPLS traffic engineering", *Proceedings of International Workshop on QoS*. Pennsylvania, junio 2000.

[9] S. Shenker, C. Partridge, R. Guerin, "Specification of Guaranteed Quality of Service", *RFC 2212*, septiembre 1997.

[10] J. Wroclawski, "Specification of the Controlled-Load Network Element Service", *RFC 2211*, septiembre 1997.

[11] "Overview and Principles of Internet Traffic Engineering", *RFC 3272*, mayo 2002.

[12] "An Architecture for Differentiated service", *RFC 2475*, diciembre 1998.

[13] "Definition of the Differentiated services field in the IPv4 and IPv6 Headers", *RFC2474*, diciembre 1998.

[14] "Requirements for Traffic Engineering Over MPLS", *RFC 2702*. septiembre 1999.

[15] "Applicability Statement for Traffic Engineering with MPLS", *RFC 3346*. agosto 2002.

[16] H. Brook, "Traffic Engineering with MPLS in the Internet", *IEEE Network*, marzo/abril 2002.

[17] B. Wang, X. Su, P. Chen, "A New Bandwidth Guaranteed Routing Algorithm for MPLS Traffic Engineering", *Communications, 2002. ICC 2002. IEEE International Conference*, vol. 2, pp.1001-1005, agosto 2002.

[18] N. Piedra, J. Chicaiza, J. López, J. García, *Study of the application of neural networks in the internet traffic engineering*. Madrid: institute of Information Theories and Applications FOI ITHEA Universidad Politécnica de Madrid, 2008.

[19] E. Calle, P. Vilá, J. Marzo, S. Cots, *Arquitectura del Sistema de Gestión del ancho de Banda y Protección (SGBP) para entornos de redes MPLS*. España: Instituto de Informática y Aplicaciones Universitat de Girona, 2002

[20] H. Wang, H. Xie, L. Qiu, R. Yang, Y. Zhang, A. Greenberg, Traffic *Engineering in Dynamic Networks*. Yale University: AT&T Labs-Research, Univ. of Texas at Austin, 2006.

[21] "Requirements for Inter-Area MPLS Traffic Engineering", *RFC 4105*, junio 2005.

[22] A. Bosco, R. Mameli, E. Manconi, F. Ubaldi, *Edge Distributed Admission Control for Performance Improvement in Traffic Engineered Net-works*. Roma: Ericson Lab Italy S.P.A., 2003.

[23] J. E. Neves, M. J. Leitao, L. B. Almeida, "Neural networks in B-ISDN flow control: ATM traffic prediction or Network modeling", *IEEE Communications Magazine*, octubre 1995.

[24] S. Deering, "Internet Protocol, Version 6 (IPv6)", *RFC 2460*, 1998.

[25] "Transition Mechanisms for IPv6 Hosts and Routers", *RFC 2893*, agosto 2000.

[26] E. Osborne, *Traffic Engineering With MPLS*. USA: Cisco System, 2003.

[27] P.P.White, "RSVP and Integrated Services in the Internet a tutorial", *IEEE Communications Magazine,* pp. 100-106, mayo1997.

[28] L. Zhang, S. Deering, D. Estrin, S. Shenker, D. Zappala, "RSVP : A New Resource Rservation Protocol". *IEEE Network Magazine,* septiembre 1993.

[29] IETF: "Internet Draft: Resource Reservation Protocol (RSVP)", *Versión 1 Functional Specification*, diciembre 1997.

[30] ReSerVation Protocol 2 (RSVP2), University of Southern California/Information Sciences Institute. [En línea]. Disponible en: http://www.ito.darpa.mil/Summaries95/D016--USC_ISI_ReSerVation2.html-size 6K-12-Sep-96 - English.

[31] E. A. Wan, "Time series prediction by using a connectionist network with internal delay lines", Stanford: University Stanford-Department of electrical engineering, 1994.

[32] M. Kodialam, T. Lacksham, "Minimum interference routing with applications to MPLS traffic engineering", Proceedings *of International Workshop on QoS*. Pennsylvania, junio 2000.

[33] Y. Donoso, R. Fabregat, *Ingeniería de Tráfico Aplicada a LSPs Punto – Multipunto en Redes MPLS*. Barranquilla (Colombia): Universidad del Norte, 2003.

[34] O. Castañeda, C. García, *Neuroplanificador de ATM Inalámbrico para predecir y comformar los Tráficos VBR Y ABR*. Instituto de Investigaciones Eléctricas, octubre 2004.

[35] F. Montesinos, D. Lopez, Á. Barriga, S. Sánchez, *Sistemas Difusos Para Control de Congestión y Calidad de Servicio en Internet*. España: RedIRIS, Red Española de I + D, 2004.

[36] Z. Ma, H. Wang, Y. Yang, A. Krishnamurthy, A. Silberschatz, *Traffic Engineering in MPLS and VPN Networks*. Yale University, Julio 2006.

[37] H. Abrahamsson, B. Ahlgren, J. Alonso, A. Andersson, P.Kreuger, *A Multi Path Routing Algorithm for IP Networks Based on Flow Optimisation*. SICS – Swedish Institute of Computer Science, 2002.

[38] M. Kodialam, T. V. Lakshman. *Minimum Interference Routing with Applications to MPLS Traffic Engineering*, Bell Laboratories, Lucent Technologies, diciembre 2002.

[39] T. Kenon, "Data Networks: Routing, Security, and Performance Optiization", *Capítulo 8: Quality of Service*, 2002.

[40] M. Pioro, D. Medhi, Routing, "Flow and Capacity Design in Communication and Computer Networks", *Capítulo 8: Fair Networks*, 2004.

[41] A. Hiramatsu, "ATM communications network control by neural networks", *IEEE Transactions on Neural Networks*, vol. 1, no. 1, marzo 1990.

[42] A. Feldmann, A. Greenberg,C. Lund, N. Reingold, J. Rexford, "NetScope: Traffic Engineering for IP Networks". *AT&T Lab,* marzo 2000.

[43] Y-K. Park, G. Lee, "Applications of neural networks in high-speed communication networks", *IEEE Communications Magazine*, octubre 1995.

[44] J. Villadangos, E. Magaña, "Garantía de la Calidad de Servicio Basada en la Predicción de Ancho de Banda". Universidad Pública de Navarra.

[45] E. Saad, D. Prokhorov, "Comparative Study of Stock Trend Prediction Using Time Delay, Recurrent and Probabilistic Neural Networks", *IEEE Transactions on Neural Networks,* noviembre 1998.

[46] M. Ibnkahla, "Aplication of Neural Networks to Digital Comunication – A Survey. National Polytechnic Institute of Toulouse", *EMSEEIHT*, 2, France: Rue Camichel, 31071 Toulouse Cedex,1997.

[47] A. Gustavo, B. Facundo, R. Claudia, T. Gonzalo, C. Ernesto, *Toma de decisiones difusa y predicción del comportamiento oponente*. Montevideo (Uruguay): Instituto de Computación, Facultad de Ingeniería, Universidad de la República, 2005.

[48] E.W.Knightly, H. Zhang, "Traffic Characterization and switch Utilization using a Deterministic Bounding Interval Dependent Traffic Model", *IEEE INFOCOM,* 1995.

[49] Visión y Principios de la Ingeniería de Tráfico en Internet, *RFC3272*, mayo 2002.

[50] S. Haykin, *Neural Networks: A Comprehensive Foundation. Englewood Cliffs,* New Jers