ESTUDIO Y CONFIGURACIÓN DE CALIDAD DE SERVICIO PARA PROTOCOLOS IPV4 E IPV6 EN UNA RED DE FIBRA ÓPTICA WDM

Sebastián Andrés Álvarez Moraga, Agustín José González Valenzuela
Universidad Técnica Federico Santa María
Avenida España 1680, Valparaíso
(56) 32 – 654300
salvarez@elo.utfsm.cl, agustin.gonzalez@elo.utfsm.cl

Resumen

En el presente escrito se aborda el tema de Calidad de Servicio para redes IP en las versiones 4 y 6, presentando una gama de herramientas existentes desarrolladas principalmente por Cisco, para los equipos Cisco Catalyst 3550 y Cisco Catalyst 2651.

Se resumen las características de cada mecanismo estudiado y se presentan resultados obtenidos en la utilización de éstos al momento de otorgar diferenciación a tráficos sensibles a factores presentes en las redes IP, tales como el ancho de banda y retardos de propagación.

Abstract

This work presents the subject of Quality of Service for IP networks in versions 4 and 6. It presents a range of existing tools, developed mainly by Cisco, for the Cisco 3550 Catalyst and Cisco Catalyst 2651 devices.

We summarize the characteristics of each studied mechanism, and the experimental results obtained in the use of these at the time of granting differentiation to traffics sensible to existing IP networks state, such as bandwidth and the propagation delays.

1.- Introducción

En las eventuales congestiones de enlaces que son parte del recorrido del tráfico entre dos equipos (host, o terminal) de distintas redes, cada paquete de información compite por un poco de ancho de banda disponible para poder alcanzar su destino. Típicamente, las redes operan en la base de entrega del mejor esfuerzo (irónicamente llamado WWW: World Wide Wait), donde todo el tráfico tiene igual prioridad de ser entregado a tiempo. Cuando ocurre la congestión, todo este tráfico tiene la misma probabilidad de ser descartado.

En ciertos tipos de datos que circulan por las redes hoy en día, por ejemplo tráficos con requerimientos de tiempo real (voz o video), es deseable que no ocurra pérdida de información, que exista un gran ancho de banda disponible, y que los retrasos en los envíos de estos paquetes de datos sean mínimos. Es por ello que surge la necesidad de aplicar Calidad de Servicio (QoS) en el nivel del transporte de datos, métodos de diferenciación de tráficos particulares con el fin de otorgar preferencia a estos datos sensibles.

Se entiende por "Calidad de Servicio", a la capacidad de una red para sostener un comportamiento adecuado del tráfico que transita por ella, cumpliendo a su vez con los requerimientos de ciertos parámetros relevantes para el usuario final. Esto puede entenderse también, como el cumplimiento de un conjunto de requisitos estipulados en un contrato (SLA: Service Level Agreement) entre un ISP (Internet Service Provider, proveedor de servicios de Internet) y sus clientes.

El protocolo de comunicación IPv4 (Internet Protocol Version 4) contiene especificaciones que permiten ejercer manipulaciones sobre estos paquetes, las cuales deben ser manejadas por los enrutadores al momento de implementar QoS. Sin embargo, en los últimos años, se han estado afinando detalles acerca de un nuevo estándar para el protocolo de Internet (IP), éste es llamado IPv6 (Internet Protocol Version 6), el cual contiene nuevas y reestructuradas especificaciones para ejercer QoS.

Al contar con QoS, es posible asegurar una correcta entrega de la información necesaria o crítica, para ámbitos empresariales o institucionales, dando preferencia a aplicaciones de desempeño crítico, donde se comparten simultáneamente los recursos de red con otras aplicaciones no críticas. QoS hace la diferencia, al prometer un uso eficiente de los recursos ante la situación de congestión, seleccionando un tráfico específico de la red, priorizandolo según su importancia relativa, y utilizando métodos de control y evasión de congestión para darles un tratamiento preferencial. Implementando QoS en una red, hace al rendimiento de la red más predecible, y a la utilización de ancho de banda más eficiente.

La Universidad Técnica Federico Santa María, a través de la adjudicación del proyecto FONDEF D00I1026 "Redes Ópticas para la Internet del Futuro" [i], montó una red de fibra óptica que la une con REUNA (Red Universitaria Nacional), utilizando la tecnología WDM (Wavelength Division Multiplexing), con el fin de experimentar con los protocolos IP y aplicaciones demandantes de ancho de banda. Utilizando esta plataforma de pruebas, compuesta por equipos Cisco para el enrutamiento de paquetes, se estudiaron y configuraron esquemas de QoS para distintos tipos de tráfico, para el actual protocolo IPv4, y para el naciente IPv6.

2.- Acercamientos de Calidad de Servicio

Si bien es posible encontrarse con variadas técnicas de implementación de QoS, todas ellas tienen en común la clasificación o diferenciación de flujos de tráfico, en grupos llamados clases.

Es probable que la mayoría de la gente, cuando se les habla de calidad de servicio, piense en clases de servicio diferenciadas, en conjunto quizá con algunos mecanismos para proveer políticas de

tráfico o control de admisión. La palabra clave en este tema es la diferenciación, debido a que antes de poder otorgar calidad de servicio a un cliente en particular, aplicación o protocolo, es necesario clasificar el tráfico en clases y determinar la forma en que serán manejadas estas clases de tráfico a medida que circula por la red.

Durante los últimos años han surgido variados métodos para establecer QoS en equipamientos de redes. Algoritmos avanzados de manejos de cola, modeladores de tráfico (traffic shaping), y mecanismos de filtrado mediante listas de acceso (access-list), han hecho que el proceso de elegir una estrategia de QoS sea más delicado. Cada red puede tomar ventaja de distintos aspectos en implementaciones de QoS para una obtener una mayor eficiencia, ya sea para redes de pequeñas corporaciones, empresas, o proveedores de servicios de Internet.

Existen tres modelos en los que se divide el despliegue de calidad de servicio:

a) **Servicio de Mejor Esfuerzo**. Se le llama servicio de mejor esfuerzo al que la red provee cuando hace todo lo posible para intentar entregar el paquete a su destino, donde no hay garantía de que esto ocurra. Una aplicación enviará datos en cualquier cantidad, cuando lo necesite, sin pedir permiso o notificar a la red. Éste es el modelo utilizado por las aplicaciones de Ftp y Http. Obviamente, no es el modelo apropiado para aplicaciones sensibles al retardo o variaciones de ancho de banda, las cuales necesitan de un tratamiento especial.

b) **Servicios Integrados**. El modelo de Servicios Integrados (IntServ: Integrated Services) provee a las aplicaciones de un nivel garantizado de servicio, negociando parámetros de red, de extremo a extremo. La aplicación solicita el nivel de servicio necesario para ella con el fin de operar apropiadamente, y se basa en la QoS para que se reserven los recursos de red necesarios antes de que la aplicación comience a operar. Estas reservaciones se mantiene en pie hasta que la aplicación termina o hasta que el ancho de banda requerido por ésta sobrepase el límite reservado para la aplicación. El modelo IntServ se basa en el Protocolo de Reservación de Recursos (RSVP) para señalizar y reservar la QoS deseada para cada flujo en la red. Debido a que la información de estados para cada reservación necesita ser mantenida por cada enrutador a lo largo de la ruta, la escalabilidad para cientos de miles de flujos a través de una red central, típicos de una red óptica, se convierte en un problema.

c) **Servicios Diferenciados**. Este modelo incluye un conjunto de herramientas de clasificación y mecanismos de cola que proveen a ciertas aplicaciones o protocolos con determinadas prioridades sobre el resto del tráfico en la red. DiffServ cuenta con los enrutadores de bordes para realizar la clasificación de los distintos tipos de paquetes que circulan por la red. El tráfico de red puede ser clasificado por dirección de red, protocolo, puertos, interfaz de ingreso o cualquier tipo de clasificación que pueda ser alcanzada mediante el uso de listas de acceso, en su variante para la implementación de QoS. Al utilizar el modelo DiffServ de obtienen varias ventajas. Los enrutadores operan más rápido, ya que se limita la complejidad de la clasificación y el encolado. Se minimiza el tráfico de señalización, y el almacenamiento. En DiffServ, se definen clases de servicio, cada flujo particular de datos es agrupado en un tipo de clase, donde son tratados idénticamente. Los enrutadores internos sólo están interesados del comportamiento por saltos (PHB: Per Hop Behavior), marcado en la cabecera del paquete. Esta arquitectura permite a DiffServ rendir mucho mejor en ambientes de bajo ancho de banda, y provee de un mayor potencial que una arquitectura IntServ.

Originalmente, para el protocolo IPv4 se diseñó el campo ToS (Type of Service) para capacitar el marcado de paquetes con un nivel de servicio requerido. Esta definición no se utilizó mayormente debido a la ambigüedad de su significado, por lo que más tarde se convirtió en el denominado campo DSCP (Differentiated Services Code Point). Este campo si tuvo una aceptación global y se asumió una interpretación estándar que permitió a las redes planificar metodologías basándose en ésta. Tal fue el éxito de esta nueva definición, que fue incluida para ofrecer las mismas ventajas en el protocolo IPv6 en el denomindo campo TC (Traffic Class).

Una vez que existe la capacidad de marcar los paquetes utilizando DSCP, es necesario proveer del tratamiento apropiado para cada una de estas clases. La colección de paquetes con el mismo valor DSCP circulando hacia una dirección determinada, es llamado Behavior Aggregate (BA). Es así como múltiples aplicaciones/fuentes, pueden pertenecer al mismo BA. El PHB se refiere a la programación, encolamiento, limitación y modelación del comportamiento de un nodo, basado en el BA perteneciente del paquete.

La Assured Forwarding (AF) PHB [ii], es la más utilizada en la arquitectura DiffServ. Dentro de esta PHB los 4 grupos AF (llamados clase AF1, AF2, AF3 y AF4 o clases Cisco), son divididos en 3 grupos "olímpicos": oro, plata y bronce, representando la tendencia a descartar paquetes. Cada paquete será entregado a una clase de servicio mientras se apegue a un perfil de tráfico. Cualquier exceso de tráfico será aceptado por la red, pero tendrá mayor probabilidad de ser descartado según la clase de servicio y grupo. Cada nodo con DiffServ, deberá implementar alguna forma de reservación de ancho de banda para cada clase AF, y alguna forma de otorgar prioridad para permitir políticas de esta índole.

3.- Métodos de Calidad de Servicio

Existen varios niveles en los cuales se puede proveer de calidad de servicio en una red IP. Uno de ellos es el de contar con una estrategia de manejo de los paquetes en caso de congestión, o el evitar que la red alcance este estado, descartando paquetes a medida que estos ingresan a la red.

El "manejo de congestión" es un término general usado para nombrar los distintos tipos de estrategia de encolamiento que se utilizan para manejar situaciones donde la demanda de ancho de banda solicitada por las aplicaciones excede el ancho de banda total de la red, controlando la inyección de tráfico a la red, para que ciertos flujos tengan prioridad sobre otros.

3.1.- Manejo de Congestión

a) **FIFO**. Es el tipo más simple de encolamiento, se basa en el siguiente concepto: el primer paquete en entrar a la interfaz, es el primero en salir. Es adecuado para interfaces de alta velocidad, sin embargo no para bajas, ya que FIFO es capaz de manejar cantidades limitadas de ráfagas de datos. Si llegan más paquetes cuando la cola está llena, éstos son descartados. No tiene mecanismos de diferenciación de paquetes.

b) **Fair Queuing**. FQ, generalmente conocida como WFQ (Weighted Fair Queueing), es un método automatizado que provee una justa asignación de ancho de banda para todo el tráfico de la red, utilizado habitualmente para enlaces de velocidades menores a 2048 [Mbps]. WFQ ordena el tráfico en flujos, utilizando una combinación de parámetros. Por ejemplo, para una conversación TCP/IP, se utiliza como filtro el protocolo IP, dirección IP fuente, dirección IP destino, puerto de origen, etc. Una vez distinguidos estos flujos, el enrutador determina cuáles son de uso intensivo o sensibles al retardo, priorizándolos y asegurando que los flujos de alto volumen sean empujados al final de la cola, y los volúmenes bajos, sensibles al retardo, sean empujados al principio de la cola. WFQ es apropiado en situaciones donde se desea proveer un tiempo de respuesta consistente ante usuarios que generen altas y bajas cargas en la red, ya que WFQ se adapta a las condiciones cambiantes del tráfico en la red. Sin embargo, la carga que significa para el procesador en los equipos de enrutamiento, hace de esta metodología poco escalable, al requerir recursos adicionales en la clasificación y manipulación dinámica de las colas.

c) **Priority Queuing**. El Encolamiento de Prioridad (PQ: Priority Queueing), consiste en un conjunto de colas, clasificadas desde alta a baja prioridad. Cada paquete es asignado a una de estas colas, las cuales son servidas en estricto orden de prioridad. Las colas de mayor prioridad son siempre atendidas primero, luego la siguiente de menor prioridad, y así. Si una cola de menor prioridad está siendo atendida, y un paquete ingresa a una cola de mayor prioridad, ésta es atendida inmediatamente. Este mecanismo se ajusta a condiciones donde existe un tráfico importante, pero puede causar la total falta de atención de colas de menor prioridad (starvation).

d) **Custom Queuing**. Para evadir la rigidez de PQ, se opta por utilizar Encolamiento Personalizado (CQ: Custom Queueing). Permite al administrador priorizar el tráfico sin los efectos laterales de inanición de las colas de baja prioridad, especificando el número de paquetes o bytes que deben ser atendidos para cada cola. Se pueden crear hasta 16 colas para categorizar el tráfico, donde cada cola es atendida al estilo Round-Robin. CQ ofrece un mecanismo más refinado de encolamiento, pero no asegura una prioridad absoluta como PQ. Se utiliza CQ para proveer a tráficos particulares de un ancho de banda garantizado en un punto de posible congestión, asegurando para este tráfico una porción fija del ancho de banda y permitiendo al resto del tráfico utilizar los recursos disponibles.

e) **Class-Based WFQ**. WFQ tiene algunas limitaciones de escalamiento, ya que la implementación del algoritmo se ve afectada a medida que el tráfico por enlace aumenta; colapsa debido a la cantidad numerosa de flujos que analizar. CBWFQ fue desarrollada para evitar estas limitaciones, tomando el algoritmo de WFQ y expandiéndolo, permitiendo la creación de clases definidas por el usuario, que permiten un mayor control sobre las colas tráfico y asignación del ancho de banda. Algunas veces es necesario garantizar una determinada tasa de transmisión para cierto tipo de tráfico, lo cual no es posible mediante WFQ, pero si con CBWFQ. Las clases que son posibles implementar con CBWFQ pueden ser determinadas según protocolo, ACL, valor DSCP, o interfaz de ingreso. Cada clase posee una cola separada, y todos los paquetes que cumplen el criterio definido para una clase en particular son asignados a dicha cola. Una vez que se establecen los criterios para las clases, es posible determinar cómo los paquetes pertenecientes a dicha clase serán manejados. Si una clase no utiliza su porción de ancho de banda, otras pueden hacerlo. Se puede configurar específicamente el ancho de banda y límite de paquetes máximos (o profundidad de cola) para cada clase. El peso asignado a la cola de la clase es determinado mediante el ancho de banda asignado a dicha clase.

f) **Low Latency Queuing**. El Encolamiento de Baja Latencia (LLQ: Low-Latency Queueing) es una mezcla entre Priority Queueing y Class-Based Weighted-Fair Queueing. Es actualmente el método de encolamiento recomendado para Voz sobre IP (VoIP) y Telefonía IP, que también trabajará apropiadamente con tráfico de videoconferencias. LLQ consta de colas de prioridad personalizadas, basadas en clases de tráfico, en conjunto con una cola de prioridad, la cual tiene preferencia absoluta sobre las otras colas. Si existe tráfico en la cola de prioridad, ésta es atendida antes que las otras colas de prioridad personalizadas. Si la cola de prioridad no está encolando paquetes, se procede a atender las otras colas según su prioridad. Debido a este comportamiento es necesario configurar un ancho de banda límite reservado para la cola de prioridad, evitando la inanición del resto de las colas. La cola de prioridad que posee LLQ provee de un máximo retardo garantizado para los paquetes entrantes en esta cola, el cual es calculado como el tamaño del MTU dividido por la velocidad de enlace.

3.2.- Evasión de Congestión

Las metodologías de evasión de congestión se basan en la manera que los protocolos operan, con el fin de no llegar a la congestión de la red.

Las técnicas de **RED** (Random Early Detection) y **WRED** (Weighted Random Early Detection) evitan el efecto conocido como Sincronización Global. Cuando múltiples conexiones TCP operan sobre un enlace común, todas ellas incrementaran el tamaño de su ventana deslizante a medida que el tráfico llega sin problemas. Este aumento gradual consume el ancho de banda del enlace, hasta congestionarlo. En este punto las conexiones TCP experimentan errores de transmisión, lo que hace que disminuyan su tamaño de ventana simultáneamente. Esto conlleva a una sincronización global, donde todos los flujos comienzan a incrementar su tasa de transmisión nuevamente para llegar a otro estado de congestión. Este ciclo es repetitivo, creando picos y valles en la utilización del ancho de banda del enlace. Es debido a este comportamiento que no se utiliza los máximos recursos de la red.

Los métodos de evasión de congestión tratan con este tipo de situación, descartando paquetes de forma aleatoria. RED fuerza a que el flujo reduzca el tamaño de su ventana de transmisión, disminuyendo la cantidad de información enviada. A medida que se alcanza el estado de congestión en la red, más paquetes entrantes son descartados con el fin de no llegar al punto de congestión en el enlace.

Lo que limita a estas técnicas de evasión de congestión es que sólo sirve para tráfico basado en TCP, ya que otros protocolos no utilizan el concepto de ventana deslizante.

3.3.- Modelamiento de Tráfico

Muchas veces es necesario limitar el tráfico saliente en una interfaz determinada, con el fin de administrar eficientemente los recursos de la red. Ante esta necesidad existen dos metodologías

de limitación de ancho de banda: Policing y Modelamiento de Tráfico (Traffic Shaping).

Mediante **Policing** se especifica la limitación a un máximo de tasa de transmisión para una clase de tráfico. Si este umbral es excedido, una de las acciones inmediatas será ejecutada: transmitir, descartar, o remarcar. En otras palabras, no es posible almacenar los paquetes para posteriormente enviarlos, como es el caso de TS.

Las técnicas de **Modelamiento de Tráfico** (Traffic Shaping) son un poco más diplomáticas en el sentido en que operan. En vez de descartar el tráfico que excede cierta tasa determinada, atrasan parte del tráfico sobrante a través de colas, con el fin de modelarla a una tasa que la interfaz remota pueda manejar. El resto del tráfico excedente es inevitablemente descartado.

Traffic Shaping (TS) es una buena herramienta en situaciones en las cuales el tráfico saliente debe respetar una cierta tasa máxima de transmisión. Este proceso es realizado independientemente de la velocidad real del circuito. Esto significa que es posible modelar tráficos de Web o Ftp a velocidades inferiores a las del receptor. TS puede hacer uso de las listas de acceso para clasificar el flujo y puede aplicar políticas restrictivas de TS a cada flujo.

Policing descarta o remarca los paquetes en exceso si es que sobrepasan el límite definido. El tráfico que se originado en ráfagas se propagan por la red, no son suavizados como en TS. Controla la tasa de salida mediante descarte de paquetes, por lo que disminuye el retardo por encolamiento. Sin embargo debido a estos descartes, el tamaño de la ventana deslizante de TCP debe reducirse, afectando el rendimiento global del flujo.

En varios casos es necesario utilizar una vía con la velocidad adecuada para transmitir un paquete de alta o baja prioridad. Por ejemplo, si se tienen dos enlaces, una con mayor velocidad que el otro, sería lógico plantear la metodología de transmisión de mejor esfuerzo para los paquetes de menor prioridad sobre el enlace de menor velocidad.

A este tipo de diferenciación se le denomina **Enrutamiento Basado en Políticas** (PBR: Policy Based Routing). La forma de implementarlo es mediante listas de acceso donde se selecciona el tráfico crítico. En la interfaz de ingreso de éste se adjunta un mapa de política, en el cual para el tráfico perteneciente a la lista de acceso creada, se plantea una nueva ruta a seguir (Next Hop) para llegar a su destino.

3.4.- Manipulación y Clasificación de Tráfico.

Para manipular los tráficos y otorgarles Calidad de Servicio, se utilizan los procedimientos básicos de clasificación y asignación de prioridad, denominados Mapas de Clase y Mapas de Política.

Un mapa de clase es un mecanismo para nombrar y aislar un flujo de tráfico específico. Éste define el criterio utilizado para comparar el tráfico para más tarde clasificarlo, el cual puede incluir selecciones mediante ACL estándar o extendida, una lista especifica de DSCP, o valores de Precedencia IP. Después que el paquete es confrontado al criterio del mapa de clase, es posible clasificarlo mediante el uso de mapas de política.

Un mapa de política específica en qué clase de tráfico actuará. Las acciones pueden ser confiar en los valores de CoS, DSCP o Precedencia IP de la clase de tráfico, establecer un valor específico de éstos, o especificar las limitaciones de ancho de banda y la acción a tomar cuando el tráfico cae fuera del perfil definido en el mapa de política. Antes que un mapa de política sea efectivo, debe adjuntarse a una interfaz.

4.- Pruebas Realizadas

4.1.- Escenario de Pruebas

En las pruebas presentadas a continuación, se utilizan dos equipos principales, que se encargan de enviar y enrutar los paquetes. El primero corresponde al Cisco Catalyst 3550, denominado **RS-IPv4-UTFSM**, y el segundo al Cisco Catalyst 2651, nombrado **R-IPv6-UTFSM**. Al igual que en la UTFSM, se encuentran dos ejemplares en REUNA y la UCHILE, denominados **RS-IPv4-REUNA**, **R-IPv6-REUNA** y **RS-IPv4-UCHILE**, **R-IPv6-UCHILE** respectivamente [iii].

En la subred ubicada en la UTFSM se cuenta con tres computadores, equipos denominados **Spock1, Spock2**, y **WDM1**, donde se encuentran instalados los sistemas operativos Microsoft Windows XP y Red Hat 7.0 con soporte IPv4 e IPv6. Estos equipos cuentan con tarjetas de red Ethernet de 10/100 Mbps, las cuales los interconectan con los **RS-IPv4-UTFSM** y **R-IPv6-UTFSM**, logrando acceso a la red del proyecto mediante la fibra óptica. También se utilizó de un equipo llamado **Boromir**, ubicado en la UCHILE para propósitos de generación de tráfico.

Además, se cuenta con el acceso a la red del proyecto mediante el establecimiento de un túnel IPv4 sobre IPv4, utilizando el protocolo GRE (Generic Routing Encapsulation), el cual circula por la red tradicional de Internet que posee la UTFSM. Mediante la utilización del túnel GRE es posible comparar los parámetros de ancho de banda, jitter y pérdida de paquetes entre una red de fibra óptica y una red Internet tradicional.

4.2.- Enrutamiento Basado en Políticas

Mediante esta prueba, se exponen las diferencias cuantitativas en la utilización del enlace de fibra óptica y el túnel GRE configurado. Se utilizó el host **Spock2**, para efectuar las mediciones de rendimiento utilizando IPv4 sobre el túnel. La idea es seleccionar el tráfico que genere este equipo hacia la red del proyecto, para que éste transite a través del túnel GRE en vez de hacerlo por la fibra óptica. De esta manera, es posible comparar en tiempo real, estadísticas de rendimiento y pérdida de paquetes, con otros equipos que cursan su tráfico a través del medio óptico en forma simultánea.

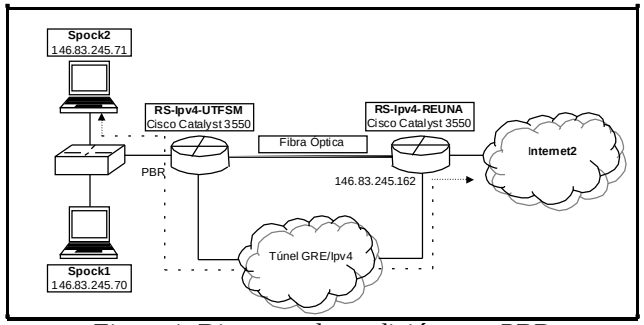

Figura 1. Diagrama de medición para PBR

En primer lugar, se configura en el enrutador **RS-IPv4-UTFSM**, una lista de acceso en la cual se selecciona como tráfico a tratar, todo aquel generado por el host **Spock2**. Una vez apartado el tráfico, se configura un mapa de ruta que se aplicará a los tráficos encontrados en la lista de acceso anterior. En este mapa de ruta se toma dicho tráfico, y se le asigna por defecto el siguiente salto (de enrutamiento) el extremo del túnel GRE ubicado en REUNA según se observa en la figura 1.

Después de haber efectuado estos cambios se comprobó mediante el comando **ping** y **traceroute**, que la ruta utilizada para alcanzar las redes pertenecientes a la red del proyecto, direcciones IP en REUNA y la UCHILE, tomaba 15 [ms] promedio en recorrer el enlace. Por lo tanto, comparando este comportamiento con el mismo comando efectuado desde **Spock1**, cuyo tiempo era de 2 [ms], se corroboró que la política de ruteo funcionaba correctamente.

Más tarde se utilizó la herramienta de video conferencia VRVS, para visualizar la cantidad de paquetes perdidos utilizando el enlace de túnel. Durante esta prueba, se observó que cerca de un 30% de los paquetes se perdían en el trayecto a REUNA, lo que se reflejaba en un audio y video entrecortado.

Sin bien los paquetes generados por **Spock2** estaban siendo enrutados por el túnel GRE, el tráfico de regreso continuaba transitando por la fibra óptica; era necesario reconfigurar a **RS-IPv4-REUNA** para que sus paquetes destinados a **Spock2** fuesen enrutados por el túnel.

En **RS-IPv4-REUNA**, se procedió a configurar de manera similar una lista de acceso y un mapa de ruta, de forma tal que todos los paquetes generados desde Internet2, con destino a **Spock2**, fuesen redirigidos hacia el túnel GRE.

Se utilizó nuevamente la herramienta VRVS, pero de forma distinta, es decir, los paquetes generados por **Spock2** hacia el reflector en Internet2 eran devueltos hacia este mismo, simulando así una conversación espejo, originada desde Internet2 y transitando por el túnel GRE en su regreso hacia **Spock2**. Fue posible observar que existía una pérdida media de un 5% de los paquetes al utilizar el túnel GRE, mientras que realizando la misma prueba de forma simultánea, utilizando la fibra óptica, la pérdida media fue de 0.0%.

De esta manera, se concluye que mediante PBR es posible asignar otras rutas de circulación para tráficos especiales, ya sea con el propósito en particular de seleccionar medios físicos distintos (como es este caso), o para decidir entre distintas vías existentes por las cuales debe circular un tráfico de una prioridad particular.

4.3.- Prioridad a Tráfico Multimedial

La siguiente prueba se diseño con el objetivo de evaluar la pérdida de paquetes y la variación del retardo para tráficos de alta prioridad (audio y video) al momento de existir congestión en una de las interfaces un enrutador particular debido a la utilización intensa del ancho de banda por tráficos no prioritarios (Ftp y Http).

Para la realización de esta prueba se utilizó el equipo **Spock1**, ubicado en la UTFSM, y el equipo **Spock2**, ubicado en REUNA. Además se configuró el equipo **RS-IPv4-UTFSM** con el fin de clasificar 4 tipos de tráfico distintos, cada uno especificado según protocolo UDP/TCP y puerto de destino. Estos flujos son originados desde **Spock2** en REUNA, son clasificados en la interfaz de entrada Gigabit Ethernet 0/1 del **RS-IPv4-UTFSM**, y son tratados con QoS en la interfaz de acceso a la subred UTFSM Gigabit Ethernet 0/12, donde serán evaluados los parámetros de ancho de banda, retardos y pérdida de paquetes para cada uno de ellos mediante **Spock1**.

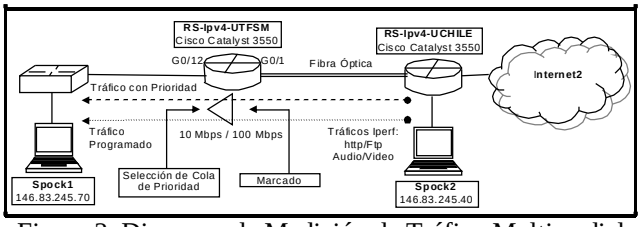

Figura 2. Diagrama de Medición de Tráfico Multimedial

La clasificación de los tráficos es la siguiente:

Protocolo	Puerto Destino	Tipo de Flujo	Limitación	Garantía
RTP/UDP	10000	Audio	1 [Mbps]	
HTTP/TCP	20000	Web	-	9/10 BW disponible
FTP/TCP	30000	Ftp	-	1/10 BW disponible
RTP/UDP	40000	Video	2 [Mbps]	

Tabla 1. Planificación de Servicio para Tráficos

Para generar el estado de congestión se limita la velocidad de transmisión de la interfaz de acceso a la red UTFSM, Gigabit Ethernet 0/12 a 10 [Mbps].

Más tarde se configura el mapa de política que limita la tasa de transferencia de los tráficos de Audio y Video, y asigna los valores DSCP respectivos a los tráficos Web y Ftp que seleccionan implícitamente una de las cuatro colas de egreso en la interfaz Gigabit Ethernet 0/12. Luego, la política es adjuntada en la interfaz de ingreso del **RS-IPv4-UTFSM**, Gigabit Ethernet 0/1, y se configura los pesos de las colas de salida y la cola de prioridad estricta en la interfaz de salida Gigabit Ethernet 0/12.

Los flujos son generados en **Spock2** mediante la herramienta Iperf. Se ejecuta el envío de tráfico de Audio durante 40 segundos a una tasa de 2500 [Kbps]. Durante el quinto segundo comienza en envío de tráfico Web. Durante el segundo 10 comienza el envío de tráfico Ftp, y durante el segundo 15, comienza el tráfico de Video a una tasa de 3600 [Kbps].

En **Spock1** se monitorea cada uno de estos tráficos a intervalos de un segundo, a medida que son enviados desde **Spock2**. Los resultados obtenidos en **Spock1**: ancho de banda, jitter, y pérdida de paquetes.

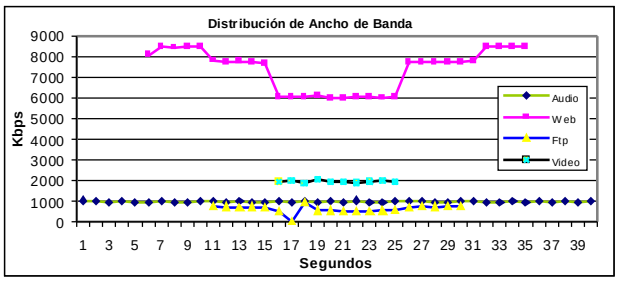

Gráfico 1. Distribución de Ancho de Banda

Mediante el gráfico de distribución de ancho de banda entre los distintos tráficos, se observa que los flujos de Video y Audio no presentan variaciones ante la presencia de tráficos consumidores de recursos como lo es el Web y Ftp. Por el contrario, los tráficos de menor prioridad se ajustan eficientemente al ancho de banda disponible, dividiendo dicho recurso en la proporción configurada mediante los pesos en las colas de egreso.

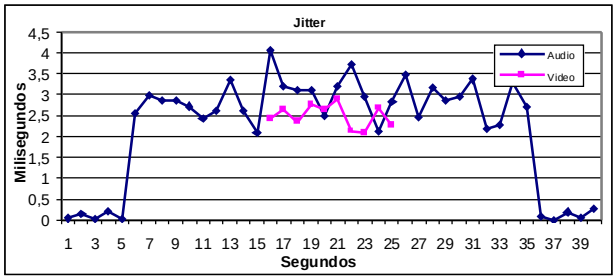

Gráfico 2. Distribución de Jitter

Es posible notar que sin la presencia de otros tráficos, el jitter es prácticamente cero. Al momento de ingresar el tráfico Web y Ftp, se observa un incremento del jitter, el cual se mantiene dentro del rango de 2 [ms] y 4 [ms]. Además se percibe que el jitter para el tráfico de Audio es ligeramente mayor al del tráfico de Video, a pesar de tener mayor prioridad el tráfico de Audio.

4.4.- Asignación de Prioridad en IPv6

Surge la inquietud de si es posible utilizar un esquema de asignación de ancho de banda como el utilizado para dar prioridad al tráfico multimedia en IPv4, descrito anteriormente. Para esto, se crearon listas de acceso Ipv6 que seleccionan el tráfico de Audio, Video, Http y Ftp, según la dirección origen (**Spock2**) y el puerto de destino usado. Se crean mapas de clase donde se adjuntan cada una de estas listas. A continuación se crean dos mapas de política, uno que se encarga de limitar y asignar valores DSCP al tráfico, y otra que reserva el ancho de banda mínimo para cada una de los tráficos. La política de limitación y clasificación se aplica a la interfaz Fast Ethernet 0/1 del **R-IPv6-UTFSM**, mientras que la política de asignación de ancho de banda se aplica a la interfaz Fast Ethernet 0/0.

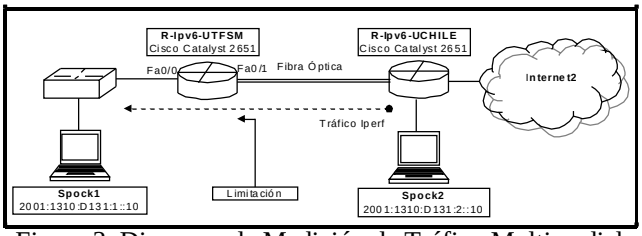

Figura 3. Diagrama de Medición de Tráfico Multimedial

Se utilizó la herramienta Iperf para generar los flujos desde **Spock2** hacia **Spock1** en cada uno de los puertos asignados a cada clase. Como era de esperar, la política de clasificación y limitación de ancho de banda para el tráfico de Audio funcionó correctamente, como se aprecia en las estadísticas mostradas por el enrutador para las políticas de Audio y Video.

En el equipo **Spock1**, al monitorear la cantidad de paquetes recibidos desde **Spock2**, se observó que el tráfico de Audio y Video alcanzaban la tasa máxima de limitación de la política, 1 [Mbps] y 2 [Mbps] respectivamente. Sin embargo, no se cumplía con la asignación de prioridad al tráfico de Http sobre el de Ftp; ambos se repartían el ancho de banda disponible de forma equitativa.

5.- Conclusiones

Los variados esquemas de encolamiento estudiados proveen de cierto nivel de servicio para aplicaciones críticas. Los parámetros para la asignación de recursos, normalmente basados en dirección IP de destino, son insuficientes para alcanzar los requerimientos de hoy en día. Policy Based Routing (PBR) provee la diferenciación de tráfico basado en puerto de origen dirigiendo este tráfico a interfaces determinadas o modificando el nivel de servicio de lo paquetes.

Clasificando los paquetes en los bordes de la red, en distintas clases, se puede proveer servicios diferenciados a los paquetes sin tener que examinar cada uno en detalle en cada salto. Después de ser marcados una vez mediante Precedencia IP o DSCP, mecanismos de manejo y evasión de congestión pueden actuar sobre ellos a medida que circulan por la red. Esta es la esencia del modelo Diffserv.

Sin duda, para la mayoría de las redes, DiffServ, y los valores DSCP junto al de Precedencia IP serán más convenientes y funcionales. La estandarización del procedimiento de asignación e interpretación de dichos valores provee las bases para lograr implementar esquemas de calidad de servicio de una forma global. Además, el reciente IPv6, utiliza los mismos conceptos involucrados con Servicios Diferenciados, por lo que el despliegue de QoS para estos ambientes es muy estable, ya tiene años de depuración.

A diferencia de IPv4, las especificaciones del protocolo IPv6 en lo referente a la descripción del campo de QoS, ofrecen la capacidad de la implementación de una calidad de servicio escalable y sin lugar a múltiples interpretaciones. Mediante las pruebas realizadas fue posible constatar la viabilidad de seleccionar y aislar tráfico IPv6, limitando las tasas de transferencia en éstos. Sin embargo, habiendo diseñado todo un esquema de asignación de ancho de banda para distintas clases de tráfico, no fue posible lograr la verificación de la programación de colas en el enrutador Cisco Catalyst 2651, para IPv6.

6.- Referencias y Bibliografía

[i] Proyecto FONDEF D00I1026. http://redesopticas.reuna.cl

[ii] RFC-2597, Grupo PHB de envíos garantizados. http://www.ietf.org/rfc/rfc2597.txt

[iii] "Documento de Diseño de la red óptica IP, FONDEF D00I1026", Christian Henry. Agosto 2002.

[iv] Catalyst 3550 Multilayer Switch Software Configuration Guide, Cisco, PDF.

[v] Software Configuration Guide, For Cisco 3600 Series and Cisco 2600 Series Routers, PDF.