

Análisis e implementación de algoritmos de control de tráfico en RouterOS

Adlercreutz Gustavo Daniel
Chiapero Mauricio
Grupo de Investigación y Desarrollo
Instituto Universitario Aeronáutico
Córdoba, Argentina
gustavoadlercreutz@gmail.com
mauricio.chiapero@gmail.com

Ing. Galleguillo Juan
Ing. Giovanardi Ezequiel
Grupo de Investigación y Desarrollo
Instituto Universitario Aeronáutico
Córdoba, Argentina
jgalleguillo@iua.edu.ar
ggiovanardi@iua.edu.ar

Resumen— Debido al creciente surgimiento de empresas del rubro internet por aire o WISP que utilizan como soporte equipos Mikrotik y dado en general el desconocimiento y la complejidad que a priori implica una buena gestión de los recursos disponibles en contraposición a la utilización de métodos simples de encolamiento, se decidió el estudio de la optimización del AB implementando mecanismos de encolamiento avanzado y QoS.

Se llevó a cabo para este fin el análisis de algoritmos y métodos de priorización mediante comparación en pruebas de laboratorio de distintas configuraciones utilizando marcado, resultando HTB (Hierarchical Token Bucket) junto a un módulo de priorización por protocolos y colas PCQ[1] (Per Connection Queue) como el método más eficiente.

Palabras Claves— WISP, QoS, Protocolo, Mikrotik, Mediciones, HTTP, ICMP, VoIP.

I. INTRODUCCIÓN

Cuando se comenzó el estudio de la problemática del control de ancho de banda y calidad de servicio sobre Mikrotik, rápidamente se encontró que la información disponible era poca, incompleta y difícil de encontrar, reforzando la idea de que su implementación es escasa entre sus usuarios.

Luego de investigar varios procesos y recomendaciones se diseñó el método que aquí se detalla utilizando marcado, priorización y colas.

En este artículo se muestran los resultados obtenidos en las pruebas junto a ejemplos de marcado y la configuración final.

La unión de los términos Calidad y Servicio, como concepto, describe en definitiva qué tan bien se comporta la red y es un intento de cómo definir las características y propiedades específicas de cada servicio.

A medida que los paquetes atraviesan los dispositivos que componen las distintas redes se van sumando retrasos debidos,

entre otros factores, a tiempos de procesamiento, tamaño de búferes, ruidos, interferencias, limitación en el ancho de banda, etc.

“En el marco de redes de computadoras y otras redes basadas en conmutación de paquetes, el concepto de Calidad de Servicio refiere a los mecanismos de control de reserva de recursos más que a la calidad de la experiencia alcanzado”[2].

Por lo tanto podemos definir que los factores que enmarcan la QoS son divididos en dos grupos, que podemos denominar como “Humanos” y “Técnicos” los cuales abarcan los siguientes conceptos.

La QoS “técnica” refiere a la habilidad de proveer diferentes prioridades a diferentes aplicaciones, usuarios o flujos de datos.

Es muy importante si la capacidad de la red es un recurso limitado, especialmente para aplicaciones que requieren un flujo de bit constante, como VoIP, IP-TV, etc.

La otra definición, es la QoS “humana”, es específica de servicios de capa de aplicación, como telefonía y streaming de video. Esta métrica se realiza con el reflejo o la predicción de la experiencia subjetiva de la calidad. En este contexto se define:

La QoS experimentada por las personas es la percepción del usuario al efecto acumulado de todas las imperfecciones que afectan al servicio de las aplicaciones, esto se conoce también como Calidad de la experiencia o QoE[2][3][4].

El objetivo de este trabajo es estudiar el mejor método para gestionar ambos conceptos de calidad desde una plataforma centralizada.

II. MATERIALES Y MÉTODOS

Todas las configuraciones se realizaron sobre un Router RB433AH en modo Router utilizando la interfaz ether 1 para la conexión WAN y la ether 2 para la LAN.

Para la confección del trabajo se realizaron los siguientes pasos:

- Análisis de los métodos de control de ancho de banda existentes

- Creación de una política de priorización como por ejemplo el tráfico VoIP por sobre otros protocolos como P2P.
- Comparación del desempeño de los protocolos HTB versus queue simple.
- Realización de mediciones para determinar las capacidades y limitaciones de cada método.
- Utilización de expresiones regulares de capa 7 para “matcheo” de paquetes.
- Determinación de condiciones óptimas para cada una de las configuraciones evaluadas.

La técnica de marcado se utiliza para realizar una clasificación de tráfico mientras este circula dentro de Router. Esta marca o “mangle” agregada al paquete solo existirá dentro de Router y desaparecerá cuando el paquete salga del mismo.

El método utilizado en este caso es el de generar marcas de conexión para cada protocolo de interés definido en las políticas de red, para luego realizar una marca de paquetes del mismo protocolo, esto se realiza de esta manera para lograr un menor consumo de recursos.

Luego se genera un árbol de colas que tendrá como objetivo la asignación de prioridades, anchos de banda mínimos, máximos para cada protocolo y el total de las conexiones.

En particular se diseñó una priorización escalonada para http con la finalidad de capturar el tráfico de descargas realizadas por el puerto 80, todos estos flujos controlados por colas PCQ que aseguran una distribución equitativa del ancho de banda disponible, como también el ahorro en recursos ya que a diferencia de la comúnmente utilizada “cola simple” PCQ solo genera colas en los lugares asignados y es en definitiva más simple de gestionar en entornos con gran cantidad de usuarios

Para generar condiciones estandarizadas, se diseñaron procedimientos que aseguran que cada prueba consiga valores iniciales, tipo y volumen de tráfico idéntico. En base a esto se creó un entorno de laboratorio controlado sobre el cual se realizaron todas las pruebas utilizando Wireshark® para realizar los estudios.

Se evaluará el rendimiento de los distintos servicios en las siguientes condiciones a comparar.

- Sin Carga/control AB (tomado como caso ideal)
- Queue simple
- Queue tree (o HTB)

Los servicios que se desean priorizar son los siguientes:

- Navegación web
- DNS
- ICMP

- P2P
- VoIP (Sip y Skype)
- Descargas
- Otros

III. RESULTADOS

MEDICIONES HTTP

En Tabla 1 se observan las mediciones tomadas para el tráfico WEB

Mediciones Http			
Valores	Sin Carga	Q Simple	HTB
La Voz	7,702 [s]	49,206 [s]	34,768 [s]
Gaceta	10,237 [s]	72,187 [s]	45,416 [s]
Google	1,949 [s]	7,200 [s]	5,676 [s]

Tabla 1

MEDICIONES ICMP

Mediciones ICMP			
Destino	Sin Carga	Q Simple	HTB
8.8.8.8	61,75 [ms]	1075,25 [ms]	653,5 [ms]
Gateway Lan	0 [ms]	11,75 [ms]	0 [ms]
Gateway Wan	0 [ms]	13,75 [ms]	0 [ms]

Tabla 2

LAYER-7

Si bien HTB fue útil para la administración del ancho de banda la utilización del mismo tiene la desventaja de que la clasificación del tráfico que se estudió se limita a Capa 3/4. Es decir IP origen, IP destino, puerto origen y puerto destino. La clasificación/detección de tráfico de los diversos servicios es una de las operaciones más complejas sobre todo si se utilizan reglas de firewall con las antes mencionadas para tráfico “inteligente” como el de Skype® o aplicaciones p2p.

Aquí es donde la utilización de filtros de Capa 7 es de mucha ayuda. La detección se realiza desmembrando los paquetes y aplicando sentencias de expresiones regulares de “matcheo,” de esta forma la comparación con algunos parámetros de la carga útil del paquete determinará el tipo de tráfico.

Como se puede pensar esto tiene también sus inconvenientes, y no se debe abusar de su utilización. En primer lugar este tipo de control consume más CPU que los filtros de capa 3/4, lo que deriva en un problema para el funcionamiento en procesadores lentos. Además muchas de estas expresiones tienen el problema de la detección de un falso positivo, es decir muchas veces se clasifica tráfico en forma errónea. Sumado a esto la mayoría del tráfico que se encripta en capa 7 está en constante desarrollo y cambio, lo

que obliga a un seguimiento constantes de las expresiones regulares para detectarlo.

En este caso solo se evaluó la capacidad de los distintos métodos de detección de “capturar” el tráfico cursado ya que este es el principal reto en este tipo servicios.

Mediciones P2P Capa 7			
Valores	Total trafico	Marca P2P	Capa 7
Medición 1	112,9 Mb	2,9 Mb	2,2 Mb
Medición 2	52,2 Mb	1,8 Mb	23,9 Mb
Medición 3	254,1 Mb	65,1 Mb	86,9 Mb
Media	419,2 Mb	69,8 Mb	113,0 Mb
		16,64%	26,95%

Tabla 5

Como se observa capa 7 sirvió para incrementar el porcentaje de marcado en un 27% sobre el total de tráfico descargado, lo que sumado al 16,64% del marcado automático de P2P de Mikrotik da un total de 43,6 %.

Si bien el aumento fue notorio el mayor porcentaje de la marca fue sobre el bit torrent. En el caso del Ares las expresión regular utilizada no detectó ningún tráfico. Esto se debe a que esta fue realizada en base a la versión 1.8 y actualmente se utiliza la 2.2.

El siguiente gráfico muestra el uso del CPU del Router cuando se realizaron las pruebas de marcado de capa 7. En este caso se encontraban en funcionamiento todas las expresiones de P2P y Skype que se probaron un total de 8 reglas.

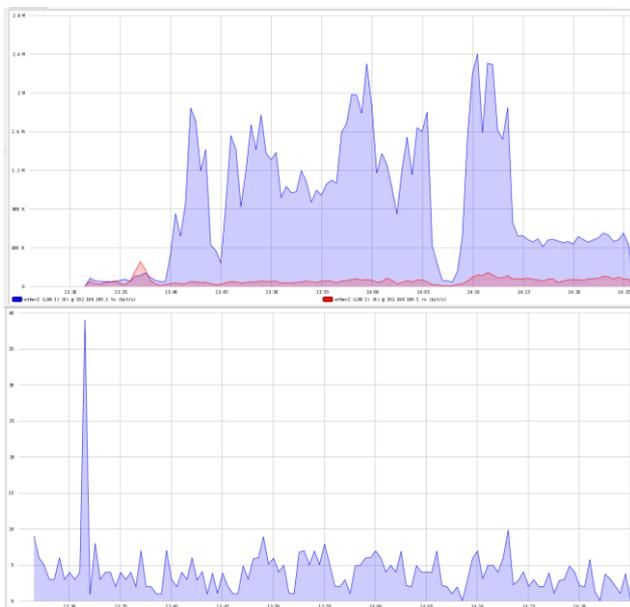


Figura 1

El primer pico observado en la medición del CPU no debe tenerse en cuenta ya que fue en ese momento cuando se aplicaban las reglas. Luego se puede ver que el uso del micro ronda el 5% para un throughput cercano a 1 Mbps. En el

horario de las 14:13 se ve que este llega al 10% cuando el throughput medido fue de 2,1 Mbps, y recordemos que solo se utilizaron 8 reglas. Si bien este no es un resultado extremo queda en evidencia que no se debe abusar del uso de este tipo de marcadores y debemos utilizarlos solo cuando los identificadores de capa 3/4 no sean suficientes.

IV. CONCLUSIONES

Luego de la realización de las mediciones se concluye que la utilización de HTB brinda una optimización superior en casi todos los protocolos.

Respecto de la utilización de capa-7 no se considera crítica su inmediata implementación ya que la gran mayoría del tráfico fue detectado en capa 4 (OSI), con lo cual su utilización, pensando en la relación “costo-beneficio” es prácticamente irrelevante, salvo en casos particulares donde se considere necesario que servicios como Skype® deban ser controlados.

Por otro lado, como la característica de uso del usuario promedio es más o menos constante (aproximadamente el 50% de las paginas consultadas es siempre la misma) la utilización de un WebCache aumentara el rendimiento de la conexión, mejorando la QoE.

V. REFERENCIAS

- [1] Mikrotik - Consultado febrero 2012 - <http://wiki.mikrotik.com/wiki/Manual:IP/Firewall/Mangle>
- [2] Mikrotik - Consultado febrero 2012 - http://wiki.mikrotik.com/wiki/Manual:Packet_Flow
- [3] Mikrotik - Consultado febrero 2012 - http://wiki.mikrotik.com/wiki/Manual:Queues_-_PCQ_Examples
- [4] Mikrotik - Consultado febrero 2012 - http://wiki.mikrotik.com/wiki/Manual:Queues_-_PCQ
- [5] Mikrotik - Consultado febrero 2012 - http://mum.mikrotik.com/presentations/US09/megis_qos.pdf
- [6] Consultado febrero 2012 - <http://www.tiktube.com/video/JpcD3eCCChqGnDIJFJEEsCvExCIIoEKDH=>