Sistemas & Telemática
ISSN: 1692-5238
EditorSyT@icesi.edu.co
Universidad ICESI
Colombia

Suarez R., Alexander; Solarte A., Zeida María; Cuéllar Q, Juan Carlos
Herramienta para el monitoreo de parámetros de Calidad de Servicio en redes NGN
Sistemas & Telemática, vol. 11, núm. 26, julio-septiembre, 2013, pp. 81-94
Universidad ICESI
Cali, Colombia

Artículo original

Herramienta para el monitoreo de parámetros de Calidad de Servicio en redes NGN

Tools for monitoring Quality of Service parameters in Next Generation Networks

Alexander Suarez R.
alex_a321@hotmail.com

Zeida María Solarte A. MSc.
zsolarte@uao.edu.co

Universidad Autónoma de Occidente
Cali - Colombia

Juan Carlos Cuéllar Q. MSc.
jcuellar@icesi.edu.co
Universidad Icesi
Cali – Colombia

Fecha de recepción: Agosto 13 de 2013
Fecha de aceptación: Septiembre 9 de 2013

Palabras clave
IPTD; IPDV; IPLR; QoS; Y.1540; Y.1541.

Keywords
IPTD; IPDV; IPLR; QoS; Y.1540; Y.1541.

Colciencias tipo 1

Resumen

El artículo presenta la descripción funcional de la herramienta *Eagle Network Sniffer*, desarrollada para la medición de parámetros de calidad de servicio en redes de próxima generación. Adicionalmente muestra el esquema de laboratorio implementado para la prueba del *Eagle Network Sniffer* y los datos comparativos obtenidos con otra herramienta de uso libre, con el fin de evaluar y verificar su funcionamiento.

Abstract

The article presents the functional description about Eagle Network Sniffer tool, developed to measure quality of service parameters in next generation networks. Additionally we show the testbed implemented to test the Eagle Network Sniffer tool and the comparative data obtained with other free use tool, in order to evaluate and verify it operation.

I. Introducción

La evolución de las redes de datos convencionales hacia redes de próxima generación [*Next Generation Networks*, NGN] ha generado retos que la infraestructura de la red debe estar en capacidad de garantizar. Uno de ellos es utilizar la misma infraestructura para transportar múltiples servicios como VoIP, videoconferencia, IPTV, navegación, datos transaccionales, etc.; otro, ofrecer y garantizar calidad de servicio [QoS] a los servicios que la red NGN transporta, entendiendo como QoS lo definido por Crawley, Nair, Rajagopalan, y Sandick (1998) en el RFC 2386 de la *Internet Engineering Task Force* [IETF]: es decir, como un conjunto de requisitos de servicio que debe cumplir la red durante el transporte de un flujo.

Con base en esto, al analizar la estructura por capas de la red NGN, como lo plantea Cuellar (2010), se define una capa de calidad de servicio intermedia entre la capa de servicios y la capa de transporte. Ésta capa tácita es la encargada de ofrecer QoS a los servicios y aplicaciones, y está compuesta por tres estratos: contratación, verificación e infraestructura, como se aprecia en la Figura 1.

Figura 1. Estratos dentro de la capa de QoS en una red NGN (Cuellar, 2010)

En el estrato inferior, *Infraestructura*, se ejecutan los procedimientos para garantizar QoS; estos procedimientos hacen referencia a configuraciones que se realizan en dispositivos de interconectividad, como también en configuraciones que se hagan al interior de la red de núcleo, como configuración de VLANs o configuración de MPLS.

En el estrato *Verificación* se comprueba si se está garantizando y ofreciendo QoS a los servicios que son transportados por la red NGN. Para esto, el sector de normalización de la *International Telecommunication Union* [ITU-T] definió dos recomendaciones, la Y.1540 (ITU-T, 2011a) –en la cual se definen los parámetros de calidad de funcionamiento para transmisión de paquetes en redes IP– y la Y.1541 (ITU-T, 2011b) –que define los límites que deben alcanzar dichos parámetros para garantizar QoS a los servicios y las aplicaciones–.

Por su parte, en el estrato Contratación se establecen los acuerdos entre el proveedor del servicio y el usuario, para así conocer que servicios serán transportados, con el fin de que el proveedor pueda clasificarlos y garantizar la QoS a cada uno de ellos.

Lo anterior destaca la necesidad de medir los parámetros de QoS especificados en la recomendación Y.1541, de tal manera que se pueda de verificar si efectivamente se está ofreciendo QoS a las aplicaciones. Para lograrlo existen múltiples herramientas de uso libre –y otras diseñadas por fabricantes–, que le entregan al usuario la medición de los parámetros de QoS. Desafortunadamente no se tiene claridad del procedimiento empleado por la herramienta para obtener dichas medidas, razón por lo que se considera importante el diseño e implementación de una herramienta que permita obtener estas mediciones, indicando claramente el proceso utilizado para obtener la medición de estos parámetros.

Para indicar como fue el proceso de diseño e implementación de la herramienta para la medición de parámetros de QoS este artículo está organizado de la siguiente manera. En la sección II se describe de manera resumida el contenido de las recomendaciones Y.1540 y Y.1541 de la ITU; en la sección III se describe el diseño de la herramienta implementada; en la sección IV se presenta el montaje experimental que se implementó para probar el funcionamiento de la herramienta y los datos comparativos obtenidos con una herramienta de uso libre para la medición de parámetros de QoS; finalmente se presentan las conclusiones, el trabajo futuro y las referencias consultadas.

II. Recomendaciones Y.1540 y Y.1541

En la Recomendación Y.1540 se definen los parámetros para evaluar la calidad de servicio para la transferencia de paquetes en una red IP. Los parámetros definidos se aplican al servicio IP de extremo a extremo o punto a punto; define (Cuellar, 2010) principalmente cuatro parámetros:

» IPTD [*IP Packet Transfer Delay*]. Corresponde al tiempo que tarda el paquete en pasar por un componente de la red (host, dispositivo de interconetividad o segmento de red). Éste es uno de los parámetros principales –y críticos– para todas las aplicaciones que utilicen una red convergente. El cálculo se realiza utilizando la ecuación 1:

$$IPTD: \frac{\sum_{i=1}^{n} x_i}{n} \qquad (Ecuación\ 1)$$

Donde: x_i: retardo del i-ésimo paquete.
n: número de paquetes

» IPDV [*IP Packet Delay Variation*]. También conocido como *jitter*, corresponde al tiempo esperado de llegada de cada paquete. Este parámetro se calcula utilizando la ecuación 2.

$$IPTD: \frac{\sqrt{\sum_{i=1}^{n} {x_i}^2 - n * Retardo^2}}{n-1} \qquad (Ecuación\ 2)$$

» IPLR [*IP Packet Loss Ratio*]. Rata (tasa) de pérdida de paquetes. Su valor se obtiene de la relación entre el total de paquetes perdidos y el total de paquetes transmitidos en un flujo de datos.

» IPER [*IP Packet Error Ratio*]. Tasa de paquetes con errores; su valor se obtiene de la relación entre el total de paquetes con errores y el total de paquetes sin errores transmitidos en un flujo de datos determinado

La recomendación Y.1541, por su parte, especifica valores de calidad de servicio para cada uno de los parámetros definidos en la recomendación Y.1540; para ello, define un número de clases de QoS en las que se enmarcan los diferentes servicios y/o aplicaciones. Los valores establecidos para cada clase y cada parámetro se pueden apreciar en la Tabla 1.

Las clases tienen tipos de aplicaciones o servicios específicos, así:

Clase 0-1. Aplicaciones en tiempo real, sensibles al retardo y de interacción alta (e.g. VoIP, videoconferencia y difusión de audio).

Clase2-3. Aplicaciones de datos transaccionales interactivos (e.g., navegación y señalización).

Clase 4. Aplicaciones que soportan pérdidas y no presentan problemas con el retardo (e.g., transmisión de video y transferencia de archivos).

Tabla 1. Parámetros de calidad de funcionamiento que determinan la QoS en NGN. Tomado de ITU-T Rec. Y.154 (ITU, 2011b)

Parámetro de calidad de funcionamiento de red	Clases de QoS					
	Clase 0	**Clase 1**	**Clase 2**	**Clase 3**	**Clase 4**	**Clase 5 ***
IPTD	100ms	400ms	100ms	400ms	1s	U
IPDV	50ms	50ms	U	U	U	U
IPLR	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	U
IPER			1×10^{-4}			U

*Clase no especificada.
"U" significa no especificado o sin límites.

III. Diseño de la herramienta

Para definir los requerimientos de la herramienta, se realizó un análisis de varias herramientas disponibles en el mercado; esto, con el fin de observar las funcionalidades que ellas ofrecían y su manera de presentar las mediciones de los parámetros de QoS al usuario. Entre las herramientas analizadas están: Cisco SAA [*Service Assurance Agent*] (Cisco, 2005), *VVQManager* (Zoho, 1997) y D-ITG [*Distributed Internet Traffic Generator*] (DITG, s.f; Botta, Pescapè, & Dainotti, 2012; Botta, Dainotti, & Pescape, 2007), *TamoSoft Throughput Test* (Schumann, Huntgeburth, & Maruschke, 2011) e Iperf (Schroder, 2007).

Después del análisis se definieron los requisitos que debía cumplir la herramienta a desarrollar, así:

- » estar en capacidad de monitorear y capturar cualquier tipo de tráfico que se transporte en la red y, con el tráfico capturado, poder realizar el análisis necesario para obtener la medición de los parámetros de QoS;
- » no estar ligada a ningún hardware propietario para realizar el monitoreo de los parámetros de QoS;
- » la interfaz a través de la cual se suministraran los datos debe ser intuitiva, para facilitar la labor de la persona que está realizando los análisis; y
- » el tiempo de duración de la captura debe ser ingresado por el usuario.

A la herramienta de análisis diseñada se le colocó el nombre de *Eagle Network Sniffer* [ENS]; funciona capturando el tráfico que se genera en la red en modo pasivo y está compuesta por dos componentes: servidor y cliente, los cuales se describen a continuación.

A. Componente en el servidor

El componente servidor es una parte fundamental de la herramienta ya que cumple con la función de capturar los paquetes en un extremo de la red. Los paquetes capturados son filtrados, dependiendo de configuraciones definidas en la interfaz de usuario. Estos datos son almacenados en un archivo para ser procesados de manera conjunta con los datos capturados en el cliente y así obtener las medidas de los parámetros de QoS. La Figura 2 corresponde al diagrama de flujo este componente.

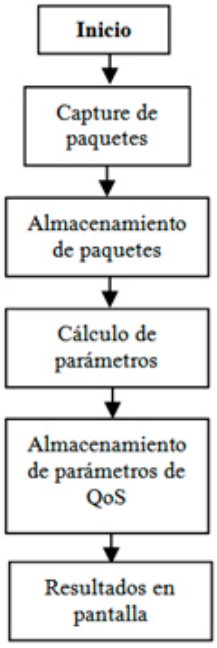


Figura 2. Diagrama de flujo - componente *Servidor*

El bloque definido como *Captura de paquetes* tiene la función que su nombre índica, capturar los paquetes que circulan en la red; para ello previamente se deben haber configurado algunos parámetros como la elección de la tarjeta de red y el tiempo de captura y filtros que se requieren para realizar la captura. Una vez definidos estos parámetros de configuración se procede a capturar las marcas de tiempo, el identificador de cada paquete (id) y su longitud durante el tiempo definido. En la Figura 3 se puede apreciar este proceso de manera detallada.

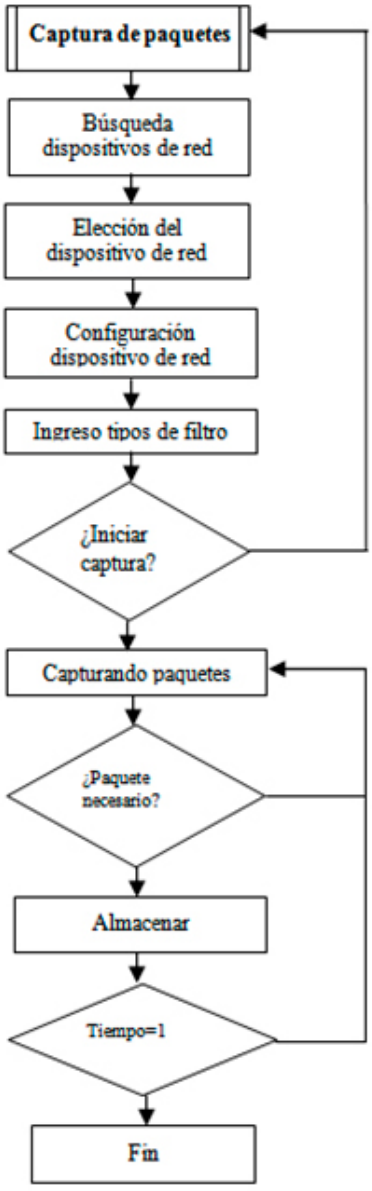


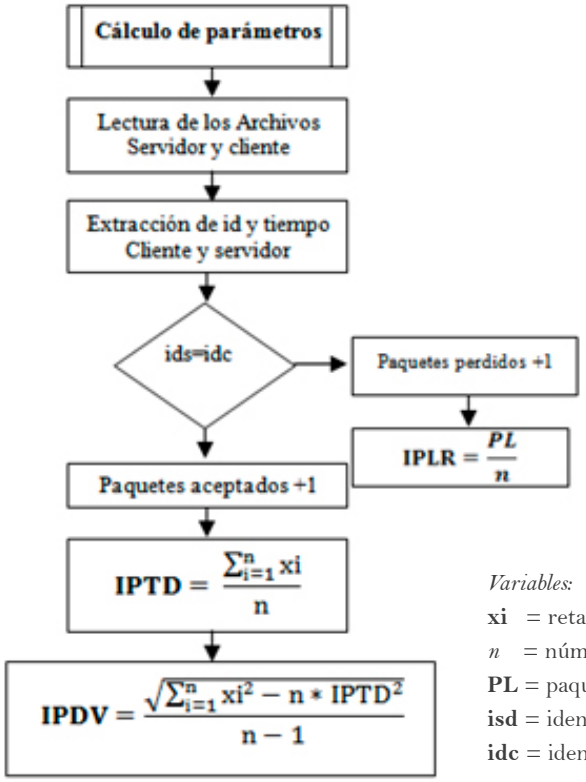
Figura 3. Diagrama de flujo *Captura de paquete*

Los datos capturados en el componente servidor se almacenan en un archivo de texto de nombre *Servidor.txt*, con el fin de procesarlos posteriormente, cuando se realicen los cálculos para obtener la medición de los parámetros de QoS.

En el bloque definido como *Cálculo de parámetros*, como se aprecia en la ver Figura 4, se calcula cada uno de los parámetros de QoS (siempre y cuando se cuente con los archivos de texto generados en el cliente y el servidor, con las marcas de tiempo, la id y la longitud de cada paquete).

De cada uno de los archivos se obtiene la información de los paquetes y se compara su identificación; si ellas coinciden, el paquete se cuenta como *enviado satisfactoriamente* y se analizan las marcas de tiempo para calcular el IPTD (*IP Packet Transfer Delay*) y la IPDV (*IP Packet Delay Variation*); si por el contrario las identificaciones no coinciden, el paquete se cuenta como *perdido* y se calcula la IPLR (*IP PacketLoss Ratio*); al finalizar, se cuenta el número de paquetes enviados satisfactoriamente y el número de paquetes perdidos obteniendo el total de los paquetes.

Una vez calculado cada uno de los parámetros requeridos se procede a almacenar estos datos en archivo con extensión *.txt* (que para este caso se le identificará con el nombre de *Resultado.txt*); este archivo podrá ser visualizado en cualquier momento y exportado a cualquier tipo de herramienta de análisis.



Variables:
xi = retardo por paquete.
n = número de paquetes.
PL = paquetes perdidos.
isd = identificador de paquetes servidor.
idc = identificador de paquetes cliente.

Figura 4. Diagrama de flujo *Cálculo de parámetros*

Al final, se realiza la lectura del archivo de texto *Resultado.txt* con el propósito de mostrar los datos de archivos utilizados en el proceso de captura de datos, en una ventana generada en la interfaz de usuario.

B. Componente en el cliente

El cliente complementa la herramienta, ya que cumple con la función de capturar los paquetes en el extremo contrario del servidor; se inicia con la sincronización con el servidor –necesario porque es imprescindible que manejen la misma marca de tiempo, para evitar problemas en los cálculos posteriores–; una vez sincronizados cliente y servidor se procede a definir, en la interfaz de usuario, los paquetes que se deseen filtrar. En la Figura 5 se muestra en detalle los bloques que componen el cliente.

El bloque definido como *Sincronización* se encarga de que, tanto el cliente como el servidor, trabajen con un reloj común, con el fin de que el cálculo de los parámetros de QoS no se afecte por medidas erróneas. *Eagle Network Sniffer* utiliza una sincronización *master/slave* debido a que las medidas deben realizarse con un reloj en común entre las máquinas.

Una vez que el cliente se sincroniza, se procede a definir el tipo de tráfico que se quiere capturar. En la Figura 6 se puede apreciar la pantalla inicial de la herramienta con la descripción de cada campo para su configuración. Posteriormente se genera un archivo con el nombre cliente el cual contiene los datos capturados por la tarjeta de red; estos datos se envían al servidor para ser procesados.

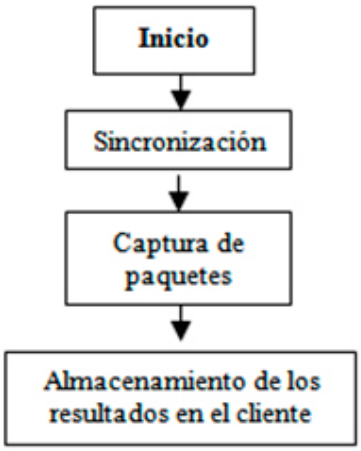


Figura 5. Diagrama de flujo del componente *Cliente*

IV. Montaje experimental del laboratorio

Con el fin de analizar los resultados que genera la herramienta *Eagle Network Sniffer*, se implementó el esquema que se aprecia en la Figura 7, el cual está conformado por dos enrutadores Cisco con una conexión *back-to-back* y dos *switches* Cisco. Como

Figura 6. Configuración de parámetros

herramienta comparativa se seleccionó el D-ITG; se escogió por ser una herramienta de uso libre y por entregar la medición de los parámetros de manera similar a la manera como se desarrollo el ENS.

Se descarga un archivo de 600KB, el cual se encuentra en el cliente, y se produce una transferencia hacia el servidor. Se toman las medidas utilizando tanto el D-ITG como la herramienta *Eagle Network Sniffer*, con una velocidad de enlace 64Kbps y 256Kbps, con el fin de que *se presenten* distintos niveles de congestión en los enlaces.

En la Tabla 2 se pueden apreciar los resultados obtenidos para un ancho de banda en el enlace WAN de 64Kbps. La razón de las diferencias radica en la manera como el D-ITG empieza a colocar los datos en el enlace: no se tiene certeza del momento que empieza y termina la medición de los parámetros, ya que cuando se trabaja con el D-ITG, al terminar el tiempo de envío de datos configurado, pasan alrededor de 5 a 9 segundos para que cierre el flujo y cese el envío de información.

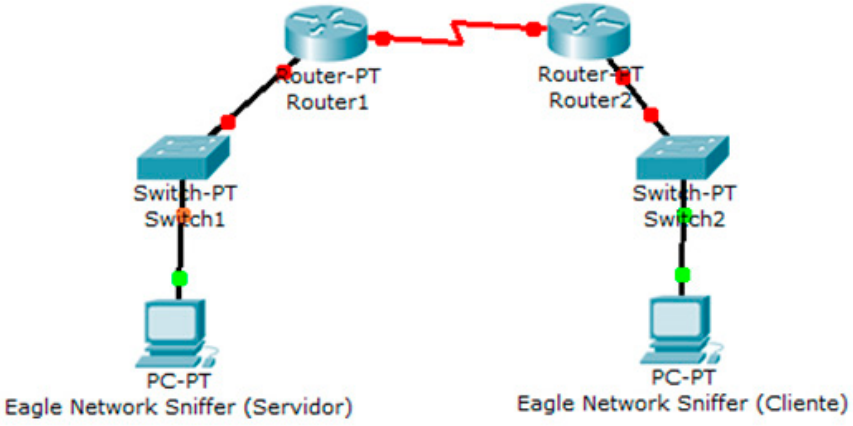


Figura 7. Montaje experimental prueba FTP

Tabla 2. Resultados obtenidos para la aplicación de ftp utilizando *Eagle Network Sniffer* y D-ITG, con un ancho de banda de 64Kbps

Parámetro	Resultados D-ITG	Resultados Eagle Network Sniffer
Total Time (s)	19.719328	19.68555307
Total packets	132	132.0
Minimum delay (s)	0.302434	0.242093086
Maximum delay (s)	10.133899	10.03705000
Average delay (s)	7.485182	7.402843213
Average jitter (s)	0.080542	3.230482505
Delay standard deviation (s)	3.233416	----
Bytes received	132000	----
Average bitrate	53.551521 Kbit/s	-----
Average packet rate	6.693940 pkt/s	6.7054250
Packets dropped	113 (86.67 %)	115

En la Figura 8 se observa el montaje que se utilizó para realizar una prueba de VoIP; se efectúa una llamada desde la extensión 100 hacia la extensión 101, haciendo uso de la central telefónica de 3CX de Windows. Una vez establecida la comunicación se inicia la captura mediante *Eagle Network Sniffer* –posteriormente se realiza otra prueba utilizando el D-ITG– en un tiempo de 30 segundos.

En la Tabla 3 se pueden apreciar los datos obtenidos con el D-ITG y el *Eagle Network Sniffer* para el tráfico de VoIP. Existen discrepancias en algunos de los parámetros; ello se debe a la manera como el D-ITG coloca los datos en los enlaces: basándose en una distribución estadística determinada, mientras que la prueba que se hizo con el *Eagle Network Sniffer* se realizó sobre una llamada real, en la cual las condiciones pueden ser variadas dependiendo del tono y dialogo de prueba de los interlocutores.

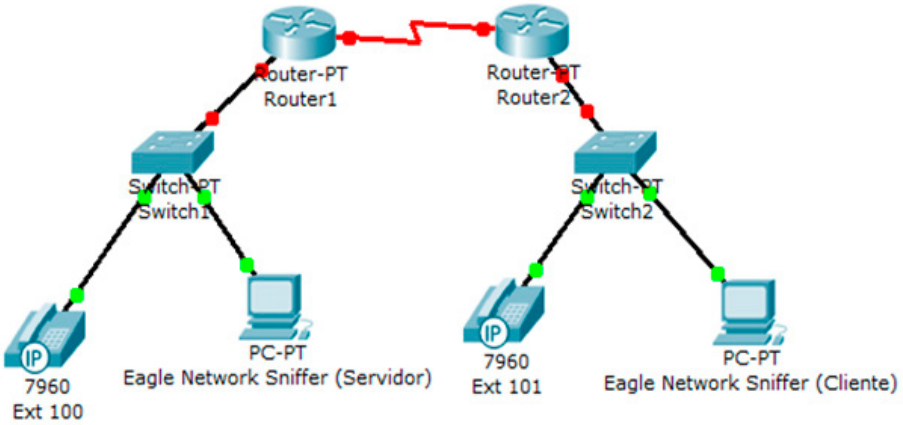


Figura 8. Montaje experimental prueba VoIP

Tabla 3. Resultados obtenidos para la aplicación de VoIP utilizando *Eagle Network Sniffer* y D-ITG

Parámetro	Resultados D-ITG	Resultados Eagle Network Sniffer
Total Time (s)	31.142867	31.184264
Total packets	894	1010
Minimum delay (s)	0.324632	0.3126857
Maximum delay (s)	3.2568546	3.4925467
Average delay (s)	4.1895634	4.3678524
Average jitter (s)	1.2487963	----
Delay standard deviation (s)	2.582364	2.894612
Bytes received	894000	----
Average bit rate	30.5246 Kbit/s	----
Average packet rate	28.70641pkt/s	32.3881 pkt/s
Packets dropped	606(60.6 %)	490

Conclusiones

Las diferencias entre las mediciones obtenidas por el D-ITG y el *Eagle Network Sniffer* [ENS] se deben a varios aspectos. Uno de ellos que el ENS realiza las mediciones sobre el tráfico real generado por las aplicaciones, mientras que el D-ITG coloca el tráfico sobre la red utilizando por defecto las distribuciones estadísticas que más se ajustan al comportamiento de cada aplicación. Adicionalmente no se tiene certeza de cuándo y cómo el D-ITG termina el flujo de datos enviado y el proceso de medición de los parámetros.

Al realizar la configuración de la herramienta *Eagle Network Sniffer*, extremo a extremo, tanto del servidor como del cliente, se debe ser muy cuidadoso para definir de manera correcta el filtro a utilizar, debido a que el software funciona con las identificaciones de cada paquete, por lo que al cometer un error digitando el filtro, los parámetros calculados podrían ser erróneos.

Se recomienda que el tiempo de captura definido por el usuario no exceda de 10 minutos, debido a que el proceso de cálculo de los parámetros se podría demorar un tiempo similar o superior, por el proceso de análisis de los archivos que contienen los datos para los cálculos. Se espera que para la próxima versión de la herramienta superar esta dificultad.

Trabajo futuro

Contar con herramientas que midan parámetros de QoS es de gran utilidad para los proveedores de los servicios de telecomunicaciones, pues permite monitorear el

funcionamiento y desempeño de las aplicaciones y tener así un punto de comparación entre las herramientas comerciales que ofrecen los fabricantes de dispositivos de interconectividad.

Como trabajo futuro se plantea modificar la herramienta ENS de tal manera que los cálculos de QoS se realicen en línea; esta modificación traería consigo la disminución del procesamiento en la máquina donde se esté ejecutando la herramienta (lo que es una limitante de esta primera versión).

Adicionalmente, con el fin de obtener datos más precisos de desempeño del ENS, se podría realizar un mayor número de pruebas, incluyendo su comparación con otras herramientas disponibles en el mercado. ST

Referencias bibliográficas

Botta, A., Pescapè. A., & Dainotti, A. (2012). A tool for the generation of realistic network workload for emerging networking scenarios. *Computer Networks (Elsevier), 56*(15), 3531-3547

Cisco Systems. (2005, oct. 25). *Measuring Delay, Jitter, and Packet Loss with Cisco IOS SAA and RTTMON* [Document ID: 24121]. Recuperado de http://www.cisco.com/image/gif/paws/24121/saa.pdf

Crawley, E., Nair, R., Rajagopalan, B. & Sandick, H. (1998, agosto). *A Framework for QoS-based Routing in the Internet* [Request for Comments: 2386. IETF - en linea]. Recuperado de http://tools.ietf.org/html/rfc2386.html

Cuéllar J.C. (2010). Análisis de configuraciones en el núcleo de una red NGN para garantizar QoS. *Sistemas & Telemática, 8*(15), 39-50

Botta, A., Dainotti, A., & Pescape A., (2007). *Multi-protocol ans multi-plataform traffic generation and measurementv* [INFOCOM 2007, Demo Session, Anchorage, Alaska, USA, May 2007]. Recuperado de http://wpage.unina.it/a.botta/pub/demoInfocom.pdf

Dipartimento di Informatica e Sistemistica D-ITG, Distributed Internet Traffic Generator [Online]. http://traffic.comics.unina.it/software/ITG/documentation.php

International Telecommunications Union - Standardization Sector [ITU-T]. (2011a). Internet protocol data communication service – IP packet transfer and availability performance parameters: Ginebra, Suiza: ITU

International Telecommunications Union - Standardization Sector [ITU-T]. (2011b). ITU-T, Recomendation Y.1541 : Network performance objectives for IP-based services. : Ginebra, Suiza: ITU

Schroder, C. (2007, ene 31). Measure Network Performance with Iperf [en línea]. Recuperado de http://www.enterprisenetworkingplanet.com/netos/article.php/3657236/Measure-Network-Performance-with-iperf.htm.

Schumann, S., Huntgeburth, B., & Maruschke, M. (2011). Opensource

based prototype for quality of service (QoS) monitoring and quality of experience (QoE) estimation in telecommunication enviroments. En Fifth International Conference on Next Generation Mobile Applications and Services.(pp.161-168). Piscataway, NJ: IEEE

Zoho Corporation. (1996). VQManager [en línea]. Recuperado de http://www.manageengine.com

Currículum vitae

Alexander Suarez Ramirez.
Ingeniero Electrónico y de Telecomunicaciones de la Universidad Autónoma de Occidente (Cali). Investigador afiliado al Grupo de Investigación en Telemática e Informática Aplicada [GITI] de la Universidad Autónoma de Occidente.

Zeida María Solarte.
Ingeniera electrónica, Especialista en Redes y Servicios Telemáticos y Magister en Telemática, de la Universidad del Cauca. Docente e investigadora afiliada al Grupo de Investigación en Telemática e Informática Aplicada [GITI] de la Universidad Autónoma de Occidente.

Juan Carlos Cuellar Q.
Ingeniero Electricista egresado de la Universidad del Valle, Especialista en Redes y Servicios Telemáticos de la Universidad del Cauca, Especialista en Redes y Comunicaciones de la Universidad Icesi. Maestría en Telecomunicaciones en la Universidad Pontificia Bolivariana de Medellín. Actualmente se encuentra desarrollando sus estudios de doctorado en telemática en la Universidad del Cauca. Profesor de tiempo completo en la Universidad Icesi y coordinador del Departamento de Ciencias Físicas y Tecnológicas y las actividades en el Laboratorio de Redes y Comunicaciones. Sus áreas de interés QoS y QoE en Redes de Próxima Generación (NGN) y configuración de dispositivos de interconectividad.