

**Universidad Central de Venezuela
Facultad de Ciencias
Escuela de Computación**

Lecturas en Ciencias de la Computación
ISSN 1316-6239

**Análisis Comparativo de
Herramientas de Evaluación de
Desempeño en Redes de
Computadores**

Prof. Karima Velásquez
Prof. Eric Gamess

RT-2009-08

Análisis Comparativo de Herramientas de Evaluación de Desempeño en Redes de Computadores

Karima Velásquez* y Eric Gamess†

RESUMEN

En la actualidad existe una amplia gama de herramientas de evaluación de desempeño en redes de computadores, lo que ofrece a investigadores y administradores de red múltiples opciones con las cuales trabajar. A pesar de que esto suena alentador, podría dificultar el proceso de selección de la herramienta apropiada. Incluso, algunas veces los usuarios se ven forzados a usar más de una herramienta hasta encontrar la que sea capaz de calcular el indicador deseado, por lo que es necesario aprender a utilizar diferentes herramientas y cómo interpretar los resultados arrojados. Este reporte ofrece una recopilación de herramientas de evaluación de desempeño de redes actualmente en uso, con la intención de guiar a los usuarios en el proceso de selección, resaltando sus principales características, fortalezas y debilidades.

1. INTRODUCCIÓN

Es común que investigadores y/o administradores de red necesiten medir distintos indicadores de red. Existen varias herramientas disponibles para este propósito, pero no todas poseen las mismas características o evalúan los mismos parámetros de rendimiento.

En ocasiones, los usuarios se ven en la obligación de usar varias herramientas para completar sus experimentos y encontrar resultados significativos. De acuerdo a la prueba a realizar, y a la red o al dispositivo de red a evaluar, una herramienta de benchmarking puede ser más apropiada que otra. Esto complica y retrasa el proceso de evaluación, ya que los usuarios se ven forzados a aprender a utilizar diferentes herramientas. Por ejemplo, Gamess y Velásquez [5] tuvieron que usar dos herramientas y programar una propia para evaluar el rendimiento de reenvío de paquetes en distintos sistemas operativos. Este trabajo presenta una recopilación actualizada de herramientas de benchmarking, a manera de ayudar a los usuarios a tomar una decisión acerca de la herramienta que sea más apropiada para sus necesidades. Adicionalmente, se plantean características deseables para una herramienta de evaluación de desempeño a ser desarrollada en un futuro.

El resto del trabajo se organiza de la siguiente manera. En la Sección 2, se presentan trabajos relacionados con este estudio. La Sección 3 muestra un profundo estudio y descripción de ocho (8) herramientas de benchmarking populares actualmente. La Sección 4 refleja un análisis comparativo de las ocho herramientas. Las conclusiones y trabajos futuros se muestran en la Sección 5.

2. TRABAJOS RELACIONADOS

Botta et al. [2] presentan un estudio minucioso sobre el estado del arte de herramientas de estimación de ancho de banda disponible. Ellos dividen el estudio en tres categorías: (1) herramientas de estimación de capacidad extremo-a-extremo, (2) herramientas de estimación de ancho de banda disponible, y (3) herramientas de medición de capacidad de transferencia y throughput TCP. Adicionalmente, introducen una herramienta llamada *BET* (*Bandwidth Estimation Tool*) y la comparan con otras herramientas de desempeño, en términos de precisión y tiempo total requerido para completar el proceso de medición. Ubik y Král [16] resumen su experiencia con herramientas de estimación de ancho de banda; se enfocan en la localización de cuellos de botella y sus tamaños. Presentan una clasificación de herramientas de estimación de ancho de banda extremo-a-extremo basándose en algunas propiedades que incluyen determinar el ancho de banda (ancho de banda instalado) vs. throughput (ancho de banda disponible), software exclusivo del lado del emisor vs. software del lado del emisor y del receptor, etc. Además describen las propiedades de un

* Laboratorio de Comunicación y Redes (LACORE) – karima.velasquez@ciens.ucv.ve

† Laboratorio de Comunicación y Redes (LACORE) – egamess@gmail.com

subconjunto de herramientas, presentan resultados de mediciones con una herramienta particular (*pathload*) sobre un escenario de alta capacidad. Gupta et al. [6] realizaron una comparación experimental entre herramientas activas y pasivas para estimación de ancho de banda de redes inalámbricas IEEE 802.11, concluyendo que para redes inalámbricas las técnicas pasivas proveen mayor precisión.

Strauss et al. [15] describen *Spruce*, una herramienta simple para medición de ancho de banda disponible, y luego la comparan con otras herramientas existentes. Su estudio se basa en precisión, patrones de falla, y cuestiones de implementación. Montesino [10] presenta un análisis comparativo a manera de estado del arte sobre herramientas y técnicas de estimación de ancho de banda activo. Ofrece una revisión corta de un conjunto de pruebas realizadas sobre diferentes condiciones y escenarios, con el propósito de medir el desempeño de las herramientas de estimación de ancho de banda activo. Mingzhe et al. [9] presentan *WBest*, una herramienta de estimación de ancho de banda para enlaces inalámbricos en redes IEEE 802.11, explicando que la mayoría de las herramientas existentes no fueron diseñadas para redes inalámbricas. Ellos definen el algoritmo usado en *WBest* y presentan una serie de experimentos y análisis de los resultados. Adicionalmente, comparan su herramienta con otras como *pathchirp* [13] y *pathload* [7].

3. HERRAMIENTAS DE EVALUACIÓN DE DESEMPEÑO

Para este estudio, se seleccionaron ocho herramientas diferentes de medición de throughput y capacidad de transferencia en lote: *Netperf*, *D-ITG*, *NetStress*, *MGEN*, *LANforge*, *Network Traffic Generator*, *Rude & Crude*, y *WlanTV*. Se seleccionaron estas herramientas por su popularidad y porque son proyectos activos. Estas herramientas también ofrecen diferentes características, lo que brinda un rango más amplio para el análisis.

El enfoque es presentar una descripción clara de las herramientas disponibles que permita guiar el proceso de selección de una herramienta sobre otra para un experimento dado. Adicionalmente, se plantean algunas características deseables para herramientas de medición de throughput y capacidad de transferencia en lote ya que la meta final es la implementación de una nueva herramienta de benchmarking.

De acuerdo a [12], las herramientas incluidas en el estudio pertenecen al grupo *throughput and bulk transfer capacity (BTC)*, que son benchmarks que emplean transferencias TCP y/o UDP de gran volumen para medir el throughput disponible en un enlace end-to-end. Las herramientas analizadas son *Netperf* versión 2.4.4, *D-ITG* versión 2.6.1d, *NetStress* versión 1.0.8350, *MGEN* versión 4.2b6, *LANforge* versión 5.0.9, *Network Traffic Generator* versión 0.1.3.1, *Rude & Crude* versión 0.62, y *WlanTV* versión 1.3.0. Para ambientes Unix, las pruebas se realizaron bajo un sistema Linux Debian 5.0 (Lenny) con kernel versión 2.6.26. Para ambientes Windows, las pruebas se realizaron bajo un sistema Windows XP Professional SP3. Los resultados del estudio de cada herramienta fueron divididos en tres categorías: *Instalación y Documentación*, *Pruebas y Usabilidad*, y *Plataformas y Protocolos Soportados*.

3.1. Netperf

*Netperf*¹ es una herramienta de benchmark de código abierto que puede usarse para medir varios aspectos del rendimiento de una red. Su enfoque principal es en la transferencia de grandes volúmenes de datos y el desempeño en tráfico de tipo solicitud/respuesta, usando TCP y UDP usando la interfaz de sockets BSD.

Netperf está diseñado siguiendo el paradigma cliente-servidor. Hay dos ejecutables (*netperf* y *netserver*). El programa *netserver* puede ser invocado por *inetd* (el demonio del sistema), o puede ser ejecutado como un demonio *standalone*. En el primer método, el usuario deben tener privilegios de administrador; el segundo método implica que el usuario debe recordar ejecutar el programa de forma explícita. El programa se puede ejecutar sin opciones, a menos que el usuario desee cambiar el puerto usado por defecto (con la opción *-p*) o desee trabajar con IPv6 (con la opción *-6*) en lugar de IPv4.

¹ <http://www.netperf.org>

3.1.1. Instalación y Documentación

Netperf fue instalado usando *Aptitude*, una utilidad manejadora de paquetes del sistema. Para lograr esto, se debió editar el archivo `/etc/apt/sources.list` (en este paso se necesitan privilegios de administrador), para añadir la rama *non-free* en los repositorios existentes, y que así el paquete pudiese ser ubicado. También es posible la instalación desde archivos fuente cuando la versión binaria no está disponible para el sistema en cuestión.

En el sitio web oficial de la herramienta se encuentra disponible la documentación. Esta incluye información detallada sobre el proceso de instalación usando los archivos fuente, y una descripción general de la herramienta. Adicionalmente, se describe cómo se pueden llevar a cabo diferentes pruebas. Finalmente, se incluyen una sección de ejemplos y otra de manejo de errores (troubleshooting).

La información reflejada en las páginas man de la herramienta no es correcta. De hecho, muchas opciones son inconsistentes con su uso real en la herramienta. Podría suponerse que las páginas man no han sido actualizadas con nuevas versiones de la herramienta, y que en realidad corresponden a versiones anteriores. Se recomienda seguir las indicaciones de la ayuda de la herramienta (que puede ser invocada con la opción `-h`), en lugar de usar las páginas man.

3.1.2. Pruebas y Usabilidad

Netperf puede ejecutarse desde una consola con el comando `netperf -H <nombreHost|direcciónIP>`, especificando el nombre del host remoto o su dirección IP, respectivamente. Al ejecutar *netperf*, se establece una conexión de control hacia el sistema remoto (*netserver*) para intercambiar parámetros de configuración y resultados hacia y desde el sistema remoto. La conexión de control es una conexión TCP que usa sockets BSD.

La duración de la prueba puede ser configurada. Los resultados finales incluyen tamaño del socket de emisor y receptor en bytes, tamaño del mensaje enviado en bytes, duración de la prueba en segundos, y throughput. Los resultados se reportan en formato de tabla. Es posible fijar diferentes unidades para la salida reportada, pero estas modificaciones deben ser indicadas al inicializar la prueba.

3.1.3. Plataformas y Protocolos Soportados

Netperf es soportado únicamente por plataformas Unix. Como protocolo de capa de red es posible usar IPv4 o IPv6, con sólo especificar la opción `-4` o `-6`, respectivamente. También es posible usar tanto TCP como UDP como protocolo de capa de transporte.

3.2. D-ITG

*D-ITG*² (Distributed Internet Traffic Generator) es una plataforma de código abierto para la generación de tráfico, capaz de producir tráfico IPv4 e IPv6 para paquetes con tamaño y tiempo inter-salida variable. Está concebida para ser usada como una herramienta distribuida de medición de rendimiento, capaz de calcular el retardo de ida (OWD – One Way Delay) y de ida-y-vuelta (RTT – Round Trip Time), la tasa de pérdida de paquetes, el jitter y el throughput [1].

D-ITG sigue el modelo cliente-servidor. Hay cuatro ejecutables básicos que implementan los componentes de la plataforma: *ITGSend*, *ITGRecv*, *ITGLog*, e *ITGDec*. *ITGSend* actúa como el cliente, y puede generar varios flujos de datos de forma simultánea siguiendo las especificaciones del archivo de entrada (o archivo de configuración). *ITGRecv* actúa como el servidor y puede recibir varios flujos de datos de diferentes clientes de forma simultánea. *ITGLog* es el servidor de almacenamiento (log) de la plataforma, y recibe información de *ITGSend* e *ITGRecv*. *ITGDec* es una utilidad que permite analizar los resultados de los experimentos realizados. Adicionalmente se cuenta con dos ejecutables más: *ITGPlot* e *ITGapi*. *ITGPlot* es una

² <http://www.grid.unina.it/software/ITG/index.php>

herramienta basada en Octave³ para graficar los datos contenidos en los archivos log construidos con ITGDec (como `delay.dat`, `bitrate.dat`, `jitter.dat` y `packetloss.dat`), que contienen un promedio del retardo, tasa de bits, jitter y tasa de pérdida, respectivamente, que son calculados cada milisegundos y reportado en el archivo respectivo. ITGapi es un API de C++ que permite el control remoto de la generación de tráfico.

Cuando *D-ITG* se ejecuta, se establece una conexión de control al sistema remoto, para entregar los parámetros de configuración de la prueba, como el protocolo de red a utilizar.

3.2.1. Instalación y Documentación

En el sitio web se pueden descargar dos archivos. El primero de ellos, `D-ITG-2.3-Familiar.zip`, contiene los binarios precompilados para ejecutar la herramienta. Esta versión no funcionó en la versión de Debian usada (Linux Debian 5.0). El segundo archivo, `D-ITG-2.6.1d.zip`, contiene los archivos fuente para su compilación. Siguiendo las instrucciones de compilación incluidas en la distribución, se usó el comando `make` y no se logró la compilación de los archivos. Es presumible la incompatibilidad entre esta versión de la herramienta y la versión de Debian empleada. Finalmente, se intentó instalar la herramienta sobre un sistema Debian más antiguo, con kernel 2.6.24; esta vez se logró la compilación de los archivos fuente siguiendo las instrucciones, y se procedió a transferir los archivos binarios resultantes al sistema original (kernel 2.6.26), donde fueron ejecutados de manera correcta.

Para plataformas Windows, se pueden descargar dos archivos: `D-ITG-2.6.1d-WINbinaryIPv4.zip` y `D-ITG-2.6.1d-WINbinaryIPv6.zip`. Estos contienen los archivos binarios listos para su ejecución. No se requiere proceso de instalación.

La documentación puede ser descargada desde el sitio web oficial. Esta incluye un manual (que también puede ser accedido desde la herramienta con la opción `-h`) y varios ejemplos de uso.

3.2.2. Pruebas y Usabilidad

D-ITG permite medir el retardo de ida, de ida-y-vuelta, la tasa de pérdida, el jitter, y el throughput.

La herramienta puede trabajar en dos modos: sencillo y script. En el modo sencillo se puede generar un único flujo de paquetes de un cliente (`ITGSend`) al servidor (`ITGRecv`). El modo script permite a `ITGSend` generar de forma simultánea varios flujos desde un mismo cliente. Cada flujo es manejado por un hilo, y un hilo adicional actúa como maestro coordinando al resto de los hilos. Para generar n flujos, el archivo de entrada debe contener n líneas, cada una de las cuales especifica las características de un flujo.

La ejecución se inicia vía consola (no se ofrece una GUI) usando diferentes opciones provistas por la herramienta, que pueden ser consultadas con la opción `-h`. Algunos parámetros configurables incluyen TTL (Time to Live), tiempo inter-salida, tamaño del payload, y tipo de protocolo.

3.2.3. Plataformas y Protocolos Soportados

D-ITG está disponible para plataformas Unix y Windows. Tanto IPv4 como IPv6 son soportados como protocolo de capa de red; en Linux, para seleccionar uno u otro el usuario debe especificar la dirección IP en el formato apropiado con la opción `-a` en `ITGSend`. En Windows hay dos binarios diferentes para el soporte de IPv4 e IPv6.

UDP es usado por defecto como protocolo de capa de transporte, pero es posible usar TCP e inclusive ICMP. Otros protocolos de capas superiores soportados incluyen Telnet, DNS, y RTP para aplicaciones de VoIP.

³ <http://www.octave.org>

3.3. NetStress

*NetStress*⁴ es una herramienta de benchmark sencilla que permite calcular el desempeño de redes cableadas e inalámbricas. Emplea transferencia de grandes volúmenes de datos con TCP. El rendimiento de la red se reporta en términos de throughput. Nuevamente, se emplea el modelo cliente-servidor durante el proceso de pruebas.

3.3.1. Instalación y Documentación

La instalación de *NetStress* es muy sencilla. Una vez descargado el instalador, sólo hace falta ejecutarlo y seguir las instrucciones del asistente de instalación.

En el sitio web oficial se encuentra un enlace al archivo de ayuda que contiene una breve descripción de la herramienta, los requerimientos del sistema, y explicaciones sobre cómo ejecutar el cliente y el servidor. Adicionalmente, incluye una sección sobre cómo interpretar los resultados reportados. Esta ayuda también puede ser accedida desde la aplicación, en el menú `Help`, seleccionando la opción `Contents`.

3.3.2. Pruebas y Usabilidad

NetStress sólo mide el máximo throughput de la red. Provee una GUI donde el usuario puede seleccionar diferentes opciones. Una vez iniciada la herramienta, se debe seleccionar un modo: cliente o servidor. El servidor escucha paquetes de red, mientras que el cliente transmite los paquetes a la red. La herramienta reporta la cantidad de bytes enviados, bytes recibidos, y el throughput, en modo texto y gráficamente.

No hay opción de detener la prueba, ni tampoco una forma de especificar la duración del experimento o la cantidad de datos a transferir, así que el usuario debe cerrar la aplicación para detener el experimento.

3.3.3. Plataformas y Protocolos Soportados

NetStress es soportado por plataformas Windows. Emplea IPv4 como protocolo de capa de red y TCP como protocolo de capa de transporte. No ofrece soporte para otros protocolos.

3.4. MGEN

Multi-Generator⁵ (*MGEN*) es una herramienta de código abierto desarrollada por el grupo de investigación PROTOcol Engineering Advanced Networking (PROTEAN) del Laboratorio de Investigación de la Armada (NRL - Naval Research Laboratory). *MGEN* ofrece la posibilidad de realizar pruebas de rendimiento sobre redes IP y mediciones usando tráfico UDP/IP. Soporta tanto generación de tráfico unicast como multicast. Sigue el modelo cliente-servidor, usando el mismo programa para ambos extremos.

Actualmente, existen dos versiones disponibles de *MGEN* (3.X y 4.X), que no son interoperables. Algunas versiones (3.X) poseen interfaz gráfica. *MGEN* 4.X actualmente debe ser ejecutada por líneas de comando.

3.4.1. Instalación y Documentación

Existen dos paquetes disponibles para plataformas Linux: código fuente y versión precompilada. Se decidió instalar la herramienta desde los archivos fuentes para garantizar la compatibilidad con el sistema. Se procedió a descomprimir el archivo y usar el comando `make -f Makefile.linux`, ya que se ofrecen varios *makefiles* para sistemas Unix y el usuario debe seleccionar de acuerdo al sistema en cuestión. Para plataformas Windows no hay necesidad de instalación, ya que el archivo ZIP incluye un archivo ejecutable listo para usar.

⁴ <http://www.performancewifi.net/performance-wifi/main/netstress.htm>

⁵ <http://cs.itd.nrl.navy.mil/work/mgen>

La distribución contiene un archivo `html` con documentación extensa. Allí se explica el uso de la herramienta y sus diferentes opciones. Además ofrece varios ejemplos sobre cómo usar la herramienta para medir el desempeño de la red.

3.4.2. Pruebas y Usabilidad

Se puede usar archivos de entrada (archivos de configuración) para definir patrones de carga de la red durante el tiempo. También está disponible la opción de líneas de comando.

Los archivos de entrada se pueden usar para especificar patrones de tráfico de aplicaciones unicast y/o multicast UDP/IP. Los flujos de datos definidos pueden seguir patrones periódicos (CBR – Constant Bit Rate), Poisson, y por ráfagas. Estos flujos de datos pueden ser modificados durante el experimento, ya que el archivo de entrada permite alterar un flujo dado en un momento determinado.

Algunos campos de la cabecera IP pueden ser fijados por el usuario. Cuando se define un flujo multicast, el usuario puede especificar el TTL. Tanto para flujos unicast como multicast, el valor del campo ToS (Type of Service) también puede ser especificado. Para IPv6, se puede definir el valor del campo *Flow Label*. Para flujos multicast, el usuario puede controlar cuando unirse o dejar un grupo multicast, indicando la dirección IP del grupo multicast al que unirse o abandonar y el tiempo.

Los resultados son mostrados por la salida estándar, o pueden ser redirigidos a un archivo para su posterior análisis. Estos resultados sólo representan el reporte de los paquetes intercambiados; no se ofrece información adicional.

Para obtener estadísticas, el usuario debe almacenar los resultados en un archivo, que pueda ser usado posteriormente como entrada del programa `trpr`⁶ (Trace Plot Real-time). `trpr` analiza la salida de *MGEN* y crea una salida apropiada para su graficación. Además, soporta un rango de funcionalidades para uso específico del programa de graficación `gnuplot`⁷.

Resultados importantes como throughput, latencia de entrega, tasa de pérdida, y latencia de unión/abandono de grupos multicast pueden ser calculados a partir de la información en el archivo de salida. Sin embargo, esta tarea es dejada al usuario; *MGEN* no provee resultados estadísticos.

3.4.3. Plataformas y Protocolos Soportados

La versión más reciente de *MGEN*, *MGEN* 4.0, provee soporte para plataformas Win32, y adicionalmente a una amplia gama de plataformas basadas en Unix, incluyendo MacOS X. Existen planes para varias mejoras, incluyendo el soporte a TCP, ya que actualmente sólo se soporta UDP. IPv4 e IPv6 pueden ser usados como protocolo de capa de red.

3.5. LANforge

*LANforge*⁸, de Candela Technologies, consiste en dos herramientas: *LANforge-FIRE*, usada para generación de tráfico que simula el extremo de la red simulada; y *LANforge-ICE* que es usada para simular el core de una red. *LANforge* es una herramienta propietaria que puede ser adquirida en su sitio web. Candela Technologies ofrece una gran variedad de opciones de compra. Para obtener esta herramienta, también es posible crear una cuenta que permite la posterior descarga de una versión de prueba de la misma.

3.5.1. Instalación y Documentación

Para la instalación en Linux se necesita el archivo `LANforgeServer-X.Y.Z_Linux-x64.tar.gz` (donde X.Y.Z indican la versión). Una vez que se descomprime, se ejecuta el script `install.bash`. Se

⁶ <http://pf.itd.nrl.navy.mil/protocols/trpr.html>

⁷ <http://www.gnuplot.info>

⁸ http://www.candelatech.com/lanforge_v3/datasheet.html

requiere un directorio home para la herramienta. Por defecto, se usa el directorio `/home/lanforge`, pero esto puede ser modificado por el usuario ejecutando la opción `install.bash -d <directorio>`. Una vez terminada la ejecución del archivo `install.bash`, se debe ejecutar el archivo `lfconfig` (con las opciones `-cwd`) desde el directorio local de la herramienta. Ambos scripts son auto explicativos, ofreciendo información al usuario. Para la GUI, se debe instalar el paquete `LANforgeGUI_X.Y.Z_Linux.tar.bz2`, y ejecutar el script `lfgui_install.bash`.

Para la instalación sobre plataformas Windows, fueron descargados dos archivos: `LANforge-Server-X.Y.Z-Installer.exe` y `LANforge-GUI-X.Y.Z-Installer.exe`. Luego sólo es necesario seguir las instrucciones del asistente de instalación. El proceso de instalación es sencillo y rápido.

Existe una documentación completa disponible en el sitio web de la herramienta, que incluye un manual de usuario, y guías de instalación y actualización para cada paquete. La guía de instalación incluye una descripción paso a paso del proceso; y una sección de problemas frecuentes. Adicionalmente, existen manuales disponibles en el sitio web. Estos incluyen ejemplos explícitos sobre cómo usar la herramienta en diferentes escenarios, complementada con capturas de pantallas detalladas que describen los procesos de configuración y prueba.

3.5.2. Pruebas y Usabilidad

LANforge es una herramienta que permite la simulación de redes y la ejecución de pruebas sobre ellas. Incluye una GUI que facilita el proceso de pruebas. Se puede realizar un conjunto de pruebas, que incluye la configuración de routers virtuales (sólo en la versión de Linux). Entre los resultados obtenidos se puede mencionar bytes recibidos y transmitidos, bits por segundo (bps) recibidos y transmitidos, colisiones y errores. Los resultados se muestran en modo texto y gráficamente.

El usuario puede configurar muchos detalles, incluyendo el número de paquetes a enviar, el tipo de interfaz del *endpoint* a simular (ISDN, T1, modem, etc), e incluso *payloads* personalizados.

LANforge también incorpora un generador de llamadas de VoIP (Voice over IP), el cual soporta actualmente H.323 y SIP (Session Initiation Protocol). El *payload* de voz es transmitido vía RTP (Real-time Transport Protocol) que se encapsula en UDP.

La GUI de *LANforge* tiene muchas solapas que agrupan diferentes pruebas, y puede ser complejo de usar debido al gran número de opciones ofrecidas. Sin embargo, existe información detallada de cada solapa en el manual de usuario de la GUI, que se encuentra disponible en el sitio web. Este manual incluye varios ejemplos y capturas de pantalla que aclaran el proceso.

3.5.3. Plataformas y Protocolos Soportados

Existen versiones disponibles para Linux, Windows y Solaris. Los protocolos soportados incluyen, pero no están limitados a, Ethernet crudo, MPLS, IPv4, IPv6, ICMP, OSPF, BGP, UDP, TCP, FTP, HTTP, y HTTPS.

3.6. Network Traffic Generator

*Network Traffic Generator*⁹ es una herramienta de código abierto que genera tráfico TCP y UDP de cliente(s) a servidor(es) a manera de estresar routers y firewalls bajo una carga pesada de tráfico. No reporta resultados de rendimiento de la red (throughput, retardo, tasa de pérdida), sino que sólo envía tráfico con el objetivo de saturar dispositivos de red.

⁹ <http://sourceforge.net/projects/traffic>

3.6.1. Instalación y Documentación

El proceso de instalación es simple, siguiendo los pasos del archivo README incluido en el tar. La herramienta usa el modelo cliente-servidor. El archivo tar incluye dos archivos ejecutables: *trafserver* y *trafclient*, que son el servidor y cliente, respectivamente, que se usan desde la línea de comandos. Existen planes de incluir una GUI próximamente.

La documentación se ofrece a través del archivo README que se encuentra en el tar, y también en la ayuda de la herramienta, a la que se accede ejecutando el cliente sin parámetros.

3.6.2. Pruebas y Usabilidad

Todos los parámetros se deben especificar vía consola, no se ofrece la opción de crear un archivo de entrada (o de configuración) de manera de acelerar el proceso para pruebas repetidas.

3.6.3. Plataformas y Protocolos Soportados

Es posible especificar el protocolo a usar (TCP o UDP), el tamaño del *payload*, y el número de clientes que enviarán tráfico.

3.7. Rude & Crude

*Rude*¹⁰ (Real-time UDP Data Emitter) es un programa que genera tráfico de red, y *Crude* (Collector for *Rude*) recibe el tráfico generado por *Rude*, siguiendo el paradigma cliente-servidor. Actualmente, sólo genera y mide tráfico UDP.

3.7.1. Instalación y Documentación

Para instalar *Rude* se debe descargar el paquete y descomprimirlo. Luego, se usa el script *configure* para crear el *makefile*, y usarlo mediante los comandos *make* y *make install*. Para el proceso de instalación se requieren privilegios de administrador.

La documentación se ofrece vía páginas *man*, que se encuentran disponibles una vez que la herramienta se instala. Adicionalmente, en el sitio web se encuentran instrucciones para el proceso de instalación.

3.7.2. Pruebas y Usabilidad

El funcionamiento y la configuración son similares a los de *MGEN*, pero estos proyectos no comparten código. El usuario debe escribir un archivo de entrada (archivo de configuración) que define el experimento. Se pueden definir múltiples flujos en el archivo de entrada. En la documentación se incluye un archivo ejemplo, que también está descrito en las páginas *man*.

Los resultados se muestran por defecto en la salida estándar, pero pueden ser redirigidos a un archivo para ser procesados posteriormente. Estos resultados incluyen estadísticas del número de paquetes recibidos, número de paquetes recibidos fuera de secuencia, paquetes perdidos, total de bytes recibidos, retardo promedio, jitter, y throughput.

3.7.3. Plataformas y Protocolos Soportados

La herramienta se ejecuta en plataformas Unix. Los protocolos soportados son UDP/IPv4.

¹⁰ <http://rude.sourceforge.net>

3.8. Wlan Traffic Visualizer

*WLAN Traffic Visualizer*¹¹ (*WlanTV*) permite medir la carga de la red y visualizar secuencias de tramas en redes WLAN IEEE 802.11 [16]. Se encuentra publicada bajo licencia GPL. Está desarrollada en Java, y se encuentran disponibles para la descarga en el sitio web versiones fuente y JAR.

3.8.1. Instalación y Documentación

WlanTV requiere *Wireshark*¹² (Windows) o *TShark* (Linux), y Java Runtime Environment JRE 1.6 o superior para la compilación y ejecución del programa. Sólo se requieren los paquetes estándar de Java. Se usa *TShark* para decodificar archivos log y para realizar capturas en vivo.

Al instalar *WlanTV* a partir de la distribución JAR, y usando el comando `java -jar wlanTV.jar` se abre la GUI desde donde el usuario puede realizar los experimentos.

La documentación no es muy extensa. La distribución incluye un archivo README muy pequeño con pocas instrucciones sobre los prerrequisitos del sistema y pocas instrucciones sobre la instalación y ejecución. También se encuentra disponible para su descarga en el sitio web una captura ejemplo.

3.8.2. Pruebas y Usabilidad

Esta herramienta no usa el modelo cliente-servidor. Sólo se necesita un computador para realizar los experimentos. Este computador captura el tráfico de una red IEEE 802.11 y reporta resultados obtenidos en esa captura.

Para los experimentos, el usuario puede utilizar una captura previa, o iniciar una captura en vivo. Esta segunda opción obliga al usuario a detener la captura para poder observar los resultados; que incluyen un conteo de tramas, conteo de bytes, duración de la captura, throughput, información detallada de cada paquete (protocolos, longitud, direcciones, etc.), y distribución del ancho de banda. Los resultados se despliegan en modo texto y gráficamente.

3.8.3. Plataformas y Protocolos Soportados

WlanTV se encuentra disponible para plataformas Linux y Windows. La herramienta reporta estadísticas para protocolos IEEE 802.11.

4. ANÁLISIS COMPARATIVO

En la Tabla 1 se comparan las herramientas evaluadas. Se consideran algunas características importantes a resaltar, como: última actualización, A/P, privilegios, plataforma soportada, protocolos soportados, y sincronización. La fecha de la última actualización es importante ya que muestra qué tan activo es el proyecto. La categoría A/P indica si la herramienta es activa (A) o pasiva (P). Las herramientas activas afectan el tráfico normal de la red, inyectando paquetes propios a la misma; mientras que las herramientas pasivas sólo capturan el tráfico que pasa a través de la interfaz. La fila *Privilegios* ofrece información sobre los permisos de usuario requeridos para instalar o ejecutar la aplicación. El estudio de plataformas soportadas se limitó a Windows y Linux. En cuanto a los protocolos, se estudian los protocolos de capa de red y de transporte. Para los resultados reportados el estudio se centró en retardo, jitter y throughput. En la fila etiquetada *Sincroniz. requerida* se indica la necesidad de sincronizar los relojes de las estaciones donde se ejecutan los procesos de prueba.

De acuerdo a la Tabla 1, algunos proyectos son más activos que otros. Al parecer, *Rude & Crude* y *Network Traffic Generator* no han estado activos por algún tiempo, ya que la última versión fue publicada hace más de

¹¹ <http://sourceforge.net/projects/wlantv>

¹² <http://www.wireshark.org>

6 años. Otro aspecto importante es el costo. La mayoría de las herramientas evaluadas son gratuitas, a excepción de *LANforge*. Los precios de *LANforge* oscilan entre los \$1999 (USD) y los \$49000 (USD); esto puede ser un impedimento para algunos investigadores o administradores de red. También es importante notar si la herramienta es activa o pasiva. Entre las herramientas estudiadas, sólo *WlanTV* no inyecta tráfico adicional a la red; sin embargo, esto implica que la herramienta no es capaz de medir el throughput de la red, sino que sólo reporta los resultados de la tasa de transmisión de los paquetes capturados durante la prueba.

También es notable que sólo *Network Traffic Generator* y *Rude & Crude* requieren privilegios de administrador (root) para su instalación; mientras que *WlanTV* necesita privilegios de administrador para su ejecución, ya que debe colocar la tarjeta de red en modo promiscuo para realizar las capturas de tráfico. Se puede decir que Linux se destaca como la opción más popular entre las plataformas soportadas. Adicionalmente, se puede ver que la mayoría de las herramientas ya incluye soporte para IPv6. El throughput de red es el resultado reportado más comúnmente, seguido por el retardo y el jitter. *Network Traffic Generator* no reporta resultados, ya que su principal objetivo es inyectar tráfico a la red para estresar switches y routers.

Tabla 1: Características Principales de las Herramientas Evaluadas

Aspecto	Netperf	D-ITG	NetStress	MGEN	LANforge	Network Traffic Generator	Rude & Crude	WlanTV
Versión evaluada	2.4.4	2.6.1d	1.0.8350	4.2b6	5.0.9	0.1.3.1	0.62	1.3.0
Última actualiz.	10/2007	09/2008	09/2008	10/2005	04/2009	01/2003	09/2002	12/2008
Gratis	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí
Open source	Sí	Sí	No	Sí	No	Sí	Sí	Sí
A/P	Activa	Activa	Activa	Activa	Activa	Activa	Activa	Pasiva
Privilegios	Usuario	Usuario	Usuario	Usuario	Usuario	Root	Root	Root
Plataforma soportada	Linux	Linux, Windows	Windows	Linux, Windows	Linux, Windows	Linux	Linux	Linux, Windows
Protocolo de red	IPv4, IPv6	IPv4, IPv6, ICMPv4, ICMPv6	IPv4	IPv4, IPv6	IPv4, IPv6, ICMPv4, ICMPv6	IPv4	IPv4	IPv4, IPv6
Protocolo de transporte	TCP, UDP	TCP, UDP	TCP	UDP	TCP, UDP	TCP, UDP	UDP	TCP, UDP
Resultados reportados	Throughput	Retardo, jitter y throughput	Throughput	Retardo y throughput	Retardo, jitter y throughput	--	Retardo, jitter y throughput	Throughput
Interfaz de usuario	Consola	Consola	GUI	Consola	GUI	Consola	Consola	GUI
Sincroniz. requerida	No	No	No	No	No	--	Sí	--

En relación a la interfaz de usuario, pocas herramientas ofrecen GUI. Para facilitar el proceso de evaluación, algunas herramientas (*D-ITG*, *MGEN*, y *Rude & Crude*) usan un archivo de entrada que contiene los parámetros y la descripción de la prueba, lo que resulta más flexible que el tradicional pase de argumentos a través de la línea de comandos.

Un último aspecto de gran importancia es la sincronización, especialmente cuando se mide retardo. La sincronización manual no es recomendada, por su pobre precisión. Una solución es usar NTP (Network Time

Protocol); esto requiere configuración adicional y un mayor conocimiento por parte del investigador o administrador de red.

5. CONCLUSIONES Y TRABAJOS FUTUROS

En este trabajo se analiza la evaluación y comparación de varias herramientas de benchmarking. Se estudiaron ocho herramientas: *Netperf*, *D-ITG*, *NetStress*, *MGEN*, *LANforge*, *Network Traffic Generator*, *Rude & Crude*, y *WlanTV*. La evaluación fue categorizada en instalación y documentación, pruebas y usabilidad, y plataformas y protocolos soportados. La Tabla 1 resume el resultado del estudio. Se puede observar que ninguna de las ocho herramientas resulta como clara ganadora, así que de manera general, los usuarios deberán instalar varias de estas herramientas para realizar experimentos básicos de desempeño de red. *Netperf* es una herramienta sencilla y muy fácil de usar; sin embargo los resultados de las pruebas están limitados al throughput. *D-ITG* es una herramienta más poderosa que reporta resultados más variados, como Ritter, retardo, y throughput; pero los tiempos reportados por esta herramienta no son realistas. En los experimentos realizados, se obtuvieron retardos mayores a una hora. Se asume que no es un problema de instalación, puesto que hay algunos experimentos reportados en el manual de la herramienta con tiempos similares. Adicionalmente, los usuarios deben enfrentar algunos problemas durante la instalación en algunas versiones de Debian. *NetStress* es una herramienta fácil de usar que además ofrece una GUI; pero tiene un pobre soporte de protocolos, y las pruebas no pueden ser parametrizadas ni detenidas. *MGEN* permite la parametrización de las pruebas, y también ofrece una documentación completa; sin embargo, no es muy sencilla de utilizar, debido a la gran cantidad de opciones que ofrece. Además, no muestra los resultados de las pruebas directamente, sino que los usuarios deben calcularlos a partir de la información de los paquetes intercambiados.

LANforge ofrece soporte para muchos protocolos y pruebas; es fácil de instalar y tiene una buena documentación. Su principal desventaja es el alto costo de la licencia. *Network Traffic Generator* puede usarse para estresar dispositivos de red (switches y routers), pero no reporta ningún resultado de desempeño. *Rude & Crude* es muy fácil de usar y ofrece muchos indicadores para evaluar el desempeño de la red. *WlanTV* es una herramienta pasiva que ofrece indicadores relevantes del rendimiento del tráfico capturado en una red WiFi.

Para trabajos futuros se plantea el diseño y la implementación de una herramienta de medición de desempeño para redes de computadores que incorpore las fortalezas de las herramientas evaluadas en este estudio, y eliminando sus debilidades, siguiendo el modelo cliente/servidor. La herramienta debe ser compatible con los RFCs 1242 [3], 2544 [4], y 5180 [11], donde se definen una serie de recomendaciones para el desarrollo de benchmarks. Uno de los principales intereses es ofrecer soporte al protocolo IPv6. Adicionalmente, será distribuida bajo la licencia GNU General Public License.

Entre las características que se plantea incluir en la herramienta, se encuentra el cálculo de la tasa de pérdida, throughput, y RTT para diferentes protocolos (TCP, UDP, ICMP, e IP). Las pruebas serán parametrizadas, permitiendo a los usuarios definir la generación del tráfico siguiendo distintos modelos (variables aleatorias) que incluyen CBR, ráfaga, Poisson y Exponencial. Los usuarios podrán especificar los valores de algunos campos de las cabeceras de los paquetes, como TTL y ToS en IPv4, y CoS, Hop Limit y Flow Label en IPv6.

Como se mostró en el análisis, la mayoría de las herramientas no ofrece soporte específico para redes WiFi. Para redes IEEE 802.11 sólo se ofrece evaluación de desempeño end-to-end. Los usuarios no tiene forma de obtener resultados (ancho de banda, retardo, tasa de pérdida) entre la estación móvil y el punto de acceso (o router inalámbrico). Por esto, también se planea adaptar la herramienta para su uso sobre puntos de acceso. Este desarrollo se realizara para puntos de acceso que soporten DD-WRT¹³ u OpenWrt¹⁴, dos firmwares gratuitos basados en Linux para routers inalámbricos.

¹³ <http://www.dd-wrt.com>

¹⁴ <http://www.openwrt.org>

REFERENCIAS

- [1] A. Botta, A. Dainotti, and A. Pescapé. Multi-Protocol and Multi-Platform Traffic Generation and Measurement. INFOCOM 2007 Demo Session. May 2007.
- [2] A. Botta, A. Pescapé, and G. Ventre. On the Performance of Bandwidth Estimation Tools. In proceedings of the 2005 Systems Communications (ICW'05). August 2005.
- [3] S. Bradner. Benchmark Terminology for Network Interconnection Devices. RFC 1242. July 1991.
- [4] S. Bradner and J. McQuaid. Benchmarking Methodology for Network Interconnect Devices. RFC 2544. March 1999.
- [5] E. Gamess and K. Velásquez. IPv4 and IPv6 Forwarding Performance Evaluation on Different Operating Systems. XXXIV Conferencia Latinoamericana de Informática (CLEI 2008). September 2008.
- [6] D. Gupta, D. Wu, P. Mohapatra, and C. Chuah. Experimental Comparison of Bandwidth Estimation Tools for Wireless Mesh Networks. IEEE INFOCOM Mini-Conference. April 2009.
- [7] M. Jain and C. Dovrolis. Pathload: A Measurement Tool for End-to-End Available Bandwidth. In Proceedings of Passive and Active Measurements (PAM) Workshop. March 2002.
- [8] V. Kumar, M. Korpi, S. Sengodan, and V. Kumar. IP Telephony with H.323: Architectures for Unified Networks and Integrated Services. Wiley; 1st edition. March 2001.
- [9] L. Mingzhe, M. Claypool, and R. Kinicki. WBest: a Bandwidth Estimation Tool for IEEE 802.11 Wireless Networks. In Proceedings of 33rd IEEE Conference on Local Computer Networks (LCN). October 2008.
- [10] F. Montesino. Assessing Active Bandwidth Estimation Tools in High Performance Networks. TERENA Networking Conference. June 2004.
- [11] C. Popoviciu, A. Hamza, G. Van de Velde, and D. Dugatkin. IPv6 Benchmarking Methodology for Network Interconnect Devices. RFC 5180. May 2008.
- [12] R. Prasad, M. Murray, C. Dovrolis, and K. Claffy. Bandwidth Estimation: Metrics, Measurement Techniques, and Tools. IEEE Network, vol. 17 No. 6, Nov-Dec 2003, pp. 27-35. April 2004.
- [13] V. Ribeiro, R. Riedi, R. Baraniuk, J. Navratil, and L. Cottrell. pathChirp: Efficient Available Bandwidth Estimation for Network Paths. In Proceedings of Passive and Active Measurements (PAM) Workshop. April 2003.
- [14] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. SIP: Session Initiation Protocol. RFC 3261. June 2002.
- [15] J. Strauss, D. Katabi, and F. Kaashoek. A Measurement Study of Available Bandwidth Estimation Tools. IMC2003. October 2003.
- [16] S. Ubik and A. Král. End-to-End Bandwidth Estimation Tools. CESNET Technical Report. 25/2003. November 2003.
- [17] H. Unander and W. Wenjuan. Accurate Measurement and Visualization of Traffic Load in IEEE 802.11 WLANs. Master Thesis. University of Agder. Norway. May 2008.

GLOSARIO DE TÉRMINOS

Benchmark: prueba que mide el performance de un sistema o subsistema en una tarea o conjunto de tareas bien definidas.

Firmware: bloque de instrucciones de programa para propósitos específicos, grabado en una memoria de tipo no volátil (ROM, EEPROM, flash), que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo.

GNU Public License: Licencia creada por la *Free Software Foundation* orientada principalmente a defender la libre distribución, modificación, y uso del software.

GUI (Graphic User Interface): tipo de interfaz de usuario que utiliza un conjunto de imágenes y objetos gráficos para representar la información y acciones disponibles en la interfaz.

Jitter: variación en cuanto a la latencia entre paquetes de datos que se reciben.

Manejador de paquetes: colección de herramientas que sirven para automatizar el proceso de instalación, actualización, configuración, y eliminación de paquetes de software.

Memoria FLASH: tipo de memoria ROM en la cual puede escribirse en cualquier momento sin borrar todo el contenido anterior, ya que permite actualizaciones a nivel de byte.

OWD (One Way Delay): retardo desde un extremo a otro, en un solo sentido de la comunicación.

RTT (Round Trip Time): tiempo que tarda un paquete enviado desde un emisor en volver a este mismo emisor habiendo pasado por el receptor de destino.

Throughput: tasa máxima en la que ninguna de las tramas es descartada por el dispositivo de red.

Tiempo inter-salida: tiempo transcurrido entre el envío de dos frames consecutivos.