# Gráficos de tráfico y estadísticas usando MRTG

La presentación de gráficos estadísticos para evaluar el uso del ancho de banda a Internet se considera una característica opcional de un router; sin embargo, es importante saber esta información para entender si en el acceso a Internet hay ineficiencias debido a la pobre distribución de ancho de banda entre los tipos de tráficos (VoIP, Web, P2P, FTP,...) que compiten en la utilización de la conexión a Internet.
Muchos de los enrutadores utilizan SNMP (Simple Network Management Protocol) para exportar el valor de los contadores de tráfico entrante y saliente para cada una de las interfaces de red. Usando software tales como MRTG (Multi Router Traffic Grapher) posibilitan que en repetidas ocasiones, y en intervalos de tiempos regulares, se ejecuten consultas SNMP hacia estos routers y guarden los contadores de tráfico. Una vez hecho esto, MRTG permite el análisis gráfico, a través de un navegador, de la progresión del tráfico entrante y saliente de las interfaces del router.

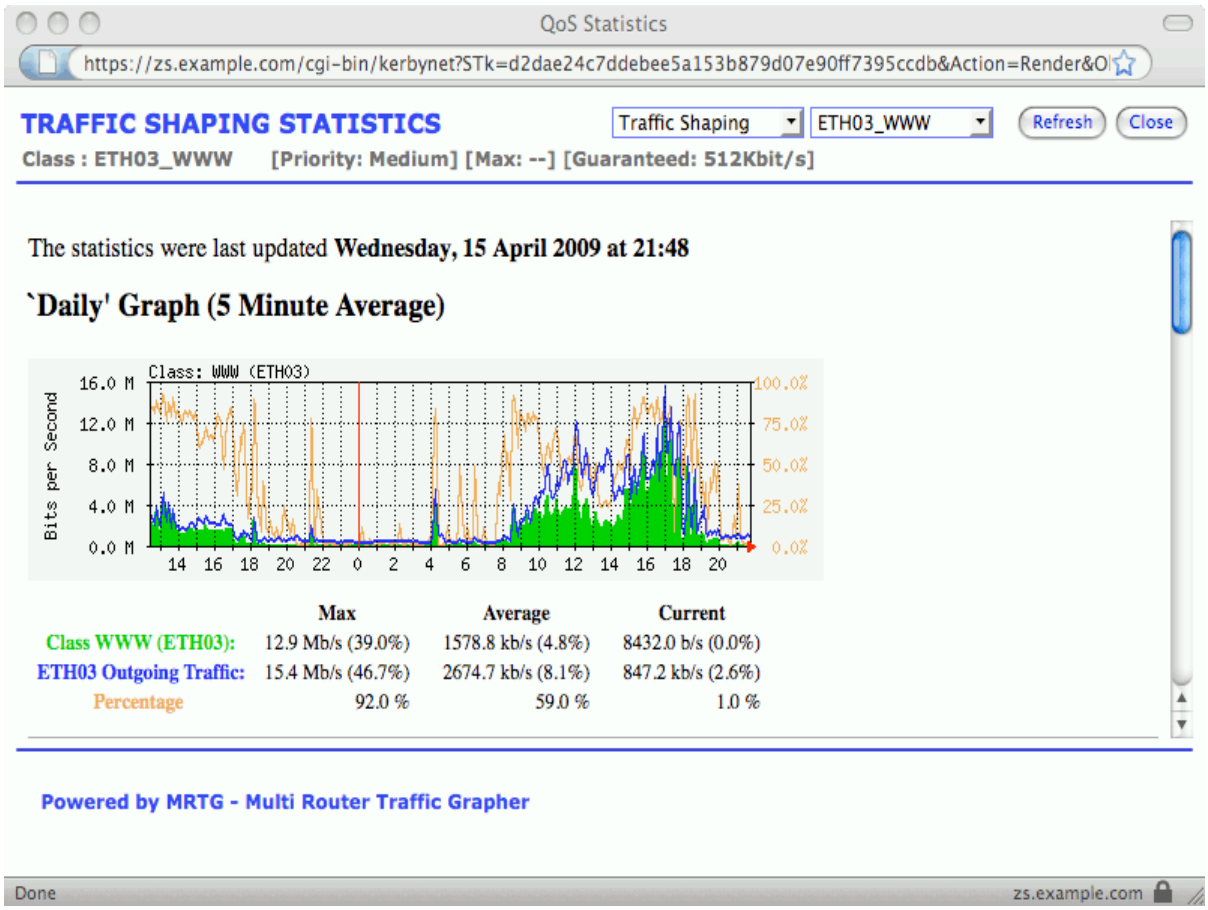


**Figure 1 – Ejemplo de un grafico MRTG relacionado con la clasificación del trafico para WWW.**

Zeroshell no sigue esta estrategia de exportación mediante SNMP (ver nota *), sino que integra directamente dentro de MRTG para permitir el análisis de los parámetros que van más allá de los obtenidos utilizando SNMP. En virtud de ello, los siguientes parámetros pueden ser analizados directamente desde la interfaz Web Zeroshell:

- Sistema de carga
- Número de conexiones activas (TCP / UDP) desde y hacia Internet;
- Interfaz de tráfico entrante y saliente, ya sea una tarjeta Ethernet, una red VLAN 802.1Q, una VPN, un puente, un vínculo, una conexión PPPoE (ADSL por ejemplo) o una conexión móvil de 3G (UMTS, por ejemplo / HSDPA);
- Tráfico clasificados por la modulación del tráfico en una clase determinada QoS (VoIP, HTTP, peer to peer, ...) en relación con el tráfico general de la interfaz de salida;

- Balance del tráfico de Internet en varias puertas de enlace WAN (Balanceo de carga y conmutación por error) en comparación con el total de tráfico desde y hacia Internet.

El resto del documento se subdivide en las siguientes secciones:

- Promedio del Sistema de carga
- Conexiones TCP / UDP activas
- Tráfico entrante y saliente de una interfaz de red
- Gráficos de Tráfico sub-divididos por clases QoS
- Distribución del tráfico en las puertas de enlaces de Internet en equilibrio de carga
- Activación de MRTG en Zeroshell
    - Claves de activación

## *Promedio del Sistema de carga*

La información estadística sobre la carga media no cubre directamente el tráfico de una red, sin embargo es útil para comprender si los recursos de hardware del router (el procesador en particular) son un cuello de botella para la LAN y ralentiza las conexiones independientes de la banda disponible en el acceso a enlaces a la Internet. Para ver el grafico de carga del sistema haga clic en el enlace [Gráficos] en el marco de la parte superior derecha. Aparecerá una ventana como la que se muestra a continuación.

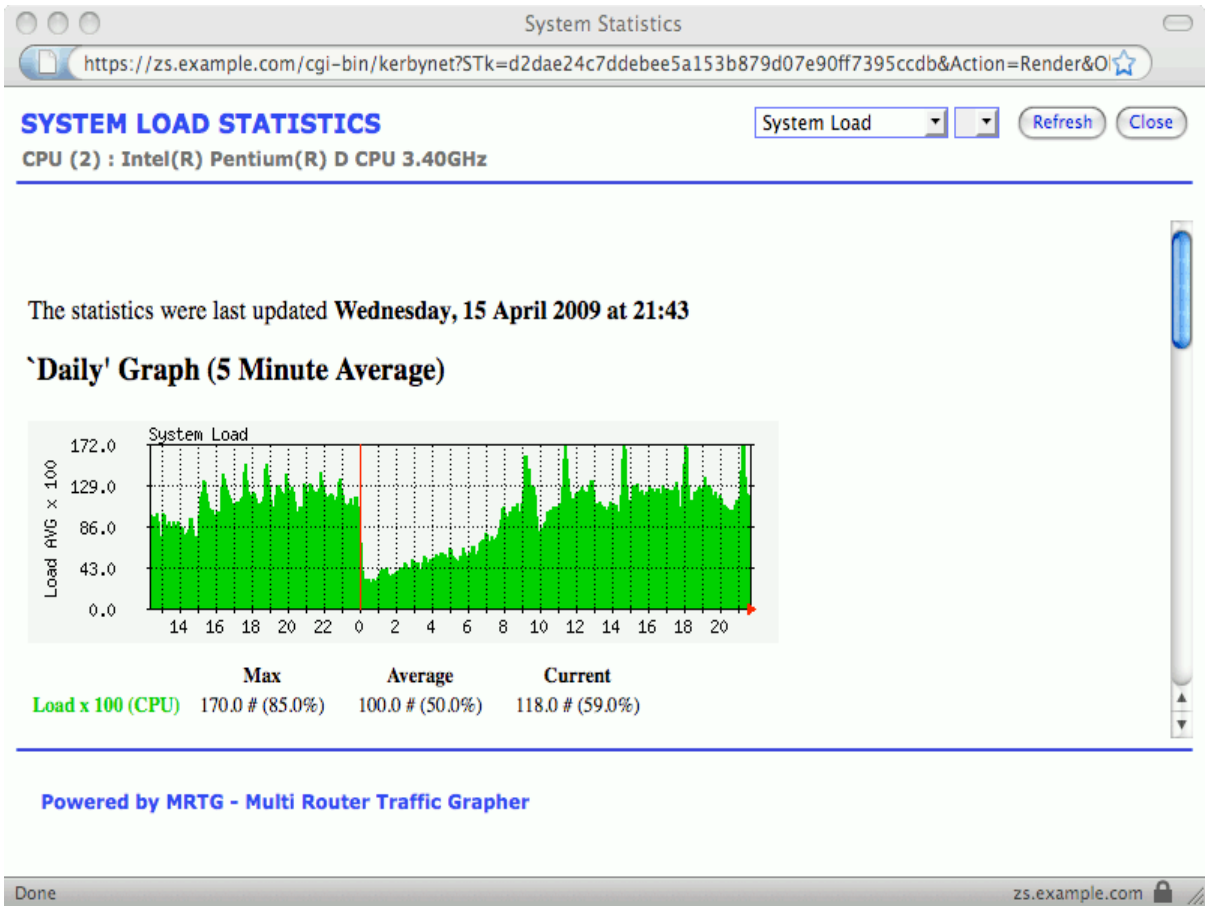


**Figure 2 Gráfico relacionado con la carga del sistema.**

La carga promedio es calculada cada 5 minutos multiplicados por 100 se toma en consideración. El porcentaje de uso del sistema (que figura en paréntesis) tiene en cuenta el número de CPU del router. En otras palabras, vamos a asumir una carga de 100 en un sistema con 2 procesadores, el porcentaje de utilización que indica es de 50%. Por lo tanto, el umbral crítico para que el router pueda ser sospechoso de ser un cuello de botella es de 200 igual a 100% de uso.

Los factores que contribuyen principalmente al uso de la CPU en orden creciente son: \

- las reglas del firewall, la clasificación QoS y el equilibrio de carga manual
- las reglas del firewall y QoS que utilizan los filtros de capa 7 para ejecutar el DPI, cuando muchas conexiones están presentes. Tenga en cuenta que los filtros de L7 inspeccionan el contenido de los paquetes sólo en cuanto se establece una conexión, mientras que el resto se identifican mediante el seguimiento de conexiones (Connection Tracking). Esto pone de manifiesto que los filtros de nivel de aplicación no cargan el sistema basándose en la banda utilizada, sino sobre la base del número de nuevos TCP / UDP abiertos.

- Escribir el resultado del seguimiento de conexiones (Connection Tracking) en los registros. Hacer un seguimiento de las conexiones TCP / UDP no es una funcionalidad muy derrochadora en términos de CPU. Sin embargo, puede ser si el sistema está configurado para registrar las conexiones (IP de origen, puerto de origen, de destino IP, puerto de destino) en los registros.
- Captive Portal activos en una LAN con muchos clientes activos, pero aún no autenticados. A menudo, la presencia de gusanos u otros programas que utilizan el protocolo TCP en puertos 80 y 443 para otras solicitudes de HTTP/HTTPS pueden empeorar la situación.
- El uso del HTTP Proxy transparente con antivirus (ClamAV) o un filtro de contenido Web (DansGuardian). De hecho, tener que examinar el contenido de las páginas Web inevitablemente sobrecarga la CPU. En tales casos, es necesario también garantizar una cantidad de memoria RAM suficiente para evitar el intercambio de discos.

## *Conexiones TCP / UDP activas*

La progresión del número de conexiones activas es un buen índice para monitorear la actividad de la red. Por ejemplo, un elevado número de conexiones podría significar el intercambio de archivos utilizando técnicas de P2P.

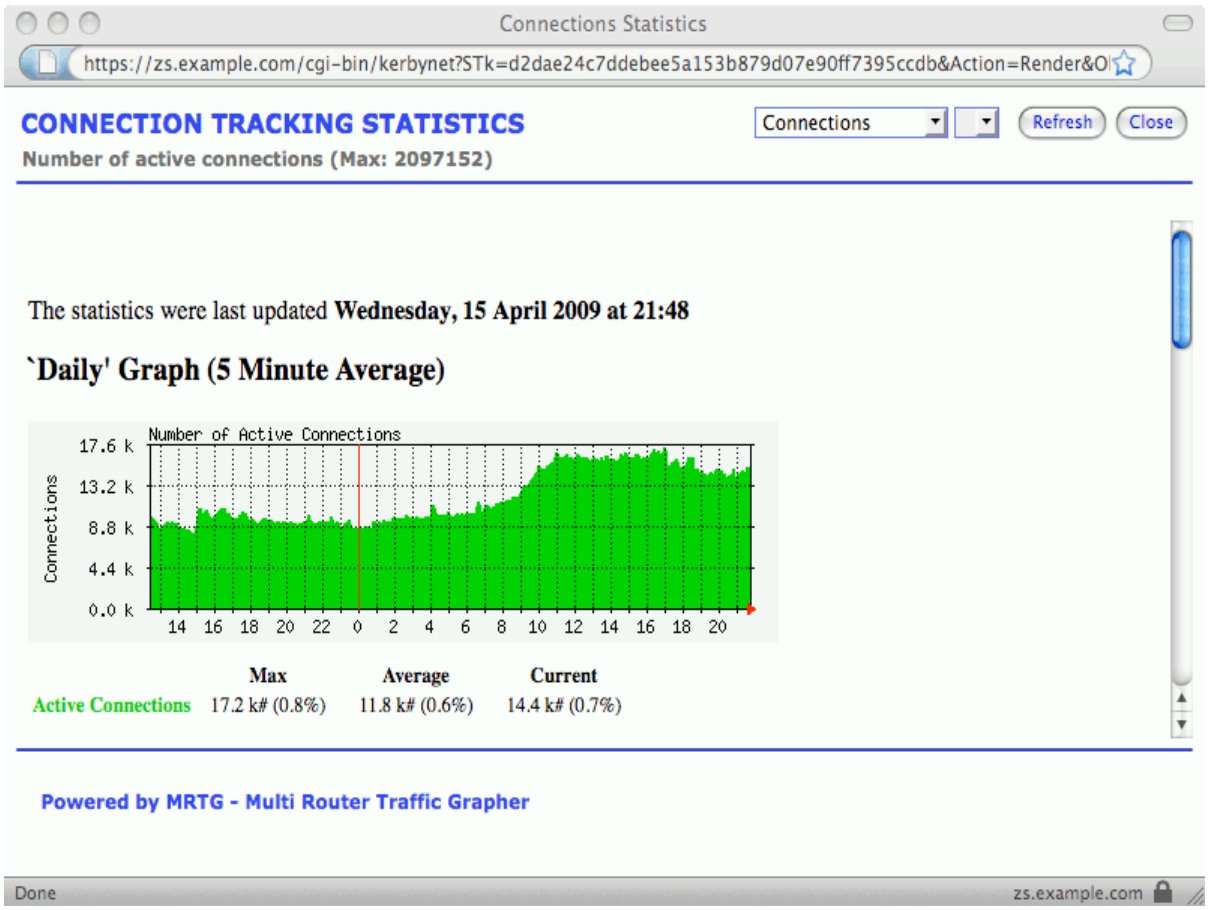


**Figure 3 - Gráfico relacionado con el número de conexiones activas.**

Recuerde que Zeroshell es diferente desde determinados enrutadores que se olvidan de las conexiones TCP en un período corto de tiempo de espera; esto se debe a que está configurado para realizar un seguimiento de las conexiones que no intercambian tráfico incluso durante largos periodos de tiempo (por ejemplo, sesiones interactivas de SSH en reposo para días). Por un lado, esto es una ventaja; por el otro, donde las conexiones no están correctamente cerradas, puede provocar que las conexiones que no han estado activas por un tiempo sean salvadas. Si desea establecer un tiempo de espera para las conexiones TCP, establezca el parámetro */proc/sys/net/netfilter/nf_conntrack_tcp_timeout_established* al número de segundos que una conexión se considera expirada, después de la inactividad, y por lo tanto cancelada por las tablas de seguimiento de conexiones (Connection Tracking).

## *Tráfico entrante y saliente de una interfaz de red*

El uso tradicional del MRTG es permitir el seguimiento del tráfico de las interfaces de red de un router, tanto de flujo arriba como abajo. El mismo gráfico sigue el tráfico entrante en **VERDE**, mientras que el tráfico saliente en **AZUL**.

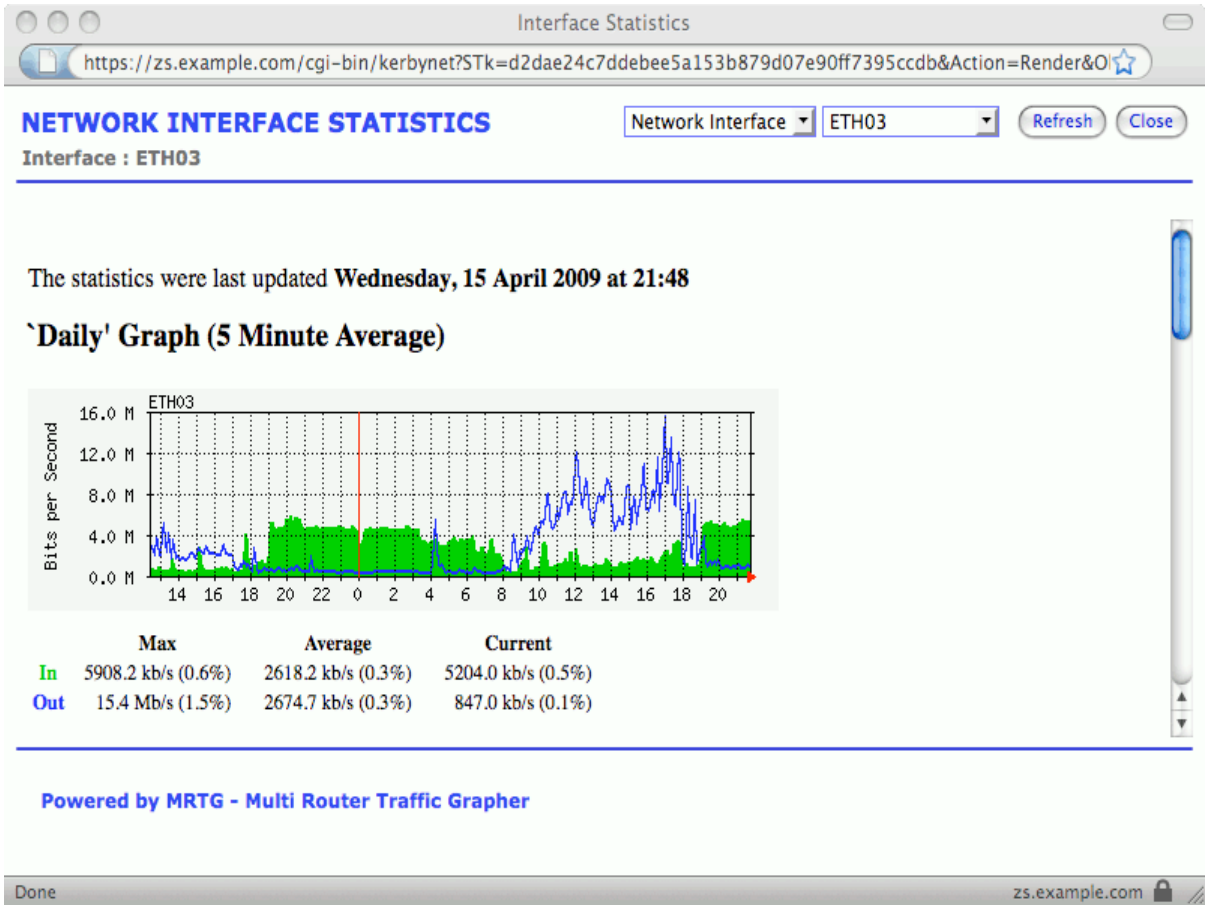


**Figure 4 – Gráfico relación entre trafico entrante y saliente de una interfaz de red.**

Los porcentajes se refieren, en lo posible, a la banda máxima que la interfaz puede soportar. Zeroshell permite al gráfico de tráfico obtener datos en descarga/subida de los tipos de interfaces siguientes: Ethernet, VPN, PPPoE y 3G. Lo mismo puede decirse de las combinaciones de interfaz como los lazos y los puentes y para la VLAN 802.1q. Además, si Zeroshell se utiliza como una conexión Wi-Fi Access Point con SSID múltiple, es posible obtener el gráfico del tráfico para cada SSID.

## *Gráficos de Tráfico sub-divididos por clases QoS*

Si el tráfico está activo en la configuración de una interfaz de red, es posible mostrar el gráfico sobre el tráfico de salida clasificado por tipo de tráfico. El diagrama del tráfico total de salida de la interfaz se muestra en **AZUL**, mientras que el tráfico clasificado en la categoría correspondiente QoS en **VERDE**.

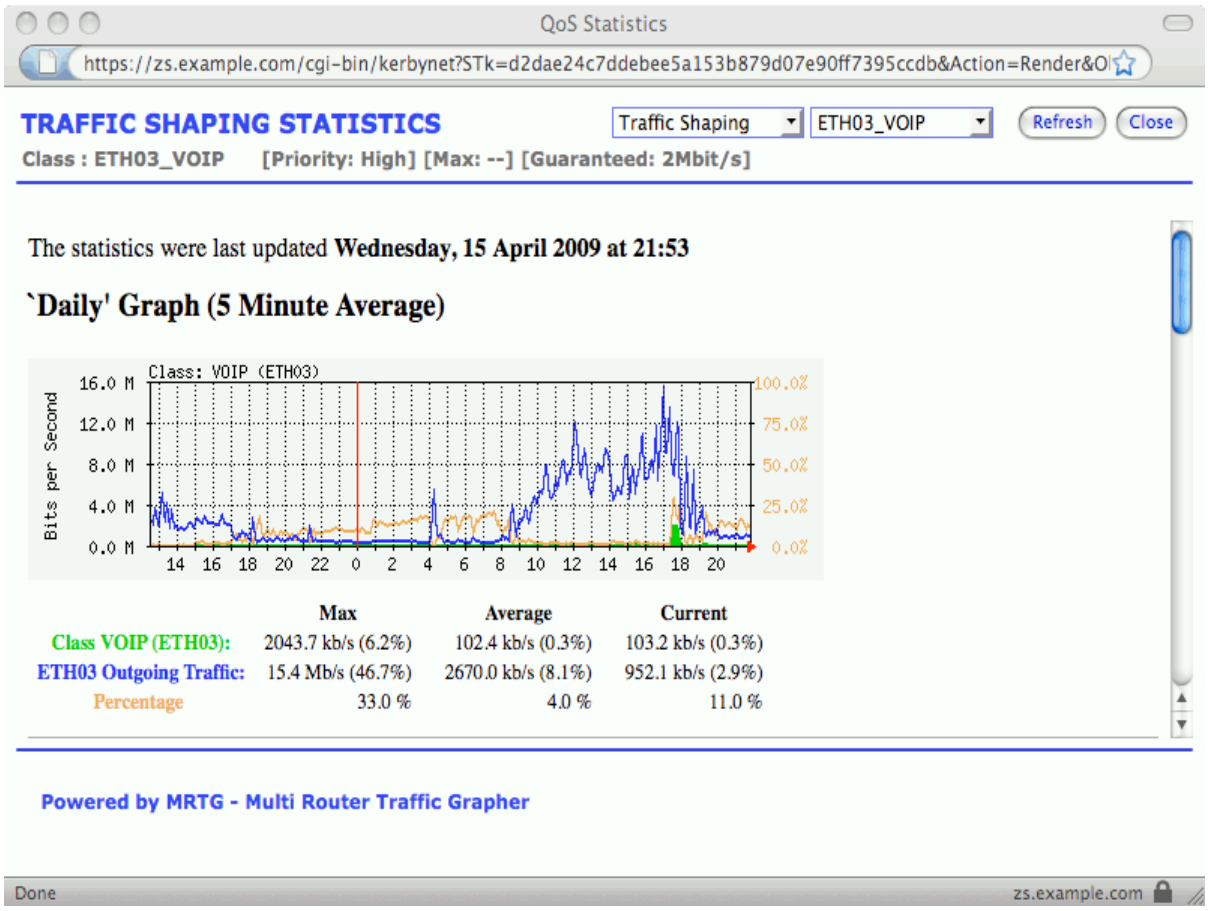


**Figure 5 – Gráfico relación de tráfico por QoS categorías**

El color **AMBAR** representa el porcentaje de uso de QoS en comparación con el tráfico total de la interfaz. Por lo tanto, la figura arriba muestra fácilmente que la VoIP saliente, tráfico de interfaz ETH03, es en promedio el 4% del tráfico total, con picos del 33%.

## *Distribución del tráfico en las puertas de enlaces de Internet en equilibrio de carga*

Gracias a Balancer Net, Zeroshell puede distribuir el tráfico de acceso a Internet a través de múltiples conexiones WAN que puede ser xDSL, 3G u otra. El equilibrio puede ser automático, con Round-Robin ponderado o manual con reglas (similares a las de Firewall y clasificador QoS) que obligan a determinados tipos de tráfico a utilizar una puerta de enlace determinada. Para el balanceo de carga automático, es útil consultar el gráfico de distribución del tráfico para comprender si las puertas de enlaces se utilizan en proporción al ancho de banda máximo disponible para ellos. Si por el contrario el peso de la puerta de enlace puede ser modificado. Este parámetro es, de hecho, directamente proporcional a la probabilidad de que la conexión es enrutada en ese enlace.

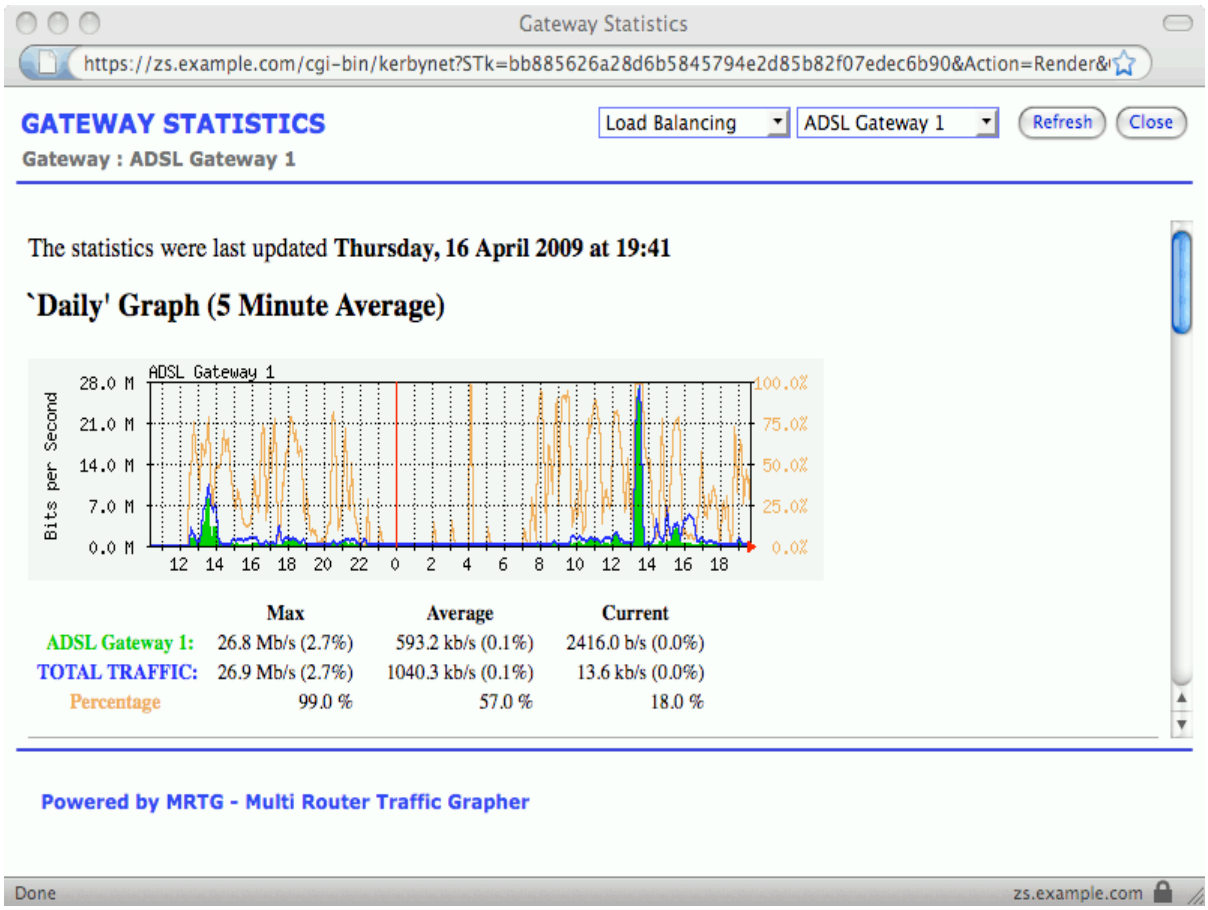


**Figure 6 Gráfico relación de la distribución del tráfico en una puerta de enlace de Internet.**

**VERDE** indica el tráfico entrante y saliente por la puerta de enlace elegida, mientras que el **AZUL** indica el tráfico total de Internet.
La relación porcentual entre el tráfico en el enlace elegido y el tráfico en general es en mostrado con el color **AMBAR**.

## *Activación de MRTG en Zeroshell*

MRTG puede ser configurado en Zeroshell desde la versión 1.0.beta11 o posteriores, como una actualización externa (C110). En versiones posteriores, MRTG se incluirá directamente en la distribución y por lo tanto no requieren la instalación manual como una actualización. En la versión 1.0.beta11, MRTG se instalarán escribiendo los siguientes comandos utiliza un cable VGA/SERIAL consola o conexión SSH:

*cd /Database*
*wget http://www.zeroshell.net/listing/C110-MRTG-Statistics-beta11-v2.tar.bz2*
*tar xvfj C110-MRTG-Statistics-beta11-v2.tar.bz2*
*cd C110*
*./install.sh*

Después de haber instalado el software, el botón/enlace [Gráficos] aparecerá. Utilice esta opción para acceder al formulario Web de gestión de MRTG. La forma más fácil de llegar al enlace [Gráficos] es la que aparece en el cuadro en la parte superior derecha de presentación de reportes de la información del sistema. Si este vínculo no está disponible inmediatamente después de la instalación, pulse [Actualizar] en este marco.

## *Claves de activación*

A diferencia de las otras funcionalidades Zeroshell, algunos de los gráficos estadísticos sólo se generan si se activa mediante una clave de activación. Los siguientes gráficos no requieren de desbloqueo:

- Sistema de carga
- Número de conexiones activas
- Trafico entrante / saliente de VPN, puente, lazos PPPoE y UMTS / HSDPA
- Clases QoS conectados a VPN, puente, lazos PPPoE y UMTS / HSDPA

Mientras que los gráficos a continuación requieren ser desbloqueos utilizando una clave de activación:

- Trafico entrante / saliente en Ethernet / Wireless y 802.1Q e interfaces VLAN
- Clases QoS conectados a interfaces Ethernet / Wireless
- Balance de Carga para conexiones a Internet

Las claves de activación dependen de la dirección MAC de las tarjetas de red. Cada tarjeta de red presente en el sistema requiere una clave de activación diferente para obtener el gráfico correspondiente. Sin embargo, mediante la activación de la gráfica para una interfaz Ethernet, se puede usar la misma clave para activar automáticamente el gráfico relativo a la VLAN y las clases de QoS. Si múltiples SSID se definen en la misma conexión Wi-Fi de la tarjeta de red, basta con activar el gráfico correspondiente a una sola SSID y los otros gráficos relacionados con otro SSID automáticamente se desbloquearan.
Como se ha mencionado antes, las claves de activación dependen exclusivamente de la MAC de las interfaces Ethernet /Wireless y, en consecuencia, si Zeroshell está instalado en el mismo hardware o simplemente cuando un nuevo perfil de configuración es creado, entonces las claves de activación ya obtenidas pueden ser reutilizadas con éxito.
Las claves de activación se genera en base a los códigos de función comunicados a través de e-mail (ver http://www.zeroshell.net/eng/activation) y pueden ser comunicados varios códigos de función en la misma petición. Se necesita de una contribución al desarrollo de Zeroshell para obtener las claves de activación. En la actualidad pueden ser contribuciones como:

- Creación de un documento en formato HTML o PDF en un aspecto de la configuración de Zeroshell. También puede ser una simple descripción de su experiencia con Zeroshell. El autor del documento debe ser especificado y,

posiblemente, (opcional) su e-mail de referencia para permitir un contacto de los lectores. Todas las actualizaciones para el documento debe ser hecha por el autor de alojamiento en un espacio Web con acceso de edición. El URL del documento estará vinculado en la sección de documentación.

- Una donación modesta a través de PayPal. Los ingresos serán utilizados para la compra de hardware con fines de testeo y/o para cubrir los gastos de gestión.

La producción de la documentación es, sin duda la contribución más positive, pues esperamos realmente apoyar a aquellos que desean configurar y utilizar Zeroshell. La donación a través de Paypal sólo debe ser seleccionado cuando no tienes el tiempo para el proyecto o la oportunidad de aportar a la documentación.
También tenga en cuenta que el mecanismo de clave de activación no influye en el paquete MRTG cuyo código fuente se compila como disponible en su sitio oficial. La activación se refiere a un lugar externo plug-in, escrito específicamente para Zeroshell, por la que MRTG se configura para recopilar datos estadísticos.

Nota:
(*) Si en lugar de utilizar el paquete MRTG integrado prefiere exportar los contadores de tráfico a través de SNMP y el uso de un paquete de control externo, instale el paquete net-snmp compilados para Zeroshell.