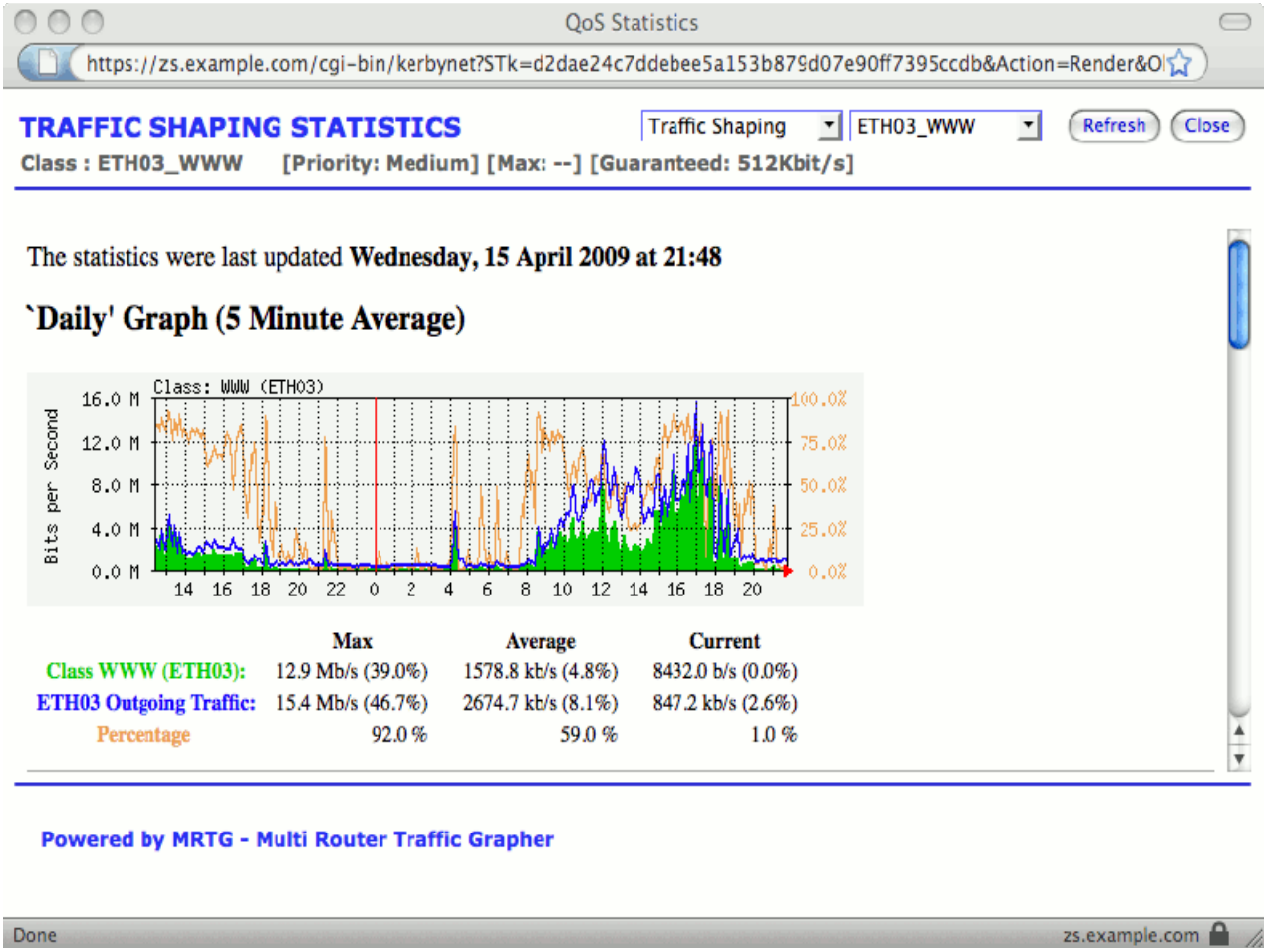
Graphes de trafic et Statistiques utilisant MRTG

L'affichage des statistiques graphiques pour l'évaluation de la bande passante Internet utilisée est considéré comme une fonction optionnelle sur un routeur. Pourtant, il est important de connaitre ces informations pour mieux comprendre si l'accès à Internet connait des inefficacités devant la pauvre distribution de la bande passante entre les différents types de trafic (VoIP, WWW, P2P, FTP…) rivalisant pour utiliser la Connexion à Internet.

Beaucoup de routeurs utilisent *SNMP* (Simple Network Management Protocol) pour exporter la valeur des compteurs de trafic entrant et sortant pour chacune des interfaces réseaux. Avec l'utilisation des logiciels comme *MRTG* (Multi Router Traffic Grapher) il est possible par répétition et à intervalles de temps réguliers de lancer des requêtes SNMP vers ces routeurs, de sauvegarder les compteurs de trafic. Une fois cela fait, MRTG permet l'analyse graphique de la progression du trafic sur les interfaces de ces routeurs, via un navigateur,.



Exemple d'un graphe MRTG relatf à un trafic WWW

Zeroshell ne suit pas cette stratégie d'exportation utilisant SNMP (voir note *), mais intègre directement MRTG pour permettre l'analyse des paramètres qui vont au-delà de ceux obtenus par l'utilisation de SNMP. En vertu de cela, les paramètres suivants peuvent être analysés directement de l'interface Web de Zeroshell :

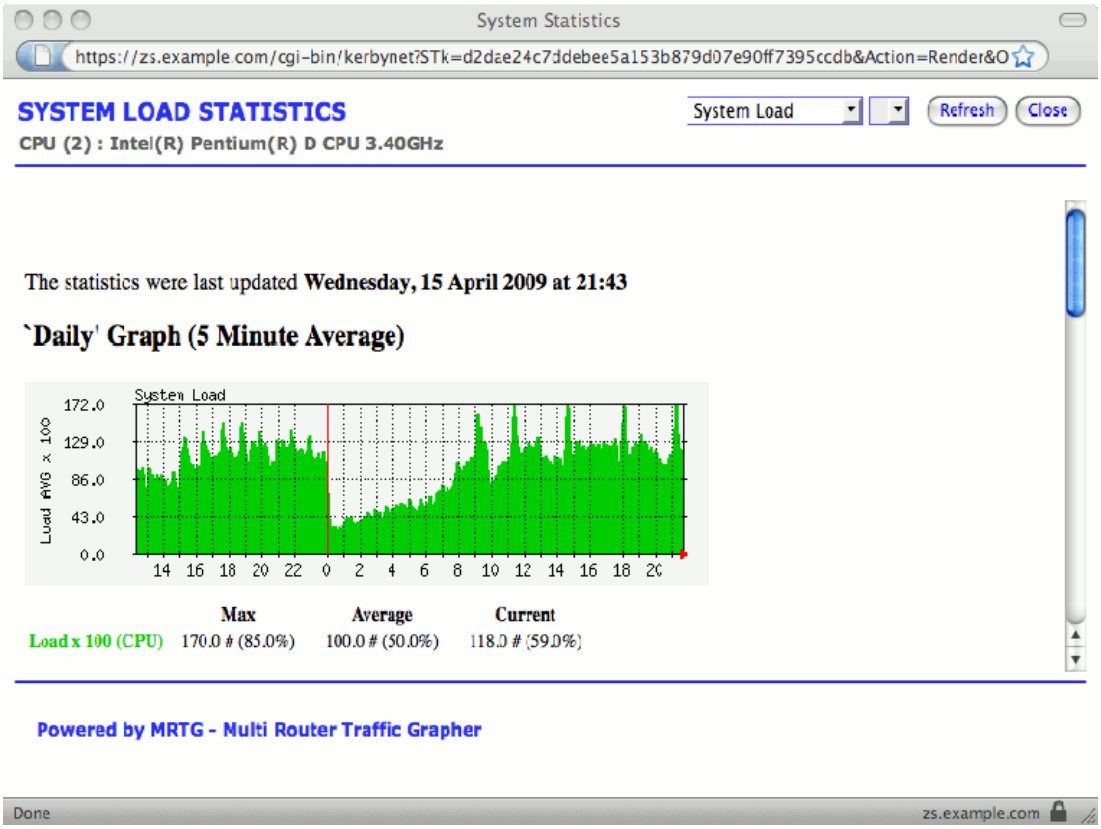
- La charge du Système
- Nombre de connexions (TCP/UDP) actives de et vers Internet;

- Trafic d'interface Entrant et Sortant, que se soit une carte Ethernet, un VLAN 802.1q, un VPN, un Pont, un lien, une connexion PPPoE (ex. ADSL) ou une connexion mobile 3G (ex. UMTS/HSDPA);
- Trafic classifié par profil dans une classe de QoS déterminée (VoIP, HTTP, peer to peer, ...) par rapport à l'interface du trafic sortant;
- Equlibrage de charge du trafic Internet sur différentes passerelles WAN (Load Balancing et Failover) comparé à l'ensemble du trafic Internet entrant et sortant.

Le reste du document est subdivisé dans les sections suivantes :

Charge moyenne du système

Les informations sur la Moyenne statistique des Charges ne couvrent pas directement le trafic réseau, mais sont cependant utiles pour comprendre si les ressources matériels du routeur (le processeur en particulier) sont un goulot d'étranglement pour le réseau local et ralentissent les connexions indépendantes de la bande disponible sur les liaisons d'accès à Internet. Pour afficher le graphe de la charge du système, cliquer sur le lien [Graphics] en haut à droite. Une fenêtre similaire à celle-ci apparait.



Graphe relatif à la charge système

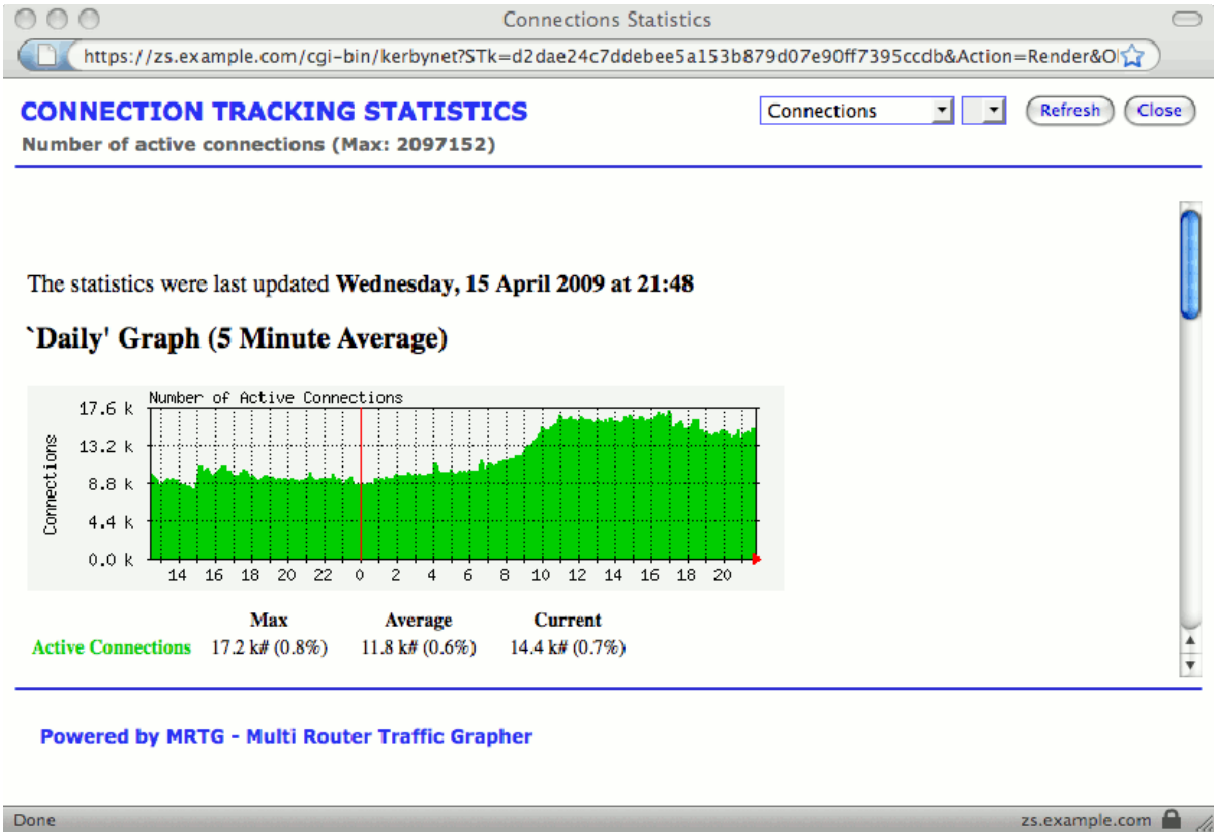
La charge moyenne calculée toutes les 5 minutes et multipliée par 100 est prise en considération. Le pourcentage d'utilisation du système (reporté en parenthèse) prend en compte le nombre de CPU de routeurs. En d'autres termes, supposons une charge de 100 sur un système à 2 processeurs, le pourcentage d'utilisation indiqué est 50%. En conséquence le seuil critique pour lequel le routeur peut-être suspecté d'être un goulot d'étranglement est 200 égales à 100% d'utilisation.

Les facteurs contribuant principalement à l'utilisation du CPU dans l'ordre croissant sont :

- Règles du Pare-feu, classification QoS et équilibrage de charge manuel
- Les règles de Pare-feu et la QoS qui utilisent les filtres de la couche 7 pour exécuter le DPI quand plusieurs connexions présentes. Notez que les filtres de la couche 7 inspectent le contenu des paquets seulement quand une connexion est établie, tandis que le reste est identifié en utilisant le suivi de connexion. Cela met en évidence le fait que les filtres de niveau d'application ne chargent pas le système sur la base de la bande passante utilisée, mais sur la base de nouvelles connexions TCP/UDP ouvertes.
- Ecriture dans les journaux du résultat du suivi des connexions. Garder une trace des connexions TCP/UDP n'est pas une fonctionnalité dispendieuse en termes de CPU. Pourtant elle peut l'être si le système est configuré pour enregistrer les connexions (IP source IP, port source, IP de destination, port de destination) dans les journaux.
- Portail Captif actif sur un réseau local avec beaucoup de clients actifs, mais non encore authentifié. Souvent, la présence de VERS ou d'autres logiciels qui utilisent les ports TCP 80 et 443 pour des demandes autres que des demandes de type HTTP/HTTPS classiques, peuvent détériorer la situation.
- Utilisation transparente de proxy http avec antivirus (ClamAV) ou un filtre sur le contenu Web (DansGuardian). En fait, l'examination du contenu de pages Web occupera inévitablement lourdement le CPU. Dans de tels cas, il est aussi nécessaire de prévoir une quantité de mémoire (RAM) adéquate pour éviter les échanges de disque.

Connexions TCP/UDP actives

La progression du nombre de connexions actives est un bon indice pour contrôler l'activité du réseau. Par exemple, un nombre important de connexions pourrait signifier des échanges de fichiers utilisant des techniques P2P.



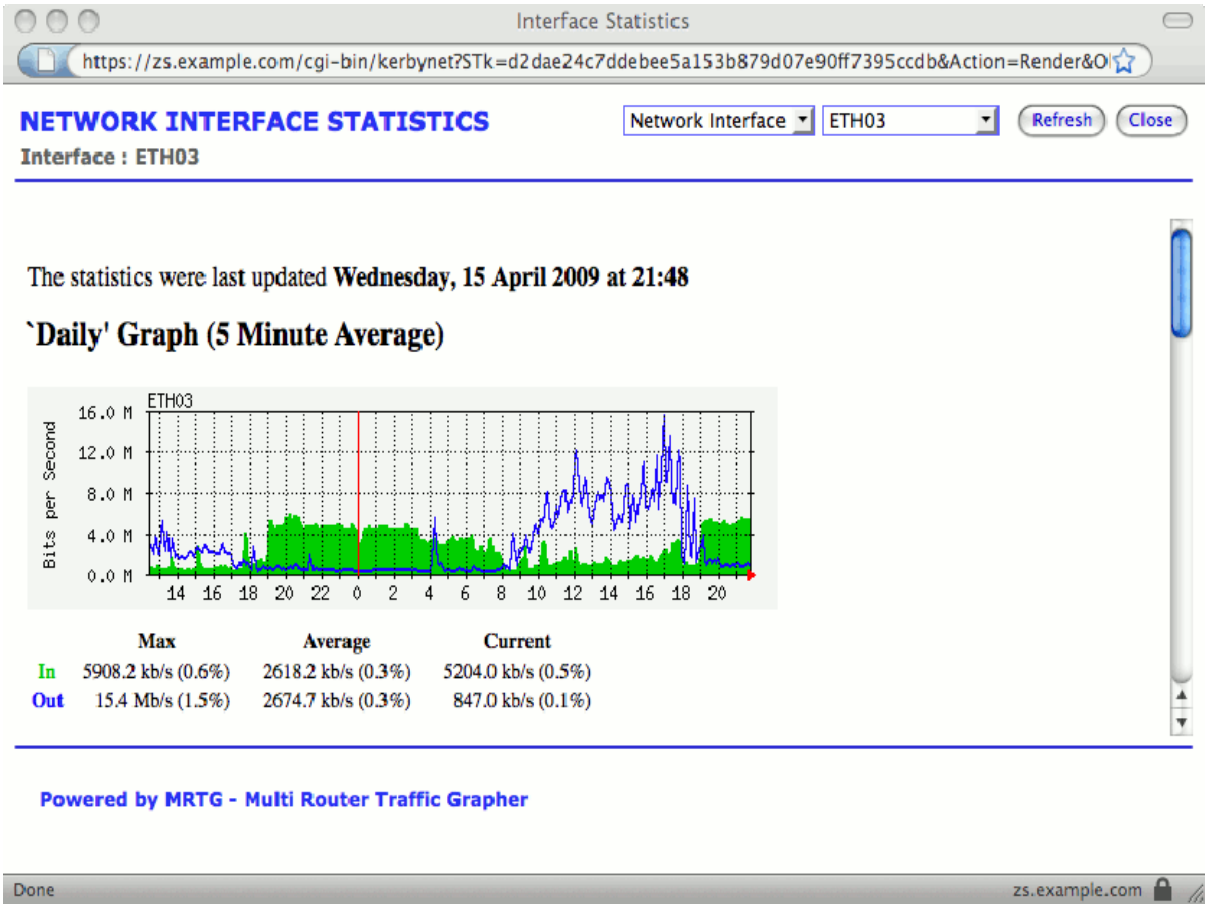
Graphe relatif au nombre de connexions actives

Rappelez-vous que Zeroshell diffère des certains routeurs qui oublient des connexions TCP au cours de courte période d'inactivité, parce qu'il est configuré pour garder la trace des connexions qui n'échangent pas de trafic même durant de longues périodes de temps (ex. sessions SSH interactives INOCCUPÉES pendant des jours).

Si d'une part c'est un avantage, d'un autre, quand les connexions ne sont pas correctement fermées, il peut entrainer la sauvegarde des connexions non actives depuis un moment. Si vous voulez paramétrer les temps d'inactivité (timeout) pour les connexions TCP, mettre le paramètre */proc/sys/net/netfilter/nf_conntrack_tcp_timeout_established* au nombre de secondes après lequel une connexion est considérée comme expirée, après inactivité, et en conséquence effacée de la table de suivi des connexions.

Trafic entrant et sortant d'une interface réseau

L'utilisation traditionnelle de MRTG consiste à activer le contrôle du trafic des interfaces réseau d'un routeur tant en amont qu'en aval. Les mêmes graphiques pistent le trafic entrant en **VERT**, tandis que le trafic sortant est en **BLEU**.

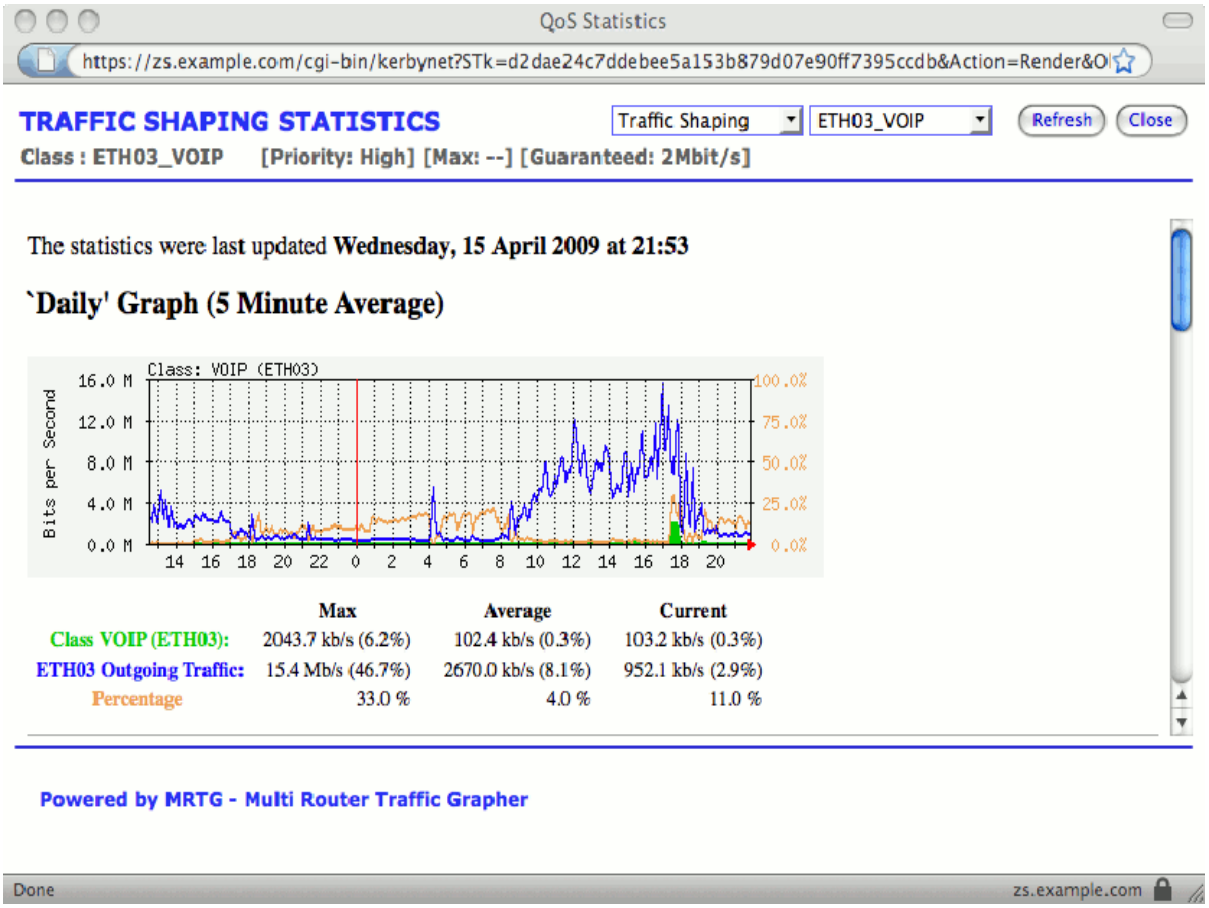


Graphe relative au trafic entrant et sortant d'une interface réseau

Les pourcentages se réfèrent, autant que possible, à la bande passante maximale que peut supporter l'interface. Zeroshell permet l'obtention de graphe du trafic de téléchargement DOWN/UP des interfaces suivantes : Ethernet, VPN, PPPoE et 3G. Cela s'applique aussi à des interfaces comme les liens, les ponts et les VLAN 802.1q. En outre, si Zeroshell est utilisé comme un Point d'Accès WiFi avec SSID multiple, il est possible d'obtenir le graphe du trafic pour chaque SSID.

Graphes de trafic subdivisés par classes de QoS

Si le profil de trafic est actif sur une interface réseau, il est possible d'afficher le graphique touchant au trafic sortant classifié par type de trafic. Le diagramme du trafic total sortant de l'interface est suivi à la trace en **BLEU**, tandis que le trafic classifié dans la classe de QoS choisie est en **VERT**.



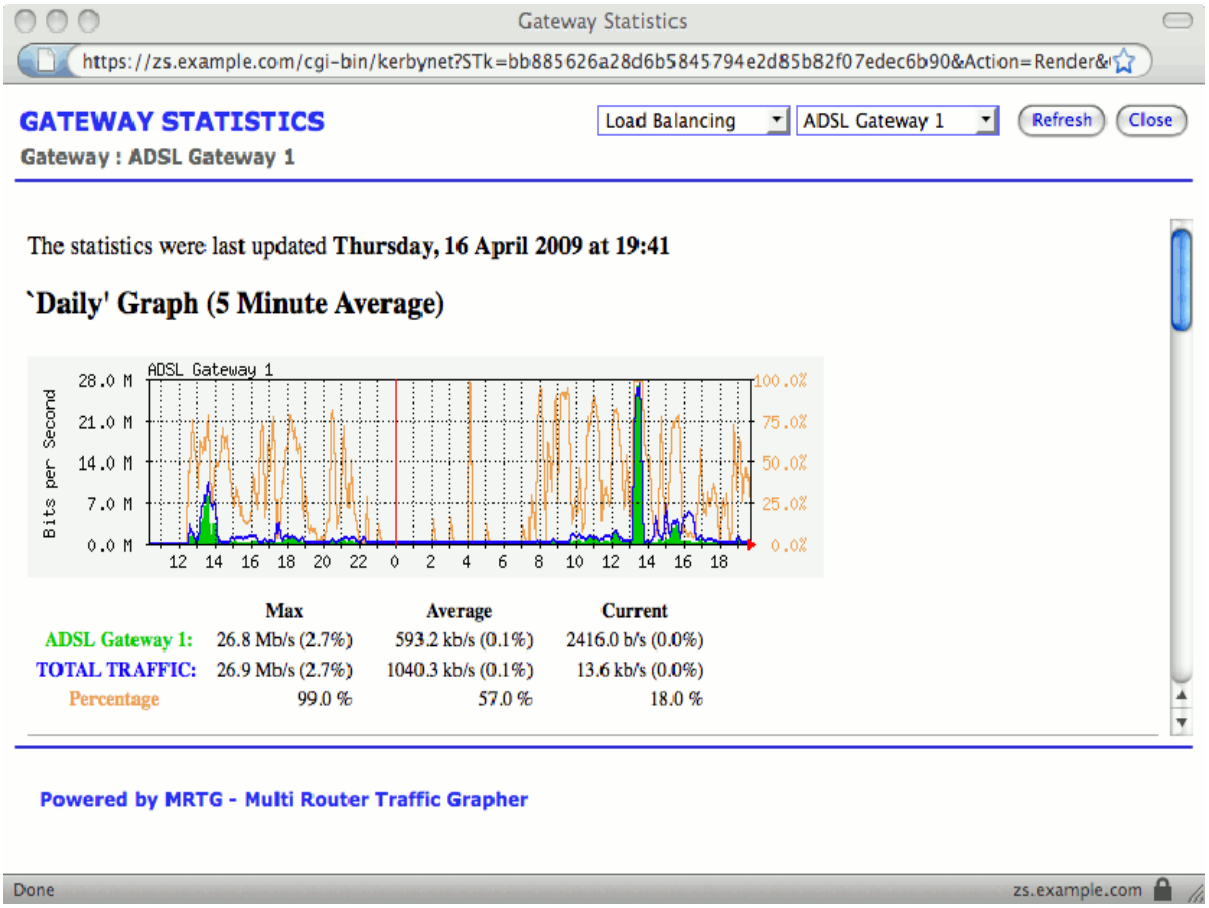
Graphe relatif au trafic par classe de QoS

La couleur **AMBRE** représente le pourcentage d'utilisation QoS comparée au trafic total de l'interface. Donc, la figure affichée ci-dessus montre facilement que le trafic VoIP sortant, le trafic sur l'interface ETH03 a une moyenne de 4 % du trafic total, avec des sommets atteignant 33 %.

Distribution du trafic sur les passerelles Internet

Grâce au Net Balancer (équilibreur réseau), Zeroshell peut distribuer le trafic d'Accès à Internet sur de multiples connexions WAN qui peuvent être xDSL, 3G ou autre. L'équilibrage peut être automatique avec une distribution Circulaire pondérée ou manuel avec des règles semblables à celles du Pare-feu et du classificateur QoS qui le type de trafic à utiliser une passerelle déterminée.

Pour la répartition automatique de charge, il est utile de consulter la distribution graphique du trafic pour comprendre si les passerelles sont utilisées dans la proportion à la bande passante maximale disponible pour elles. Si au contraire le poids de la passerelle peut être modifié. Ce paramètre est en fait directement proportionnel à la probabilité qu'à la connexion d'être acheminée sur cette liaison.



Graphe relative à la distribution du trafic sur une passerelle Internet

VERT indique le traffic entrant et sortant sur une passerelle choisie, tandis que le **BLEU** indique le trafic Internet total.
La proportion de pourcentage entre le trafic sur la liaison choisie et le trafic complet est en couleur **AMBRE**.

Activation MRTG sur Zeroshell

MRTG peut être configuré sur Zeroshell depuis la version 1.0.beta11 comme une mise à jour externe (C110). Dans les versions ultérieures, MRTG sera directement inclus dans la distribution et n'exigera pas donc l'installation manuelle comme une mise à jour. Dans la sortie 1.0.beta11, MRTG sera installé en entrant les commandes suivantes à partir de la console VGA/SERIAL ou une connexion 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

Une fois le logiciel installé, le bouton/lien [Graphics] apparaîtra. Utilisez-le pour accéder au formulaire de gestion Web de MRTG (voir la figure ci-dessus). La mode le plus facile pour

accéder au lien [Graphics] est celui apparaissant dans le cadre supérieur droit. Si cette liaison n'est pas disponible immédiatement après l'installation, appuyer sur [Rafraîchir].

Clés d'Activation

Différant des autres fonctionnalités Zeroshell, quelques uns de ces statistiques graphiques sont seulement générés si le produit est activé avec une clé. Les graphismes suivants n'exigent pas de déblocage pour s'afficher :

- Charge du système
- Nombre de connexions actives
- Trafic entrant/sortant sur VPN, bridge, bond PPPoE et UMTS/HSDPA
- Classes QoS connectées sur VPN, bridge, bond PPPoE et UMTS/HSDPA

Tandis que les graphes suivants exigent une clé d'activation pour s'afficher:

- Trafic entrant/sortant sur interfaces Ethernet/Sans fil et VLAN 802.1q
- Classes QoS connectées sur interfaces Ethernet/Sans fil
- Equilibrage de charge sur connexions Internet

Les clés d'activation dépendent de l'adresse MAC des cartes réseau. Chaque carte réseau présente dans le système exige une clé d'activation distincte pour pouvoir obtenir le graphe approprié. Pourtant, en activant le graphique pour une interface Ethernet, la même clé active automatiquement le graphique touchant aux CLASSES de QoS et de VLAN.

Si de multiples SSID sont définis sur la même carte de réseau WiFi, en activant juste le graphique approprié à un SSID on débloque automatiquement les graphismes touchant aux autres SSID.
Comme mentionné ci-dessus, les clés d'activation dépendent exclusivement du MAC des interfaces Ethernet/Sans-fil, en conséquence, si Zeroshell est installé sur le même matériel ou simplement quand un nouveau profil de configuration est créé, les clés d'activation déjà obtenues peuvent être réutilisées avec succès.

Les clés d'activation sont générées sur la base des Codes de Fonction communiqués via courrier électronique (voir http://www.zeroshell.net/eng/activation), l'on peut communiquer de multiples Codes de Fonction dans la même demande. Une contribution au développement de Zeroshell est exigée pour obtenir les clés d'activation, qui se présente comme suit :

- La création d'un document au format HTML ou PDF sur un aspect de la configuration de Zeroshell. Cela peut aussi être une description simple de votre expérience en tant qu'utilisateur Zeroshell. L'auteur du document doit être spécifié et probablement (facultatif) sa référence de courrier électronique pour permettre le contact par les lecteurs. N'importe quelles mises à jour du document devraient être faites par l'auteur les hébergeant dans un espace Web. L'URL du sera lié à la page documentation section.
- Une modeste donation via PayPal. Les revenus seront utilisés pour acheter du matériel pour les tests et peut-être aussi pour la maintenance du matériel et les coûts de gestion.

La production de documentation est sans doute la contribution la plus bienvenue que nous espérons soutiendra vraiment ceux voulant configurer et utiliser Zeroshell. La donation via Paypal devrait seulement être choisie quand vous n'avez pas le temps de rédiger ou la chance de contribuer à la documentation.

Notez aussi que le mécanisme d'activation clé n'influence pas le paquet MRTG dont le code source a été compilé comme disponible sur son site officiel. L'activation concerne au lieu de cela un module d'extension externe, écrit spécifiquement pour Zeroshell, par lequel MRTG est configuré pour collecter des données statistiques.

Note:
(*) Si au lieu d'utiliser le paquet MRTG intégré vous préférez exporter les compteurs de trafic via SNMP et utiliser un moniteur externe de paquets, installez le paquet net-snmp compilé pour Zeroshell.