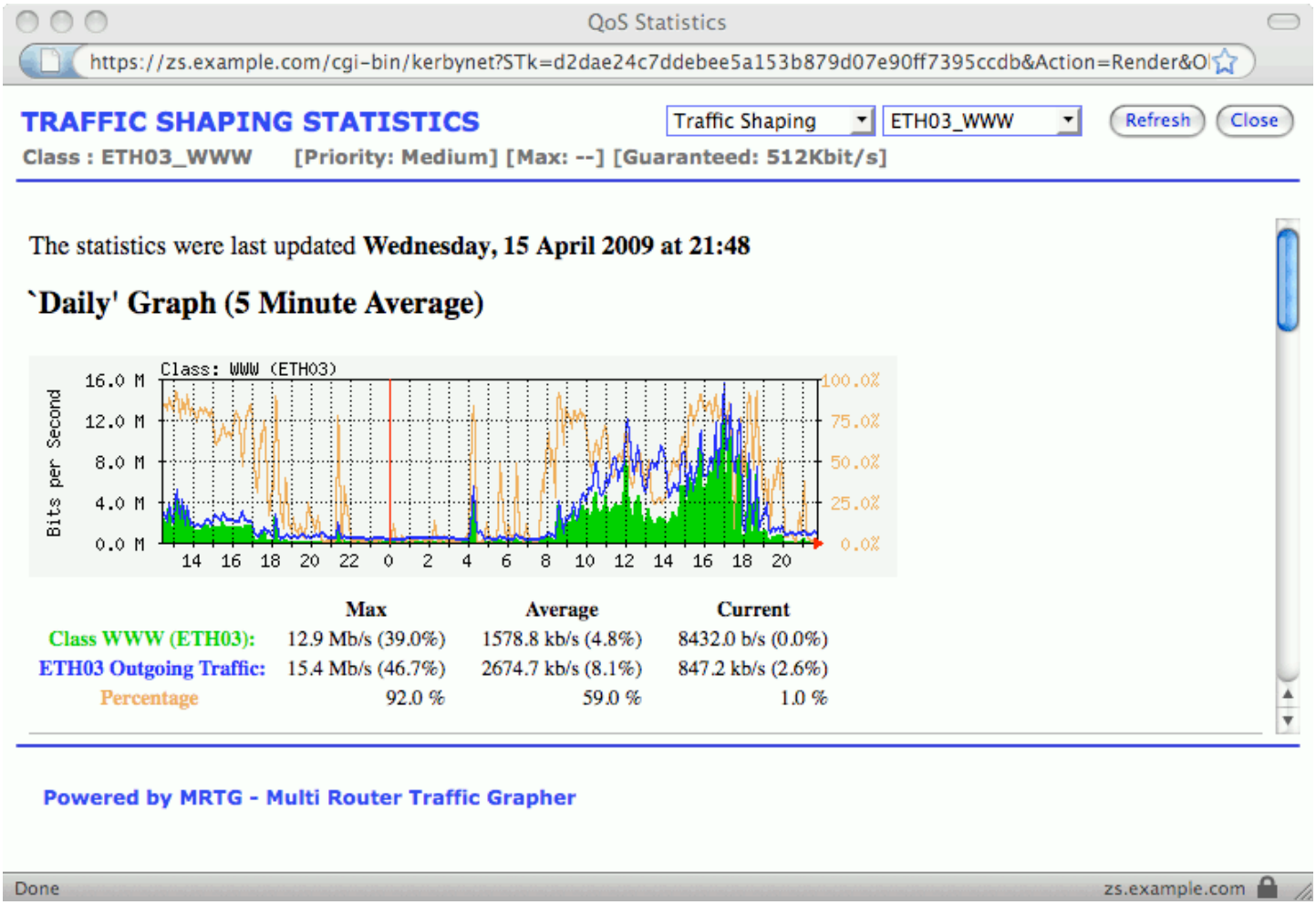
Forgalmi grafikák és statisztika MRTG-vel

Az internetes sávszélesség terheltségét ábrázoló grafikonok és statisztikák egy routerben általában opciós lehetőségek – vagy még opcióként sem elérhetőek. Mégis bizonyos esetekben ez jól jöhet, pl ha meg szeretnénk győződni arról, hogy a fontosabb forgalmi típusoknak (VoIP, web, P2P, FTP, stb) van-e elegendő sávszélességük a megfelelő működéshez.
Sok router használ SNMP-t (Simple Network Management Protocol) a be- és kimenő forgalom közlésére. Az MRTG egy olyan szoftver, amely adott időközönként lekérdezi ezeket a forgalmi adatokat, majd az adatokból grafikát készít, melyeket akár egy internetböngészőn keresztül is megtekinthetünk.



MRTG példa a WWW osztályba sorolt forgalomról

A Zeroshell statisztikái közvetlenül SNMP-n nem érhetőek el, viszont az MRTG integrálva van a szoftverbe, így könnyen megtekinthetők a fontosabb adatok, amit egyébként SNMP protokollon keresztül kellene elérnünk. Az alábbi lényegesebb információkat érhetjük így el, közvetlenül a Zeroshell webes felületéről.

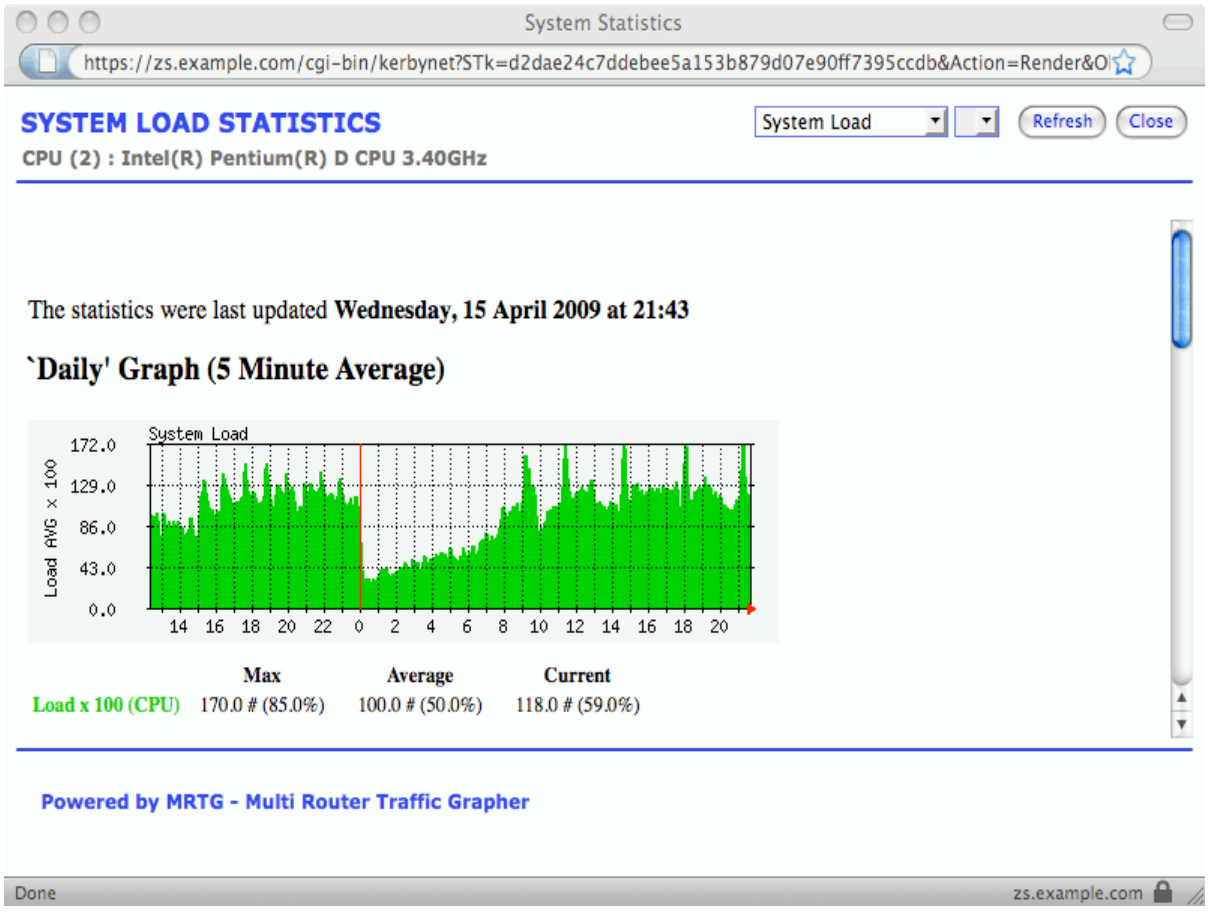
- Rendszer terhelés
- Aktív kapcsolatok száma (TCP/UDP) bejövő és kimenő
- Bejövő és kimenő interface forgalma, legyen az Ethernet kártya, egy VLAN 802.1q eszköz, VPN, bridge, PPPoE kapcsolat (pl ADSL) vagy akár egy 3G mobil kapcsolat (pl UMTS/HSDPA);
- Forgalom osztályzás és irányítás QoS osztályok segítségével (VoIP, HTTP, peer to peer, stb) az összes kimenő forgalom függvényében
- Bejövő és kimenő internetes forgalom elosztása különböző WAN Gatewayek között (Load Balance és Failover)

A továbbiakban a következőkről lesz szó:

* Rendszerterhelés
* Aktív TCP/UDP-kapcsolatok
* Adott eszközön keresztül történő adatforgalom
* Grafikai ábrázolás a különböző QoS osztályok szerint
* Terheléskiegyenlített forgalom továbbítás a gatewayek felé
* MRTG aktiválása a Zeroshell –ben
    * Aktivációs kulcsok

Rendszerterhelés

A rendszer terhelését ábrázoló grafikon nem feltétlen függ össze a hálózat terhelésével, de mindenképpen hasznos segítség, hogy felügyeljük a hardveres erőforrásokat (különösen a processzort), észleljünk olyan hibákat a hálózatunkban, amik lassíthatják annak működését (LAN és WAN). A Terhelést ábrázoló grafikon megnyitásához kattintsunk az ablak jobb felső sarkában található [Grapics] linkre. Az alábbihoz hasonló ábrát fogunk látni.



Rendszer terhelés grafikusan ábrázolva

Az átlagos terhelés adatai 5 percenként frissülnek, 100 –ig terjedő skálán kapnak értéket. A rendszer használatának aránya (zárójelben jelölve) figyelembe veszi a processzorok számát is. Más szavakkal tehát 100-as load egy 2 processzoros gép esetén 50% -os kihasználtságot jelent. Ha a routerünk kezdi elérni a kritikus határt, könnyen lehet belőle egy „szűkület”, ami visszafogja az egész hálózatot. 200-as load esetén 100% -osan terhelt a rendszerünk.

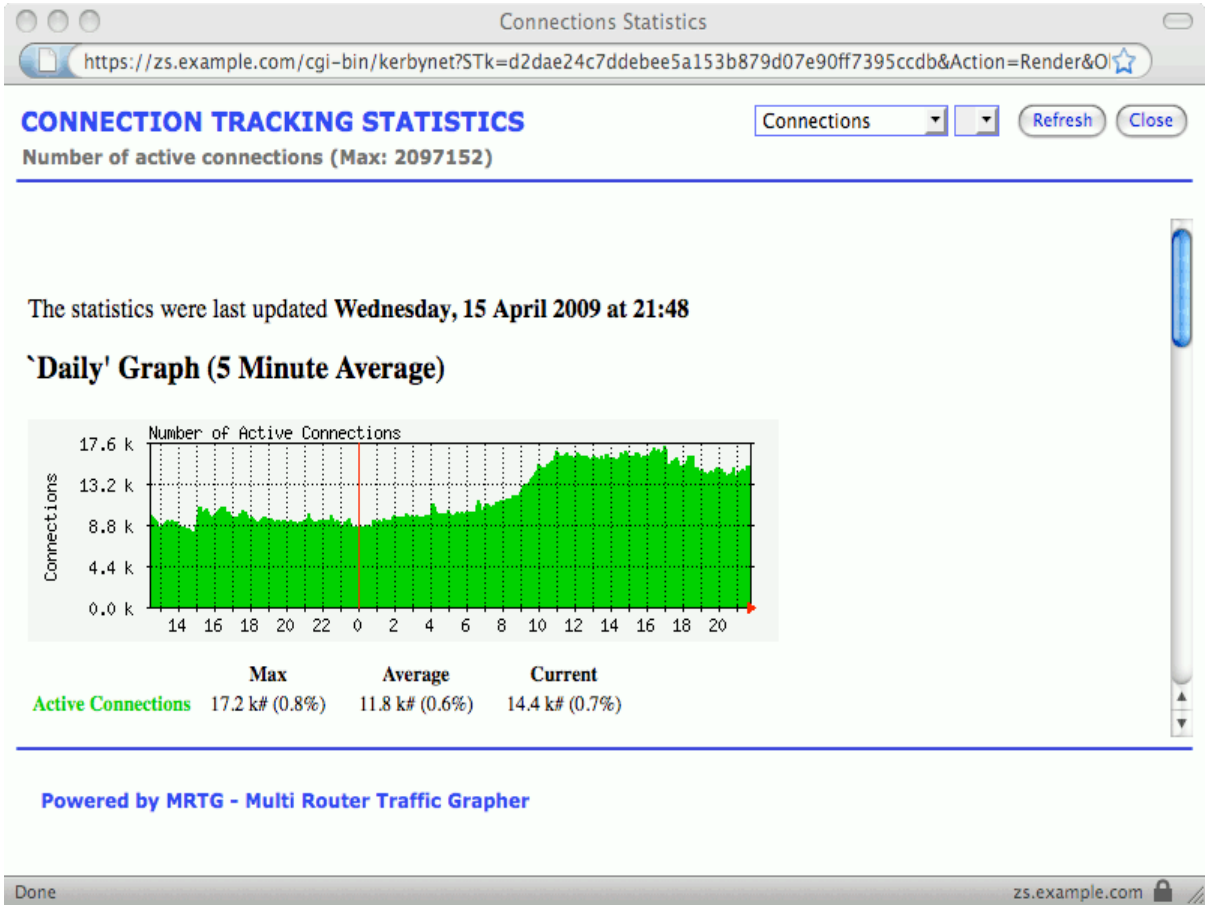
A következő tényezők/szolgáltatások igénylik a nagyobb erőforrásokat (növekvő sorrendben):

- Tűzfal szabályok, QoS osztályozás és manuális Load Balancing

- Olyan tűzfal szabályok és Qos ütemezések, amelyek Layer7 –es szűrőt használnak. Jegyezzük meg, hogy a L7 szűrők csak akkor vizsgálják meg a csomagok tartalmát, amikor a kapcsolat létrejön, a többi azonosítására használható a „Connection Tracking”. Az alkalmazás szintű szűrők nem „pazarolják” a sávszélességet, viszont elég sok TCP/UDP kapcsolatot nyithatnak.
- „Connection Tracking” eredményeinek LOG-okban tárolása. A TCP/UDP kapcsolatokat fenntartása nem túl megterhelő a CPU számára. Néha mégis az tud lenni, pl ha a rendszer úgy van konfigurálva, hogy regisztrálja a kapcsolatokat (forrás IP, forrás port, cél IP, cél port) a LOG-okba.
- Működő „Captive Portal” egy LAN hálózatban, sok aktív, de még nem ellenőrzött klienssel. Gyakran találkozhatunk férgekkel vagy olyan szoftverekkel melyek a 80 és/vagy 443-as TCP portot használják. Ezek tovább rontják a helyzetet.
- Transzparens HTTP Proxy vírus szűréssel (pl ClamAV) és/vagy tartalom szűréssel (pl DansGuardian). A weblapok vizsgálata elkerülhetetlenül igényli a CPU-t, és ebben az esetben gondoskodnunk kell elegendő mennyiségű RAM memóriáról is, hogy elkerüljük a SWAP –olást.

Aktív TCP/UDP-kapcsolatok

Az aktív kapcsolatok elég jól mutatják a hálózati aktivitást. Például jelentő mennyiségű kapcsolat esetén valószínűleg P2P alapú programokat használnak a hálózatban.

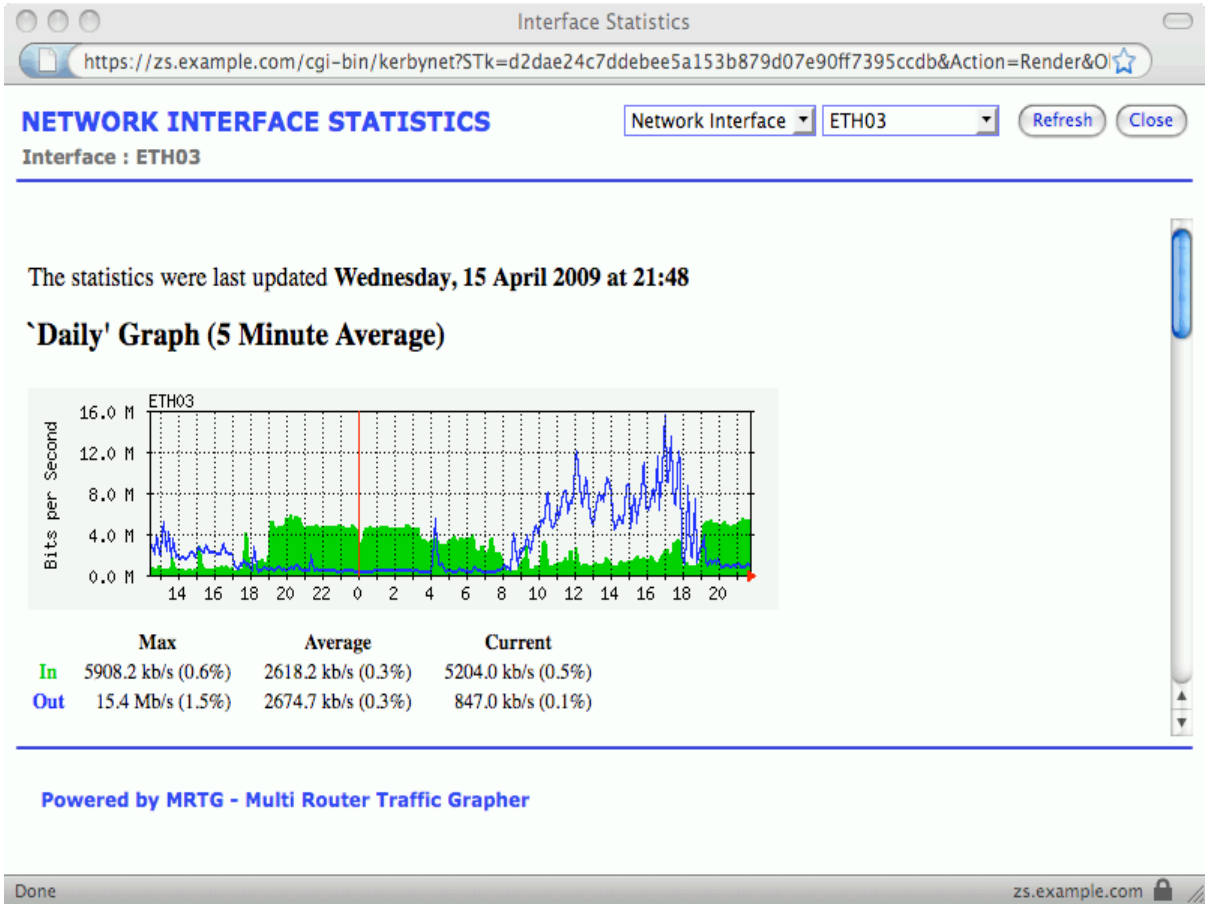


Aktív kapcsolatok grafikusan ábrázolva

Emlékeztetőül még egyszer, a Zeroshell különbözik a legtöbb routertől, amelyek egy rövid idő után elfelejtik a TCP kapcsolatokat. A Zeroshell úgy van konfigurálva, hogy akkor is tartsa meg a kapcsolatot, ha hoszabb ideig nem történik adatfolyamat (pl egy interaktív SSH session, napokra „elfelejtve”). Ez egyik oldalról előny, a másikról viszont hátrány. Ahol a kapcsolatok nem helyesen lettek lezárva, újabb kapcsolatokat jöhetnek létre, hogy megmentsék az előző kapcsolatot. Ha szeretnéd módosítani a TCP kapcsolatok időtúllépését akkor a /proc/sys/net/netfilter/nf_conntrack_tcp_timeout_established fájlba írd bele, hogy mp inaktivitás után szakadjon meg a kapcsolat.

Adott eszközön keresztül történő adatforgalom

Az MRTG hagyományos felhasználása az, hogy engedélyezzük a be és kimenő forgalom monitorozását. A **ZÖLD** szín jelzi a bejövő, a **KÉK** pedig a kimenő forgalmat.

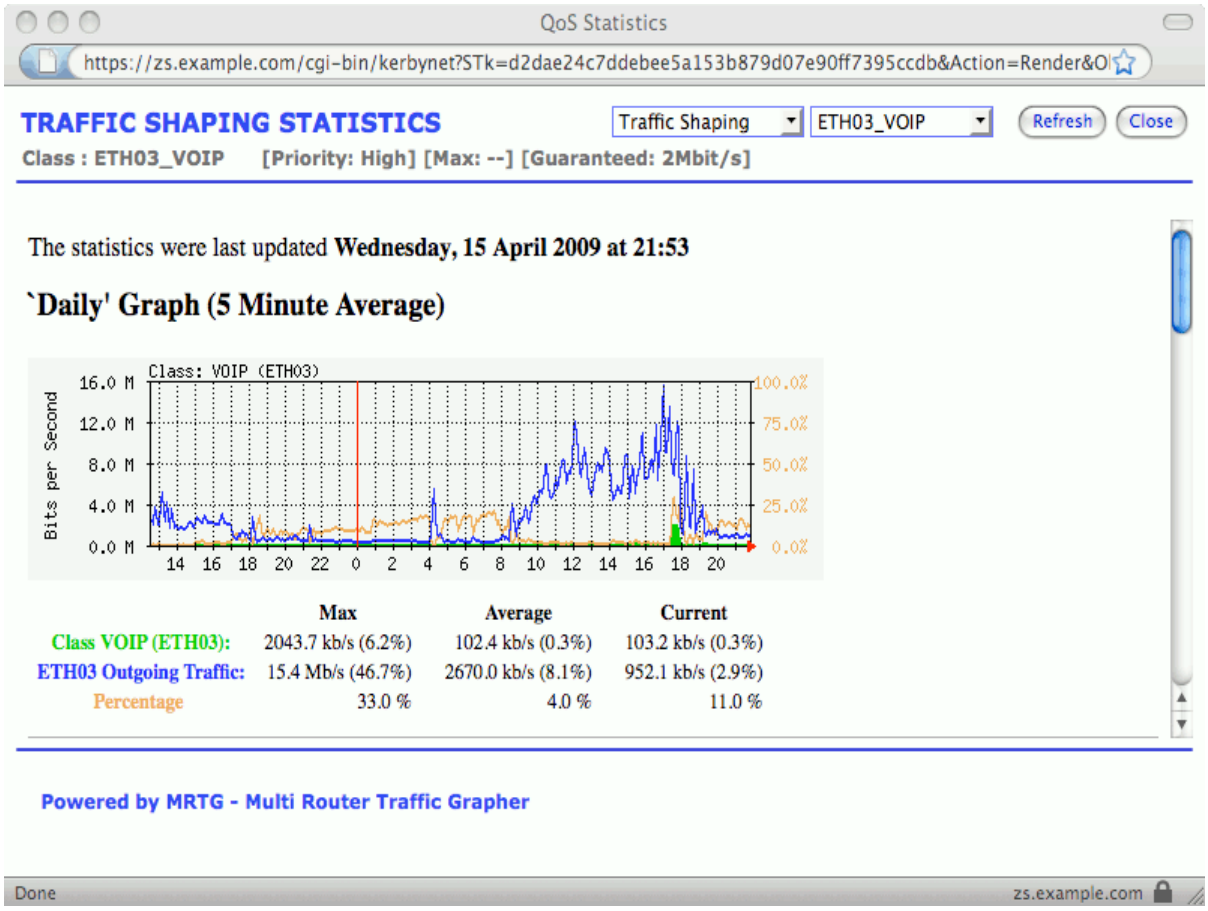


Hálózati forgalom grafikusan ábrázolva

A zárójelben lévő értékek jelzik, hogy a maximálisan támogatott sávszélesség hány százalékát használja az eszköz. A Zeroshell segítségével a következő típusú eszközöket monitorozhatunk: Ethernet, VPN, PPoE, 3G. Különböző eszközöket is használhatunk egyidejűleg. Amennyiben a Zeroshellt Wi-Fi AP –ként használjuk, többféle SSID –vel, lehetőségünk van külön-külön megtekinteni azokat.

Grafikai ábrázolás a különböző QoS osztályok szerint

Ha a forgalom felügyelet engedélyezve van egy hálózati eszközön, akkor lehetőség van a kimenő forgalom grafikus megtekintésére az előzőleg definiált forgalmi osztályok szerint. A diagramon **KÉK** színnel látható az összes kimenő forgalom, és **ZÖLD** szín jelöli a kiválasztott QoS osztályt.
A **NARANCS** szín jelöli a QoS kihasználtságát a teljes forgalomhoz képest. Jól látható, hogy az ETH03 interfész átlagos forgalma 4% volt, VoIP híváskor ez viszont elérte a 33%-ot is.

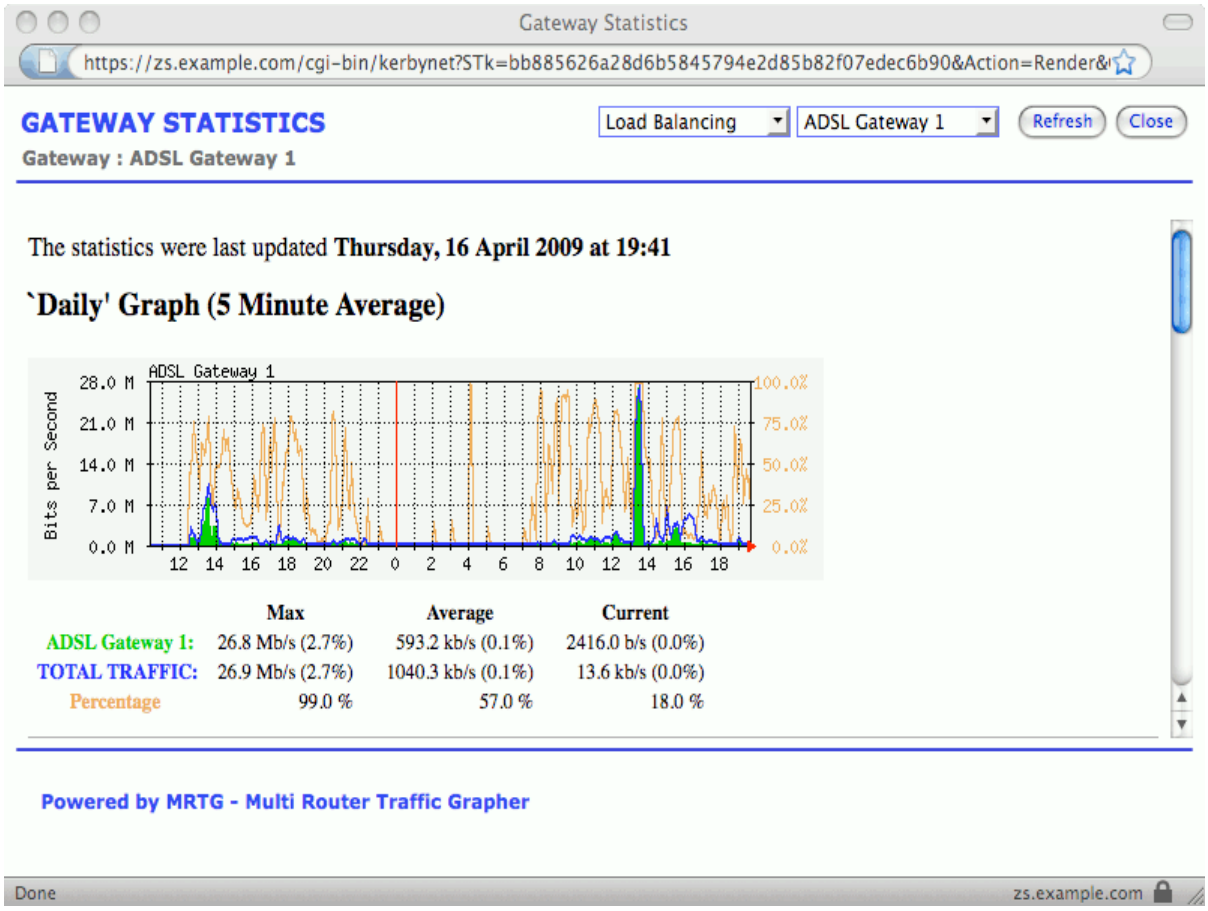


Hálózati forgalom grafikusan ábrázolva, QoS osztályok szerint

Terheléskiegyenlített forgalom továbbítás a gatewayek felé

Köszönet a Net Balancer -nek, a Zeroshell képes szétosztani a forgalmat több WAN kapcsolaton keresztül. Ez lehet xDSL, 3G, Modem, szinte bármi. Az szabályozás lehet automatikus, amikor is a kapcsolatok súlyozzuk, vagy manuálisan is adhatunk meg szabályokat (úgy mint a tűzfal vagy a QoS esetén), hogy milyen forgalom mely kapcsolaton keresztül történjen. Automatikus terhelés elosztás esetén hasznos lehet ez a grafika, hogy megállapítsuk, a kapcsolatok milyen kihasználtsággal üzemelnek. A súlyozás módosításával korrigálhatunk. Minél több pontot adunk egy gatewaynek, annál nagyobb lesz a részesedése az összes forgalomból.

ZÖLD szín jelöli a kiválasztott gateway forgalmát.
KÉK szín jelöli az összes forgalmat.
NARANCS szín pedig a kiválasztott interface részesedését az összes forgalomból.



Load Balancing

MRTG aktiválása a Zeroshell –ben

Az MRTG a Zeroshell 1.0beta11 kiadásától kezdve része a „telepítőnek”. A régebbi rendszerekhez külön update (C110) formájában érhető el. Az újabb rendszerek esetén nem szükséges az update kézi telepítése.

1.0beta11 verzió esetén a telepítéshez a következő parancsokat adjuk ki:

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

Sikeres telepítés után megjelenik egy [Graphics] gomb, amire kattintva megtekintheti a grafikákat.

Aktivációs kulcsok

A Zeroshell legtöbb funkciójától eltérően néhány statisztika csak aktivációs kód megadása után érhető el. Az alábbi grafikák korlátlanul elérhetőek:

- Rendszer terhelés
- Aktív kapcsolatok száma
- Bejövő/kimenő forgalom (VPN, bridge, PPPoE, UMTS/HSDPA)
- QoS osztályok grafikonja (VPN, bridge, PPPoE, UMTS/HSDPA)

A következő grafikák viszont aktiválást igényelnek:

- Bejövő/kimenő forgalom Ethernet/Wireless és VLAN 802.1q interfészeken
- Alkalmazott QoS osztályok Ethernet/Wireless interfészeken
- Internet kapcsolat terhelés elosztása

Az aktivációs kulcs függ a hálózati kártyánk MAC címétől. Minden egyes hálózati kártyánk a rendszerben saját aktivációs kulcsot kér a grafikákhoz. Egy Ethernet kártyához tartozó grafika aktiválásakor ugyanazzal a kulccsal automatikusan aktiválódnak a hozzá tartozó VLAN és QoS osztályok grafikonjai is. Ha egy Wi-Fi kártyához több SSID is tartozik, elég az egyik grafikont aktiválni, és a többi SSID –hez tartozó is automatikusan elérhető lesz. Ahogy korábban említettük az aktiváló kulcsok pusztán az Ethernet/Wireless eszközök MAC címétől függenek, tehát ha ugyanazon a gépen újratelepítik a Zeroshellt, vagy új profilt hoznak létre, a kulcsok újra felhasználhatóak lesznek. Az aktiváló kulcsok a „Feautre Code" alapján kerülnek legenerálásra, melyeket emailben várunk, egyszerre több kódot is elküldhet. A Zeroshell fejlesztéseinek támogatásával (is) igényelhetnek aktivációs kulcsokat:

- Készítsen dokumentumokat HTML vagy PDF formátumban, melyben bemutatja a Zeroshell lehetőségeit. Ez akár egy egyszerű leírás is lehet, Ön hogyan és milyen célre használta fel a Zeroshellt. A leírás készítőjének meg kell adnia az elérhetőségét, hogy szükség esetén az olvasók kapcsolatba tudjanak lépni vele. A leírás frissítéséhez hozzáférést kell biztosítani. A leírás linkelve lesz a dokumentációk között.
- Bármilyen adomány PayPal –on keresztül. Ezt hardverek beszerzésére és tesztelésére fordítjuk.

Kétség nélkül legszívesebben dokumentációkat várunk, leginkább ezzel tudjuk támogatni azokat, akik szeretnék használni a Zeroshellt. PayPal támogatást inkább csak akkor kérnénk, ha nincs időd és/vagy lehetőséged dokumentáció készítésére.
Fontos megjegyzés, hogy az aktiválási folyamat nem változtatja meg az MRTG működését, mely forrása a saját weboldalukról elérhető.

Megjegyzés:
(*) Ha a beépített MRTG helyett mégis azt szeretnéd, hogy a SNMP –n keresztül legyenek elérhetőek a statisztikák, csak telepítsd fel a net-snmp csomagot, amit a Zeroshellhez készítettek.