RouterOS: Vizualizace datových toků

Obsah

Verze dokumentu

Verze 1.1 ze dne 29.3.2004

Autor

Zdeněk Švarc (zdenek.svarc@promedia.cz), pracuje ve společnosti PROMEDIA.CZ, s.r.o.

Úvod

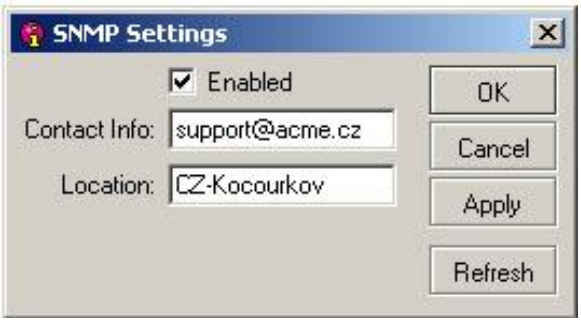
Díky SNMP agentu obsaženém v RouterOS, můžeme v reálném čase získat řadu informací o stavu směrovače. Nejčastěji je používán pro vizualizaci datových toků. RouterOS nám umožňuje vytvářet nejen grafy síťových toků na jednotlivých síťových rozhranní, ale od verze RouterOS 2.8 také grafy jednotlivých queues, tedy například toky od/k jednotlivých IP adresám.

K dispozici je celá řada programů, které umožňují zpracování SNMP dat. Následující dokument se bude týkat převážně programu MRTG. Domnívám se totiž, že MRTG, dostupný zdarma, je správnou volbou v případě, kdy hledáte vhodné řešení pro vizualizaci síťových toků Vašeho směrovače. Informace v tomto dokumentu obsažené, Vám však budou užitečné i v případě, že budete pro zpracování SNMP informací využívat jiný program.

Nastavení SNMP agenta na straně RouterOS

SNMP nastavujeme v RouterOS výběrem SNMP v hlavním menu. Je nutné definovat tzv. community name s omezenými právy jen pro čtení. Dále můžeme specifikovat vzdálenou IP adresu, ze které dovolíme SNMP komunikaci. Uvádím příklad pro Winbox:

Defaultní jméno komunity ve většině síťových zařízení je `public`. My jsme použili odlišné jméno komunity `acme_mrtg`

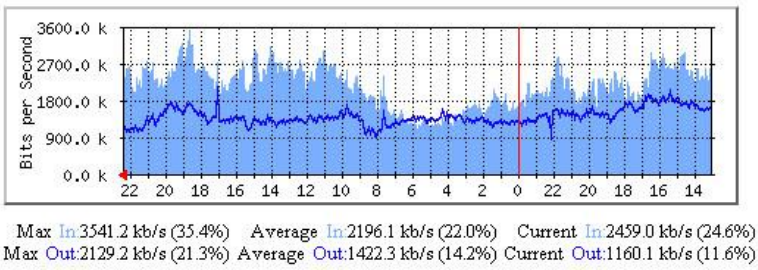


Dále můžeme specifikovat `Contact Info` a `Location`. Jedná se o volitelné záznamy.

MRTG (pro Unix i Windows)

Multi Router Traffic Grapher je šířen pod licencí GPL. Můžete jej tedy získat a používat zcela zdarma (www.gnu.org/copyleft/gpl.html). Existuje ve verzích jak pro UNIX, tak i Windows. Ke svému běhu potřebuje Perl, což v případě UNIXU není žádný problém. Pro Windows se osvědčil Active Perl (ve verzi 5.6 a výš), který je taktéž k dispozici zdarma. Výstupy MRTG jsou ve formátu html.

Ukázka výstupu z programu MRTG



Návod pro instalaci MRTG naleznete na jeho domovské stránce. K dispozici jsou zdrojové kódy i binární balíčky (např. pro Debian jako `apt-get install mrtg`). Výborného průvodce konfigurací MRTG napsal Milan Gigel. Seriál jeho článků naleznete na serveru Root.cz www.root.cz/clanek/833

Příklad konfiguračního souboru pro zobrazovaní datového toku procházejícího přes čtyři síťové rozhranní (zde se jedná o zařízení Engeno M440, které pohání RouterOS):

```
# Adresar s vystupy
WorkDir: /var/www/mrtg

# Globalni nastaveni barvy grafu, jazyku, atd.
Colours[_]: LIGHT BLUE#7aafff,BLUE#1000ff,DARK BLUE#000066,VIOLET#ff00ff,GREEN#00ff00
Language: English
Options[_]: bits,transparent
Forks: 10
#<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">

# Sledovana sitova zarizeni

### Engeno M440 - interfaces ###

Target[M440-ether1]: 1:jmeno_komunity@adresa.naseho.routeru:
SetEnv[M440-ether1]: MRTG_INT_IP="adresa.naseho.routeru" MRTG_INT_DESCR="Ethernet port"
MaxBytes[M440-ether1]: 1250000
Title[M440-ether1]: Sitova zatez na M440-ether1.nas.router
PageTop[M440-ether1]: <H1><FONT FACE="Arial">Traffic Analysis</FONT></H1>
 <TABLE>
```

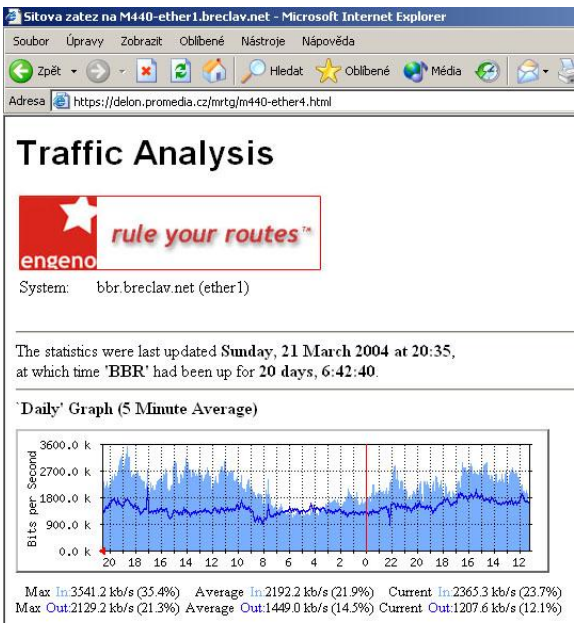
```
   <TR><TD>System:</TD>     <TD> adresa.naseho.routeru (ether1) </TD></TR>
   <TR><IMG SRC="engeno.jpg" ALT="engeno.com"></TR>
 </TABLE>

Target[M440-ether2]: 2:jmeno_komunity@adresa.naseho.routeru:
SetEnv[M440-ether2]: MRTG_INT_IP="adresa.naseho.routeru" MRTG_INT_DESCR="Ethernet port"
MaxBytes[M440-ether2]: 1250000
Title[M440-ether2]: Sitova zatez na M440-ether1.nas.router
PageTop[M440-ether2]: <H1><FONT FACE="Arial">Traffic Analysis</FONT></H1>
 <TABLE>
   <TR><TD>System:</TD>     <TD> adresa.naseho.routeru (ether1) </TD></TR>
   <TR><IMG SRC="engeno.jpg" ALT="engeno.com"></TR>
 </TABLE>

Target[M440-ether3]: 3:jmeno_komunity@adresa.naseho.routeru:
SetEnv[M440-ether3]: MRTG_INT_IP="adresa.naseho.routeru" MRTG_INT_DESCR="Ethernet port"
MaxBytes[M440-ether3]: 1250000
Title[M440-ether3]: Sitova zatez na M440-ether1.nas.router
PageTop[M440-ether3]: <H1><FONT FACE="Arial">Traffic Analysis</FONT></H1>
 <TABLE>
   <TR><TD>System:</TD>     <TD> adresa.naseho.routeru (ether1) </TD></TR>
   <TR><IMG SRC="engeno.jpg" ALT="engeno.com"></TR>
 </TABLE>

Target[M440-ether4]: 4:jmeno_komunity@adresa.naseho.routeru:
SetEnv[M440-ether4]: MRTG_INT_IP="adresa.naseho.routeru" MRTG_INT_DESCR="Ethernet port"
MaxBytes[M440-ether4]: 1250000
Title[M440-ether4]: Sitova zatez na M440-ether1.nas.router
PageTop[M440-ether4]: <H1><FONT FACE="Arial">Traffic Analysis</FONT></H1>
 <TABLE>
   <TR><TD>System:</TD>     <TD> adresa.naseho.routeru (ether1) </TD></TR>
   <TR><IMG SRC="engeno.jpg" ALT="engeno.com"></TR>
 </TABLE>
```

Výstup generovaný tímto konfiguračním souborem pak vypadá takto:



Obdobným způsobem můžeme vytvářet grafy jednotlivých queues. Následuje popis pro vizualizaci simple queues. OID (object ID) zvoleného queue je třeba zapsat do konfiguračního souboru mrtg do direktivy `Target` takto (pozor, jedná se o zápis na jeden řádek):

```
Target[M440-queue1]:
1.3.6.1.4.1.14988.1.1.2.1.1.8.1686&1.3.6.1.4.1.14988.1.1.2.1.1.9.1686:
jmeno_komunity@adresa.naseho.routeru:
```

RouterOS specifikuje pro každé queue následující formát OID:

`1.3.6.1.4.1.14988.1.1.2.1.1.`**`X.Y`**

kde **X** specifikuje:

2	pojmenování queue (pokud jste jej nezadávali, pak je shodné s target IP)
3	target IP adresa
4	target IP maska
5	destination IP adresa
6	destination IP maska
8	přijaté bajty
9	odchozí bajty
10	příchozí pakety
11	odchozí pakety

V rámci MRTG nás zajímají hodnoty příchozích a odchozích bajtů, tedy 8 a 9 mezi něž v direktivě `Target` vkládáme znak `&`

Y specifikuje OID číslo queue. Zjitit které OID queue číslo patří jednotlivé queue je možné zjistit v terminálovém režimu RouterOS příkazem:

```
print oid
```

Příklad zjištění OID čísla queue:

```
[admin@BBR] queue simple> print oid
Flags: X - disabled, I - invalid, D - dynamic
 0    name=.1.3.6.1.4.1.14988.1.1.2.1.1.2.1686
      bytes-in=.1.3.6.1.4.1.14988.1.1.2.1.1.8.1686
      bytes-out=.1.3.6.1.4.1.14988.1.1.2.1.1.9.1686
      packets-in=.1.3.6.1.4.1.14988.1.1.2.1.1.10.1686
      packets-out=.1.3.6.1.4.1.14988.1.1.2.1.1.11.1686

 1 X  name=.1.3.6.1.4.1.14988.1.1.2.1.1.2.1687
      bytes-in=.1.3.6.1.4.1.14988.1.1.2.1.1.8.1687
      bytes-out=.1.3.6.1.4.1.14988.1.1.2.1.1.9.1687
      packets-in=.1.3.6.1.4.1.14988.1.1.2.1.1.10.1687
      packets-out=.1.3.6.1.4.1.14988.1.1.2.1.1.11.1687

 2    name=.1.3.6.1.4.1.14988.1.1.2.1.1.2.1688
      bytes-in=.1.3.6.1.4.1.14988.1.1.2.1.1.8.1688
      bytes-out=.1.3.6.1.4.1.14988.1.1.2.1.1.9.1688
      packets-in=.1.3.6.1.4.1.14988.1.1.2.1.1.10.1688
      packets-out=.1.3.6.1.4.1.14988.1.1.2.1.1.11.1688

 3    name=.1.3.6.1.4.1.14988.1.1.2.1.1.2.1689
      bytes-in=.1.3.6.1.4.1.14988.1.1.2.1.1.8.1689
      bytes-out=.1.3.6.1.4.1.14988.1.1.2.1.1.9.1689
      packets-in=.1.3.6.1.4.1.14988.1.1.2.1.1.10.1689
```

Pro MRTG existují utility, které umí dále pracovat s MRTG log soubory. Tímto způsobem je možné vytvářet přehledy se sumami přenesených dat, které slouží například jako podklad pro fakturace počítaných linek v případě, že jste ISP.

Program MRTG je dostupný na adrese: www.mrtg.org
Program ActivePerl je dostupný na adrese: www.activestate.com/Products/ActivePerl

RRD tool

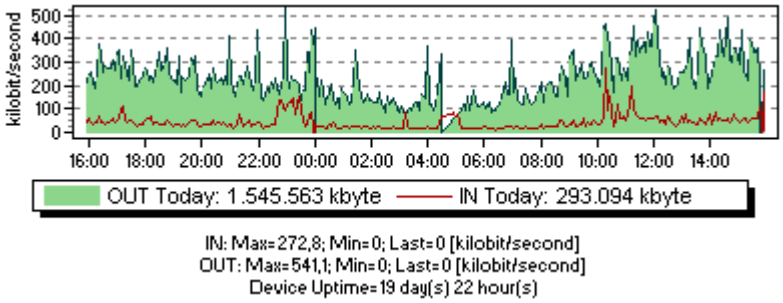
Round Robin Database Tool je nová generace MRTG, pocházející od stejného autora. Začátečník by měl dát přednost o poznání jednoduššímu MRTG. Na druhou stranu nabízí RDDT řadu propracovaných funkcí. Více se dozvíte na domovské stránce projektu.

Program RRD tool je dostupný na adrese: www.rrdtool.org

PRTG (pro Windows)

Uživatelé Windows, zvlášť ti méně zdatní, by měli zvážit, zda-li by pro ně nebylo vhodnější použít některý z komerčních programů určených pro vizualizaci přenášených dat. Nemluvíme nutně o enterprise řešeních typu HP OpenView. Za cenu do dvou tisíc korun je dostupný výborný program PRTG, který je prezentován jako „windowsová“ obdoba unixového MRTG. Zdarma si můžete vyzkoušet jeho free verzi, která je, mimo jiné, omezena pouze na zobrazování jednoho grafu a neumožňuje běh jako služba (service). PRTG umožňuje uživatelsky specifikovat OID, takže je možné vytvářet grafy jak síťových rozhranní, tak i queues. PRTG vytváří nejen grafy datových doků, ale také sumy přenesených dat, což se výborně hodí jako podklad pro fakturaci ISP u tarifů s počítaným množstvím dat. Výstupy je samozřejmě možné generovat do html.

Ukázka výstupu z programu PRTG



Program PRTG je dostupný na adrese: www.paessler.com
Prodej PRTG v ČR zajišťuje společnost PROMEDIA.CZ: www.promedia.cz