Network Monitoring and Management

MRTG and RRDtool

MRTG: Multi Router Traffic Grapher

- Tool to monitor traffic load on network links

- Generates HTML pages with PNG images

- Almost live visual representation of traffic

- Available at http://oss.oetiker.ch/mrtg/.

MRTG is ubiquitous...

- Uses simple SNMP queries on a regular interval to generate graphs.

MRTG

- External MRTG readers to interpret data as needed
- Can build graphs of anything with SNMP MIB like CPU load, disk availability, temperature, etc.
- Data sources can be anything that provides a counter or gauge value – not necessarily SNMP.
- For example, graphing round trip times
- MRTG can be extended to work with RRDTool

MRTG: Issues

- Generates a new graph every 5 minutes... Lots of overhead if lots of graphs.

- Very few customizable graphing options.

- Disk space can be an issue.

- MRTG management is tedious.

Using MRTG

- Get the required packages
- Compile and install the packages
- Make cfg files for router interfaces with `cfgmaker`
- Create html pages from the cfg files with `indexmaker`
- Trigger MRTG periodically from cron or run it in daemon mode

RRDtool

- Round Robin Database for time series data storage

- Command line based

- From the author of MRTG

- Made to be faster and more flexible

- Includes CGI and Graphing tools, plus APIs

- Solves the Historical Trends and Simple Interface problems as well as storage issues

Find RRDtool here: http://oss.oetiker.ch/rrdtool/

Defining the Output (Archives)

`RRA:AVERAGE:0.5:1:24`

`RRA:AVERAGE:0.5:6:10`

RRA = Round Robin Archive

AVERAGE = consolidation function

0.5 = up to 50% of consolidated points may be UNKNOWN

- 1:24 = this RRA keeps each sample (average over one 5 minute primary sample), 24 times (which is 2 hours worth)

- 6:10 = one RRA keeps an average over every six 5 minute primary samples (30 minutes), 10 times (which is 5 hours worth)
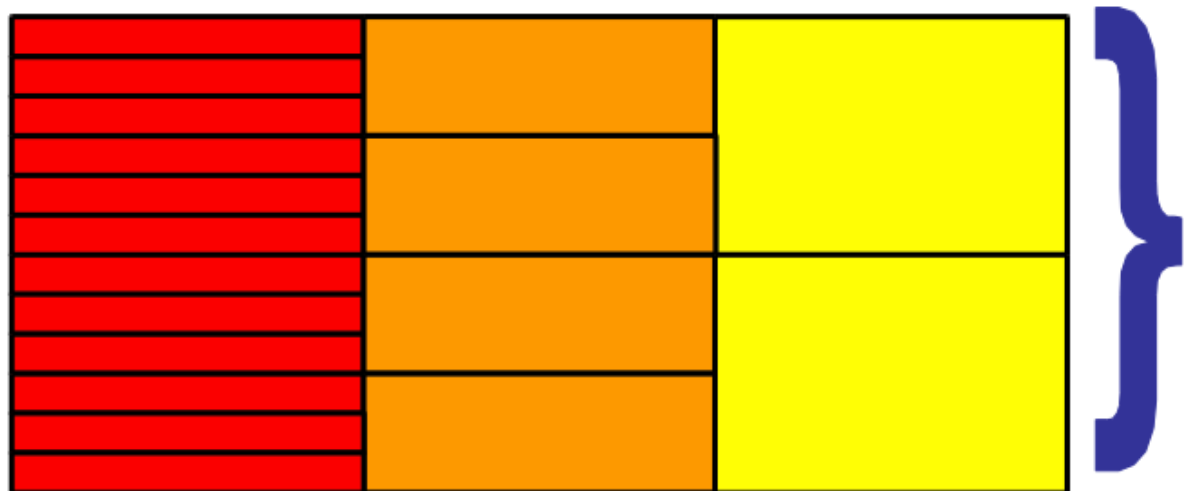
Clear as mud!

- All depends on original step size which defaults to 5 minutes

RRDtool Database Format

Recent data stored once every 5 minutes for the past 2 hours (1:24)

Old data averaged to one entry per day for the last 365 days (288:365)

--step 300

(5 minute input step size)

RRD File

RRA 1:24

RRA 6:10

RRA 288:365

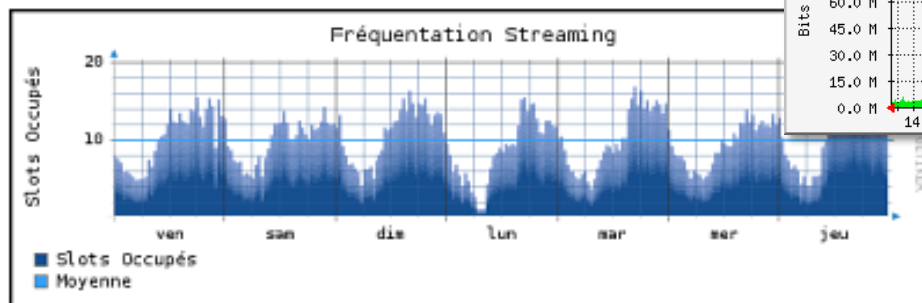Medium length data averaged to one entry per half hour for the last 5 hours (6:10)
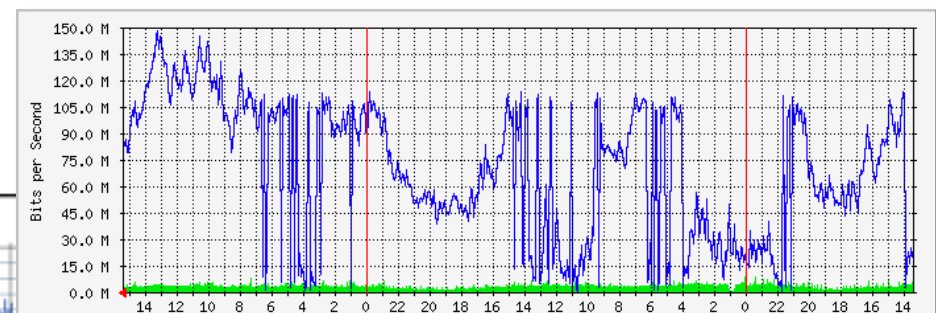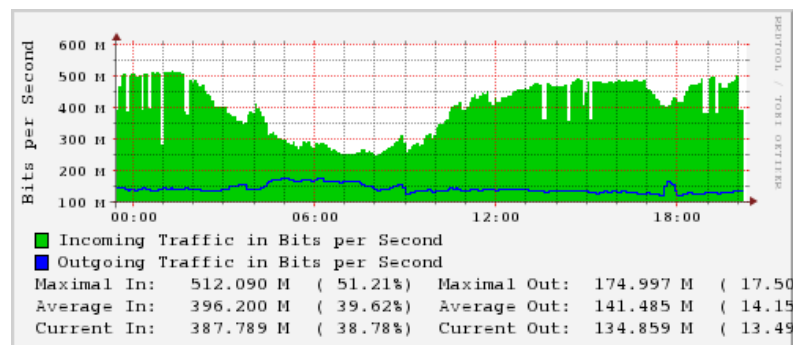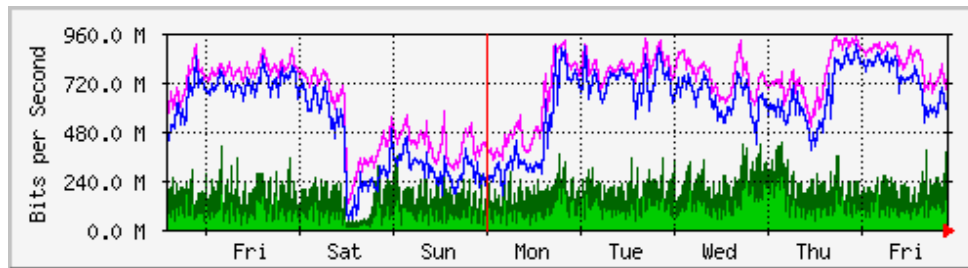
So simple…

```
rrdtool create /var/nagios/rrd/host0_load.rrd -s 600
   DS:1MIN-Load:GAUGE:1200:0:100 DS:5MIN-Load:GAUGE:
   1200:0:100 DS:15MIN-Load:GAUGE:1200:0:100
   RRA:AVERAGE:0.5:1:50400 RRA:AVERAGE:0.5:60:43800

rrdtool create /var/nagios/rrd/host0_disk_usage.rrd -s
   600 DS:root:GAUGE:1200:0:U DS:home:GAUGE:1200:0:U
   DS:usr:GAUGE:1200:0:U DS:var:GAUGE:1200:0:U
   RRA:AVERAGE:0.5:1:50400 RRA:AVERAGE:0.5:60:43800

rrdtool create /var/nagios/rrd/apricot-INTL_Ping.rrd -
   s 300 DS:ping:GAUGE:600:0:U RRA:AVERAGE:0.5:1:50400
   RRA:AVERAGE:0.5:60:43800

rrdtool create /var/nagios/rrd/host0_total.rrd -s 300
   DS:IN:COUNTER:1200:0:U DS:OUT:COUNTER:600:0:U
   RRA:AVERAGE:0.5:1:50400 RRA:AVERAGE:0.5:60:43800
```

What it looks like…

Questions?

?

MRTG

In Ubuntu / Debian

```
$ sudo apt-get install mrtg
```

Configuration

- /etc/mrtg/<device.mrtg>

- Global directory : /var/www/mrtg/

- Run MRTG against the configuration file from cron

cfgmaker

Uses `snmpwalk` and creates an mrtg configuration file

```
/usr/bin/cfgmaker                       \
  --output=/etc/mrtg/router.mrtg        \
  --global 'workdir: /var/www/mrtg'     \
  --global 'options[_]: growright,bits' \
  NetManage@10.10.0.254
```

Sample

Part of /etc/mrtg/device.mrtg

```
### Interface 1 >> Descr: 'FastEthernet0/0' | Name: 'Fa0/0' | Ip: '' | Eth: '' ###

Target[10.10.0.254_Fa0_0]: #Fa0/0:NetManage@10.10.0.254:

SetEnv[10.10.0.254_Fa0_0]: MRTG_INT_IP="" MRTG_INT_DESCR="FastEthernet0/0"

MaxBytes[10.10.0.254_Fa0_0]: 12500000

Title[10.10.0.254_Fa0_0]: Traffic Analysis for Fa0/0 -- rtr.ws.nsrc.org.nsrc.org

PageTop[10.10.0.254_Fa0_0]: <h1>Traffic Analysis for Fa0/0 -- rtr.ws.nsrc.org.nsrc.org</h1>
```

Creating HTML with indexmaker

Execute `indexmaker` like this:

```
/usr/bin/indexmaker                      \
--output=/var/www/mrtg/device.html    \
/etc/mrtg/device.mrtg
```

If your mrtg configuration file is well commented, the html is nice and detailed.

Lab Instructions

In a separate file