Monitoring the vital signs of a network with Multi Router Traffic Grapher (MRTG)

Peter K. Chow

GIAC Security Essential Certification (GSEC)
Practical Assignment
Version 1.4b
Option 2 – Case Study

April 8, 2004

Abstract

Network engineers are responsible for maintaining the health of their networks. They ensure that the network's resources hold the highest levels of Confidentiality, Integrity, and Availability (CIA triad). One way to maintain a healthy and secure network is to monitor the network interworking devices, such as the router or switch interface's throughput. Another way would be to monitor the network devices processor performance and memory utilization. By monitoring these attributes fundamental security principles are applied toward maintaining a healthy network infrastructure. A network infrastructure can be compared to the workings of a human body. A network infrastructure is like a human body in that it has inputs, outputs, memory, and processing power. Therefore, the network's interfaces can be compared to an arm that links to other networks to exchange bits of information. The processor is its' heart that controls the flow of information, and the memory is its' brain that records and remembers where everything needs to go. All these vital elements are important and need to be monitored in order to have a healthy functioning network infrastructure, just like the human body needs to be monitored in order to have a healthy and long life.

This paper will describe how to use Multi Router Traffic Grapher (MRTG) to monitor the vital signs of network infrastructure devices. We will see how MRTG can be used to monitor router's and switches' vital components. We will also see how MRTG can be used to forecast network growth, network outages and high traffic utilization. And finally, we will see how MRTG can be applied toward maintaining Confidentiality, Integrity, and Availability, (the CIA triad).

Background Information

How does a network engineer know when a network is operating within its' normal or acceptable parameters? In order to answer that question, the first thing is to know what is considered normal and/or acceptable. Therefore, the first thing is to setup a baseline. Without a baseline, there is nothing to compare to, and there is no way to really tell if it is operating within limits. Establishing a baseline can show that network utilization is peeking higher than acceptable limits, or if memory utilization is operating above normal. Setting a baseline can show trending patterns of a network, and it can quickly help identify abnormalities and establish a reference point for when a problem started and ended.

There are many tools available to monitor the performance of a network, however, the right tool to use would depend on the network infrastructure. Some considerations for the right tool or application should include; easy installation and setup, monitoring of multiple devices or interfaces, sustained or continued monitoring, trending, real-time monitoring, graphic outputs, and viewable via a web browser. Multi Router Traffic Grapher (MRTG) is such a tool that can do all of the above, and the best thing about MRTG is that it is free and has been in use for almost 9 years.

Multi Router Traffic Grapher (MRTG) Overview

Tobias Oetiker created Multi Router Traffic Grapher version 1.0, as an in-house application in the summer of 1994. In 1995 MRTG-2 was published on the Internet for the general public as a free tool available under the terms of the GNU General Public Licenses[1]. In November 1997, a complete redesign of MRTG was released. The current version is MRTG-3, MRTG 2.10.13. A complete overview and history can be found at http://people.ee.ethz.ch/~oetiker/webtools/mrtg/paper.

MRTG was written in Perl and C languages and works in a UNIX or Windows environment. MRTG generates HTML pages that display graphical images and can be accessed either locally or remotely, such as on the Internet. The use of a web browser to display the data was a new concept, “MRTG's approach for long term analysis and the friendly presentation on the Web was new”[2].

Highlights of MRTG

- Works on most UNIX platforms and Microsoft Windows Environments
- Uses Perl for customization and scripting
- Uses standard SNMP (Simple Network Management Protocol) and MIB (Management Information Base)
- Simple semi-automatic configuration tool
- Easy Installation and setup
- Generates Graphic results
- Sustained monitoring and trending
- Displays Maximums, Averages, and Current Inputs and Outputs
- Monitors multiple devices and interfaces
- MRTG is available under the GNU General Public License.

MRTG Requirements

MRTG will run on UNIX and Windows environments. It uses Particle Extraction and Report Language (Perl) script programming language to export the outputs into HTML pages. Prerequisites require both Perl programming language, and a web server application such as Apache or Microsoft Windows IIS to be installed.

Batch files are created to automatically run the Perl scripts. To automatically run the batch files in UNIX, Cron[3] can be used, or in Windows the Microsoft Scheduled Tasks can be used.

[1] http://www.gnu.org/copyleft/gpl.html

[2] http://people.ee.ethz.ch/~oetiker/webtools/mrtg/paper/

[3] http://www.unixgeeks.org/security/newbie/unix/cron-1.html

Installation Requirements

All examples within this document will be based on the Windows 2000 Server platform. An overview of the installation and application will be addressed herein. For full details of the application and installation, see the MRTG NT guide located in the documentation directory labeled "doc" (C:\MRTG\mrtg-2.10.13\doc\mrtg-nt-guide.html).

Software

To run MRTG the following software is needed and should be installed in the following order.

A. Microsoft Windows 2000 (or NT 4.0) Server Operating System
B. Multi Router Traffic Grapher (MRTG)
C. Particle Extraction and Report Language (Perl)
D. Apache Web server

Microsoft Windows 2000 Server Operating System Installation

Installation of Microsoft Windows 2000 Server Operating System software will not be addressed within this document. See Microsoft Windows 2000 Server User/Owner manual, or seek a Network or Systems Administrator for assistance.

Multi Router Traffic Grapher (MRTG) Installation

Obtain a copy of Multi Router Traffic Grapher (MRTG)[4]. The latest release of MRTG is version MRTG 2.10.13. Download mrtg-2.10.13.zip file into a directory (e.g. C\MRTG).

The MRGT files are compressed into a zipped file and need to be unzipped. A copy of WinZip can be obtained at www.download.com. Download WinZip to a directory and double click on the icon to install WinZip. After WinZip has been installed, unzip the MRTG files.

Particle Extraction and Report Language (Perl) Installation

Obtain a copy of ActivePerl at ActiveState[5]. Download ActivePerl 5.8.2 build 808. Install ActivePerl by double clicking the icon and following the prompts.

Testing MRTG and Perl Installation

After unzipping MRTG into a directory and installing Perl, test that Perl and MRTG are correctly installed and working by completing the following.

- Click on the Windows "Start" button
- Click on the "Run" button
- Type "cmd" and click "OK" button to open a DOS prompt
- Change to the directory where MRTG was downloaded (cd c:\mrtg)

[4] http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/pub/
[5] http://www.activestate.com/Products/Download/Download.plex?id=ActivePerl

- Change to the directory where MRTG was unzipped (cd mrtg-2.10.13)
- Change to the “bin” directory (cd bin)
- Type “perl mrtg” If it is working correctly it will look like the following, if it doesn’t then try reloading Perl and/or downloading and unzipping MRTG again.

  Correct:

  ```
  C:\MRTG\mrtg-2.10.13\bin>perl mrtg
  Usage: mrtg <config-file>

  mrtg-2.10.13 is the Multi Router Traffic Grapher.

  If you want to know more about this tool, you might want
  to read the docs. They came together with mrtg!

  Home: http://people.ee.ethz.ch/~oetiker/webtools/mrtg/

  C:\MRTG\mrtg-2.10.13\bin>
  ```

  Incorrect:

  ```
  C:\MRTG\mrtg-2.10.13\bin>perl mrtg
  'perl' is not recognized as an internal or external command,
  operable program or batch file.

  C:\MRTG\mrtg-2.10.13\bin>
  ```

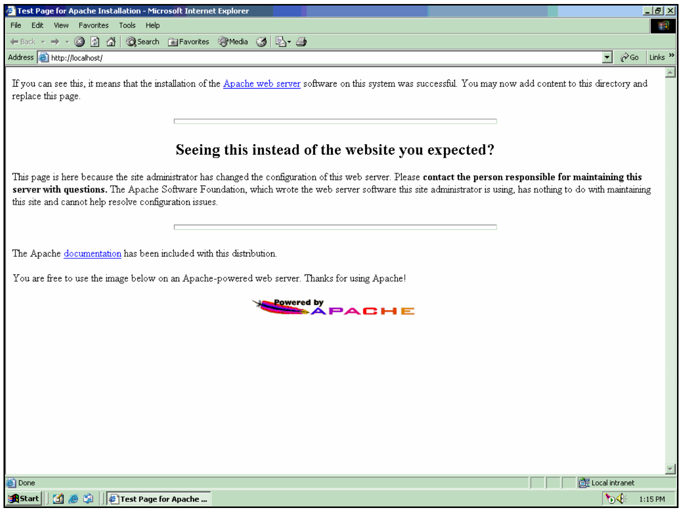
Apache Web Server Installation

Obtain a copy of Apache Web Server for Microsoft Windows[6]. Install Apache Web Server by double clicking the icon and following the prompts. After Apache has been installed it will require the system to be rebooted. Apache Web Server services should startup automatically after boot up, if it does not, then manually execute the program. The current release is apache_2.0.49-win32-x86.

Testing Apache Web Server

Open a Web Browser and in the Web Browser’s Address box enter the IP address of the system or type “localhost”. If it is correctly installed, the default Apache webpage “Test Page for Apache Installation” will be displayed as shown in Figure 1.

[6] http://apache.130th.net/httpd/binaries/win32/


Test Page for Apache Installation - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go
Links
Done
Local intranet
Start
Test Page for Apache ...
1:15 PM

http://localhost/

If you can see this, it means that the installation of the Apache web server software on this system was successful. You may now add content to this directory and replace this page.

Seeing this instead of the website you expected?

This page is here because the site administrator has changed the configuration of this web server. Please **contact the person responsible for maintaining this server with questions.** The Apache Software Foundation, which wrote the web server software this site administrator is using, has nothing to do with maintaining this site and cannot help resolve configuration issues.

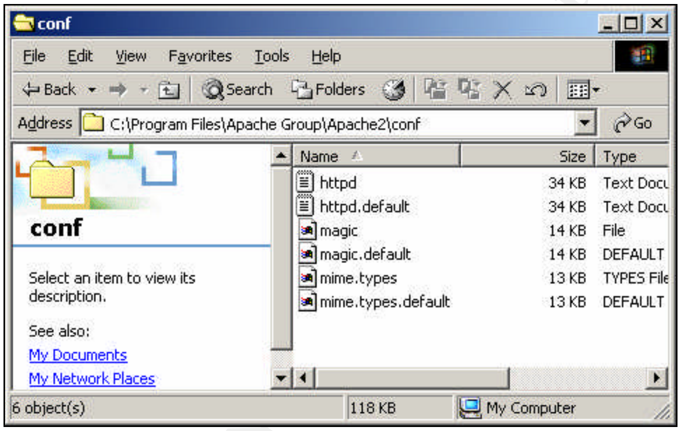
The Apache documentation has been included with this distribution.

You are free to use the image below on an Apache-powered web server. Thanks for using Apache!

Figure 1

Configuring Apache Web Server

After Perl, MRTG and Apache Web server have been installed and tested, the next step is to configure Apache Web server to point to the directory where the MRTG files will be stored. Figure 2, illustrates the default path for the Apache directory. Open the file called httpd.conf using Microsoft "Notepad"



C:\Program Files\Apache Group\Apache2\conf

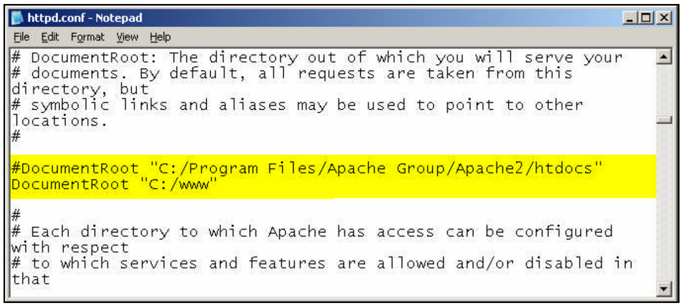
Name	Size	Type
httpd	34 KB	Text Docu
httpd.default	34 KB	Text Docu
magic	14 KB	File
magic.default	14 KB	DEFAULT
mime.types	13 KB	TYPES File
mime.types.default	13 KB	DEFAULT

6 object(s) 118 KB

Figure 2

As shown in Figure 3, in the httpd.conf file locate "DocumentRoot "C:/Program Files/Apache Group/Apache2/htdocs"" and replace it with "DocumentRoot "C:\www"" (Used the # sign to comment out the line without deleting it), save and close the file.

(To comment out the change, place a # in front of DocumentRoot "C:/Program Files/Apache Group/Apache2/htdocs")



```
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this
directory, but
# symbolic links and aliases may be used to point to other
locations.
#

#DocumentRoot "C:/Program Files/Apache Group/Apache2/htdocs"
DocumentRoot "C:/www"

#
# Each directory to which Apache has access can be configured
with respect
# to which services and features are allowed and/or disabled in
that
```

Figure 3

As shown in Figure 4, after changes have been made to the httpd.conf file the Apache Web Services need to be restarted in order for them to take affect. Open the "Apache Service Monitor" located at the lower right-hand corner of the Windows taskbar and Stop and Start the service.

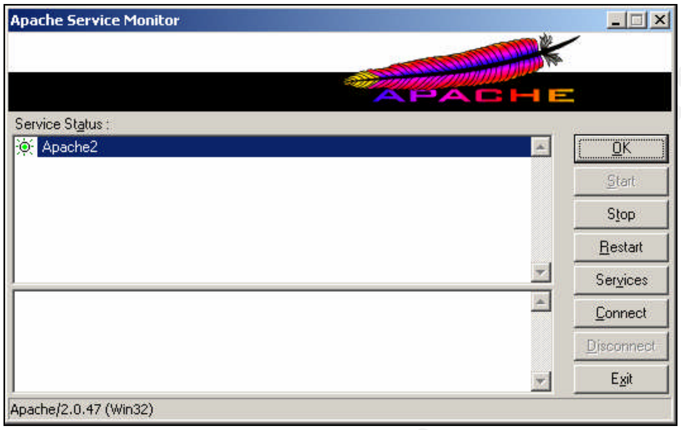
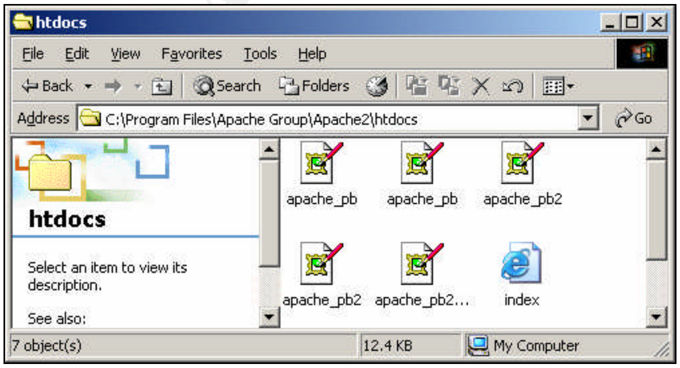


Figure 4

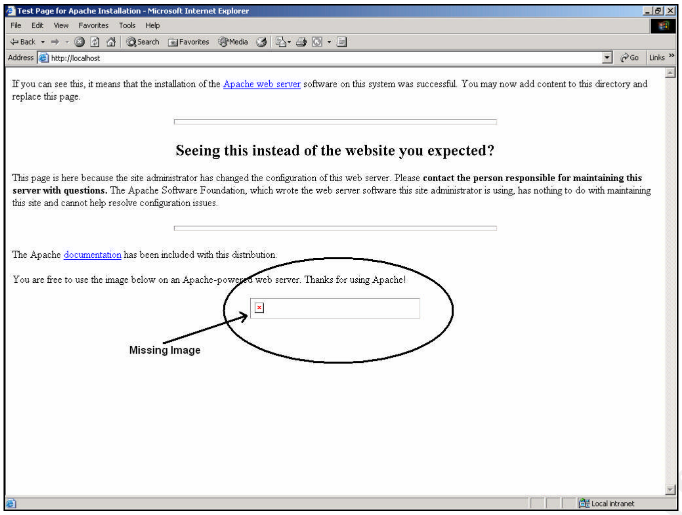
After configuring the Apache Web Server to point to the default web page, C:\www directory, copy the "index.http" file located in the C:\Program Files\Apache Group\Apache2\htdocs to C:\www. This will be used to test if the Web Server is pointing to the correct directory, as illustrated in Figure 5.



htdocs
File Edit View Favorites Tools Help
Back
Search
Folders
Address C:\Program Files\Apache Group\Apache2\htdocs
Go
htdocs
Select an item to view its description.
See also:
apache_pb
apache_pb
apache_pb2
apache_pb2
apache_pb2...
index
7 object(s)
12.4 KB
My Computer

Figure 5

If everything is working correctly the “Test Page for Apache Installation” web page will be displayed. Note that the “Powered by Apache” image is missing. This is because the image was not copied into the C:\www directory. See Figure 6.


Test Page for Apache Installation - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost
Go Links
Local intranet
Missing Image

If you can see this, it means that the installation of the Apache web server software on this system was successful. You may now add content to this directory and replace this page.

Seeing this instead of the website you expected?

This page is here because the site administrator has changed the configuration of this web server. Please **contact the person responsible for maintaining this server with questions.** The Apache Software Foundation, which wrote the web server software this site administrator is using, has nothing to do with maintaining this site and cannot help resolve configuration issues.

The Apache documentation has been included with this distribution.

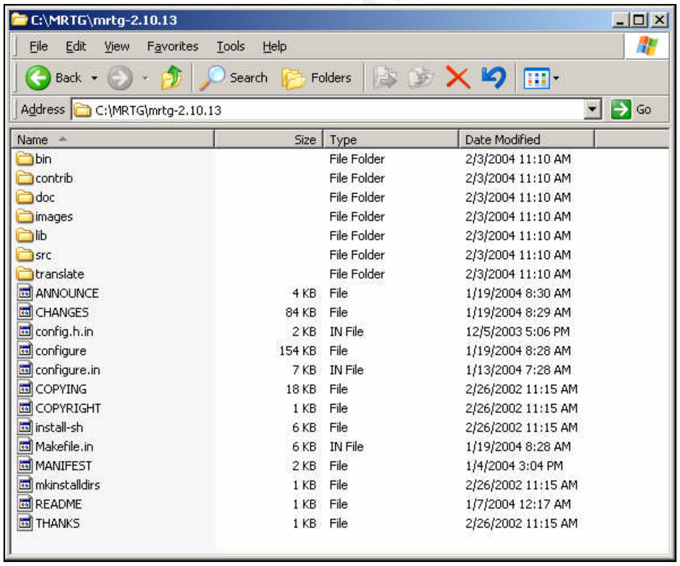
You are free to use the image below on an Apache-powered web server. Thanks for using Apache!

Figure 6

MRTG Directories

Now that all the required software has been downloaded, installed and configured, before running MRTG an overview of the directories structure will be reviewed.

The following are directories that were created after unzipping the mrtg-2.10.13.zip. See Figure 7.


C:\MRTG\mrtg-2.10.13
File Edit View Favorites Tools Help
Back Search Folders
Address C:\MRTG\mrtg-2.10.13
Go

Name	Size	Type	Date Modified
bin		File Folder	2/3/2004 11:10 AM
contrib		File Folder	2/3/2004 11:10 AM
doc		File Folder	2/3/2004 11:10 AM
images		File Folder	2/3/2004 11:10 AM
lib		File Folder	2/3/2004 11:10 AM
src		File Folder	2/3/2004 11:10 AM
translate		File Folder	2/3/2004 11:10 AM
ANNOUNCE	4 KB	File	1/19/2004 8:30 AM
CHANGES	84 KB	File	1/19/2004 8:29 AM
config.h.in	2 KB	IN File	12/5/2003 5:06 PM
configure	154 KB	File	1/19/2004 8:28 AM
configure.in	7 KB	IN File	1/13/2004 7:28 AM
COPYING	18 KB	File	2/26/2002 11:15 AM
COPYRIGHT	1 KB	File	2/26/2002 11:15 AM
install-sh	6 KB	File	2/26/2002 11:15 AM
Makefile.in	6 KB	IN File	1/19/2004 8:28 AM
MANIFEST	2 KB	File	1/4/2004 3:04 PM
mkinstalldirs	1 KB	File	2/26/2002 11:15 AM
README	1 KB	File	1/7/2004 12:17 AM
THANKS	1 KB	File	2/26/2002 11:15 AM

Figure 7

Description of Directories

Bin Directory

The Bin directory contains the program files used to create and configure Multi Router Traffic Grapher. This directory is where most of the work will be done.

Contrib Directory

The Contrib directory contains subdirectories with example files to add features to MRTG configuration, (i.e. examples of perl files to monitor memory and processor utilization for Cisco routers).

3.3 Doc Directory

The Doc directory contains all the necessary documentation for installing, configuring, and the user's guide for Multi Router Traffic Grapher.

3.4 Images Directory

The Image directory contains GIF images (MRTG logo) for the default webpage. Copy all the .gif images and place them in the directory where the Apache Web server is pointing to prevent broken links (C:\www).

3.5 Lib Directory

The Lib directory contains library files for Multi Router Traffic Grapher.

3.6 Src Directory

The Src directory contains the source code for Multi Router Traffic Grapher.

Translate Directory

The Translate directory contains language types to be used by Multi Router Traffic Grapher.

Multi Router Traffic Grapher (MRTG) Perl Scripts

Located in the bin directory (C:\MRTG\mrtg-2.10.13\bin) are CFGMAKER, MRTG, and INDEXMAKER files. These three files are the main Perl scripts that will be used to create MRTG files. The CFGMAKER is used to gather the SNMP information about a Targeted Device and to create configuration files to be used by MRTG Perl script. After creating a configuration file of a Targeted Device the MRTG Perl script is used to create HTML codes and to batch query updates. The INDEXMAKER Perl script will be use to create an Index HTML page. This is very useful when the Targeted Device has multiple interfaces.

Target Device Information

Before creating a configuration file for MRTG, there are several things needed. The first is to set the SNMP parameter of the intended device. On most internetworking devices, such as a Cisco Router, the SNMP features are disabled. However, if they are enabled, there are default settings. The default setting for Cisco Routers read-only SNMP community string is "public". To change a Cisco router's SNMP parameters, follow the example.

Cisco SNMP Syntax

```
CiscoRouter #
CiscoRouter #configure terminal
CiscoRouter(config)#snmp-server community public RO (where "public" is the Read-only
community string)
```

CiscoRouter(config)#snmp-server community private RW (where "private" is the Read-Write community string)
CiscoRouter(config)#snmp-server contact Network_Team (where " Network_Team " is the Contact information)

The following example of setting and verifying SNMP on Catalyst 5500 switches can be found at the Cisco Website[7].

Enable SNMP Community Strings

Follow these steps to enable SNMP community strings on a catalyst switch.

1. Telnet to the Catalyst Switch (the Catalyst 5500 is used in the example below):
   prompt# telnet 172.16.99.55

2. Enter the enable mode by entering the enable password at the prompt:
   Cat5500>enable
   Password:
   Cat5500> (enable)

3. To enable Read-only (RO) community string, use the command below:
   Cat5500> (enable) set snmp community read-only XXXX
   (where "XXXX" is the Read-only community string)

4. To enable Read-write (RW) community string, use the command below:
   Cat5500> (enable) set snmp community read-write YYYY
   where "YYYY" is the Read-write community string

Note: The Catalyst 4000, 5000, and 6000 series switches do not have Start-up configurations. That's why there is no write memory command in these switches compared to the routers.

5. Verify that the new community strings have been added:
   Cat5500> (enable) show snmp

```
RMON:                    Enabled
Extended RMON:           Enabled
Extended RMON Netflow:   Enabled
Extended RMON Vlanmode:  Disabled
Extended RMON Vlanagent: Disabled
SPAN Configuration:
Traps Enabled:
Port,Module,Chassis,Bridge,Repeater,Vtp,Auth,ippermit,Vmps,config,
   entity,stpx,syslog
Port Traps Enabled: 3/1-9,4/1-24,7/1-12,9/1-16,10/1-12,11/1-24
Community-Access    Community-String
----------------    ----------------
read-only           XXXX (XXXX is the new Read-only community string)
read-write          YYYY (YYYY is the new Read-write community string)
read-write-all      secret
....
--<snip>--
```

[7] http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094aa4.shtml#configsnmp

For more information, see the documentation in the "mrtg-faq's", located in C:\MRTG\mrtg-2.10.13\doc\mrtg-faq.html) or visit the Cisco website on "SNMP Introduction"[8] and "How to Configure SNMP Community Strings"[9]

After SNMP has been configured on the Target Devices, the next step is to obtain the IP address or hostname and the SNMP port number, (if non-standard), of the target device to be monitored. (e.g. IP address for Internet Router, 10.0.0.1)

With SNMP set and the IP address of the Target Device gathered, make sure that device is accessible, and that there are no firewalls or Access Control Lists (ACLs) blocking it.

Example Configuration

The following example is a Cisco Router called "Gateway" with the IP address of 10.0.0.6 and the SNMP read-only community configured as "public".

Using CFGMAKER

To create a configuration file so MRTG can use it to compile the html code, use the CFGMAKER Perl script.

Open a DOS prompt and change to the directory where the CFGMAKER, MRTG, and INDEXMAKER files are located (e.g. C:\mrtg\mrtg-2.10.13\bin).

In the DOS prompt type "perl cfgmaker public@10.6.252.6 > gateway.cfg"

- perl – Executable command for Perl
- cfgmaker – Perl scrip for MRTG Configuration Maker
- public – SNMP read-only community string
- @ – Connects the SNMP read-only community string with the targeted device IP address
- 10.6.252.6 – Targeted device's IP address
- > gateway.cfg – Creates a configuration file called gateway.cfg

The created gateway.cfg file provides the parameters used by MRTG to compile the HTML codes. Open the "gateway.cfg with Microsoft Notepad (or another text editor). Locate the line "# WorkDir: C:\mrtgdata", this is where MRTG will place the compiled HMTL codes. In our example, change it to "WorkDir: C:\www" (Without the "") and save the file.

[8] http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tech_protocol_home.html
[9] http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094aa4.shtml

Using MRTG

To create the HTML codes and to start retrieving the SNMP data from the Targeted Device, open a DOS prompt and in the directory c:\mrtg\mrtg-2.10.13\bin, type “perl mrtg gateway.cfg”.

- perl – Executable command for Perl
- mrtg – Perl scrip for MRTG
- gateway.cfg – Configuration file for the Targeted device

Use Microsoft Explorer to open C:\www directory. Verify that MRTG has created the HTML files using the Targeted Devices SNMP information.

Using INDEXMAKER

INDEXMAKER is used to create an index.html to consolidate the HTML files. Open a DOS prompt and in the directory c:\mrtg\mrtg-2.10.13\bin, type “perl INDEXMAKER gateway.cfg > c:\www\index.html”.

- perl – Executable command for Perl
- indexmaker – Perl scrip for MRTG
- gateway.cfg – Configuration file for the Targeted device
- > index.html – Creates an index.html file in the c:\www directory

Testing MRTG

Open a web browser and enter the host IP address or type “localhost” in the Address bar. Figure 8 shows the index page.

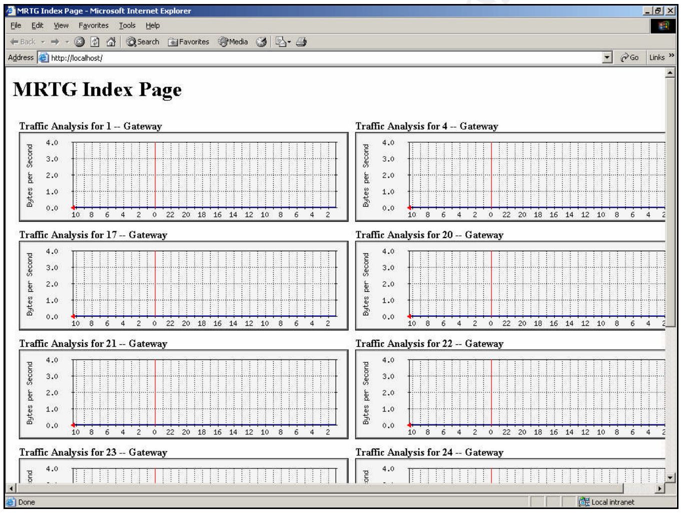

MRTG Index Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost/
Go Links
MRTG Index Page
Traffic Analysis for 1 -- Gateway
Traffic Analysis for 4 -- Gateway
Traffic Analysis for 17 -- Gateway
Traffic Analysis for 20 -- Gateway
Traffic Analysis for 21 -- Gateway
Traffic Analysis for 22 -- Gateway
Traffic Analysis for 23 -- Gateway
Traffic Analysis for 24 -- Gateway
Bytes per Second
4.0
3.0
2.0
1.0
0.0
10 8 6 4 2 0 22 20 18 16 14 12 10 8 6 4 2
Done
Local intranet

Figure 8

Gathering additional data

Update the Targeted Devices SNMP data, by running the “perl MRTG gateway.cfg” again. It is best to run this in five minute increments. Note that it will not recreate all the HTML files; it will only update the data. Updated data will display from left to right, as shown in Figure 9.

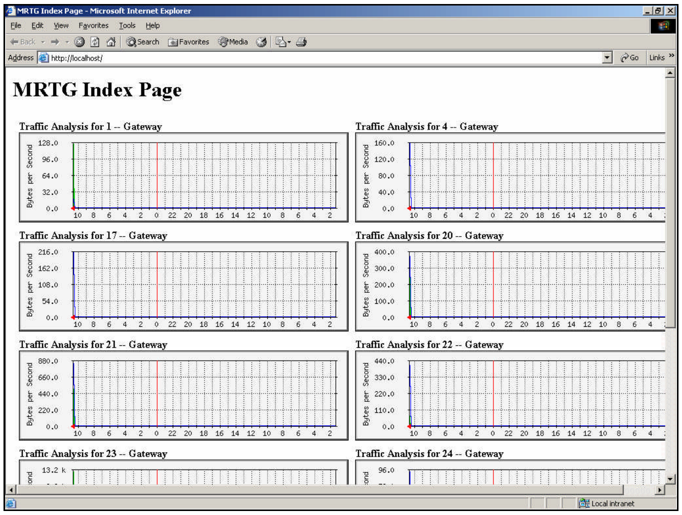

MRTG Index Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost/
Go Links
MRTG Index Page
Traffic Analysis for 1 -- Gateway
Traffic Analysis for 4 -- Gateway
Traffic Analysis for 17 -- Gateway
Traffic Analysis for 20 -- Gateway
Traffic Analysis for 21 -- Gateway
Traffic Analysis for 22 -- Gateway
Traffic Analysis for 23 -- Gateway
Traffic Analysis for 24 -- Gateway
Bytes per Second
Local intranet

Figure 9

Automating Processes

To automate the process of updating the data, first create a batch process and second create a Scheduled Task.

To create a batch process, open a DOS prompt and in the MRTG working directory C:\MRTG\mrtg-2.10.13\bin, type “edit run.bat”. This will create a file called “run.bat”. In this file type “perl MRTG gateway.cfg”, save and exit. Test this batch file, by opening a DOS prompt and in the MRTG working directory, typing “run.bat”. Next open a web browser to verify that the data has been updated.

Use “Microsoft’s Scheduled Tasks” to create an automated process to run the run.bat file. Open the “Control Panel” by clicking the Start -> Settings -> Control Panel. Double click the “Scheduled Tasks” icon and then double click on the “Add Scheduled Task” to create a new task. The “Scheduled Task Wizard” will walkthrough this process. Follow the prompts and add the “run.bat” file. Open the “Advanced Properties” and in the “Advanced Schedule Options” check the “Repeat Task” box and change it to “Every” 5 minutes, and in the “Until” box check the Duration” radio button and enter 9999 hours.

Test this “Scheduled Task” by right-clicking on “Run” in the “Scheduled Tasks,” click “Run”. Next open a web browser and verify that the data is being updated every 5 minutes. The web browser will automatically refresh. More information about “Microsoft Scheduled Tasks” can be found at the iopus website[10].

[10] http://www.iopus.com/guides/winscheduler.htm

CFGMAKER Options

The CFGMAKER Perl script has a variety of “Options” to create a customized configuration file to be used by MRTG. These options make it easier to create the desired outputs without using a default configuration file and without having to later edit it to produce the desired outputs.

For example, instead of displaying the “IP Address” of an interface, display the “Interface Description”, or change the default directory path from C:\Inetpub\wwwroot to C:\www instead.

A complete of list of “Options” can be found in the Appendix A section of this document. For a comprehensive explanation look in the “Description” of cfgmaker.html located in the MRTG doc directory (C:\MRTG\mrtg-2.10.13\doc\cfgmaker.html)

Sample of Options

--ifref=nr	interface references by Interface Number (default)
--ifref=ip	... by IP Address
--ifref=eth	... by Ethernet Number
--ifref=descry	... by Interface Description
--ifref=name	... by Interface Name
--ifref=type	... by Interface Type
--ifdesc=nr	interface description uses Interface Number (default)
--ifdesc=ip	... uses IP Address
--ifdesc=eth	... uses Ethernet Number
--ifdesc=descry	... uses Interface Description
--ifdesc=name	... uses Interface Name
--ifdesc=alias	... uses Interface Alias
--ifdesc=type	... uses Interface Type

CFGMAKER Options Syntax

To create a configuration file using “Options” in the CFGMAKER, the syntax is:
perl CFGMAKER [options] [community@]router]

CFGMAKER Options Example

In this example, the working directory will be in C:\www. To use the Interface Name as the identifier, display the data from right-to-left, refresh the webpages every 600 seconds, don’t display any downed interfaces, use the read-only SNMP community string “public”, the targeted device IP address 10.6.252.6 and export the configuration file to EA-2600-RT-01.cfg, use the following CFGMAKER Syntax.

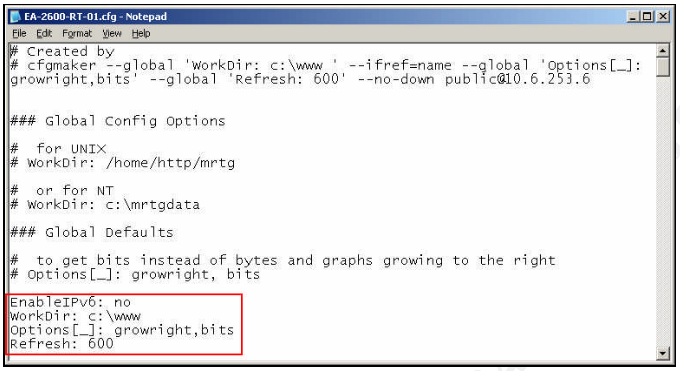
```
perl cfgmaker --global "WorkDir: c:\www " --ifref=name --global "Options[_]:
growright,bits" --global "Refresh: 600" --no-down public@10.6.253.6 > EA-2600-
RT-01.cfg
```

- perl – Executable command for Perl
- cfgmaker – Perl scrip for MRTG Configuration Maker

- --global "WorkDir: c:\www " – Working directory where the HTML code will be stored
- --ifref=name – To use the Interface Name
- --global "Options[_]: growright,bits" – Display the data from right-to-left
- --global "Refresh: 600" –
- --no-down –
- public – SNMP read-only community string
- @ – Connects the SNMP read-only community string with the targeted device IP address
- 10.6.253.6 – Targeted device IP address
- > EA-2600-RT-01.cfg – Creates a configuration file called EA-2600-RT-01.cfg

Verifying CFGMAKER Options Example

Open EA-2600-RT-01.cfg, shown in Figure 10. This figure illustrates where the default "Options" have been replaced with the Options in the line command, thus reducing the need to open and edit the configuration file after it has been created.



```
# Created by
# cfgmaker --global 'WorkDir: c:\www ' --ifref=name --global 'Options[_]:
growright,bits' --global 'Refresh: 600' --no-down public@10.6.253.6


### Global Config Options

#  for UNIX
# WorkDir: /home/http/mrtg

#  or for NT
# WorkDir: c:\mrtgdata

### Global Defaults

#  to get bits instead of bytes and graphs growing to the right
# Options[_]: growright, bits

EnableIPv6: no
WorkDir: c:\www
Options[_]: growright,bits
Refresh: 600
```

Figure 10

Executing a Batch File

To simplify operations, create a batch file to automate all the necessary processes. There are three main processes. First is to create a configuration file, second to create an index page, and third run MRTG.

The following example creates a batch file to automate all three processes:
Open a DOS prompt and in the working MRTG bin directory, type "edit EA-2600-RT-01.bat" Enter the following and save the file:

```
perl cfgmaker --global "WorkDir: c:\www " --ifref=name --global "Options[_]: growright,bits" --global "Refresh: 600" --no-down public@10.6.253.6 > EA-2600-RT-01.cfg

perl indexmaker --title="Ennis: Intranet EA-2600-RT-01 10.6.253.6" --enumerate EA-2600-RT-01.cfg > c:\www\EA-2600-RT-01.html

perl mrtg EA-2600-RT-01.cfg
```

Run this by typing "EA-2600-RT-01.bat" in the DOS prompt. Note that it will create a configuration file (EA-2600-RT-01.cfg), and then an index page (EA-

2600-RT-01.html) and finally it processes the configuration file to create the HTTP page for that device.

To verify that it works, open “EA-2600-RT-01.html” with a web browser. Figure 11 shows that it has successfully created EA-2600-RT-01.html and that entries are correct and working.

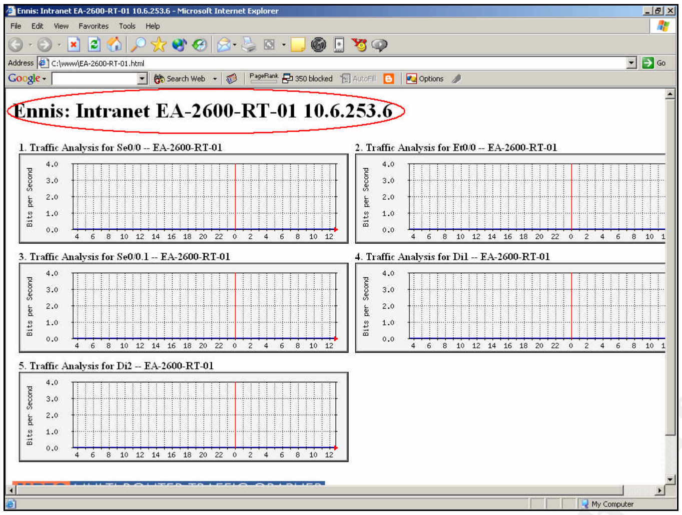

Ennis: Intranet EA-2600-RT-01 10.6.253.6 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address C:\www\EA-2600-RT-01.html
Go
Google
Search Web
PageRank
350 blocked
AutoFill
Options
Ennis: Intranet EA-2600-RT-01 10.6.253.6
1. Traffic Analysis for Se0/0 -- EA-2600-RT-01
2. Traffic Analysis for Et0/0 -- EA-2600-RT-01
3. Traffic Analysis for Se0/0.1 -- EA-2600-RT-01
4. Traffic Analysis for Di1 -- EA-2600-RT-01
5. Traffic Analysis for Di2 -- EA-2600-RT-01
Bits per Second
4.0
3.0
2.0
1.0
0.0
4 6 8 10 12 14 16 18 20 22 0 2 4 6 8 10 12
My Computer

Figure 11

Advanced Processing Batch File

Apply the same method used to create an “Executing Batch File” however, by simply adding additional device parameters into a single batch file, multiple configuration parameters are created. For example, there are four internetworking devices called Device1, Device2, Device3, and Device4.

Edit the batch file as follows:

```
perl cfgmaker --global "WorkDir: c:\www " --ifref=name --global "Options[_]:
growright,bits" --global "Refresh: 600" --no-down public@10.6.253.1 > device1.cfg
perl indexmaker --title="Device1" --enumerate device1.cfg > c:\www\ device1.html
perl mrtg device1.cfg

perl cfgmaker --global "WorkDir: c:\www " --ifref=name --global "Options[_]:
growright,bits" --global "Refresh: 600" --no-down public@10.6.253.2 > device2.cfg
perl indexmaker --title="Device2" --enumerate device2.cfg > c:\www\ device2.html
perl mrtg device2.cfg

perl cfgmaker --global "WorkDir: c:\www " --ifref=name --global "Options[_]:
growright,bits" --global "Refresh: 600" --no-down public@10.6.253.3 > device3.cfg
perl indexmaker --title="Device3" --enumerate device3.cfg > c:\www\ device3.html
perl mrtg device3.cfg

perl cfgmaker --global "WorkDir: c:\www " --ifref=name --global "Options[_]:
growright,bits" --global "Refresh: 600" --no-down public@10.6.253.4> device4.cfg
perl indexmaker --title="Device4" --enumerate device4.cfg > c:\www\ device4.html
perl mrtg device4.cfg
```

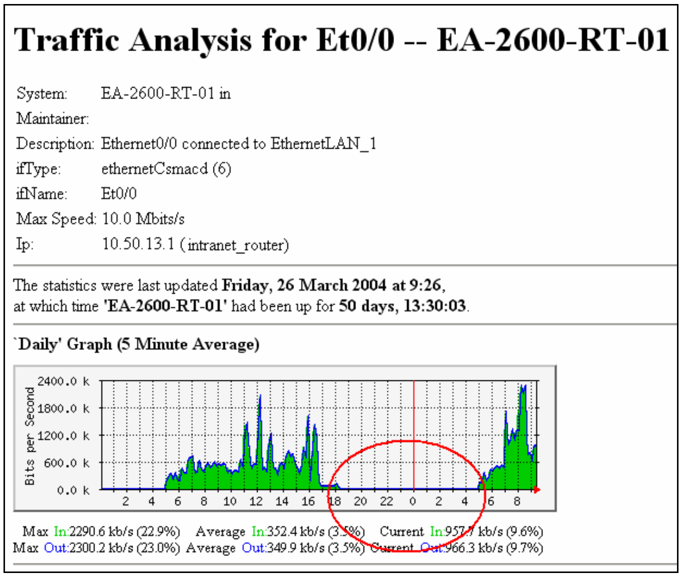
Now by executing a single batch file (i.e. multi_device.bat), MRTG will create and run multiple devices and thereby reduce administration time.

Deploying MRTG

MRTG is a powerful tool that can be used to monitor a wide range of an internetworking device's vital signs, such as a router's LAN or WAN interfaces, or a switch's Virtual Local Area Network (VLAN) segments. MRTG is an excellent monitoring tool to track and trend outages, utilization and performance. MRTG by default displays Daily, Weekly, Monthly and Yearly Maximums, Averages, and Current data inputs and outputs. Network Operating Center (NOC) technicians can use the MRTG Daily Graph to monitor and record high utilizations or outages. When there is an abnormality detected, the NOC technicians can use MRTG as a reference point to aid the Network Technician in identifying potential causes, to quickly take corrective actions, and mitigate prolonged downtime. Network Administrators can use MRTG to maintain and optimize internetworking devices and servers. MRTG can be used to monitor memory and CPU utilization or create a special script to send PINGs to a destination and monitor the latency and response time. By comparing the Weekly and Monthly Graph, the Network Administrator can compare the performances and thereby establish a baseline for improvement. Network Engineers can appreciate MRTG's Yearly graphs to track and create a trend analysis, and to predict and forecast network utilization. MRTG can aid in taking appropriate action when a device is either over or under scaled. For example, when a router WAN connection is under or over utilized it can be costly to maintain or harder to support. MRTG is a great way to provide a historical analysis of a device to be used to budget and allocate resources for future development.

Using MRGT to detect network outages

MRTG can be used to identify a Network Outage and track what was affected, when the outage started and how long it lasted. For example in Figure 12, the Ethernet connection on the LAN side of an Intranet router was down on Friday, 26 March 2004. It started at 1830 and lasted until 0450. This is very helpful information because it allows NOC technicians to alert the Network Administrator at the first indication of a network outage, so that the Network Administrator can take appropriate action. Because MRTG can monitor and record twenty-four hours a day, it is very helpful in establishing a baseline, and in creating a historical pattern for determining what is considered normal operation. This illustration also shows that on the previous day, at the same time frame, there was an outage. The conclusion could now be that this is normal and that there are no users during that time frame. Therefore, there is no need for the NOC technician to alert the Network Administrator.



Traffic Analysis for Et0/0 -- EA-2600-RT-01

System:	EA-2600-RT-01 in
Maintainer:	
Description:	Ethernet0/0 connected to EthernetLAN_1
ifType:	ethernetCsmacd (6)
ifName:	Et0/0
Max Speed:	10.0 Mbits/s
Ip:	10.50.13.1 (intranet_router)

The statistics were last updated **Friday, 26 March 2004 at 9:26**,
at which time **'EA-2600-RT-01'** had been up for **50 days, 13:30:03**.

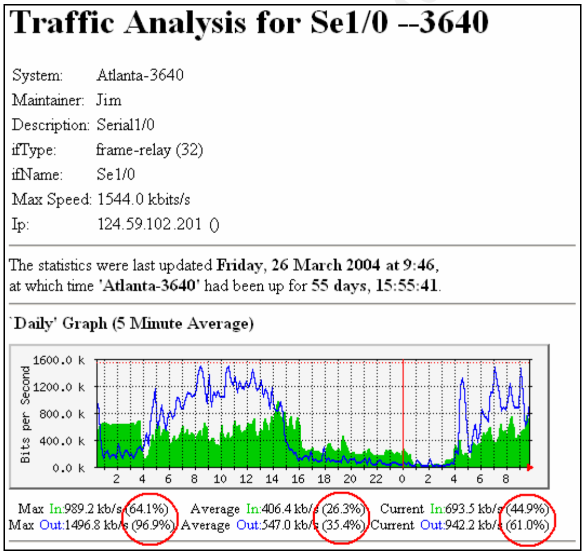
`Daily' Graph (5 Minute Average)

```
  Max In:2290.6 kb/s (22.9%)     Average In:352.4 kb/s (3.5%)    Current In:957.7 kb/s (9.6%)
Max Out:2300.2 kb/s (23.0%)  Average Out:349.9 kb/s (3.5%)  Current Out:966.3 kb/s (9.7%)
```

Figure 12

Using MRTG to detect high traffic utilization

MRTG is an excellent tool to use when there are complaints about the Network running slow. MRTG tracks Current, Average, and Max Inputs and Outputs, this is very useful in determining Utilization. For example, Figure 13 illustrates a 1544.0 kbits Frame-Relay connection to Atlanta. This Cisco 3640 router's Serial 1/0 has been up for 55 days and on Friday, 26 March 2004 at 9:46 the Current Input is at 44.9% and Output is at 61.0%. The Average Input is 26.3% and Output is 35.4% in the last twenty-four hours, and the Maximum Input peaked at 64.1% and Output peaked as high as 96.9%.



Traffic Analysis for Se1/0 --3640

System:	Atlanta-3640
Maintainer:	Jim
Description:	Serial1/0
ifType:	frame-relay (32)
ifName:	Se1/0
Max Speed:	1544.0 kbits/s
Ip:	124.59.102.201 ()

The statistics were last updated **Friday, 26 March 2004 at 9:46**,
at which time **'Atlanta-3640'** had been up for **55 days, 15:55:41**.

`Daily' Graph (5 Minute Average)

```
  Max In:989.2 kb/s (64.1%)     Average In:406.4 kb/s (26.3%)    Current In:693.5 kb/s (44.9%)
Max Out:1496.8 kb/s (96.9%)  Average Out:547.0 kb/s (35.4%)  Current Out:942.2 kb/s (61.0%)
```

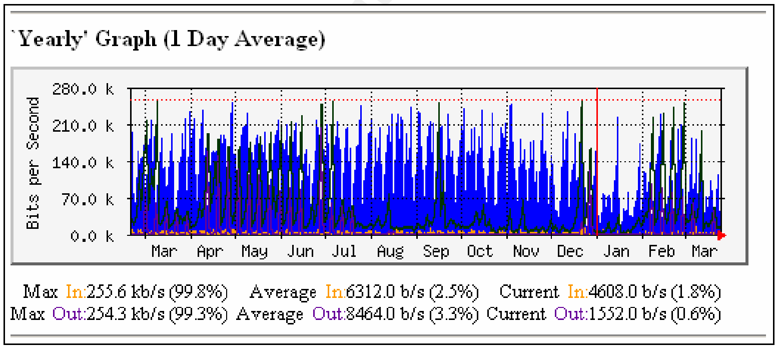
Figure 13

The “Current” In/Outputs are very useful in determining the current condition of a link. The “Average” In/Outputs can be used to compare with the “Current” In/Outputs, and determine if the link has been increasing or decreasing in traffic. The “Maximum” In/Outputs can be used to compare to the “Average” In/Output to evaluate if the traffic is sustaining High or Low utilization.

In our illustration, the Average Out bound traffic is 35.4% and the Maximum Out bound is 96.9%. Because there was a wide difference between the Average and Maximum, a difference of 61.5%, and since the Average was low at 35.4%, the conclusion here would be that there hasn’t been a sustained high usage, but there has been a spike in utilization, and therefore there is no need for alarm. However, it the margin between the Average and Maximum are closer, and the Maximum was high, for example Maximum was 96.9% and the Average was 86.9%, then the conclusion might be that there has been a sustained high utilization which would call for attention and an investigation.

Using MRTG to Forecast network growth

Use MRTG’s Yearly Graphs to forecast network growth. MRTG captures Monthly trends and displays them in a Yearly format, this is very useful in determining if a connection is either under or over utilized. The Network Engineer can determine the circuit requirements based on this information and 4make plans for forecasting changes. Figure 14, shows that the Average In bound traffic is at 2.5% and the Average Out bound traffic is at 3.3%. However, the Maximum is at 99.8% Inbound and 99.3% Outbound. Although this circuit may not sustain high traffic, it does peak at a high percentage. Therefore, it would not be prudent to scale the circuit down in the event that there is a need to surge data across the connection. In this example, the Network Engineer can make a cognitive decision about which course of action to take to improve the network infrastructure and reduce costs.



Max In:255.6 kb/s (99.8%) Average In:6312.0 b/s (2.5%) Current In:4608.0 b/s (1.8%)
Max Out:254.3 kb/s (99.3%) Average Out:8464.0 b/s (3.3%) Current Out:1552.0 b/s (0.6%)

Figure 14

Applying MRTG to Confidentiality, Integrity, and Availability

Using MRTG to monitor and track a network’s usage patterns and utilization would aid in maintaining the Confidentiality, Integrity, and Availability of a network infrastructure.

Trending the networks Inputs and Outputs can aid in identifying if data is being copied or removed, which could mean a breach in Confidentiality or Integrity. For example if the normal outbound traffic is 20% on a given day, and the outbound traffic surged to 80%, this may be an indication that data is being copied "From" a server, such as a FTP or SCP. The opposite would be true, if the inbound traffic surged to 80%. This could be an indication that the data is being copied "To" a server.

Availability is the ability of the users to gain access to resources. Monitoring "Current" inputs can identify if utilization is high or if network connections are down or lost. High network utilizations may be an indication of a Denial-Of-Service (DoS) attack, or that the network is undersized. However, in either case, the network is unavailable to users, and either case would call for action to be taken. MRTG can be used to monitor the LAN or WAN inputs to mitigate availability problems. It can also be used to monitor a server's memory and processor to evaluate availability.

MRTG can be used in many ways to prevent network security related problems. MRTG's ability to track, trend, and display current and historical data, makes it an excellent first line of defense against breaching network Confidentiality, Integrity, and Availability.

Conclusion

MRTG can monitor a variety of an internetworking device's or server's vital signs, and mitigate security related problems. From a device's interfaces, memory, processor, PING, Drops, and whatever SNMP or MIB parameters you wish to specify. The benefits of using MRTG are many, but most of all it is a free, flexible and powerful tool. Creating a monitoring tool using MRTG is easy, fast, and does not require a great deal of prep work, programming or understanding, to get working results. There are many companies using MRTG in lieu of a commercial branded product, not only because it's free, but because it can sustain monitoring over time, is viewable via a web browser, and works with SNMP and MIB standards. Because MRTG works in a Windows environment and is included in most Linux builds, there have been many implementations, (see the Appendix B section of this document for links and examples of MRTG being used to monitor environments). MRTG is a great tool for any Network Engineer who wants to maintain a healthy network infrastructure, to minimize troubleshooting and repair time, and to ensure Confidentiality, Integrity, and Availability.

Appendix A
CFGMAKER Options

OPTIONS

--ifref=nr	interface references by Interface Number (default)
--ifref=ip	... by Ip Address
--ifref=eth	... by Ethernet Number
--ifref=descry	... by Interface Description
--ifref=name	... by Interface Name
--ifref=type	... by Interface Type
--ifdesc=nr	interface description uses Interface Number (default)
--ifdesc=ip	... uses Ip Address
--ifdesc=eth	... uses Ethernet Number
--ifdesc=descry	... uses Interface Description
--ifdesc=name	... uses Interface Name
--ifdesc=alias	... uses Interface Alias
--ifdesc=type	... uses Interface Type
--if-filter=f	Test every interface against filter f to decide whether or not to include that interface into the collection. Currently f is being evaluated as a Perl expression and it's truth value is used to reject or accept the interface. (Experimental, under development, might change)
--if-template=templatefile	Replace the normal target entries for the interfaces with an entry as specified by the contents in the file templatefile. The file is supposed to contain Perl code to be executed to generate the lines for the target in the configuration file. (Experimental, under development, might change)
--host-template=templatefile	In addition to creating targets for a host's interfaces, it also creates targets for the host itself as specified by the contents in the file templatefile. The file is supposed to contain Perl code to be executed to generate the lines for the host related targets (such as CPU, ping response time measurements etc.) in the configuration file. (Experimental, under development, might change)
--global "x: a"	add global config entries
--no-down	do not look at admin or opr status of interfaces
--show-op-down	show interfaces which are operatively down

--subdirs=format
give each router its’ own subdirectory, naming each per "format", in which HOSTNAME and SNMPNAME will be replaced by the values of those items -- for instance, --subdirs=HOSTNAME or --subdirs="HOSTNAME (SNMPNAME)"

--noreversedns
do not reverse lookup ip numbers

--community=cmty
Set the default community string to "cmty" instead of "public".

--enable-ipv6
Enable IPv6 support, if the required libraries are present. Numeric IPv6 addresses must be enclosed in square brackets, e.g. public@[2001:760:4::1]:161

--use-16bit
Use 16bit SNMP request IDs to query all routers.

--snmp-options=:[<port>][:[<tmout>][:[<retr>][:[<backoff>][:<ver>]]]]
Specify default SNMP options to be appended to all routers following. Individual fields can be empty. Routers following might override some or all of the options given to --snmp-options.

--dns-domain=domain
Specifies a domain to append to the name of all routers following.

--nointerfaces
Don't generate any configuration lines for interfaces, skip the step of gathering interface information and don't run any interface template code.

--interfaces
Generate configuration lines for interfaces (this is the default). The main purpose of this option is to negate an --nointerfaces appearing earlier on the command line.

--help
brief help message

--man
full documentation

--version
print the version of cfgmaker --output=file output filename default is STDOUT

Appendix A

MRTG Examples[11]

Monitoring switch interfaces and VLANs at rou-rz-gw.ethz.ch
http://www.stat.ee.ethz.ch/mrtg/

Spam Filter Monitoring by Hugh Brown
http://selenium.dowco.com/spam/spam.html

Wireless Access Points monitored with MRTG and some custom scripts
http://openfire.coloradocollege.edu/mrtg/wireless.html

Monitoring personal Keyboard and mouse activity by Bohdan Vlasyuk
http://bodq.vstu.edu.ua/activity/

Website Monitoring with MRTG (Multiple examples)
http://sitemon.mine.nu/

Observatorio del Teide, Spain Local weather data
http://www.iac.es/weather/otdata/

Spam Filter Statistics at SystemNT.Net
http://spamstats.systemnt.net/

Seattle Public Schools, K-20 Connected Institutions
http://stats.uw.wa-k20.net/network/

[11] http://people.ee.ethz.ch/~oetiker/webtools/mrtg/users.html

References

[1]Tobias Oetiker. Multi Router Traffic Grapher (MRTG).
URL: http://people.ee.ethz.ch/~oetiker/webtools/mrtg/paper

[2] GNU's not Unix. GNU General Public License.
URL: http://www.gnu.org/copyleft/gpl.html

[3]Tobias Oetiker. Summary of MRTG 1.0.
URL: http://people.ee.ethz.ch/~oetiker/webtools/mrtg/paper/

[4] cogNiTioN,cognition@attrition.org. "Newbie: Intro to cron." December 30, 1999.
URL: http://www.unixgeeks.org/security/newbie/unix/cron-1.html

[5] Tobias Oetiker. Download latest release of MRTG.
URL: http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/pub/

[6]Actvestate. Download ActivePerl 5.8.3 build 809.
URL: http://www.activestate.com/Products/Download/Download.plex?id=ActivePerl

[6]The Apache Software Foundation. Current release of apache_2.0.49-win32-x86. March 19, 2004.
URL: http://apache.130th.net/httpd/binaries/win32/

[7]Cisco System, Inc. “How to Configure SNMP Community String”, Document ID: 7282. February 4, 2004.
URL:
http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094aa4.shtml#configsnmp

[8]Cisco System, Inc. "SNMP Introduction".
URL: http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tech_protocol_home.html

[9]Cisco System, Inc. "How to Configure SNMP Community String", Document ID: 7282. February 4, 2004.
URL:
http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094aa4.shtml#configsnmp

[10]iOpus Software. "How to use the Windows Task Scheduler". 2004.
URL: http://www.iopus.com/guides/winscheduler.htm

[11] Tobias Oetiker. Multi Router Traffic Grapher (MRTG). “ Special applications apart from traffic monitoring”.
URL: http://people.ee.ethz.ch/~oetiker/webtools/mrtg/users.html