MINT 709 PROJECT

Multi Router Traffic Grapher

Prof.MikeMacGregor
University of Alberta

NasimAbbasi

Nov 26, 2007

Abstract

MRTG used for monitoring and measuring the traffic load on network links. It allows the user to see traffic load on a network over time in graphical form. MRTG has been implemented in the MINT lab for experiment purpose and in the live environment of NorQuest College's network as well. Configured different scenarios in MINT lab and analyzed network traffic using MRTG graphs. To make more effective graphs different scripts has been integrated with MRTG.

Table of Contents

Introduction

Network Traffic Analysis Tool

Much of the work in network traffic analysis has focused on studying traffic on routers and switches in LAN and WAN environment. However, a wide range of important problems faced by network engineers today require analysis of traffic on all links simultaneously, including traffic engineering, attack detection, traffic forecasting and capacity planning.

Whole-network traffic analysis remains an important and unmet challenge. One way to address the problem of whole-network traffic analysis is to implement a effective monitoring tool.

The Multi Router Traffic Grapher, or just simply MRTG, is a software for monitoring and measuring the traffic load on network links. It allows the user to see traffic load on a network over time in graphical form. It was originally developed by Tobias Oetiker and Dave Rand to monitor router traffic, but has developed into a tool that can create graphs and statistics for almost anything.

MRTG is a advanced network traffic monitoring, analysis and reporting tool, based on Windows and Unix operating systems. It captures and analyzes all traffic transport over both Ethernet and WLAN networks and decodes all major TCP/IP and application protocols.

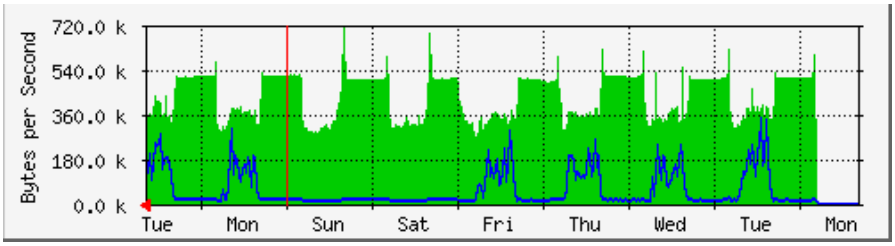
Its allows to view and log key communication protocols such as SMTP, HTTP, TCP and UDP . The comprehensive reports and graphic views enables to understand network performance and bandwidth usage quickly.

MRTG is a effective tool used to monitor network performance, prevent network problems, conduct effective troubleshooting. It is also helpful in monitoring network bandwidth, network accounting, auditing and network planning purposes.

Our MINT project is based on MRTG tool which we implemented in two phases, in first phase MTRG has been implemented in MINT Lab and in second phase MRTG has been implemented in live environment of NorQuest College's network.

Multi-Router Traffic Grapher (MRTG)

Multi-Router Traffic Grapher is a standalone tool that collects, stores, and graphs data at a given time intervals daily (5 min average), weekly (30 min average), monthly (2 hour average) and yearly (1 day average). MRTG uses Perl script which uses simple network management protocol to read the traffic counters of network devices and a fast C program which logs the traffic data and creates graphs representing the traffic on the network links. These graphs are in the html format, which can be viewed from any browser such as internet explorer or mozilla firefox.
There are many features of MRTG that make it desirable over many other network analysis tools. It is fairly simple to set up, the configuration file MRTG.cfg which can be written manually or auto-generated. MRTG's data files do not grow due to the use of a unique data consolidation algorithm. However, like any other packages there are few issues with the MRTG.



MRTG Graph

Issues with MRTG

- The main issue with MRTG is that it makes all the graphs again every time it updates.
- With a large number graphing of interfaces on a large number of routers results is a heavy CPU utilization every 5 minutes when graph get updates.
- Graphs are nice, but have very little flexibility and few customization options.

Installation And Configuration Of MRTG

MRTG can be an valuable tool for diagnosing network problems because its not only indicates the current status of the network but also lets you visually compare this with the history of network utilization, MRTG is based on Perl and C, and runs on Windows and UNIX . MRTG is successfully used at many sites around the network.

MRTG used SNMP to be enabled on the routers or other network hardware required for the traffic analysis. Using the variables, MRTG sends SNMP requests every five minutes and stores the responses in a specialized data format. This format allows MRTG to present the daily, weekly, monthly, and yearly graphs and its remain growing larger as it keep updating. It does this by summarizing the older data as necessary. The graphs themselves are created in Portable Network Graphics (PNG) format and can be included in Web pages or used in other applications.

MRTG is an extremely useful tool that captures traffic and displays it with graphical view. In its simplest configuration displays the bandwidth (data) in and out from any SNMP enabled network device. This includes, but is not limited to routers, and switches. With MRTG we can capture and graphing the following:

- Connection rate (in connections per second)
- Bandwidth in and out in bits or bytes per second
- Total number of concurrent sessions
- Bandwidth in and out of a particular VIP/virtual server or node/real server
- Any parameter that has an SNMP counter or gauge object/OID

MRTG Installation (Windows Version)

MRTG is a open source and it is available at http://www.mrtg.org/ for download. After downloading it can be unzipped at C:\mrtg-2.15.2 (default location) on the Windows machine. Perl a scripting language is required for the MRTG to work, it can be downloaded from the following site for the installation.

http://www.activestate.com/Products/Download/Download.plex?id=ActivePerl

After installation on the Windows system, Perl binary directory should be listed in the system path i.e C:\Perl\bin;%SystemRoot%\system32;%SystemRoot%;. If it is missing in the system path then we have to enter it manually in the Windows using the following option.

[Control Panel]->[System]->[Environment]

To verify the installation we can run perl mrtg from the command prompt from the dos path *c:\mrtg\bin*. If we get the error message asking about the missing MRTG configuration file meaning we have successfully installed MRTG and Perl.

Enable SNMP

SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. It consists of a set of standards for network management, including an Application Layer protocol, a database schema, and a set of data objects. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried by managing application.

The majority of operating systems do not have the SNMP support enabled by default. The SNMP software has to be installed or enabled in order to get the SNMP OID data collection working. The SNMP support offers the SNMP client, which listens for SNMP requests coming from a NMS (network management station) and delivers the requested SNMP values.

Before creating a configuration file for MRTG we should know the following information:

- The IP address or hostname and the SNMP port number of the device need to be monitored.
- To monitor something other than data in and out, the SNMP OID should be used for that particular service.
- The read-only SNMP community string for the device. In our case it is **public** that is the default.

We have enabled SNMP on the routers IOS used in the network which we have setup in the MINT lab for the project with Community string **public**.

Cisco IOS commands for the SNMP configuration:

(config)#snmp-server community <name> <access-type>
(config)#snmp-server enable traps [notification-type]

MRTG Configuration

Creating MRTG Config File (mrtg.cfg)
MRTG CFG file is required for each monitoring host (or device) the first thing we have to do is creating a default config file. A .cfg file contains the SNMP OIDs for each entity that intend to monitor from the destination host. MRTG parses the associated .cfg file and collects the SMNP values for all OIDs defined in the .cfg file. For creation of .cfg file a "cfgmaker" script which resides in the \mrtg\bin\ directory will run with the host IP address and community string **public**. This script scans a host for the network-interfaces only and constructs the .cfg file.

On dos command prompt change the path to the *c:\mrtg-2.15.2\bin* directory. Type the following command: perl cfgmaker public@ interface IP address --global "WorkDir: c:\www\mrtg" --output mrtg.cfg.

This makes an initial MRTG config file called mrtg.cfg each time we run the above command it will create new mrtg.cfg file in mrtg\bin directory which overwrites any exiting mrtg.cfg file if exists in mrtg\bin directory. In mrtg.cfg file all interfaces of the router will be captured and stored by number. These numbers are likely to change whenever we reconfigure router. In order to avoid this we can get *cfgmaker* to produce a configuration which is based on IP numbers, or even Interface Descriptions.

Sample MRTG.CFG File

TargetDevice's IP Address:Interface Number:Community:IP Address

Target[IP address]: 1:public@ IP address
This is the interface speed (Default is 10 megabits; for 100Mbit devices use 12500000 and so on...)
MaxBytes[IP address]: 1250000
Title[IP address]: LC-Bridge (sample.device): ether0

Web page headers

PageTop [IP address]: <H1>Traffic Analysis for ether0</H1>

<TABLE>
<TR><TD>System:</TD><TD>LC-Bridge inAndover</TD></TR>
<TR><TD>Maintainer:</TD><TD>Administrator</TD></TR>
<TR><TD>Interface:</TD><TD>ether0(1)</TD></TR>
<TR><TD>IP:</TD><TD>sample.device(IP address)</TD></TR>
<TR><TD>Max Speed:</TD>
<TD>1250.0 kBytes/s (ethernetCsmacd)</TD></TR>
</TABLE>

Target[IP address.2]: 2:public@ IP address.1
MaxBytes[IP address.2]: 1250000
Title[IP address.2]: LC-Bridge (): ulink0
PageTop[IP address.2]: <H1>Traffic Analysis for ulink0</H1>
<TABLE>
<TR><TD>System:</TD><TD>LC-Bridge inAndover</TD></TR>
<TR><TD>Maintainer:</TD><TD>Administrator</TD></TR>
<TR><TD>Interface:</TD><TD>ulink0(2)</TD></TR>
<TR><TD>IP:</TD><TD>()</TD></TR>
<TR><TD>Max Speed:</TD>
<TD>1250.0 kBytes/s (ethernetCsmacd)</TD></TR>
</TABLE>

Generate Graphs

To start MRTG and generate graphs to monitor traffic we have to run the following command on command prompt by changing path to the directory *c:\mrtg-2.15.2\bin*:
perl mrtg mrtg.cfg

It is normal to get errors for the first two times when we run above command. The errors will alert about the fact that there are no any log files exists before. To update the MRTG graphs we have to run perl mrtg mrtg.cfg every five minutes manually. We will see the first lines in the graphs.

Automate the process

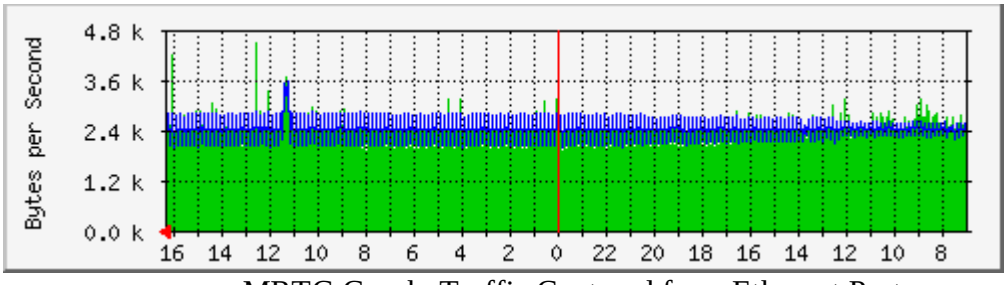
Starting MRTG by hand every time you want to update, there is a special option you can set in the MRTG configuration file so that MRTG will not terminate after it was started. Instead it will wait for 5 minutes and then run again automatically. For that following option will require to add in the mrtg.cfg file.
RunAsDaemon: yes

Start the mrtg.cfg with: start /Dc:\mrtg-2.15.2\bin perl mrtg --logging=eventlog mrtg.cfg

If you use w**perl** instead of **perl**, no console window will show up. MRTG is now running in the background. If it runs into problems it will send error code to Event Log. To stop MRTG, open the Task Manager and terminate the **perl.exe** process. Following is the command used for logging mrtg.cfg errors.

Target: perl mrtg --logging=eventlog mrtg.cfg

It is also possible if we define into windows start-up folder the following line, MRTG will now start whenever you login into windows: Start in: c:\mrtg-2.15.2\bin



MRTG Graph: Traffic Captured from Ethernet Port

MRTG Config file (MRTG.CFG) Used In MINT Lab

Following is the example of basic MRTG configuration file to monitor bytes in and out it was created in MINT lab on cisco router 2600 ---utilization on ports 1, 2 and 3.

```
# Created by : Nabbasi
# cfgmaker public@10.1.32.3 --global "WorkDir: c:\mrtgdata" --output mrtg.cfg
### 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
######################################################################
# System: routerD
# Description: Cisco Internetwork Operating System Software
#         IOS (tm) C2600 Software (C2600-J1S3-M), Version 12.2(15)T7,  RELEASE SOFTWARE (fc2)
#         TAC Support: http://www.cisco.com/tac
#         Copyright (c) 1986-2003 by cisco Systems, Inc.
#         Compiled Sat 09-Aug-03 07:18 by ccai
# Contact: Parvez Ibrahim
# Location: MINT Lab
######################################################################
### Interface 1 >> Descr: 'FastEthernet0/0' | Name: 'Fa0/0' | Ip: '10.1.32.3' | Eth: '00-08-21-bf-4b-40' ###
Target[10.1.32.3_1]: 1:public@10.1.32.3:
SetEnv[10.1.32.3_1]: MRTG_INT_IP="10.1.32.3" MRTG_INT_DESCR="FastEthernet0/0"
MaxBytes[10.1.32.3_1]: 12500000
Title[10.1.32.3_1]: Traffic Analysis for 1 -- routerD
PageTop[10.1.32.3_1]: <h1>Traffic Analysis for 1 -- routerD</h1>
                        <div id="sysdetails">
                                <table>
                                        <tr>
                                                <td>System:</td>
                                                 <td>routerD in </td>
                                        </tr>
                                        <tr>
                                                 <td>Maintainer:</td>
                                                 <td></td>
                                        </tr>
                                        <tr>
                                                 <td>Description:</td>
                                                 <td>FastEthernet0/0  </td>
                                        </tr>
                                        <tr>
                                                 <td>ifType:</td>
```

```
                                        <td>ethernetCsmacd (6)</td>
                                </tr>
                                <tr>
                                        <td>ifName:</td>
                                        <td>Fa0/0</td>
                                </tr>
                                <tr>
                                        <td>Max Speed:</td>
                                        <td>12.5 MBytes/s</td>
                                </tr>
                                <tr>
                                        <td>Ip:</td>
                                        <td>10.1.32.3 ()</td>
                                </tr>
                        </table>
                </div>

### Interface 2 >> Descr: 'Serial0/0'  |  Name: 'Se0/0' | Ip: '10.1.31.3' | Eth: " ###
Target[10.1.32.3_2]: 2:public@10.1.32.3:
SetEnv[10.1.32.3_2]: MRTG_INT_IP="10.1.31.3" MRTG_INT_DESCR="Serial0/0"
MaxBytes[10.1.32.3_2]: 193000
Title[10.1.32.3_2]: Traffic Analysis for 2 -- routerD
PageTop[10.1.32.3_2]: <h1>Traffic Analysis for 2 -- routerD</h1>
                <div id="sysdetails">
                        <table>
                                <tr>
                                        <td>System:</td>
                                        <td>routerD in </td>
                                </tr>
                                <tr>
                                        <td>Maintainer:</td>
                                        <td></td>
                                </tr>
                                <tr>
                                        <td>Description:</td>
                                        <td>Serial0/0  </td>
                                </tr>
                                <tr>
                                        <td>ifType:</td>
                                        <td>propPointToPointSerial (22)</td>
                                </tr>
                                <tr>
                                        <td>ifName:</td>
                                        <td>Se0/0</td>
                                </tr>
                                <tr>
                                        <td>Max Speed:</td>
                                        <td>193.0 kBytes/s</td>
```

```
                                        </tr>
                                        <tr>
                                                <td>Ip:</td>
                                                <td>10.1.31.3 ()</td>
                                        </tr>
                                </table>
                        </div>

### Interface 3 >> Descr: 'Serial0/1' | Name: 'Se0/1' | Ip: '10.1.29.3' | Eth: " ###

Target[10.1.32.3_3]: 3:public@10.1.32.3:
SetEnv[10.1.32.3_3]: MRTG_INT_IP="10.1.29.3" MRTG_INT_DESCR="Serial0/1"
MaxBytes[10.1.32.3_3]: 193000
Title[10.1.32.3_3]: Traffic Analysis for 3 -- routerD
PageTop[10.1.32.3_3]: <h1>Traffic Analysis for 3 -- routerD</h1>
                        <div id="sysdetails">
                                <table>
                                        <tr>
                                                <td>System:</td>
                                                <td>routerD in </td>
                                        </tr>
                                        <tr>
                                                <td>Maintainer:</td>
                                                <td></td>
                                        </tr>
                                        <tr>
                                                <td>Description:</td>
                                                <td>Serial0/1  </td>
                                        </tr>
                                        <tr>
                                                <td>ifType:</td>
                                                <td>propPointToPointSerial (22)</td>
                                        </tr>
                                        <tr>
                                                <td>ifName:</td>
                                                <td>Se0/1</td>
                                        </tr>
                                        <tr>
                                                <td>Max Speed:</td>
                                                <td>193.0 kBytes/s</td>
                                        </tr>
                                        <tr>
                                                <td>Ip:</td>
                                                <td>10.1.29.3 ()</td>
                                        </tr>
                                </table>
                        </div>
### Interface 4 >> Descr: 'Null0' | Name: 'Nu0' | Ip: " | Eth: " ###
```

```
### The following interface is commented out because:
### * it is a cisco Null0 interface
#
# Target[10.1.32.3_4]: 4:public@10.1.32.3:
# SetEnv[10.1.32.3_4]: MRTG_INT_IP="" MRTG_INT_DESCR="Null0"
# MaxBytes[10.1.32.3_4]: 536870911
# Title[10.1.32.3_4]: Traffic Analysis for 4 -- routerD
# PageTop[10.1.32.3_4]: <h1>Traffic Analysis for 4 -- routerD</h1>
#                         <div id="sysdetails">
#                                 <table>
#                                         <tr>
#                                                 <td>System:</td>
#                                                 <td>routerD in </td>
#                                         </tr>
#                                         <tr>
#                                                 <td>Maintainer:</td>
#                                                 <td></td>
#                                         </tr>
#                                         <tr>
#                                                 <td>Description:</td>
#                                                 <td>Null0  </td>
#                                         </tr>
#                                         <tr>
#                                                 <td>ifType:</td>
#                                                 <td>Other (1)</td>
#                                         </tr>
#                                         <tr>
#                                                 <td>ifName:</td>
#                                                 <td>Nu0</td>
#                                         </tr>
#                                         <tr>
#                                                 <td>Max Speed:</td>
#                                                 <td>536.9 MBytes/s</td>
#                                         </tr>
#                                 </table>
#                         </div>
### Interface 5 >> Descr: 'Foreign-Exchange-Station-1/0/0' | Name: 'Foreign Exchange Station 1/0/0' | Ip: '' | Eth: '' ###
### The following interface is commented out because:
### * it is a Voice controller
### * got 'Received SNMP response with error code
###       error status: noSuchName
###       index 1 (OID: 1.3.6.1.2.1.2.2.1.10.5)
###     SNMPv1_Session (remote host: "10.1.32.3" [10.1.32.3].161)
###                      community: "public"
###                     request ID: 826815120
###                    PDU bufsize: 8000 bytes
###                        timeout: 2s
###                        retries: 5
```

```
###                     backoff: 1)' from interface when trying to query
#
# Target[10.1.32.3_5]: 5:public@10.1.32.3:
# SetEnv[10.1.32.3_5]: MRTG_INT_IP="" MRTG_INT_DESCR="Foreign-Exchange-Station-1/0/0"
# MaxBytes[10.1.32.3_5]: 75000000
# Title[10.1.32.3_5]: Traffic Analysis for 5 -- routerD
# PageTop[10.1.32.3_5]: <h1>Traffic Analysis for 5 -- routerD</h1>
#                         <div id="sysdetails">
#                                 <table>
#                                         <tr>
#                                                 <td>System:</td>
#                                                 <td>routerD in </td>
#                                         </tr>
#                                         <tr>
#                                                 <td>Maintainer:</td>
#                                                 <td></td>
#                                         </tr>
#                                         <tr>
#                                                 <td>Description:</td>
#                                                 <td>Foreign-Exchange-Station-1/0/0  </td>
#                                         </tr>
#                                         <tr>
#                                                 <td>ifType:</td>
#                                                 <td>Voice Foreign eXchange Station (voiceFXS) (102)</td>
#                                         </tr>
#                                         <tr>
#                                                 <td>ifName:</td>
#                                                 <td>Foreign Exchange Station 1/0/0</td>
#                                         </tr>
#                                         <tr>
#                                                 <td>Max Speed:</td>
#                                                 <td>75.0 MBytes/s</td>
#                                         </tr>
#                                 </table>
#                         </div>
### Interface 6 >> Descr: 'Foreign-Exchange-Station-1/0/1' | Name: 'Foreign Exchange Station 1/0/1' | Ip: '' | Eth: '' ###
### The following interface is commented out because:
### * it is a Voice controller
### * got 'Received SNMP response with error code
###       error status: noSuchName
###       index 1 (OID: 1.3.6.1.2.1.2.2.1.10.6)
###     SNMPv1_Session (remote host: "10.1.32.3" [10.1.32.3].161)
###                      community: "public"
###                     request ID: 826815121
###                    PDU bufsize: 8000 bytes
###                        timeout: 2s
###                        retries: 5
###                        backoff: 1)' from interface when trying to query
```

```
#
# Target[10.1.32.3_6]: 6:public@10.1.32.3:
# SetEnv[10.1.32.3_6]: MRTG_INT_IP="" MRTG_INT_DESCR="Foreign-Exchange-Station-1/0/1"
# MaxBytes[10.1.32.3_6]: 75000000
# Title[10.1.32.3_6]: Traffic Analysis for 6 -- routerD
# PageTop[10.1.32.3_6]: <h1>Traffic Analysis for 6 -- routerD</h1>
#                       <div id="sysdetails">
#                               <table>
#                                       <tr>
#                                               <td>System:</td>
#                                               <td>routerD in </td>
#                                       </tr>
#                                       <tr>
#                                               <td>Maintainer:</td>
#                                               <td></td>
#                                       </tr>
#                                       <tr>
#                                               <td>Description:</td>
#                                               <td>Foreign-Exchange-Station-1/0/1  </td>
#                                       </tr>
#                                       <tr>
#                                               <td>ifType:</td>
#                                               <td>Voice Foreign eXchange Station (voiceFXS) (102)</td>
#                                       </tr>
#                                       <tr>
#                                               <td>ifName:</td>
#                                               <td>Foreign Exchange Station 1/0/1</td>
#                                       </tr>
#                                       <tr>
#                                               <td>Max Speed:</td>
#                                               <td>75.0 MBytes/s</td>
#                                       </tr>
#                               </table>
#                       </div>
### Interface 7 >> Descr: 'Loopback0' | Name: 'Lo0' | Ip: '10.230.250.0' | Eth: " ###
### The following interface is commented out because:
### * it is a Software Loopback interface
#
# Target[10.1.32.3_7]: 7:public@10.1.32.3:
# SetEnv[10.1.32.3_7]: MRTG_INT_IP="10.230.250.0" MRTG_INT_DESCR="Loopback0"
# MaxBytes[10.1.32.3_7]: 536870911
# Title[10.1.32.3_7]: Traffic Analysis for 7 -- routerD
# PageTop[10.1.32.3_7]: <h1>Traffic Analysis for 7 -- routerD</h1>
#                       <div id="sysdetails">
#                               <table>
#                                       <tr>
#                                               <td>System:</td>
#                                               <td>routerD in </td>
```

```
#                                       </tr>
#                                       <tr>
#                                               <td>Maintainer:</td>
#                                               <td></td>
#                                       </tr>
#                                       <tr>
#                                               <td>Description:</td>
#                                               <td>Loopback0  </td>
#                                       </tr>
#                                       <tr>
#                                               <td>ifType:</td>
#                                               <td>softwareLoopback (24)</td>
#                                       </tr>
#                                       <tr>
#                                               <td>ifName:</td>
#                                               <td>Lo0</td>
#                                       </tr>
#                                       <tr>
#                                               <td>Max Speed:</td>
#                                               <td>536.9 MBytes/s</td>
#                                       </tr>
#                                       <tr>
#                                               <td>Ip:</td>
#                                               <td>10.230.250.0 ()</td>
#                                       </tr>
#                                 </table>
#                       </div>
### Interface 11 >> Descr: 'Virtual-Access1' | Name: 'Vi1' | Ip: '' | Eth: '' ###
Target[10.1.32.3_11]: 11:public@10.1.32.3:
SetEnv[10.1.32.3_11]: MRTG_INT_IP="" MRTG_INT_DESCR="Virtual-Access1"
MaxBytes[10.1.32.3_11]: 12500000
Title[10.1.32.3_11]: Traffic Analysis for 11 -- routerD
PageTop[10.1.32.3_11]: <h1>Traffic Analysis for 11 -- routerD</h1>
                       <div id="sysdetails">
                               <table>
                                       <tr>
                                               <td>System:</td>
                                               <td>routerD in </td>
                                       </tr>
                                       <tr>
                                               <td>Maintainer:</td>
                                               <td></td>
                                       </tr>
                                       <tr>
                                               <td>Description:</td>
                                               <td>Virtual-Access1  </td>
                                       </tr>
                                       <tr>
```

```
                    <td>ifType:</td>
                    <td>ppp (23)</td>
                </tr>
                <tr>
                    <td>ifName:</td>
                    <td>Vi1</td>
                </tr>
                <tr>
                    <td>Max Speed:</td>
                    <td>12.5 MBytes/s</td>
                </tr>
            </table>
        </div>
```

Different OIDs Used In mrtg.cfg

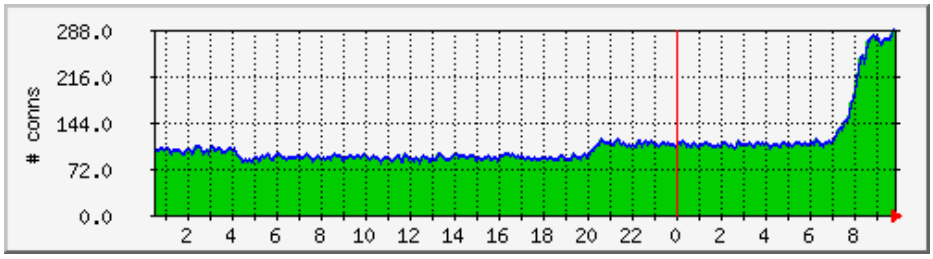
To monitor traffic for different packets including bytes in and out, we need to add different SNMP OIDs in mrtg.cfg file. In our project we have added OIDs in mrtg.cfg file for TCP and UDP packets also. To explicitly define which OID to query by using the following syntax 'OID_1&OID_2: community@router' The following example will retrieve TCP connection interface 1. MRTG needs to graph two variables, so two OID's need to be specified such as temperature and humidity or error input and error output.

Following is the part of script which is added to the mrtg.cfg for capturing traffic for TCP and UDP packets.

```
###The number of TCP connections for which the current state is either ESTABLISH.
Target[tcpopen]:.1.3.6.1.2.1.6.9.0&.1.3.6.1.2.1.6.9.0:public@192.168.0.2

Options[tcpopen]: nopercent,growright,gauge,noinfo
Title[tcpopen]: tcpCurrEstab
PageTop[tcpopen]: tcpCurrEstab
MaxBytes[tcpopen]: 1000000
YLegend[tcpopen]: # conns
ShortLegend[tcpopen]: connections
LegendI[tcpopen]:  Connections:
LegendO[tcpopen]:
Legend1[tcpopen]: tcpCurrEstab
```

#The total number of UDP datagrams delivered to UDP users.

Target[udp2]:.1.3.6.1.2.1.7.1.0&.1.3.6.1.2.1.7.1.0:public@192.168.0.2
Options[udp2]: nopercent,growright,gauge,noinfo
Title[udp2]: udpInDatagrams
PageTop[udp2]: udpInDatagrams
MaxBytes[udp2]: 1000000
YLegend[udp2]: # udp datagram
ShortLegend[udp2]: udp delivered
LegendI[udp2]: udp delivered:
LegendO[udp2]:
Legend1[udp2]: udpInDatagrams



TCP Connections

For MINT project we used following OIDs which include both TCP and UDP SNMP OIDs.

TCP OIDs

Name	OID
tcpRtoAlgorithm	.1.3.6.1.2.1.6.1
tcpRtoMin	.1.3.6.1.2.1.6.2
tcpRtoMax	.1.3.6.1.2.1.6.3
tcpMaxConn	.1.3.6.1.2.1.6.4
tcpActiveOpens	.1.3.6.1.2.1.6.5
tcpPassiveOpens	.1.3.6.1.2.1.6.6
tcpAttemptFails	.1.3.6.1.2.1.6.7
tcpEstabResets	.1.3.6.1.2.1.6.8
tcpCurrEstab	.1.3.6.1.2.1.6.9
tcpInSegs	.1.3.6.1.2.1.6.10
tcpOutSegs	.1.3.6.1.2.1.6.11
tcpRetransSegs	.1.3.6.1.2.1.6.12
tcpInErrs	.1.3.6.1.2.1.6.14
tcpOutRsts	.1.3.6.1.2.1.6.15
tcpHCInSegs	.1.3.6.1.2.1.6.17
tcpHCOutSegs	.1.3.6.1.2.1.6.18

UDP OIDs

Name	OID
udpInDatagrams	.1.3.6.1.2.1.7.1
udpNoPorts	.1.3.6.1.2.1.7.2
udpInErrors	.1.3.6.1.2.1.7.3
udpOutDatagrams	.1.3.6.1.2.1.7.4
udpHCInDatagrams	.1.3.6.1.2.1.7.8
udpHCOutDatagrams	1.3.6.1.2.1.7.9

For each OID referenced in the configuration file (mrtg.cfg), MRTG creates the following graphs:

Daily graph — 5 minute average, graph shows approximately 33 hours of data.

Weekly graph —30 minute average, graph shows approximately 8 days of data.

Monthly graph —2 hour average, graph shows approximately 5 weeks of data.

Yearly graph —1 day average, graph shows approximately 1 year of data.

Installation Steps (Review)

a. Installation of Perl
b. Installation of MRTG
c. Installation of WebServer
d. Setup configuration files (.cfg) for all monitored hosts which can be generated using cfgmaker command.
e.HTML index files for all hosts are generated and copied in the folders where the image/log/html files are.
f. Get the MRTG process running and visualize the variation graphs.

Round Robin Database (RRD) TOOL

RRDtool is an extension of MRTG's capabilities, MRTG can actually be configured to use RRDtool as its database backend and together with a CGI grapher, all your MRTG graphs can be generated on demand. Graphing with RRDtool is very flexible. Generated graphs can contain any and all information you could possibly imagine. The RRDtool graphs look similar to the MRTG graphs, except that the RRDtool graphs contain more information.

Benefit Of RRDTool and MRTG Integration

MRTG integrates with RRDTOOL which improves its performance and graphing flexibility. RRDtool is used as the logger to MRTG. It stores data samples on each of the network switch or router interfaces (ports) in a separate Round Robin Database. To minimize size of the database files, RRD uses the consolidation mechanism. It guarantees that the database does not grow over time and that old data is automatically eliminated.

RRDTool Installation And Configuration Steps

a. RRDTOOL is a open source and can be downloaded from
http://www.rrdtool.com/download and unzip it to the chosen RRD folder.

b. The package contains the binary files, the src\ folder contains four subfolders where some RRD tools are available in .exe format. Copy these files in the rrdtool\bin\ folder for an easier access. Include the rrdtool\bin in the system path of the MS Windows.

c. Register RRDTOOL package with the currently installed Perl distribution (at least Perl 5.6). Go to the "perl-shared" folder and run the following command:

ppm install rrds.ppd

RRDTOOL is now ready for use. Next step is to configure the MRTG instances to write SNMP data into the RRD databases.

Integration of MRTG with RRD database

When using mrtg with RRDtool will replacing *rateup* with the RRDtool perl module *RRDs.pm*.

The configuration steps are:

1. Build the MRTG .cfg file for the target host using the CFGMAKER

2. Make changes in the .cfg file with the following entries

- logformat: rrdtool // To enable RRDtool support in mrtg
- Workdir: folder name // rrdtool repository folder
- PathAdd: path to the rrdtool bin folder // For the location of the rrdtool executable
- LibAdd: path to the rrdtool perl-shared folder // For the location of the perl module

- RunAsDaemon: Yes // add this command in MRTG configuration file so that MRTG will not terminate after it was started.

After changes in the configuration file following effects take place when we run mrtg again.

1.mrtg will take all the old .log files and convert them to .rrd format. Mrtg will use **rrdtool** to update its databases. These will have a new format called *rrd* which is totally different than the native *log* format of the classic mrtg.

2.mrtg will **not** create any webpages of graphs anymore. It will only query the routers for traffic information and update its *rrd* databases.

The benefit of integration is that mrtg become much faster. Expect the runtime would drop to 20%. Logging process of RRDtool is very fast. The whole concept behind RRDTool MRTG integration is that it is more efficient to create graphs and WebPages on demand by using a cgi script.

Presently there is no official script available, but two contributors have created such scripts, 14all.cgi and routers2.cgi. The main difference between 14all.cgi and routers2.cgi is that the graphs created by routers2.cgi are much more detailed than in 14all.cgi

Configuration of Routers2.cgi Script

Step-by-step procedure applied successfully in different operating systems such as windows 2003, windows XP and windows Vista.

1. Prerequisite Software/Services.

In order to use routers2.cgi, we installed certain prerequisite software and service. These software/service are necessary to install before step no. 2.

a. Setup Web Server

For our project we have configured Internet Information Server on two machines all machines have different windows operating systems One was Windows Server 2003 and other WindowsXP.

Windows Server 2003 configuration:

- Enable IIS in add remove program
- Enable World Wide Web Service
- In computer management select Services and applications
- Then select Internet Information Service - web Sites- Default web site
- Right click on Default web site - properties then click on Home directory
- Then click on configuration.
- In Application configuration window we should change application mapping and add the following

  - assign drive:/path/perl.exe %s %s to .pl
  - assign drive:/path/perl.exe %s %s to .cgi
  - assign drive:/path/rrd_cgi.exe %s %s to .rrdcgi

- Start the Web Service - Web Site - right-click - Start.

- This sets PERL to execute locally whenever an app with those extensions is selected

- Modify web server so that the directory has execute permissions.

In internet browser give localhost (or local IP address) enter web server name it should display default page in the browser.

b. **ActivePerl**

ActivePerl can be downloaded from the http://www.activestate.com/ web site. It should be installed and configured and in running state.

c. **MRTG and RRDTool**

These packages are already downloaded from Tobi's sites at http://www.mrtg.org/ and http://www.rrdtool.org/ and configured in the system.

2. **Installing routers2.cgi**

In order to install router2.cgi we have to modify the '#!/usr/local/bin/perl' in the first line of the script to reflect the correct location for perl executables.

We have to install the RRDs perl libraries. While editing script we have to keep this in mind that the script is unix based so we have to check and modify all the syntax which are only used in Unix. For example windows uses backstrokes '\' as path separators, URLs use forward strokes '/'. So, when editing the routers2.conf file, we should use the correct syntax when defining URL paths and filename paths and we should make appropriate changes to directory paths, give permissions and install Perl with Windows version and made CGI-able.

Required Directories

Now we need to make directories where we put our files. For that we need the following directories.

CGI-BIN DIRECTORY: This is where the routers.cgi file goes, with read and execute permission. This directory should be visible to the web browser with exec-cgi flag set. ('Script' flag in IIS).

ICONS DIRECTORY: This is where all the .gif files are kept. This directory should be visible to your web browser. Make a note of the directory's URL. This should not be under the CGI-BIN directory, usually called /rrdicons or similar.

GRAPHS DIRECTORY: This is the work directory for the graphs. It needs to be writeable to the httpd UID, and otherwise empty. This directory also needs to be visible to web browser.

DATABASE DIRECTORY: Where the RRDTool .rrd databases are kept, this should already exist. It should not be under web server root.

MRTG CONF DIRECTORY: Where the MRTG .conf files are kept. This should already exist. It should not be under web server root.

3. **Configuration Of Perl Script**

This is now done via a separate configuration file. We should modify the script so that it knows where the conf file is and modify the path of the perl executable in the first line of the script. ($CONFFILE = "....")

The conf file should have at least 2 sections, [web] and [routers.cgi]. The first needs an entry 'backurl' to define where the 'Main Menu' button and follows by other options. The other section defines all the other options that used to be hardcoded into the script.

A fourth section, [targetnames] and A fifth section, [targettitles] are optional. A fourth section, [targetnames] which allows us to override the default short description for the routers and interfaces. A fifth section, [targettitles] allows you to give the 'long' description for each interface.

This configuration file should be kept in the inetpub\wwwroot - and then modify the script routers2.cgi so that it knows where to find this file. The line to modify is clearly indicated at the start of the script.

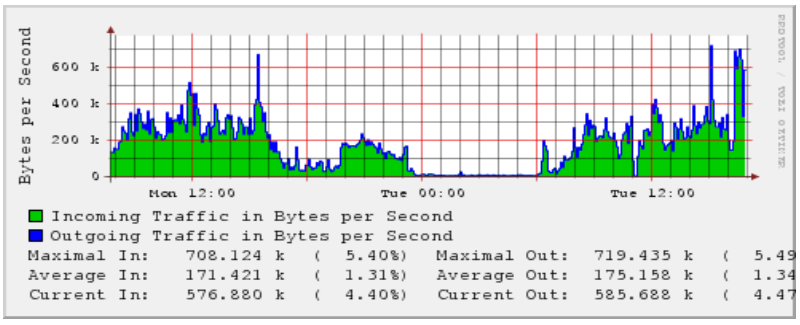
Copying the Files

Copy the routers2.cgi file to the c:\inetpub\wwwroot directory, give permission read and execute. If it is called routers2.cgi.pl in the package then rename it to routers2.cgi.

Copy the *.gif files to the ICONS directory.

4. **Testing the Web Interface**

For testing enter http://localhost/routers2.cgi in the web browser. This will open menu page with the graph of first target. Since the data has not yet been collected, the graph will probably be all grey at the moment. If you receive an error message about 'rrd file not found' then you probably have not yet run MRTG successfully to create the rrd database. The problem is, file has a lot of extra help to track down any problems you have at this stage.



MRTG Graph: After Integration of RRDTool and CGI Script.

Configuration of 14all.cgi Script (Optional)

14all.cgi is a CGI script to create html pages and graphics for mrtg. 14all.cgi parses the mrtg.cfg config file and used most of its information to create.

- **main index page**: one link for every "Directory[...]: adir"
- **group index pages**: one for every "Directory..." with small versions of the daily graphics
- **statistic pages**: one for every target with daily/weekly/monthly/yearly graphics according to "Suppress[...]: ..."

Installation and Configuration

We can install `14all.cgi` in a directory where the web server allows execution of cgi scripts. It has to be readable and executable by the user who runs web server. Check the first line of the cgi script, it has to contain the full path to the perl interpreter. It should look like this:

#C:\Perl\bin\perl

Including Library Path

14all.cgi script needs the file MRTG_lib.pm which is part of mrtg and present in mrtg\lib\mrtg2 directory. We have to edit the script and modify line 13 to add the path to this line of script file, it should look like;

use lib qw (C:\mrtg\lib\mrtg2);

We have to define mrtg config file name into the script. There is a section where the perl variable *$cfgfile* is set. Change the appropriate line. The path should be absolute.

$cfgfile = 'C:\mrtg\bin\mrtg.cfg';

Running MRTG instances with RRD database support

The MRTG instances with RRD database support can be run in the same manner as we mentioned above for example.

Run from the command prompt the following command:

start /Dc:\mrtg\bin perl mrtg --logging=eventlog mrtg.cfg

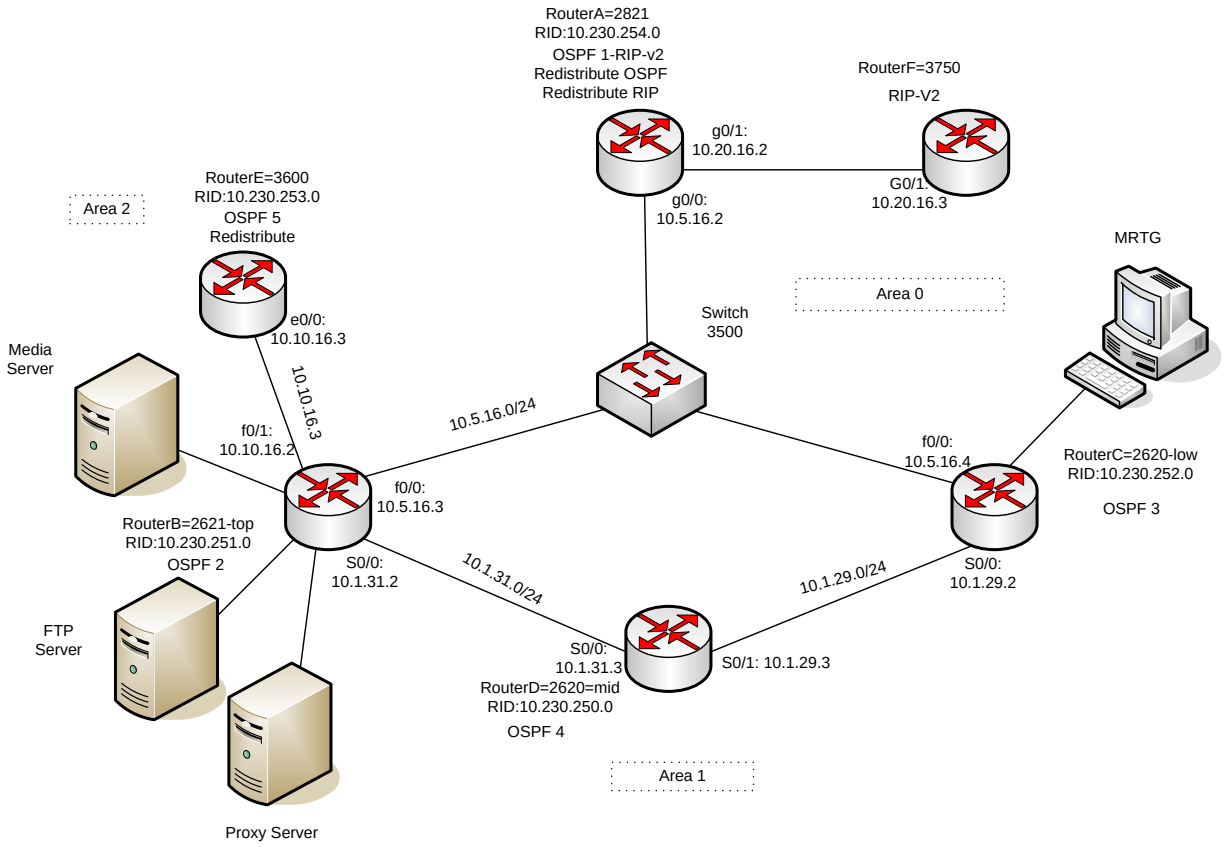
with addition of "RunAsDaemon: Yes" in mrtg.cfg config file.

MRTG will read the SNMP data at the specified interval and will add the values to the database and update the specified graphs.

Implementation OF MRTG

MRTG has been implemented in two phases, in first phase MINT lab and in second phase live environment of NorQuest College's network.

MINT LAB



The above fig showing network established in MINT lab for the project. IP addresses are assigned to each router ports, as shown three areas are created and DR and BDR are assigned.

Network Setup In MINT Lab

In MINT lab, we have setup a network of six routers and one switch. The routing protocol configured on this network is OSPF. Network has been configured into three areas that is area 0, 1 & 2. The reason of configuring network into three areas is to make it more efficient, routers within an area maintains a database for the area to which it belongs. The routers within a area doesn't have detailed information about network topology outside of its area, that is why the size of its database is not large.

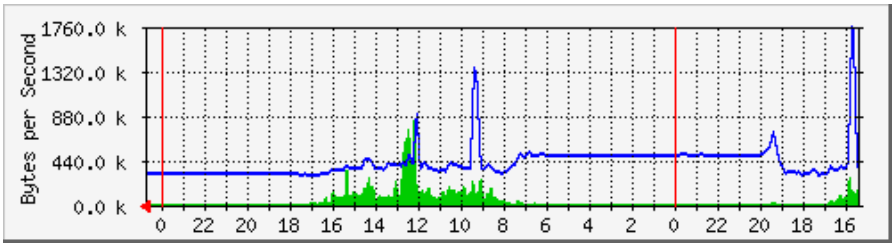
In the network, router B elected as DR (designated router) by setting its priority to 3 and router C as BDR (backup designated router). In that network we have also connected one switch. Router A, router B and routers C are directly connected to the switch. Router D is directly connected to router B and router C. Router E is connected to router B and router F is connected to router A. Router A and router E have been setup as AS (asynchronous system) in this network.

To generate more traffic flow and different type of packets on the network, we have setup the following three servers (MS Windows2003 based) and connected to the network.

- FTP Server
- Media Server
- Internet Server (Proxy)

Above servers have been connected to router B via switch and a PC with MRTG setup has been connected to router C. In order to generate traffic load and monitor from MRTG , services of all three servers have been accessed through the MINT lab's workstations.

MINT Lab: Traffic Analysis from Port2 -Router C



	Max	Average	Current
In	837.9 kB/s (0.6%)	57.6 kB/s (0.0%)	12.0 kB/s (0.0%)
Out	1750.6 kB/s (1.3%)	416.2 kB/s (0.3%)	302.2 kB/s (0.2%)

Enable SNMP on Routers

In order to capture traffic from router's interfaces, SNMP has been enabled on all routers, this is done with configuring community strings also, which act somewhat like passwords. Following are the commands ran at the routers.

snmp-server community public RO
snmp-server enable traps tty

Enable IP Multicasting on Routers/Switch

In order to stream video on routers and a switch, IP multicasting has been configured on routers B, router C, router D and router A, following commands have been used.

ip multicast-routing

ip pim sparse-dense-mode

ip pim rp-address IP address

In order to enable the switch to forward multicast packets it is necessary to set up the following command.

ip igmp snooping

Set Priority on Routers

Router priority has been set on router B and C, so that one of the router become DR and other can be BDR

- Router B is elected as DR - with highest priority.
- Router C is BDR - second highest priority.

Implementation Of MRTG In NorQuest College Network

The College currently is located in seven different sites, with four sites in the Edmonton area, those are Main campus, East court, Capital center and Westmount and the rest in major cities Stony plain, Wetaskiwin and Fort Saskatchewan.

Network Infrastructure At Main Campus

Supernet

Currently, the SuperNet is connecting the different remote sites of the College to Main Campus. When SuperNet is fully connected, only the Admin and Edu child domains will remain. SuperNet comes into all sites through the white Bell SuperNet box which then goes through a media converter from fiber to twisted-pairs. It is then connected to port 1 of the Axia Cisco Catalyst 3550. The port 2 of the Cisco Catalyst 3550 switch which is connected to the Fortigate FTG300A at Main Campus.

Fiber-Optic Link

The link between the Main campus and East court (Nursing training center) has been established through fiber-optic to provide high speed access to the resources at Main campus and also to provide the load balancing and security.

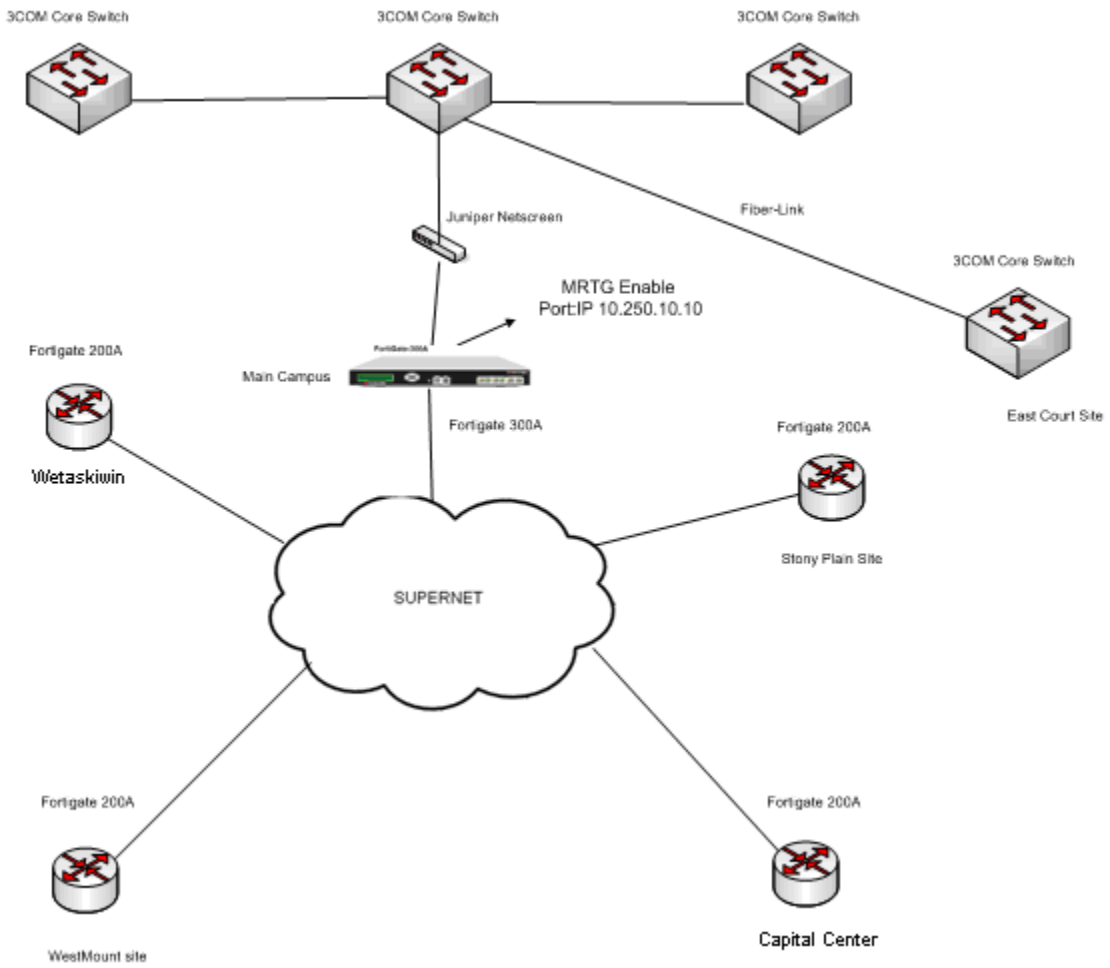
Fortigate FTG-300A (Router)

Fortigate, a routing and firewall device performing edge routing installed at each site of the College. At Main campus, due to the heavy traffic flow Fortigate FTG3600 is used for internet access and FTG300A is used for data, voice and video. At West mount and Stony plain sites Fortigate FTG300A, at Capital Center and Wetaskiwin sites Fortigate FTG200A have been used.

All the remote sites have been connected to Main campus by FTG300A, an ASIC-based layer 7 firewall that does antivirus, spam control, intrusion detect, and content filtering, FTG300A is linked to the internal network of the College through Juniper Netscreen device and 3COM core switch 3C-4050.

Fortigate FTG-300A

Norquest College Network



MRTG Implementation

MRTG Implementation

Due to the heavily used of Fortigate FTG300A at Main Campus, large amount of traffic flow has been observed on this device, type of traffic includes TCP, IP, UDP, ICMP etc. Therefore it has been decided that input ethernet port with IP address 10.250.10.10 of the FTG300A is a appropriate point for monitoring the flow of traffic, for that SNMP has also been enabled on FTG300A.

MRTG Webserver

A server machine Dell GSX260 has been setup with 250 GB hard disk, 512 MB Ram and one network interface card with Windows 2003 server operating system. Internet information server version 6.0 has also been installed on the operating system. Server has been linked to the switch and have given access to the core switch 3C4050 and Fortigate FTG-300A router.

Network Traffic At Main Campus.

Normally the traffic generates at the main campus network is due to the access of available resources and the services by internal and remote users. During the working hours thousands of internal users including staff members and students and remote users from other campuses including international students continuously accessing various types of resources/services on the network

Following is the example of resources/services available on the network.

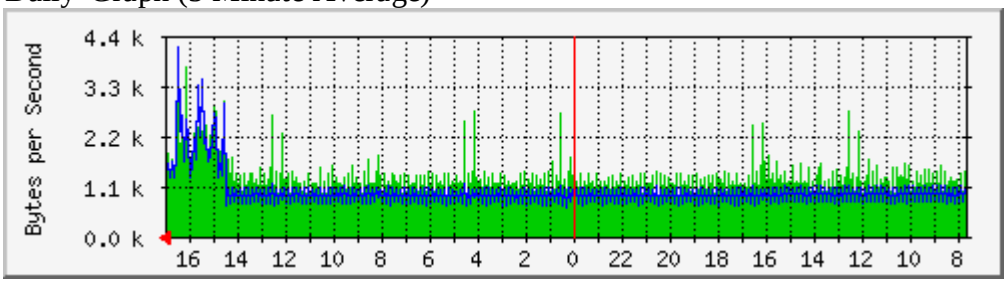
User authentication
File & print services
Internet
Email
Staff portal service
Library
Magic (ticket system)
VOIP
ERP
Databases
Educational applications
Ghost images
Terminal services

MRTG webserver continuously capturing traffic from those two ports with daily, weekly and monthly options. As a edge device Fortigate's output port received most of the traffic from remote sites during the working hours and after hours from remote users who working at home using VPN access.

Traffic Analysis at Fortigate FTG300A Port 1

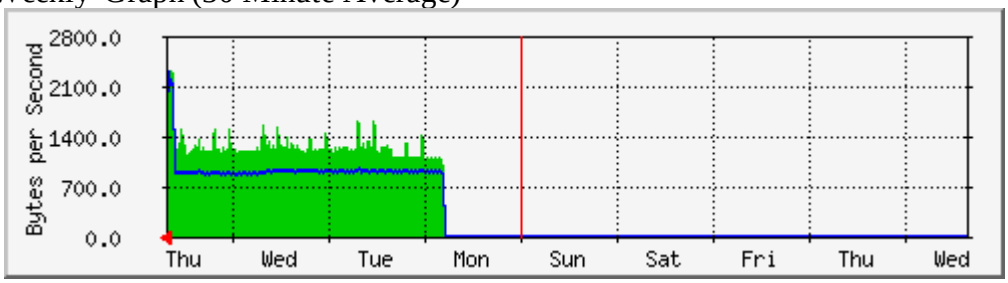
System: MC-FTG300A in
Description: port1
ifType: ethernetCsmacd (6)
Max Speed: 13.1 MBytes/s
Ip: 10.250.10.10 ()

`Daily' Graph (5 Minute Average)



	Max	Average	Current
In	3711.0 B/s (0.0%)	1339.0 B/s (0.0%)	1616.0 B/s (0.0%)
Out	4136.0 B/s (0.0%)	971.0 B/s (0.0%)	1282.0 B/s (0.0%)

`Weekly' Graph (30 Minute Average)



	Max	Average	Current
In	2677.0 B/s (0.0%)	1274.0 B/s (0.0%)	2678.0 B/s (0.0%)
Out	2554.0 B/s (0.0%)	930.0 B/s (0.0%)	2555.0 B/s (0.0%)

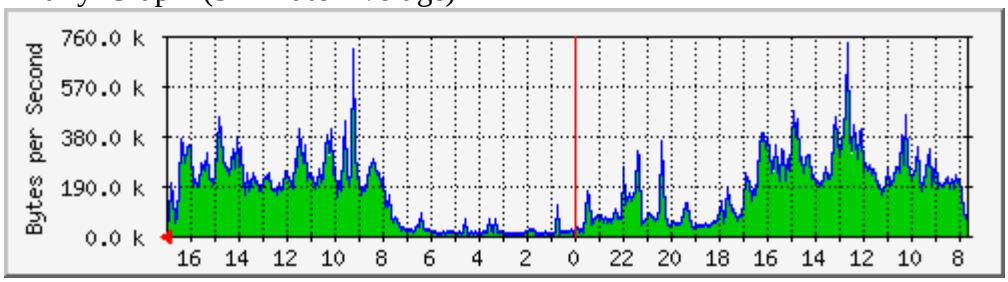
Graph Characteristic

Port1 of the Fortigate FTG 300A router is connected to the 3Com Core switch used to communicate network management data between the main campus and the remote sites used to manage the whole network from a single site (Main campus), minimal traffic transfers on this link, used continuously for monitoring purposes.
Graph shows that requests (data-out) from the Netmon station at main campus sent out to remote devices and responses (data-in) has received, the difference between the variation of both lines (blue/green) can be noticed and this is due to the amount of information received from internal network devices.

Traffic Analysis at Fortigate FTG300A- Port 3

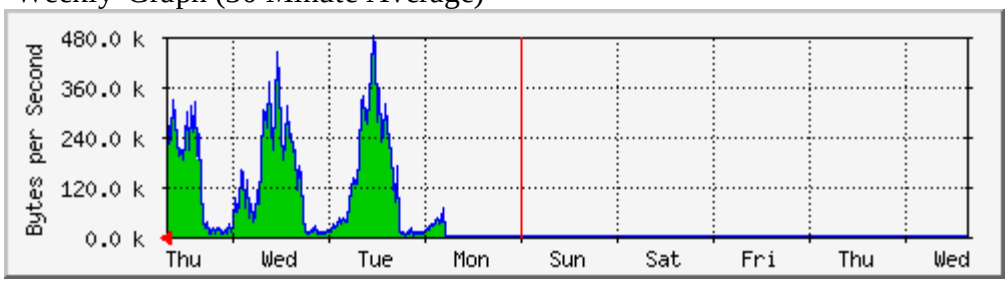
System: MC-FTG300A in
Description: port3
ifType: Ethernet Csmacd (6)
Max Speed: 13.1 MBytes/s

`Daily' Graph (5 Minute Average)



	Max	Average	Current
In	709.9 kB/s (5.4%)	156.5 kB/s (1.2%)	31.2 kB/s (0.2%)
Out	724.9 kB/s (5.5%)	161.0 kB/s (1.2%)	32.5 kB/s (0.2%)

`Weekly' Graph (30 Minute Average)



	Max	Average	Current
In	464.6 kB/s (3.5%)	125.4 kB/s (1.0%)	294.6 kB/s (2.2%)
Out	477.8 kB/s (3.6%)	128.9 kB/s (1.0%)	300.8 kB/s (2.3%)

Graph Characteristic

Port3 of the Fortigate FTG 300A router is connected to the 3Com core switch, used for internet access through Government of Alberta (GoA) resource via SuperNet. College's web and internet (Proxy) servers are linked with Fortigate's port3. Just like any internet connection more data coming in, and the requests going out are also in large number because hundreds of users (staff/students) accessing internet at the campus. The in and out data display in the graph shows the statistics of the traffic and can be categorized in three time intervals as follows.

Day time 7:30am – 5:00pm (working Hours)

As we can see in the daily graph high data coming in, during this time interval when max number of users locally and remotely accessing this link.

After Hours (5:00pm – 12:00am)

During this time interval flow of traffic decreasing but still exists, this shows that after hours less users continuing accessing the link locally and remotely.

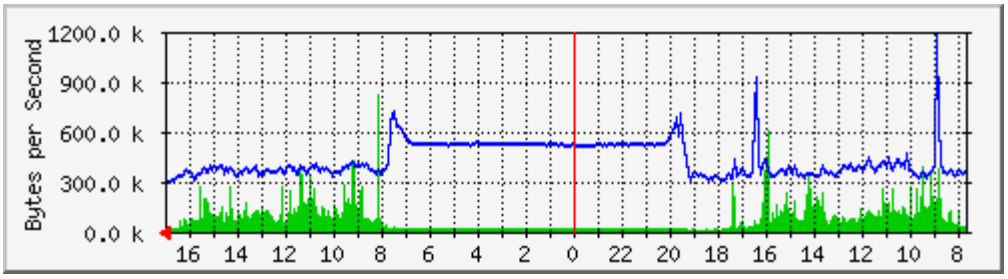
Midnight (12:am – 6:00am)

During this time period very low traffic flows across the network which is close to zero bytes per second, during this time period no user accessing the network locally except few remote users.

Traffic Analysis at Fortigate FTG300A- Port 6

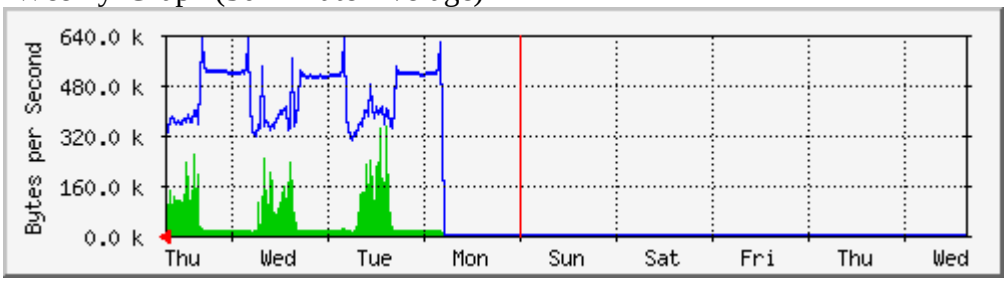
System: MC-FTG300A in
ifName: ethernetCsmacd (6)
Ip: 10.214.10.1 ()
Max Speed: 13.1 MBytes/s

`Daily' Graph (5 Minute Average)



	Max	Average	Current
In	825.3 kB/s (0.6%)	81.4 kB/s (0.1%)	19.9 kB/s (0.0%)
Out	1182.7 kB/s (0.9%)	427.2 kB/s (0.3%)	292.4 kB/s (0.2%)

`Weekly' Graph (30 Minute Average)



	Max	Average	Current
In	346.3 kB/s (0.3%)	68.4 kB/s (0.1%)	50.1 kB/s (0.0%)
Out	630.5 kB/s (0.5%)	446.7 kB/s (0.3%)	343.0 kB/s (0.3%)

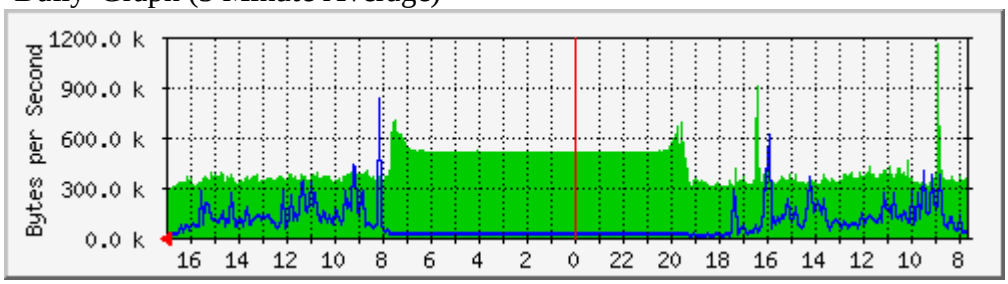
Graph Characteristic

Port6 of the Fortigate FTG 300A router is connected to the 3Com core switch, used for data, video and voice. Video streaming is used from security cameras from one of the remote site to main campus. Data include emails, applications, internet, files and print access. Remote users accessing network by using VPN and terminals services. Domain controllers replicates each other at regular time interval. Weekly graph shows almost same activity every day and high data out due to the financial application access by the remote users.

Traffic Analysis at Fortigate FTG300A- Port 4

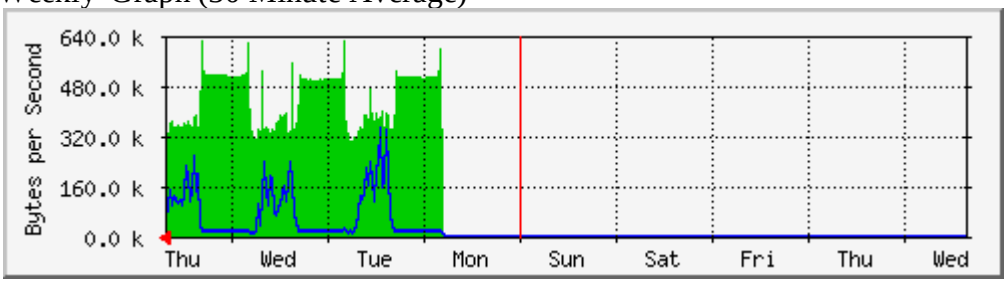
System: MC-FTG300A in
Description: port4
ifType: ethernetCsmacd (6)
Max Speed: 13.1 MBytes/s

'Daily' Graph (5 Minute Average)



	Max	Average	Current
In	1160.6 kB/s (8.9%)	420.7 kB/s (3.2%)	289.6 kB/s (2.2%)
Out	821.8 kB/s (6.3%)	79.4 kB/s (0.6%)	19.6 kB/s (0.1%)

`Weekly' Graph (30 Minute Average)



	Max	Average	Current
In	623.2 kB/s (4.8%)	440.3 kB/s (3.4%)	339.2 kB/s (2.6%)
Out	342.1 kB/s (2.6%)	66.0 kB/s (0.5%)	50.3 kB/s (0.4%)

Graph Characteristic

Port4 of the Fortigate FTG 300A router is connected to the Supernet through Cisco catalyst switch 3550. All the data including admin and edu, internet, management voice and video are coming in and out by this port to the outside (supernet), therefore high data flow can be observed on this port. In graph, data-out during midnight is close to zero as during that time no network activity normally happens in the main campus, but data-in is high due to the remote user access and video streaming from one remote site to the main campus.

Internal Network Of NorQuest Main Campus

Most of the networking devices are layer 2 and layer 3 switches and there are about 75 to 100 switches installed on the network. Servers and services are duplicated for redundancy purpose.

The network is heavily subnetted on the admin & Edu (domains) network as a result of using VLAN to provide smaller broadcast domains and having 2 NICs or 2 or more IP addresses on most servers. VLANs have been assigned on a functional basis across different floors e.g. Admin VLAN, Edu VLAN. This would provide traffic isolation and enhance security.

Core Network

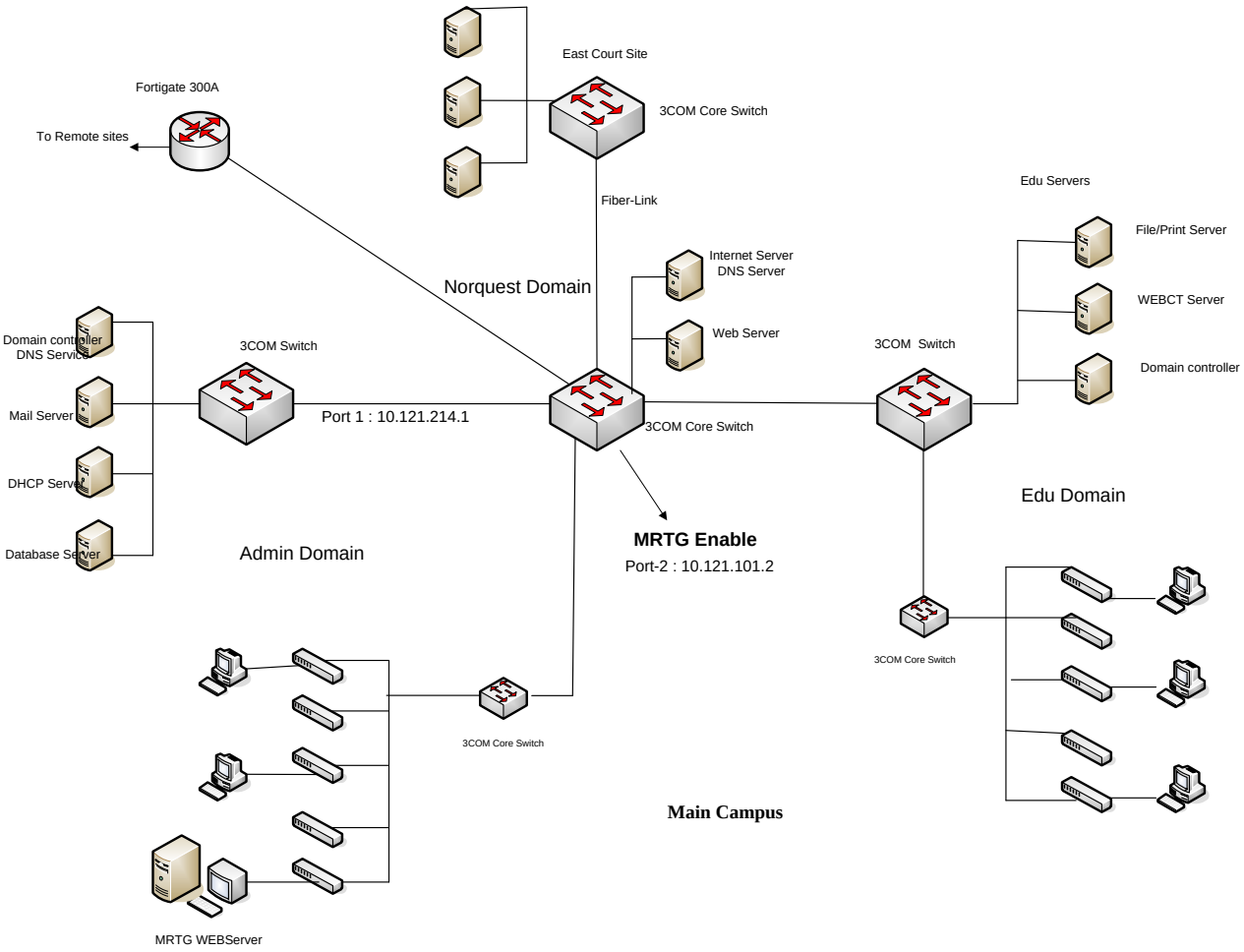
There are three core switches installed, one is 3COM 3C4050 and other two are 3C4924 installed at the backbone of the college's network at Main campus catering all the traffic flow from the ADM and EDU servers including web servers, mail server, DNS servers and internet servers to the two riser core switches (3COM 3C4924 & 3C 5500) one serving Admin network and other Edu network, these riser core switches connects to the other 3Com switches placed at the each floor of the college, these switches then connects to all the user workstations.

Another point where heavy traffic flow across the network could be at the main core of the network (backbone) where all the servers including servers in DMZ are placed and used by internal users and also remote users as well.

The core switch in the middle among the three switches is a appropriate point to monitor. This core switch directly connected to the Fortigate 300A device and handles all the traffic from remote sites, this switch also directly connected to East court site through fiber optic link and handles traffic flow from the users/servers, this switch also connected to the core Admin riser switch and handles the traffic flow from the admin staff users. This core switch is also connected with two other core switches to handles the traffic flow from Edu servers, Edu users, Admin servers and Norquest servers in DMZ zone.

Ethernet port of the core switch with IP address 10.121.214.2 has been selected due to the possible heavy flow of data at this port to capture the traffic, SNMP has also been enabled on the switch**.**

NQC Internal Network

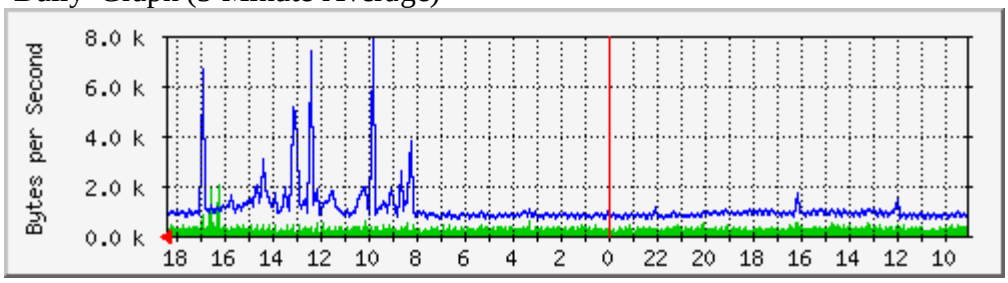


Main Campus

Traffic Analysis at 3COM-Core-Switch 3C4050 Port 2

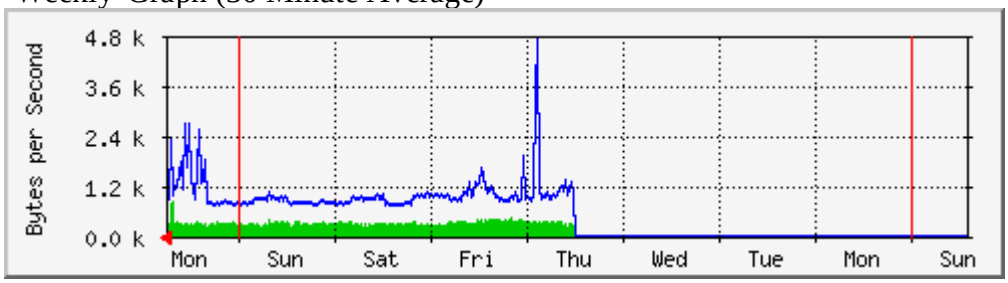
System: MC217A-EDU-SVR-XRN in MC-217A
Description: RMON-Port-02-on-unit-1
ifType: ethernetCsmacd (6)
Max Speed: 125.0 MBytes/s

`Daily' Graph (5 Minute Average)



	Max	Average	Current
In	2078.0 B/s (0.0%)	323.0 B/s (0.0%)	200.0 B/s (0.0%)
Out	7897.0 B/s (0.0%)	1036.0 B/s (0.0%)	751.0 B/s (0.0%)

`Weekly' Graph (30 Minute Average)



	Max	Average	Current
In	828.0 B/s (0.0%)	324.0 B/s (0.0%)	323.0 B/s (0.0%)
Out	4703.0 B/s (0.0%)	990.0 B/s (0.0%)	863.0 B/s (0.0%)

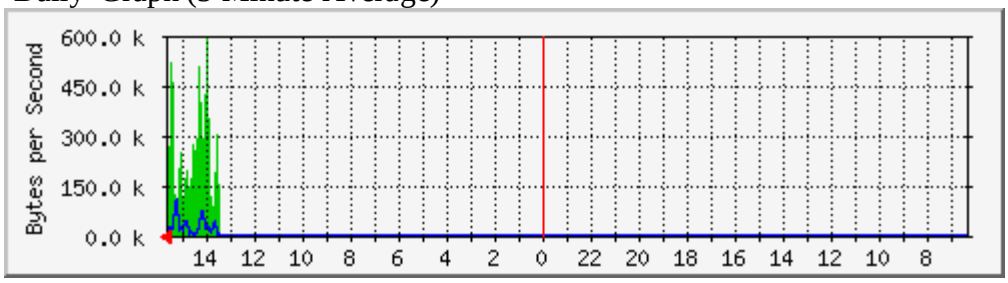
Graphs Characteristic

Port2 of the main 3COM core switch is connected to other core switch (EDU SVR) to which all Edu Servers in the Edu domain are connected. Core switch (EDU SVR) is also connected with another Edu RSR switch to which all baseline switches at each floor of the building are connected. Main core switch is also connected with Fortigate FTG 300A router device and ADM SVR core switch. Therefore it handles the network traffic from remote sites to Edu and Admin sub network and vice versa. Inconsistent variations in the graphs can be noticed due to the different services and servers (Edu & Admin) available on the network and used at different timings. Data-out (blue line) is higher then green due to the numbers of users (thousands of students) accessing network for the resources including educational applications in the Edu domain..

Traffic Analysis at 3COM-Core-Switch 3C4924 Port 1

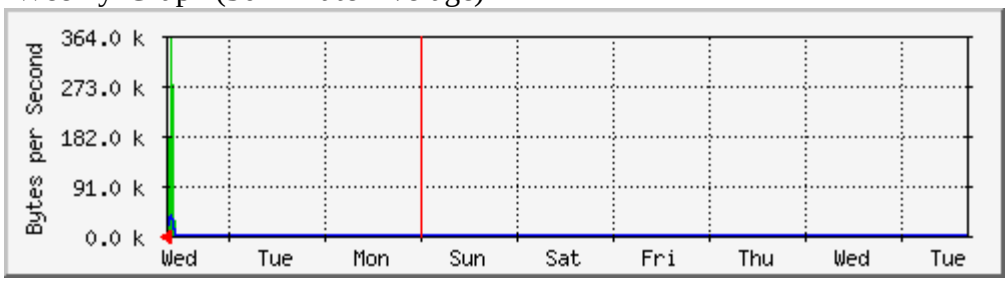
System: MC-ADM-SVR-XRN in MC-217A
Description: RMON-Port-01-on-unit-1
ifType: ethernetCsmacd (6)
Max Speed: 12.5 MBytes/s

`Daily' Graph (5 Minute Average)



	Max	Average	Current
In	596.3 kB/s (4.8%)	265.8 kB/s (2.1%)	202.6 kB/s (1.6%)
Out	106.2 kB/s (0.8%)	28.1 kB/s (0.2%)	12.4 kB/s (0.1%)

`Weekly' Graph (30 Minute Average)



	Max	Average	Current
In	360.8 kB/s (2.9%)	223.5 kB/s (1.8%)	276.8 kB/s (2.2%)
Out	46.8 kB/s (0.4%)	24.1 kB/s (0.2%)	46.8 kB/s (0.4%)

Graph Characteristic

Port1 of the ADM SVR 3COM core switch is connected to the main 3COM core switch and servers in Admin Domain. This core switch is also connected to ADM riser switch to which all baseline switches at each floor of the building are connected and serves the staff users in the admin domain. It handles the network traffic from admin domain to Edu domain and vice versa, also serves remote users through fortigate FTG-300A device upto the admin servers. Some restrictions have been implemented so that users (students) at Edu side can not access admin domain. Green line (data-in) is higher then blue (data-out) shows that users queries from Edu domain and remote sites are higher then the data retrieval.

Server Infrastructure

Currently there are about 400 to 500 staff or admin users and about 700 student users on the network, totaling to about 1,200 users.

Servers supporting the information include:

- Agresso (student, HR, finance)
- WebCT (distance learning)
- eLive (Virtual Classrooms)
- Can8 (Language learning)
- Voyager (Library website)
- Web server
- VOIP
- Exchange server (e-mail)
- File and Print servers
- Magic (help desk)
- Terminal Servers

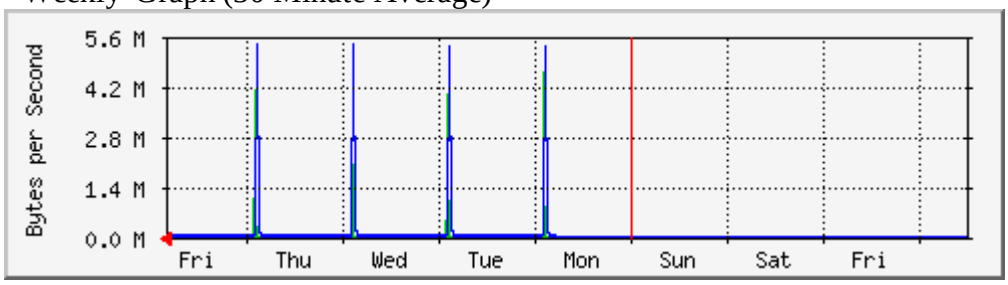
At Main Campus, currently there are three domains one Parent domain (Norquest.ca) and two child domains Admin and Edu. Admin serving staff members and Edu serving instructors and students as well. Each domain has two domain controllers for redundancy offering Directory services, DNS and DHCP services to local and remote users. Admin and Edu domains are all running Windows 2000 and 2003 server operating system .

Traffic Analysis At Domain Controller, File And Mail Servers

Traffic Analysis for 16777219 – Admin Domain Controller

Traffic Analysis for 65539 – DC11
System: DC11 in
ifType: ethernetCsmacd (6)
Max Speed: 12.5 MBytes/s
Ip: 10.214.240.3 (mail1.norquest.ca)

`Weekly' Graph (30 Minute Average)



	Max	Average	Current
In	4353.2 kB/s (3.5%)	65.9 kB/s (0.1%)	14.1 kB/s (0.0%)
Out	5454.5 kB/s (4.4%)	76.4 kB/s (0.1%)	15.9 kB/s (0.0%)

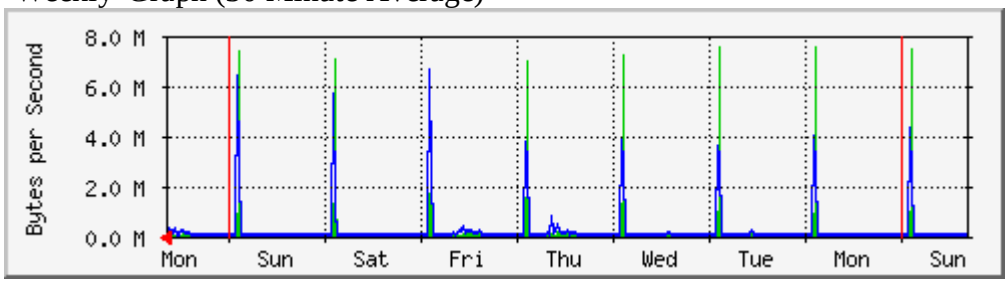
Graph Characteristic

DC11 is a college's domain controller based on Windows2000 server and installed at the Admin sub network to allow authentication to the admin (staff) users only. This server also run the login scripts upon successful user login. DC11 is also performing the role of DNS server for the local resources and also as forwarder for the external resources. Spikes in the graph produced at each day except the Saturday and Sunday shows that in the morning time when users login to the server from their workstations and their login scripts executes, this particular time server's Ethernet interface transfers high volume of packets, rest of the day no significant activity happens at the server results very low volume of traffic. On Saturday and Sunday limited users access the server produce low traffic which is close to zero.

Traffic Analysis for 65539 – File And Print server

System: FAP21 in
ifType: ethernetCsmacd (6)
Max Speed: 12.5 MBytes/s
Ip: 10.214.240.11 (mail1.norquest.ca)

`Weekly' Graph (30 Minute Average)



	Max	Average	Current
In	7580.5 kB/s (6.1%)	196.8 kB/s (0.2%)	207.5 kB/s (0.2%)
Out	6601.7 kB/s (5.3%)	171.0 kB/s (0.1%)	357.4 kB/s (0.3%)

Graph Characteristic

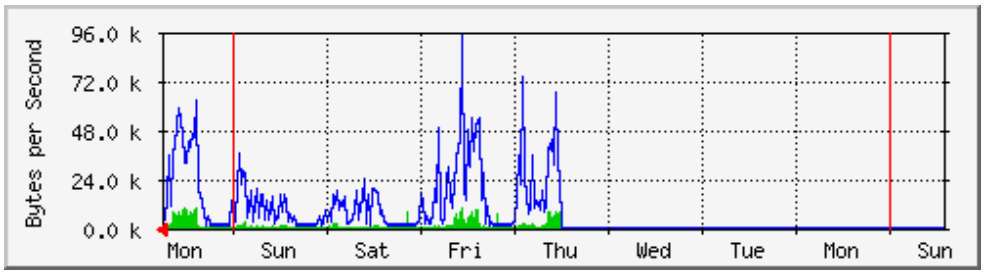
FAP21 is a college's File and Print Server based on Windows2003 server and installed at the EDU sub network give access to the sharable resources available on the server to the Edu (student & instructors) users only. Students home directory resides on this server which is mapped automatically after the login scripts executes.
This server is also performing as a print server allow sharable printing to different groups of students and instructors, also few applications such as success maker and Plato is also installed on this server for small group of students use.

Spikes in the graph produced at each day including Saturday and Sunday shows that in the morning time when students login to the server from their workstations and their login scripts executes which mapped the home directory, this particular time server's Ethernet interface transfers high volume of packets, rest of the day very low activity (file and print access) performed on the server. On Saturday and Sunday students and instructors still access the server locally and remotely.

Traffic Analysis for 16777220 – MAIL Server

MAIL01 in
ifType: ethernetCsmacd (6)
Max Speed: 12.5 MBytes/s
Ip: 10.214.240.11 (mail1.norquest.ca)

`Weekly' Graph (30 Minute Average)



	Max	Average	Current
In	9952.0 B/s (0.1%)	1786.0B/s(0.0%)	728.0 B/s (0.0%)
Out	93.2 kB/s (0.7%)	14.5 kB/s (0.1%)	5953.0B/s(0.0%)

Graph Characteristic

Mail01 is a college's Mail Server based on Windows2000 server running Microsoft Exchange2000 and installed at the Admin sub network give only access to the user's (staff) mail boxes.

High variation in the graph produced during each day including Saturday and Sunday shows that users continuously connects and access their mail boxes, meeting schedules and calendars, results server's Ethernet interface continuously transfers high volume of packets during the day. We can observe low activity in graph during the Saturday, Sunday (limited users access remotely) and no activity from midnight to early morning. Also we can notice the significant gap between blue and green lines that is because most of the users receiving the mails then sending.

Summary

We have selected MRTG a open source code for MINT 709 project. It's a good tool used to monitor network traffic on routers, switches and network interfaces configured with IP addresses and SNMP. MRTG graphing the captured traffic from different interfaces in a impressive way. It is also a good tool for the network experts to analyze, capacity plan, growth and troubleshoot the network problems.

By implementing the MRTG (Windows version) project first it has been downloaded from Tobi Oetiker's website and installed and configured on a MS Windows 2003 based machine. Set the working directories and paths in Windows Operating system to make sure application work without any error. Also installed and configured PERL on the same machine as required by MRTG.

Implemented MRTG in two phases , in first phase in MINT lab and in second phase in NorQuest College's network. First phase in MINT lab we setup a network of six routers and one switch and configured OSPF routing protocol on them, created three areas with DR and BDR routers.

Added three different servers FTP, Internet and Media to the network to generate high traffic flow. Connected MRTG workstation to the network and ran cfgmaker with router's IP address and community string Public to create mrtg.cfg config file and then ran perl mrtg mrtg.cfg at command prompt to capture traffic from ethernet interfaces, and graphs the captured traffic in html format which can be displayed in any internet browser.

In second phase MRTG has been implemented in Norquest College's network, In the network we have selected two areas to enable MRTG, one at Fortigate router device (connected between the Supernet and internal network) and other at 3COM core switch (connected to backbone of the network). Built the webserver and installed MRTG on it to capture the traffic from both the devices. In addition, network traffic on three different servers Domain controller, Mail and File/Print of the college has also been captured for analysis.

Enhancement has been made in MRTG to improve the graphs and its backend database by integrating Round Robin Database (RRD) Tool in to MRTG. Also in the same process enabled internet Information Server (IIS) service on the same machine and configured it with CGI scripts. This integration enabled MRTG to generate more flexible and detailed graphs and made the backend database efficient by minimizing its size and eliminating old data automatically.

Appendix

MRTG.CFG For Fortigate FTG-300A

IP address 10.250.10.10

```
# Created by
# cfgmaker public@10.250.10.10 --global "WorkDir: c:\inetpub\mrtg" --
output mrtg.cfg
RunAsDaemon: yes

### Global Config Options

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

#  or for NT
# WorkDir: c:\Inetpub\mrtg

### Global Defaults

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

EnableIPv6: no

######################################################################
# System: MC-FTG300A
# Description:
# Contact:
# Location:
######################################################################


### Interface 1 >> Descr: 'port1' | Name: 'port1' | Ip: '10.250.10.10'
| Eth: '00-09-0f-85-78-e1' ###

Target[10.250.10.10_1]: 1:public@10.250.10.10:
SetEnv[10.250.10.10_1]: MRTG_INT_IP="10.250.10.10"
MRTG_INT_DESCR="port1"
MaxBytes[10.250.10.10_1]: 13107200
Title[10.250.10.10_1]: Traffic Analysis for 1 -- MC-FTG300A
PageTop[10.250.10.10_1]: <h1>Traffic Analysis for 1 -- MC-FTG300A</h1>
            <div id="sysdetails">
                  <table>
                        <tr>
                              <td>System:</td>
                              <td>MC-FTG300A in </td>
                        </tr>
                        <tr>
                              <td>Maintainer:</td>
                              <td></td>
                        </tr>
```

```
                        <tr>
                              <td>Description:</td>
                              <td>port1  </td>
                        </tr>
                        <tr>
                              <td>ifType:</td>
                              <td>ethernetCsmacd (6)</td>
                        </tr>
                        <tr>
                              <td>ifName:</td>
                              <td>port1</td>
                        </tr>
                        <tr>
                              <td>Max Speed:</td>
                              <td>13.1 MBytes/s</td>
                        </tr>
                        <tr>
                              <td>Ip:</td>
                              <td>10.250.10.10 ()</td>
                        </tr>
                  </table>
            </div>


### Interface 2 >> Descr: 'port2' | Name: 'port2' | Ip:
'192.168.100.99' | Eth: '00-09-0f-85-78-e2' ###
### The following interface is commented out because:
### * it is operationally DOWN
### * has a speed of 0 which makes no sense
#
# Target[10.250.10.10_2]: 2:public@10.250.10.10:
# SetEnv[10.250.10.10_2]: MRTG_INT_IP="192.168.100.99"
MRTG_INT_DESCR="port2"
# MaxBytes[10.250.10.10_2]: 0
# Title[10.250.10.10_2]: Traffic Analysis for 2 -- MC-FTG300A
# PageTop[10.250.10.10_2]: <h1>Traffic Analysis for 2 -- MC-
FTG300A</h1>
#           <div id="sysdetails">
#                 <table>
#                       <tr>
#                             <td>System:</td>
#                             <td>MC-FTG300A in </td>
#                       </tr>
#                       <tr>
#                             <td>Maintainer:</td>
#                             <td></td>
#                       </tr>
#                       <tr>
#                             <td>Description:</td>
#                             <td>port2  </td>
#                       </tr>
#                       <tr>
#                             <td>ifType:</td>
#                             <td>ethernetCsmacd (6)</td>
#                       </tr>
#                       <tr>
#                             <td>ifName:</td>
#                             <td>port2</td>
#                       </tr>
```

```
#                       <tr>
#                             <td>Max Speed:</td>
#                             <td>0.0 Bytes/s</td>
#                       </tr>
#                       <tr>
#                             <td>Ip:</td>
#                             <td>192.168.100.99 ()</td>
#                       </tr>
#                 </table>
#           </div>


### Interface 3 >> Descr: 'port3' | Name: 'port3' | Ip: '' | Eth: ''
###

Target[10.250.10.10_3]: 3:public@10.250.10.10:
SetEnv[10.250.10.10_3]: MRTG_INT_IP="" MRTG_INT_DESCR="port3"
MaxBytes[10.250.10.10_3]: 13107200
Title[10.250.10.10_3]: Traffic Analysis for 3 -- MC-FTG300A
PageTop[10.250.10.10_3]: <h1>Traffic Analysis for 3 -- MC-FTG300A</h1>
            <div id="sysdetails">
                  <table>
                        <tr>
                              <td>System:</td>
                              <td>MC-FTG300A in </td>
                        </tr>
                        <tr>
                              <td>Maintainer:</td>
                              <td></td>
                        </tr>
                        <tr>
                              <td>Description:</td>
                              <td>port3  </td>
                        </tr>
                        <tr>
                              <td>ifType:</td>
                              <td>ethernetCsmacd (6)</td>
                        </tr>
                        <tr>
                              <td>ifName:</td>
                              <td>port3</td>
                        </tr>
                        <tr>
                              <td>Max Speed:</td>
                              <td>13.1 MBytes/s</td>
                        </tr>
                  </table>
            </div>


### Interface 4 >> Descr: 'port4' | Name: 'port4' | Ip: '10.10.10.2' |
Eth: '' ###

Target[10.250.10.10_4]: 4:public@10.250.10.10:
SetEnv[10.250.10.10_4]: MRTG_INT_IP="10.10.10.2" MRTG_INT_DESCR="port4"
MaxBytes[10.250.10.10_4]: 13107200
Title[10.250.10.10_4]: Traffic Analysis for 4 -- MC-FTG300A
PageTop[10.250.10.10_4]: <h1>Traffic Analysis for 4 -- MC-FTG300A</h1>
            <div id="sysdetails">
```

```
                  <table>
                        <tr>
                              <td>System:</td>
                              <td>MC-FTG300A in </td>
                        </tr>
                        <tr>
                              <td>Maintainer:</td>
                              <td></td>
                        </tr>
                        <tr>
                              <td>Description:</td>
                              <td>port4  </td>
                        </tr>
                        <tr>
                              <td>ifType:</td>
                              <td>ethernetCsmacd (6)</td>
                        </tr>
                        <tr>
                              <td>ifName:</td>
                              <td>port4</td>
                        </tr>
                        <tr>
                              <td>Max Speed:</td>
                              <td>13.1 MBytes/s</td>
                        </tr>
                        <tr>
                              <td>Ip:</td>
                              <td>10.10.10.2 ()</td>
                        </tr>
                  </table>
            </div>


### Interface 5 >> Descr: 'port5' | Name: 'port5' | Ip: '' | Eth: '00-
09-0f-85-78-e5' ###
### The following interface is commented out because:
### * it is operationally DOWN
### * has a speed of 0 which makes no sense
#
# Target[10.250.10.10_5]: 5:public@10.250.10.10:
# SetEnv[10.250.10.10_5]: MRTG_INT_IP="" MRTG_INT_DESCR="port5"
# MaxBytes[10.250.10.10_5]: 0
# Title[10.250.10.10_5]: Traffic Analysis for 5 -- MC-FTG300A
# PageTop[10.250.10.10_5]: <h1>Traffic Analysis for 5 -- MC-
FTG300A</h1>
#           <div id="sysdetails">
#                 <table>
#                       <tr>
#                             <td>System:</td>
#                             <td>MC-FTG300A in </td>
#                       </tr>
#                       <tr>
#                             <td>Maintainer:</td>
#                             <td></td>
#                       </tr>
#                       <tr>
#                             <td>Description:</td>
#                             <td>port5  </td>
#                       </tr>
```

```
#                       <tr>
#                             <td>ifType:</td>
#                             <td>ethernetCsmacd (6)</td>
#                       </tr>
#                       <tr>
#                             <td>ifName:</td>
#                             <td>port5</td>
#                       </tr>
#                       <tr>
#                             <td>Max Speed:</td>
#                             <td>0.0 Bytes/s</td>
#                       </tr>
#                 </table>
#           </div>


### Interface 6 >> Descr: 'port6' | Name: 'port6' | Ip: '10.214.10.1' |
Eth: '' ###

Target[10.250.10.10_6]: 6:public@10.250.10.10:
SetEnv[10.250.10.10_6]: MRTG_INT_IP="10.214.10.1"
MRTG_INT_DESCR="port6"
MaxBytes[10.250.10.10_6]: 131072000
Title[10.250.10.10_6]: Traffic Analysis for 6 -- MC-FTG300A
PageTop[10.250.10.10_6]: <h1>Traffic Analysis for 6 -- MC-FTG300A</h1>
            <div id="sysdetails">
                  <table>
                        <tr>
                              <td>System:</td>
                              <td>MC-FTG300A in </td>
                        </tr>
                        <tr>
                              <td>Maintainer:</td>
                              <td></td>
                        </tr>
                        <tr>
                              <td>Description:</td>
                              <td>port6  </td>
                        </tr>
                        <tr>
                              <td>ifType:</td>
                              <td>ethernetCsmacd (6)</td>
                        </tr>
                        <tr>
                              <td>ifName:</td>
                              <td>port6</td>
                        </tr>
                        <tr>
                              <td>Max Speed:</td>
                              <td>131.1 MBytes/s</td>
                        </tr>
                        <tr>
                              <td>Ip:</td>
                              <td>10.214.10.1 ()</td>
                        </tr>
                  </table>
            </div>
```

```
### Interface 7 >> Descr: 'E4-VL02' | Name: 'E4-VL02' | Ip:
'10.251.11.2' | Eth: '' ###
### The following interface is commented out because:
### * has a speed of 0 which makes no sense
#
# Target[10.250.10.10_7]: 7:public@10.250.10.10:
# SetEnv[10.250.10.10_7]: MRTG_INT_IP="10.251.11.2" MRTG_INT_DESCR="E4-
VL02"
# MaxBytes[10.250.10.10_7]: 0
# Title[10.250.10.10_7]: Traffic Analysis for 7 -- MC-FTG300A
# PageTop[10.250.10.10_7]: <h1>Traffic Analysis for 7 -- MC-
FTG300A</h1>
#           <div id="sysdetails">
#                 <table>
#                       <tr>
#                             <td>System:</td>
#                             <td>MC-FTG300A in </td>
#                       </tr>
#                       <tr>
#                             <td>Maintainer:</td>
#                             <td></td>
#                       </tr>
#                       <tr>
#                             <td>Description:</td>
#                             <td>E4-VL02  </td>
#                       </tr>
#                       <tr>
#                             <td>ifType:</td>
#                             <td>Layer 2 Virtual LAN using 802.1Q
(135)</td>
#                       </tr>
#                       <tr>
#                             <td>ifName:</td>
#                             <td>E4-VL02</td>
#                       </tr>
#                       <tr>
#                             <td>Max Speed:</td>
#                             <td>0.0 Bytes/s</td>
#                       </tr>
#                       <tr>
#                             <td>Ip:</td>
#                             <td>10.251.11.2 ()</td>
#                       </tr>
#                 </table>
#           </div>


### Interface 8 >> Descr: 'E4-VL10' | Name: 'E4-VL10' | Ip:
'10.200.11.2.1' | Eth: '' ###
### The following interface is commented out because:
### * has a speed of 0 which makes no sense
#
# Target[10.250.10.10_8]: 8:public@10.250.10.10:
# SetEnv[10.250.10.10_8]: MRTG_INT_IP="10.200.11.2.1"
MRTG_INT_DESCR="E4-VL10"
# MaxBytes[10.250.10.10_8]: 0
# Title[10.250.10.10_8]: Traffic Analysis for 8 -- MC-FTG300A
# PageTop[10.250.10.10_8]: <h1>Traffic Analysis for 8 -- MC-
FTG300A</h1>
```

```
#           <div id="sysdetails">
#                 <table>
#                       <tr>
#                             <td>System:</td>
#                             <td>MC-FTG300A in </td>
#                       </tr>
#                       <tr>
#                             <td>Maintainer:</td>
#                             <td></td>
#                       </tr>
#                       <tr>
#                             <td>Description:</td>
#                             <td>E4-VL10  </td>
#                       </tr>
#                       <tr>
#                             <td>ifType:</td>
#                             <td>Layer 2 Virtual LAN using 802.1Q
(135)</td>
#                       </tr>
#                       <tr>
#                             <td>ifName:</td>
#                             <td>E4-VL10</td>
#                       </tr>
#                       <tr>
#                             <td>Max Speed:</td>
#                             <td>0.0 Bytes/s</td>
#                       </tr>
#                       <tr>
#                             <td>Ip:</td>
#                             <td>10.200.11.2.1 ()</td>
#                       </tr>
#                 </table>
#           </div>


### Interface 9 >> Descr: 'E4-VL20' | Name: 'E4-VL20' | Ip:
'10.200.12.2.1' | Eth: '' ###
### The following interface is commented out because:
### * has a speed of 0 which makes no sense
#
# Target[10.250.10.10_9]: 9:public@10.250.10.10:
# SetEnv[10.250.10.10_9]: MRTG_INT_IP="10.200.12.2.1"
MRTG_INT_DESCR="E4-VL20"
# MaxBytes[10.250.10.10_9]: 0
# Title[10.250.10.10_9]: Traffic Analysis for 9 -- MC-FTG300A
# PageTop[10.250.10.10_9]: <h1>Traffic Analysis for 9 -- MC-
FTG300A</h1>
#           <div id="sysdetails">
#                 <table>
#                       <tr>
#                             <td>System:</td>
#                             <td>MC-FTG300A in </td>
#                       </tr>
#                       <tr>
#                             <td>Maintainer:</td>
#                             <td></td>
#                       </tr>
#                       <tr>
#                             <td>Description:</td>
```

```
#                               <td>E4-VL20  </td>
#                         </tr>
#                         <tr>
#                               <td>ifType:</td>
#                               <td>Layer 2 Virtual LAN using 802.1Q
(135)</td>
#                         </tr>
#                         <tr>
#                               <td>ifName:</td>
#                               <td>E4-VL20</td>
#                         </tr>
#                         <tr>
#                               <td>Max Speed:</td>
#                               <td>0.0 Bytes/s</td>
#                         </tr>
#                         <tr>
#                               <td>Ip:</td>
#                               <td>10.200.12.2.1 ()</td>
#                         </tr>
#                   </table>
#             </div>


### Interface 10 >> Descr: 'E4-VL72' | Name: 'E4-VL72' | Ip:
'10.172.11.2.2' | Eth: '' ###
### The following interface is commented out because:
### * has a speed of 0 which makes no sense
#
# Target[10.250.10.10_10]: 10:public@10.250.10.10:
# SetEnv[10.250.10.10_10]: MRTG_INT_IP="10.172.11.2.2"
MRTG_INT_DESCR="E4-VL72"
# MaxBytes[10.250.10.10_10]: 0
# Title[10.250.10.10_10]: Traffic Analysis for 10 -- MC-FTG300A
# PageTop[10.250.10.10_10]: <h1>Traffic Analysis for 10 -- MC-
FTG300A</h1>
#             <div id="sysdetails">
#                   <table>
#                         <tr>
#                               <td>System:</td>
#                               <td>MC-FTG300A in </td>
#                         </tr>
#                         <tr>
#                               <td>Maintainer:</td>
#                               <td></td>
#                         </tr>
#                         <tr>
#                               <td>Description:</td>
#                               <td>E4-VL72  </td>
#                         </tr>
#                         <tr>
#                               <td>ifType:</td>
#                               <td>Layer 2 Virtual LAN using 802.1Q
(135)</td>
#                         </tr>
#                         <tr>
#                               <td>ifName:</td>
#                               <td>E4-VL72</td>
#                         </tr>
#                         <tr>
```

```
#                               <td>Max Speed:</td>
#                               <td>0.0 Bytes/s</td>
#                         </tr>
#                         <tr>
#                               <td>Ip:</td>
#                               <td>10.172.11.2.2 ()</td>
#                         </tr>
#                   </table>
#             </div>


### Interface 11 >> Descr: 'E3-VL09' | Name: 'E3-VL09' | Ip:
'199.214.255.2.1' | Eth: '' ###
### The following interface is commented out because:
### * has a speed of 0 which makes no sense
#
# Target[10.250.10.10_11]: 11:public@10.250.10.10:
# SetEnv[10.250.10.10_11]: MRTG_INT_IP="199.214.255.2.1"
MRTG_INT_DESCR="E3-VL09"
# MaxBytes[10.250.10.10_11]: 0
# Title[10.250.10.10_11]: Traffic Analysis for 11 -- MC-FTG300A
# PageTop[10.250.10.10_11]: <h1>Traffic Analysis for 11 -- MC-
FTG300A</h1>
#             <div id="sysdetails">
#                   <table>
#                         <tr>
#                               <td>System:</td>
#                               <td>MC-FTG300A in </td>
#                         </tr>
#                         <tr>
#                               <td>Maintainer:</td>
#                               <td></td>
#                         </tr>
#                         <tr>
#                               <td>Description:</td>
#                               <td>E3-VL09  </td>
#                         </tr>
#                         <tr>
#                               <td>ifType:</td>
#                               <td>Layer 2 Virtual LAN using 802.1Q
(135)</td>
#                         </tr>
#                         <tr>
#                               <td>ifName:</td>
#                               <td>E3-VL09</td>
#                         </tr>
#                         <tr>
#                               <td>Max Speed:</td>
#                               <td>0.0 Bytes/s</td>
#                         </tr>
#                         <tr>
#                               <td>Ip:</td>
#                               <td>199.214.255.2.1 ()</td>
#                         </tr>
#                   </table>
#             </div>
```

```
### Interface 12 >> Descr: 'E6-VL1210' | Name: 'E6-VL1210' | Ip:
'10.121.10.1.1' | Eth: '' ###
### The following interface is commented out because:
### * has a speed of 0 which makes no sense
#
# Target[10.250.10.10_12]: 12:public@10.250.10.10:
# SetEnv[10.250.10.10_12]: MRTG_INT_IP="10.121.10.1.1"
MRTG_INT_DESCR="E6-VL1210"
# MaxBytes[10.250.10.10_12]: 0
# Title[10.250.10.10_12]: Traffic Analysis for 12 -- MC-FTG300A
# PageTop[10.250.10.10_12]: <h1>Traffic Analysis for 12 -- MC-
FTG300A</h1>
#           <div id="sysdetails">
#                 <table>
#                       <tr>
#                             <td>System:</td>
#                             <td>MC-FTG300A in </td>
#                       </tr>
#                       <tr>
#                             <td>Maintainer:</td>
#                             <td></td>
#                       </tr>
#                       <tr>
#                             <td>Description:</td>
#                             <td>E6-VL1210  </td>
#                       </tr>
#                       <tr>
#                             <td>ifType:</td>
#                             <td>Layer 2 Virtual LAN using 802.1Q
(135)</td>
#                       </tr>
#                       <tr>
#                             <td>ifName:</td>
#                             <td>E6-VL1210</td>
#                       </tr>
#                       <tr>
#                             <td>Max Speed:</td>
#                             <td>0.0 Bytes/s</td>
#                       </tr>
#                       <tr>
#                             <td>Ip:</td>
#                             <td>10.121.10.1.1 ()</td>
#                       </tr>
#                 </table>
#           </div>


### Interface 13 >> Descr: 'E3-VL1991' | Name: 'E3-VL1991' | Ip:
'199.214.241.1.1' | Eth: '' ###
### The following interface is commented out because:
### * has a speed of 0 which makes no sense
#
# Target[10.250.10.10_13]: 13:public@10.250.10.10:
# SetEnv[10.250.10.10_13]: MRTG_INT_IP="199.214.241.1.1"
MRTG_INT_DESCR="E3-VL1991"
# MaxBytes[10.250.10.10_13]: 0
# Title[10.250.10.10_13]: Traffic Analysis for 13 -- MC-FTG300A
# PageTop[10.250.10.10_13]: <h1>Traffic Analysis for 13 -- MC-
FTG300A</h1>
```

```
#           <div id="sysdetails">
#                 <table>
#                       <tr>
#                             <td>System:</td>
#                             <td>MC-FTG300A in </td>
#                       </tr>
#                       <tr>
#                             <td>Maintainer:</td>
#                             <td></td>
#                       </tr>
#                       <tr>
#                             <td>Description:</td>
#                             <td>E3-VL1991  </td>
#                       </tr>
#                       <tr>
#                             <td>ifType:</td>
#                             <td>Layer 2 Virtual LAN using 802.1Q
(135)</td>
#                       </tr>
#                       <tr>
#                             <td>ifName:</td>
#                             <td>E3-VL1991</td>
#                       </tr>
#                       <tr>
#                             <td>Max Speed:</td>
#                             <td>0.0 Bytes/s</td>
#                       </tr>
#                       <tr>
#                             <td>Ip:</td>
#                             <td>199.214.241.1.1 ()</td>
#                       </tr>
#                 </table>
#           </div>


### Interface 14 >> Descr: 'E6-VL1721' | Name: 'E6-VL1721' | Ip:
'10.172.10.1.2' | Eth: '' ###
### The following interface is commented out because:
### * has a speed of 0 which makes no sense
#
# Target[10.250.10.10_14]: 14:public@10.250.10.10:
# SetEnv[10.250.10.10_14]: MRTG_INT_IP="10.172.10.1.2"
MRTG_INT_DESCR="E6-VL1721"
# MaxBytes[10.250.10.10_14]: 0
# Title[10.250.10.10_14]: Traffic Analysis for 14 -- MC-FTG300A
# PageTop[10.250.10.10_14]: <h1>Traffic Analysis for 14 -- MC-
FTG300A</h1>
#           <div id="sysdetails">
#                 <table>
#                       <tr>
#                             <td>System:</td>
#                             <td>MC-FTG300A in </td>
#                       </tr>
#                       <tr>
#                             <td>Maintainer:</td>
#                             <td></td>
#                       </tr>
#                       <tr>
#                             <td>Description:</td>
```

```
#                               <td>E6-VL1721  </td>
#                         </tr>
#                         <tr>
#                               <td>ifType:</td>
#                               <td>Layer 2 Virtual LAN using 802.1Q
(135)</td>
#                         </tr>
#                         <tr>
#                               <td>ifName:</td>
#                               <td>E6-VL1721</td>
#                         </tr>
#                         <tr>
#                               <td>Max Speed:</td>
#                               <td>0.0 Bytes/s</td>
#                         </tr>
#                         <tr>
#                               <td>Ip:</td>
#                               <td>10.172.10.1.2 ()</td>
#                         </tr>
#                   </table>
#             </div>


WorkDir: c:\inetpub\mrtg
```

MRTG.CFG With Different OIDs (Sample)

```
#.................................................................

Target[tch1]: `perl c:\perl\lib\dualpri.pl public@127.1.1.1`
MaxBytes[tch1]: 46
Unscaled[tch1]:ymwd
Title[tch1]: Total Control Hub #1
PageTop[tch1]: <H1>TCH1 Modem Utilization </H1>
YLegend[tch1]:Modem Capacity
Options[tch1]:gauge,growright
ShortLegend[tch1]:Modems
Legend1[tch1]:  Utilization  
Legend2[tch1]:  Capacity  
Legend3[tch1]:  Connections  
Legend4[tch1]:  Capacity  
LegendI[tch1]:  Utilization  
LegendO[tch1]:  Capacity  

#.................................................................

Target[tch2]: `perl c:\perl\lib\dualt1.pl public@127.1.1.2`
MaxBytes[tch2]: 46
Title[tch2]: Total Control Hub #2
PageTop[tch2]: <H1>TCH2 Modem Utilization </H1>
YLegend[tch2]:Modem Capacity
Options[tch2]:gauge,growright
ShortLegend[tch2]:Modems
Legend1[tch2]:  Utilization  
```

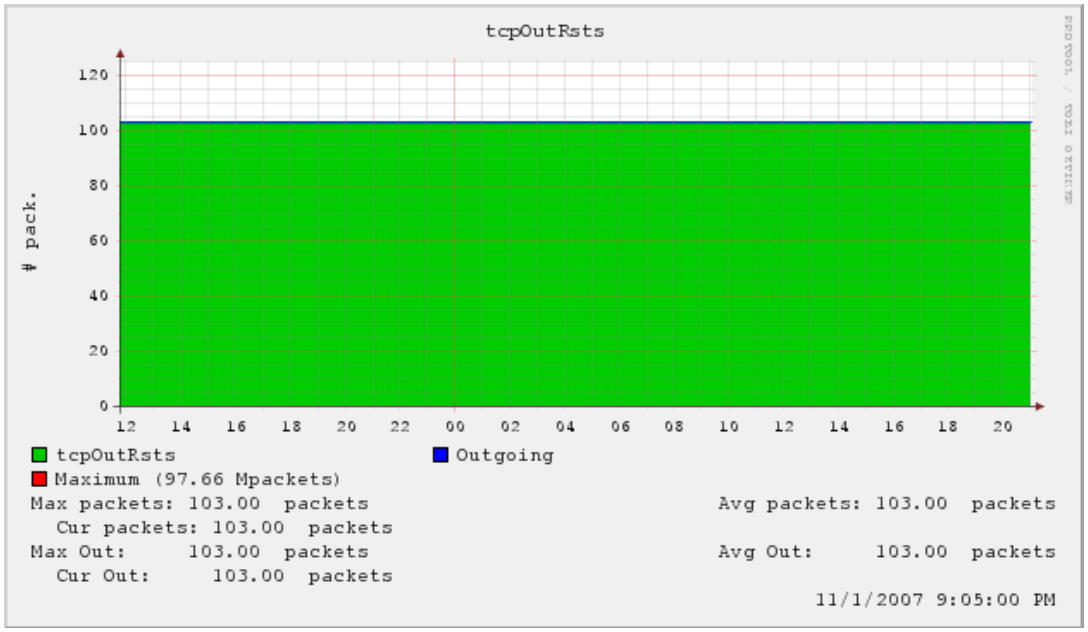
```
Legend2[tch2]:  Capacity  
Legend3[tch2]:  Connections  
Legend4[tch2]:  Capacity  
LegendI[tch2]:  Utilization  
LegendO[tch2]:  Capacity  

#.................................................................

Target[tch3]: `perl c:\perl\lib\hiperdsp.pl public@127.1.1.3`
MaxBytes[tch3]: 46
Title[tch3]: Total Control Hub #3
PageTop[tch3]: <H1>TCH3 Modem Utilization </H1>
YLegend[tch3]:Modem Capacity
Options[tch3]:gauge,growright
ShortLegend[tch3]:Modems
Legend1[tch3]:  Utilization  
Legend2[tch3]:  Capacity  
Legend3[tch3]:  Connections  
Legend4[tch3]:  Capacity  
LegendI[tch3]:  Utilization  
LegendO[tch3]:  Capacity  

#.................................................................

Target[tchtotal]: `perl c:\perl\lib\dualpri.pl public@127.1.1.1`+`perl
c:\perl\lib\dualt1.pl public@127.1.1.2`+`perl c:\perl\lib\hiperdsp.pl
public@127.1.1.3`
MaxBytes[tchtotal]: 138
Title[tchtotal]: Total Control Hub Totals
PageTop[tchtotal]: <H1>Total Modem Utilization </H1>
YLegend[tchtotal]:Modem Capacity
Options[tchtotal]:gauge,growright
ShortLegend[tchtotal]:Modems
Legend1[tchtotal]:  Utilization  
Legend2[tchtotal]:  Capacity  
Legend3[tchtotal]:  Connections  
Legend4[tchtotal]:  Capacity  
LegendI[tchtotal]:  Utilization  
LegendO[tchtotal]:  Capacity  
```

TCP Graph : tcpOutRsts

Captured from Cisco router C in MINT Lab

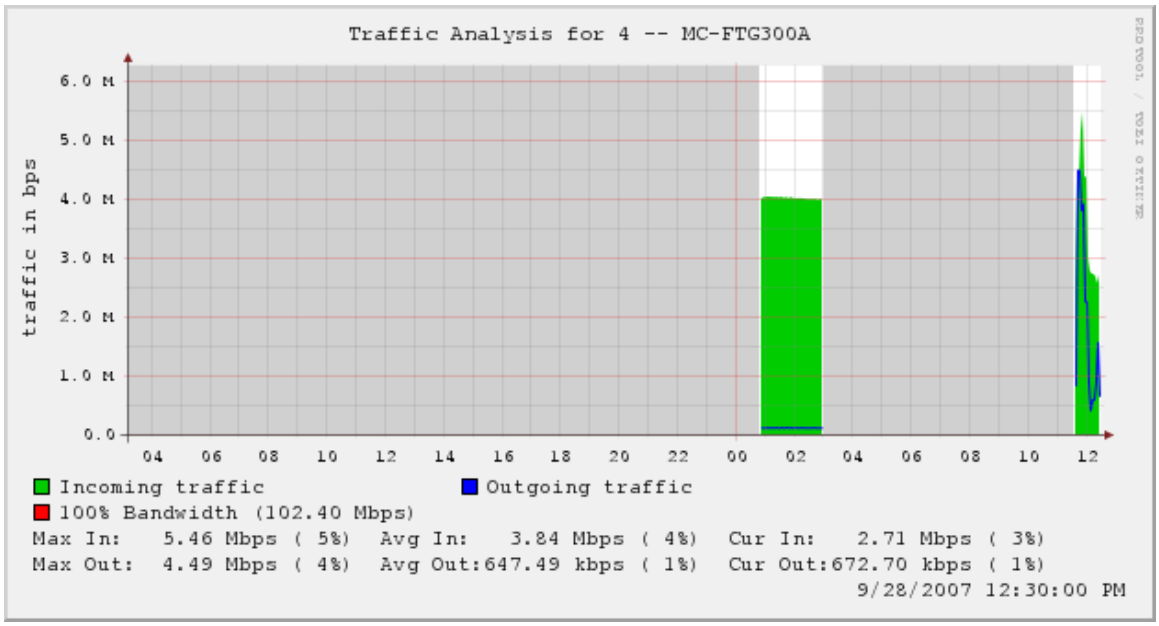
IP Address: 10.5.16.4

MRTG integrated with RRDTool and router2.cgi script.



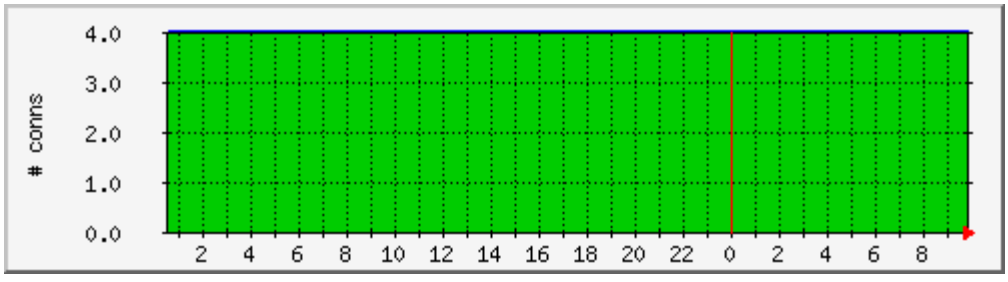
Traffic (Data) Captured From Fortigate FTG 300A

MRTG graph With RRDTool And CGI Scripts



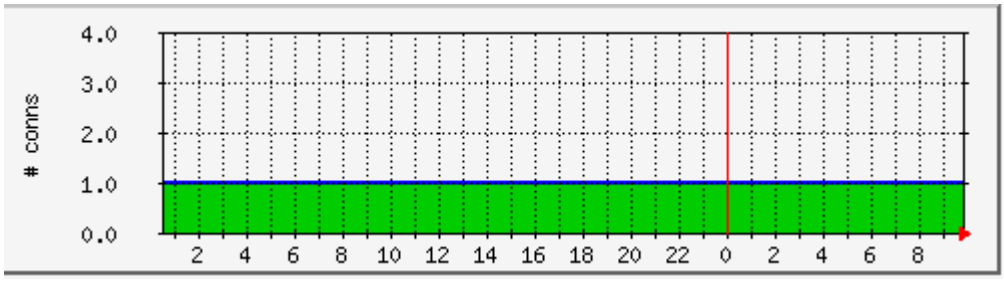
TCP (packets) Graph : Captured From 3COM Core Switch

IP Address : **10.240.1.1**



TCP Packets Captured from Cisco router B In MINT Lab

IP Address: 10.5.16.3



TCP Connections