NETWORK TRAFFIC ANALYSIS AT THE 20,000 FOOT LEVEL

OR

WHERE DID ALL THIS TRAFFIC COME FROM

Henry Steinhauer
Hewitt Associates
Lincolnshire, IL, U.S.A

Overview -

Background

Basics

Tool Found

Implement

Results

BACKGROUND-

Network Monitoring Needs

- Central Location
- Polling based
- NetView 6000
- High Bandwidth Usage caused by monitoring devices over the WAN
- Limited audience - Tied to RS/6000

Basics

RFC - SNMP - MIB - OID

RFC - Request for Comment

- RFC 2235 - Internet Timeline
- e-mail to nis-info @ nis.nsf.net
  - send rfc2235.txt
  - nis-info will send it back

Basics

SNMP - Simple Network Management Protocol

RFC - 1157, 1187

2011, 2012, 2013 - v2

3372 - v3

Basics

MIB - Management Information Base

Each managed device has a Database for items

These are Counters, Information, Status, etc

Basics

OID - Object Identifier

How SNMP Obtains information from the MIB

1.3.6.1.4 - OID for SNMP information

1.3.6.1.2.1.2.2.1.10 / 16 - Input / Output Bytes

Also known as ifInOctets / ifOutOctets

Main Platform

NetView/6000

Bay Routers

IBM Switches

Token Ring

Some E100 Switches

Reason for Change

Long Delay for data gathering

Constant changing platforms

Too Much Management Issues

Needed something **Simpler**

Web Search - MRTG

Multi Router Traffic Grapher - MRTG

url *ee-staff.ethz.ch/~oetiker/webtools/mrtg/mrtg.html*

GNU - GNU is not Unix Software - Public Use

UNIX - NT - Anything that can run Perl

What we needed to Monitor

Bay Routers - 20+ interfaces on some

Servers - 2 Interfaces each

Conclusion

Do Something

MRTG

How to invoke

Any WEB Browser Tool

(I.E. or Netscape)

Internal Web Site - No Dialer needed

Address - MRTG

MRTG - Index Page

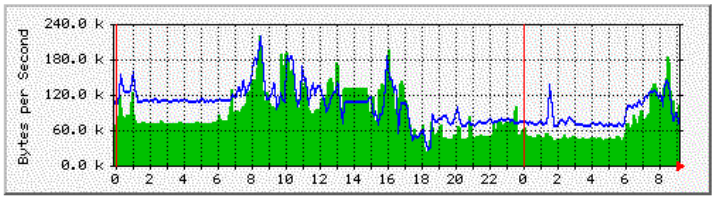
MRTG Index Pages

LOCAL REPORTS	LOCAL REPORTS	INTERNATIONAL REPORTS
Traffic Summary for Campus Interfaces	Traffic Analysis for 98 WAN	Traffic Analysis for International WAN
NetViz link	Traffic Analysis for Atlanta	
Traffic Analysis for 1OP	Traffic Analysis for NewPort Beach	
Traffic Analysis for 2op	Traffic Analysis for Orlando	
Traffic Analysis for 3OP	Traffic Analysis for Rowayton	
Traffic Analysis for Lake Cook	Traffic Analysis for Woodlands	
Traffic Analysis for 98	Index to Offices off Centers	
Traffic Analysis for 4op		Index to Other Indexes
Logical Grouping of	Volume Sets / Sonet / ATM	
Traffic Analysis for Notes	Traffic Analysis for Sonet / Atm	Traffic Analysis for 2216 Escon
Traffic Analysis for VI	Traffic Analysis for Main Servers	
Traffic Analysis for NAP Volumes	Traffic Analysis for NPP Volumes	
Traffic Analysis for Modem Pool	NFD1 Servers	

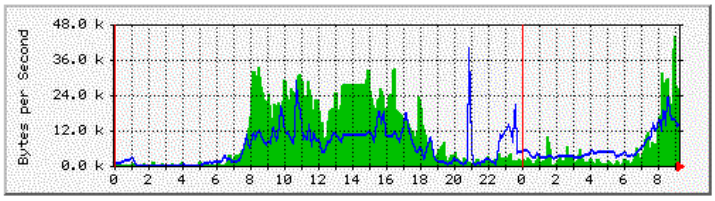
MRTG Region Information

Woodlands - Overview

Woodlands BLS SID: O21_16M_BAKBONE



Woodlands BLS SID: S31_LS_T1



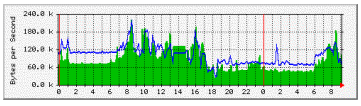
MRTG - Detail

Traffic Analysis for O21_16M_BAKBONE

System: Woodlands BLS SID: in Woodlands, TX
Maintainer: Network Support
Interface: O21_16M_BAKBONE (1)
IP: (10.131.15.254)
Max Speed: 2097.2 kBytes/s (iso88025TokenRing)

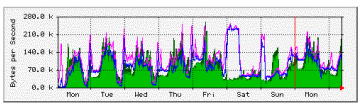
The statistics were last updated **Tuesday, 28 July 1998 at 9:15** .
at which time **'Woodlands BLN SID: 76454'** had been up for **39 days, 15:59:52**.

'**Daily' Graph (5 Minute Average)**



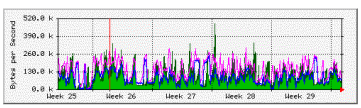
Max In: 222.4 kB/s (10.6%) Average In: 85.8 kB/s (4.1%) Current In: 104.8 kB/s (5.0%)
Max Out: 219.2 kB/s (10.5%) Average Out: 101.3 kB/s (4.8%) Current Out: 76.0 kB/s (3.6%)

'**Weekly' Graph (30 Minute Average)**



Max In: 262.8 kB/s (12.5%) Average In: 70.1 kB/s (3.3%) Current In: 115.3 kB/s (5.5%)
Max Out: 253.3 kB/s (12.1%) Average Out: 88.3 kB/s (4.2%) Current Out: 93.2 kB/s (4.4%)

'**Monthly' Graph (2 Hour Average)**



Max In: 486.0 kB/s (23.2%) Average In: 68.1 kB/s (3.2%) Current In: 62.6 kB/s (3.0%)
Max Out: 305.0 kB/s (14.5%) Average Out: 88.5 kB/s (4.2%) Current Out: 87.8 kB/s (4.2%)

MRTG

MRTG MULTI ROUTER TRAFFIC GRAPHER

2.5.2-1998/02/20 Tobias Oetiker <oetiker@ee.ethz.ch>
and Dave Rand <dlr@bungi.com>

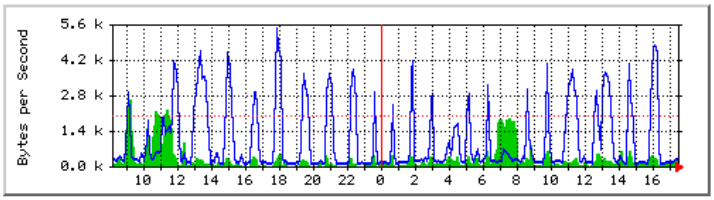
Ported to WindowsNT by Stuart Schneider <schneis@testlab.orst.edu>

MRTG
- Typical Notes Replication

Replicate each Hour -

Red line shows CIR

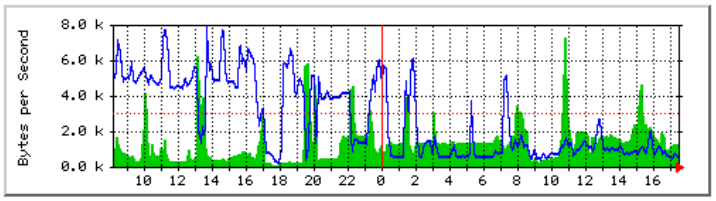
98ASN International Router (): S121 Scitor Fr202a Wiesbaden + Ljubiljana



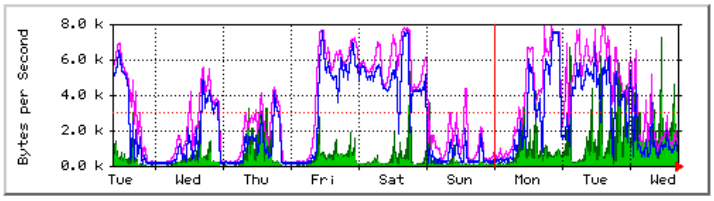
MRTG - Notes Install

First Week of Install - Setup Databases - Impact

98ASN International Router (): S121 Scitor Fr400a San Paulo + Buenos Aires



`Weekly' Graph (30 Minute Average)

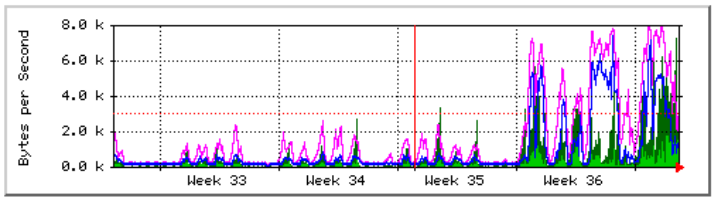


Max In: 7315.0 B/s (243.8%) Average In: 525.0 B/s (17.5%) Current In: 1258.0 B/s (41.9%)
Max Out: 7962.0 B/s (265.4%) Average Out: 2519.0 B/s (84.0%) Current Out: 723.0 B/s (24.1%)

MRTG - Notes Install

History shows the way it was.

`Monthly' Graph (2 Hour Average)



Max In: 7315.0 B/s (243.8%) Average In: 216.0 B/s (7.2%) Current In: 1717.0 B/s (57.2%)
Max Out: 7962.0 B/s (265.4%) Average Out: 913.0 B/s (30.4%) Current Out: 946.0 B/s (31.5%)

Questions ?