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
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
SNMP - Simple Network Management Protocol

RFC - 1157, 1187


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
How to invoke

Any WEB Browser Tool
(I.E. or Netscape)

Internal Web Site - No Dialer needed
Address - MRTG

MRTG - Index Page

<table>
<thead>
<tr>
<th>LOCAL REPORTS</th>
<th>LOCAL REPORTS</th>
<th>INTERNATIONAL REPORTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Summary for Campus</td>
<td>Traffic Analysis for 98 WAN</td>
<td>Traffic Analysis for International WAN</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Traffic Analysis for Atlanta</td>
<td></td>
</tr>
<tr>
<td>NetViz link</td>
<td>Traffic Analysis for NewPort Beach</td>
<td></td>
</tr>
<tr>
<td>Traffic Analysis for 1OP</td>
<td>Traffic Analysis for Orlando</td>
<td></td>
</tr>
<tr>
<td>Traffic Analysis for 2op</td>
<td>Traffic Analysis for Rowayton</td>
<td></td>
</tr>
<tr>
<td>Traffic Analysis for 3OP</td>
<td>Traffic Analysis for Woodlands</td>
<td></td>
</tr>
<tr>
<td>Traffic Analysis for Lake Cook</td>
<td>Index to Offices off Centers</td>
<td></td>
</tr>
<tr>
<td>Traffic Analysis for 4op</td>
<td>Index to Other Indexes</td>
<td></td>
</tr>
<tr>
<td>Traffic Analysis for Notes</td>
<td>Traffic Analysis for Sonet / ATM</td>
<td></td>
</tr>
<tr>
<td>Traffic Analysis for 616</td>
<td>Traffic Analysis for Main Servers</td>
<td></td>
</tr>
<tr>
<td>Traffic Analysis for NAP</td>
<td>Traffic Analysis for NTP Volumes</td>
<td></td>
</tr>
<tr>
<td>Volume</td>
<td>NFD1 Servers</td>
<td></td>
</tr>
<tr>
<td>Traffic Analysis for Modern Pool</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Woodlands - Overview

Woodlands BLS SID: O21_16M_BAKBONE

MRTG - Detail

Traffic Analysis for O21_16M_BAKBONE

Date: Woodlands IL to Woodlands TX

Summary: Network Status

Interface: O21_16M_BAKBONE (1)

ID: 00101011156

Max flow: \text{2097147} 	ext{bytes/sec} (88.977 Mbits/ sec)

The statistics were last updated Tuesday, 28 July 1999 at 09:45.

Daily Graph (5 Minute Average)

Weekly Graph (30 Minute Average)

Monthly Graph (6 Hour Average)
MRTG

- Typical Notes Replication

Replicate each Hour -

Red line shows CIR
MRTG - Notes Install

First Week of Install - Setup Databases - Impact

98ASN International Router 0: S121 Scitor Fr400a San Paulo + Buenos Aires

Weekly' Graph (30 Minute Average)

MRTG - Notes Install

History shows the way it was.
Questions?