openNMS.org
Open Network Management Software

Open Source Tools in Network Management: Waking a Sleeping Giant

Shane O'Donnell

OpenNMS.org

shaneo@opennms.org

Overview

- Defining the Market
- Defining the Players – "The Giants"
- Open Source Tools
  - What tools are there?
  - What do they do?
  - Strengths & Weaknesses
  - Emerging Tools
- Wrap-up -- Q&A

Network Management: What is it?

- The FCAPS Model
  - Fault Management
  - Configuration Management
  - Accounting Management
  - Performance Management
  - Security Management
- The Network Operations Center (NOC)
  - People - Processes - Tools

Network Management Functionalities

Discovery

Polling/Monitoring

Event Handling

Event Correlation

Notification

Performance Data Collection

Reporting

Configuration Management

Related Disciplines

- Systems Management
  - Agent-based
  - Not "remote administration"
- Application Management
  - ARM Standard
- Storage Management
  - NAS/SAN
  - Standards?

The *Real* Need for Network Management

Reducing Mean Time To Repair (MTTR)

Improving Service Availability

Providing critical reporting

Capturing Performance Metrics

Provide input to Infrastructure Planning efforts

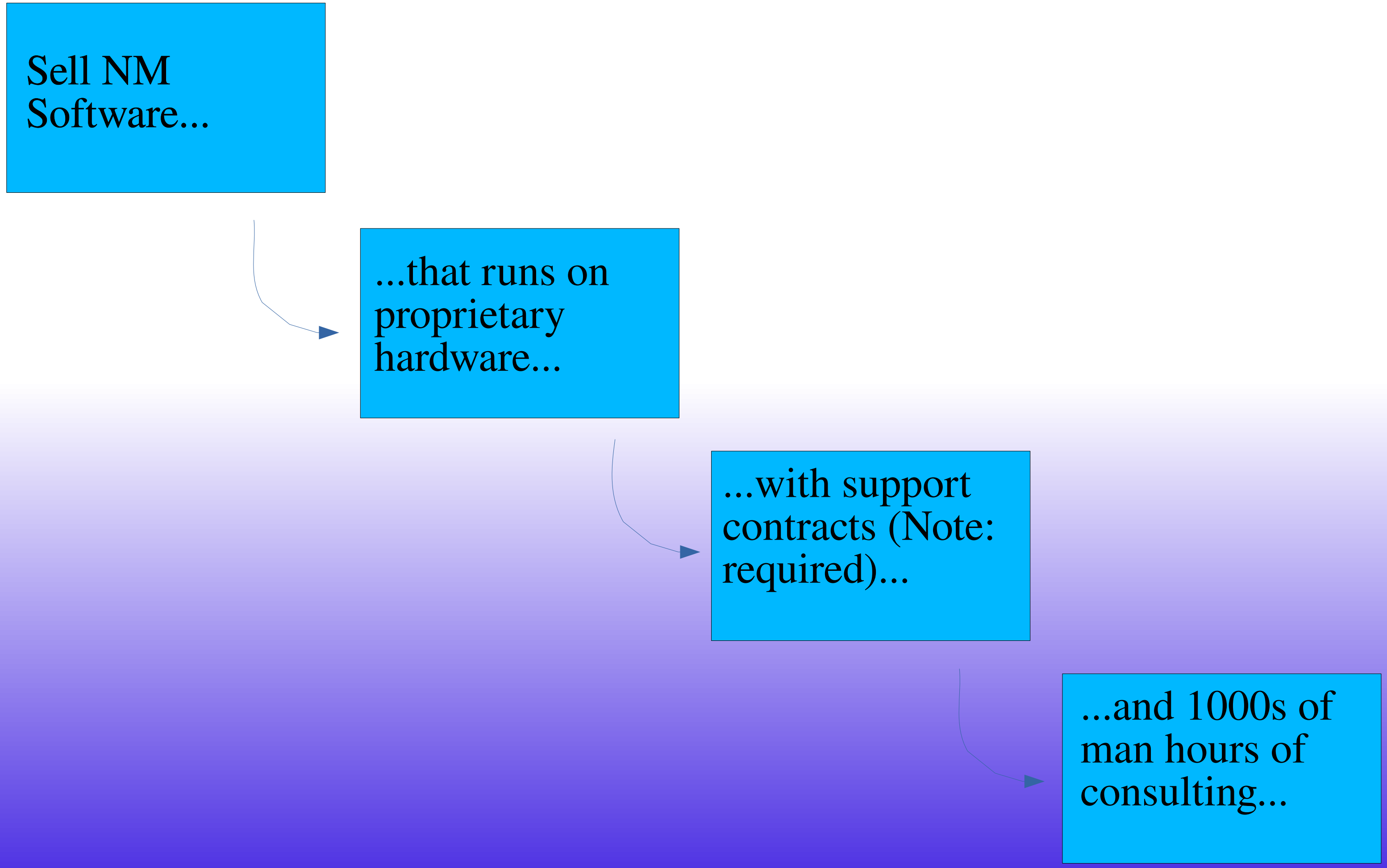
Performance testing for platforms and applications

Integration with Asset Management tools

Who Are "The Giants"?

- The Market is dominated by the "Frameworks"
- Framework Providers
  - HP OpenView Network Node Manager
  - Tivoli TME-10 Netview
  - Aprisma Spectrum (formerly Cabletron)
  - Computer Associates' UniCenter-TNG
- Point Solution Providers
  - Cisco's CiscoWorks 2000
  - Nortel's Optivity

How Do They Operate?



Sell NM Software...

...that runs on proprietary hardware...

...with support contracts (Note: required)...

...and 1000s of man hours of consulting...

How Do They Sell It?

Generate Paranoia

Point to marketshare and "Management by Magazine" ("...Everybody else is doing it...")

Hold their infrastructure hostage

Tout "out of the box" functionality...

...and plenty of follow-on services to make it work "out of the box"

Ride Buzz Word Waves

- e-Whatever

Revenue Sources in Network Management

Original Software Sale = x

- Typical entry pricing = $10K

Hardware Sale = x to 20x

- Large HP Deployment = $2.5M in HW
  - Included over 20 PA-RISC platforms & HP-UX

Deployment Services = 4x to 9x

Annual Market Size = $4B and growing (IDC)

Services & Support Opportunity =
$3-3.5 Billion Annually!

Why Open Source?

Technology is evolving quicker than existing tool providers can keep up

Shorter Time to Market

Most tool providers don't want to be

Different networks have different needs. Solutions must be customizable.

Most tools were built 10+ years ago and have code bases that aren't easily updated

Quality, quality, quality!

Why Open Source? (cont'd)

$3-3.5 Billion Annual Market for Services

$3-3.5 Billion Annual Market for Services

$3-3.5 Billion Annual Market for Services

$3-3.5 Billion Annual Market for Services

$3-3.5 Billion Annual Market for Services

$3-3.5 Billion Annual Market for Services

$3-3.5 Billion Annual Market for Services

$3-3.5 Billion Annual Market for Services

Open Source Alternatives

MRTG

RRDTool

Cricket

GxSNMP

Cheops

MON

Big Sister

OpenNMS' Bluebird

MRTG

MULTI ROUTER TRAFFIC GRAPHER

Written by Tobias Oetiker & Dave Rand

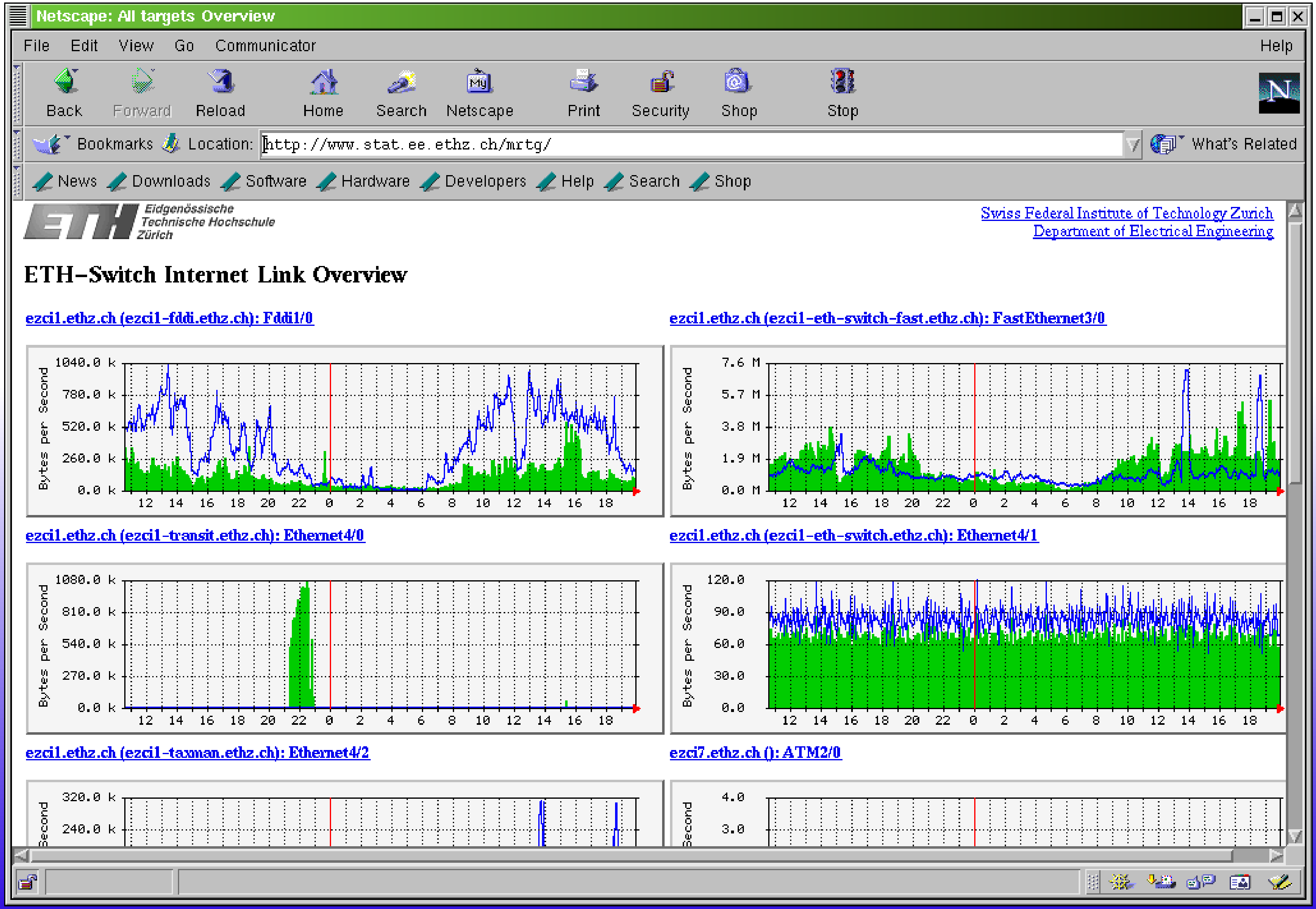
Collects SNMP data from managed devices (typically routers, as the name suggests...)

Creates HTML pages of graphs (PNG format) reflecting the data points collected

Written in Perl w/ Portable SNMP implementation (by Simon Leinen)

MRTG
MULTI ROUTER TRAFFIC GRAPHER

A Screen Shot



Netscape: All targets Overview

http://www.stat.ee.ethz.ch/mrtg/

Eidgenössische Technische Hochschule Zürich

Swiss Federal Institute of Technology Zurich
Department of Electrical Engineering

ETH-Switch Internet Link Overview

ezci1.ethz.ch (ezci1-fddi.ethz.ch): Fddi1/0

ezci1.ethz.ch (ezci1-eth-switch-fast.ethz.ch): FastEthernet3/0

ezci1.ethz.ch (ezci1-transit.ethz.ch): Ethernet4/0

ezci1.ethz.ch (ezci1-eth-switch.ethz.ch): Ethernet4/1

ezci1.ethz.ch (ezci1-taxman.ethz.ch): Ethernet4/2

ezci7.ethz.ch (): ATM2/0

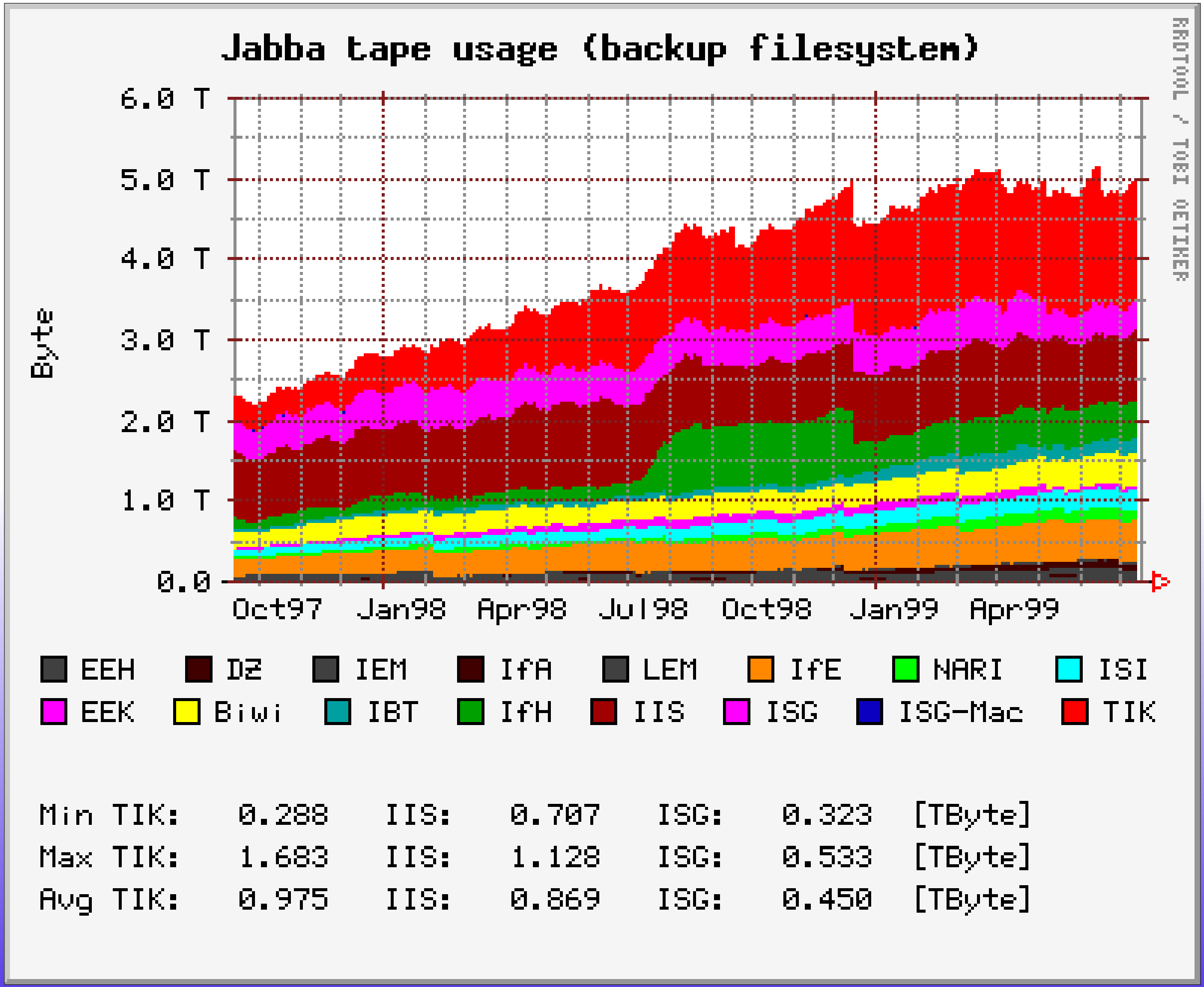
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location: What's Related
News Downloads Software Hardware Developers Help Search Shop
Bytes per Second
1040.0 k 780.0 k 520.0 k 260.0 k 0.0 k
7.6 M 5.7 M 3.8 M 1.9 M 0.0 M
1080.0 k 810.0 k 540.0 k 270.0 k 0.0 k
120.0 90.0 60.0 30.0 0.0
320.0 k 240.0 k
4.0 3.0
12 14 16 18 20 22 0 2 4 6 8 10 12 14 16 18

RRDtool

- Written by Tobias Oetiker
- Provides an effective storage mechanism for time-series data
- No data acquisition mechanism
- Data consolidation is automatic and configurable
- Effectively, the graphing and logging capabilities of MRTG, rebuilt and optimized
- The first step toward MRTG 3.0

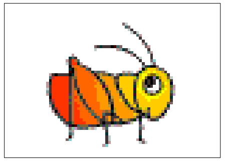
RRDtool

A Screen Shot*

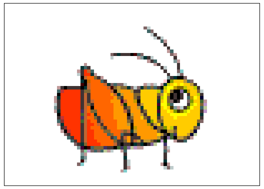


```
Min TIK:   0.288   IIS:   0.707   ISG:   0.323  [TByte]
Max TIK:   1.683   IIS:   1.128   ISG:   0.533  [TByte]
Avg TIK:   0.975   IIS:   0.869   ISG:   0.450  [TByte]
```

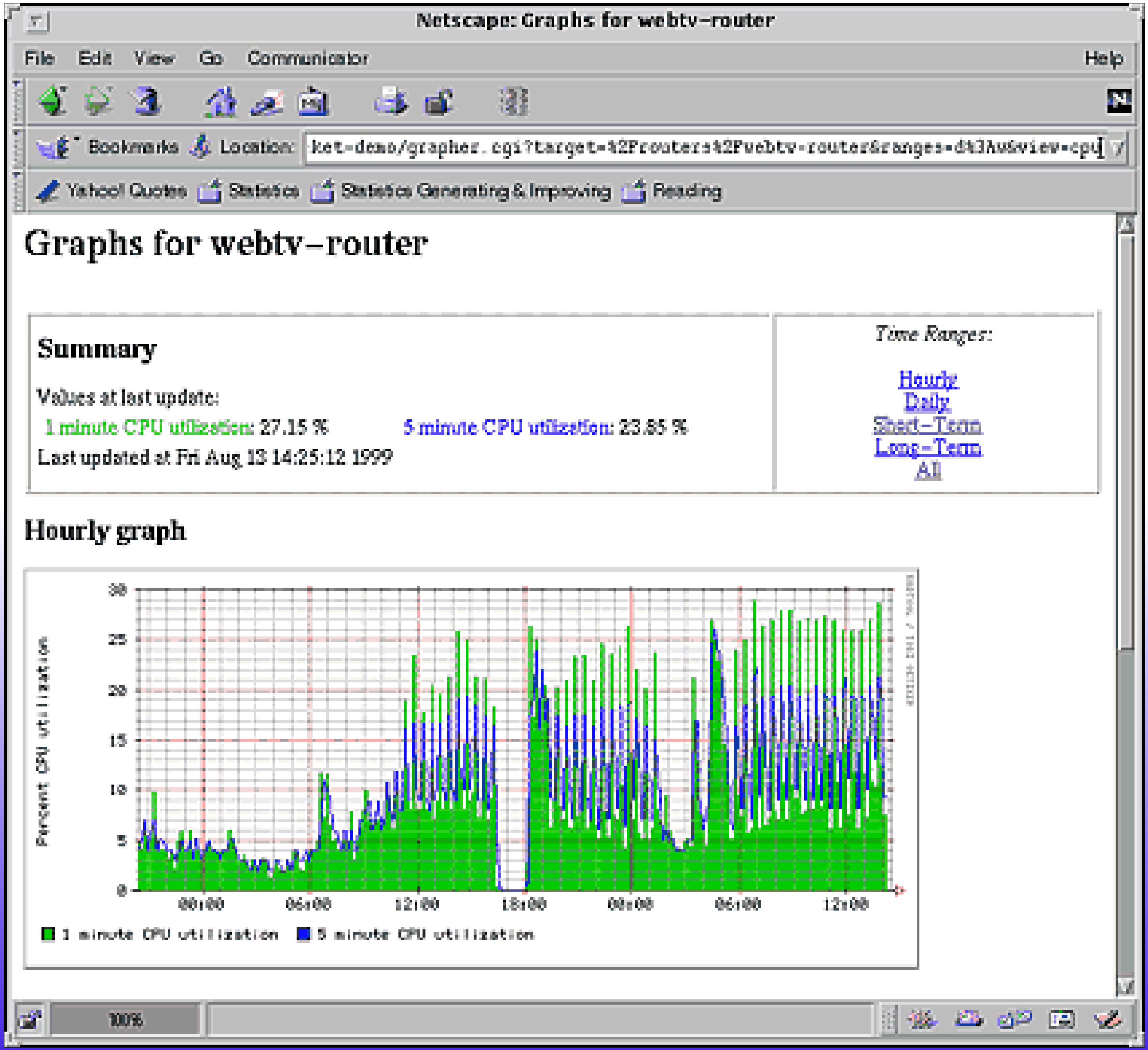
Cricket



- Written by Jeff Allen - WebTV
- Provides an MRTG-like frontend to RRDTool.
- Implements many of the features (incl. performance improvements) that Oetiker had slated for MRTG 3.0
- Allen describes a complex configuration "tree" in his paper at: http://cricket.sourceforge.net/support/doc/neta-paper/paper.html
- Relies on (and credits) RRDTool for its true performance and frontend improvements.



A Screen Shot



ket-demo/grapher.cgi?target=%2Frouters%2Fwebtv-router&ranges=d%3Aw&view=cpu

Graphs for webtv–router

Summary

Values at last update:

1 minute CPU utilization: 27.15 %   5 minute CPU utilization: 23.85 %

Last updated at Fri Aug 13 14:25:12 1999

Time Ranges:

Hourly
Daily
Short–Term
Long–Term
All

Hourly graph

GxSNMP
SNMP Manager

Written by a team, led by Jochen Friedrich

A network management application as part of the GNOME project

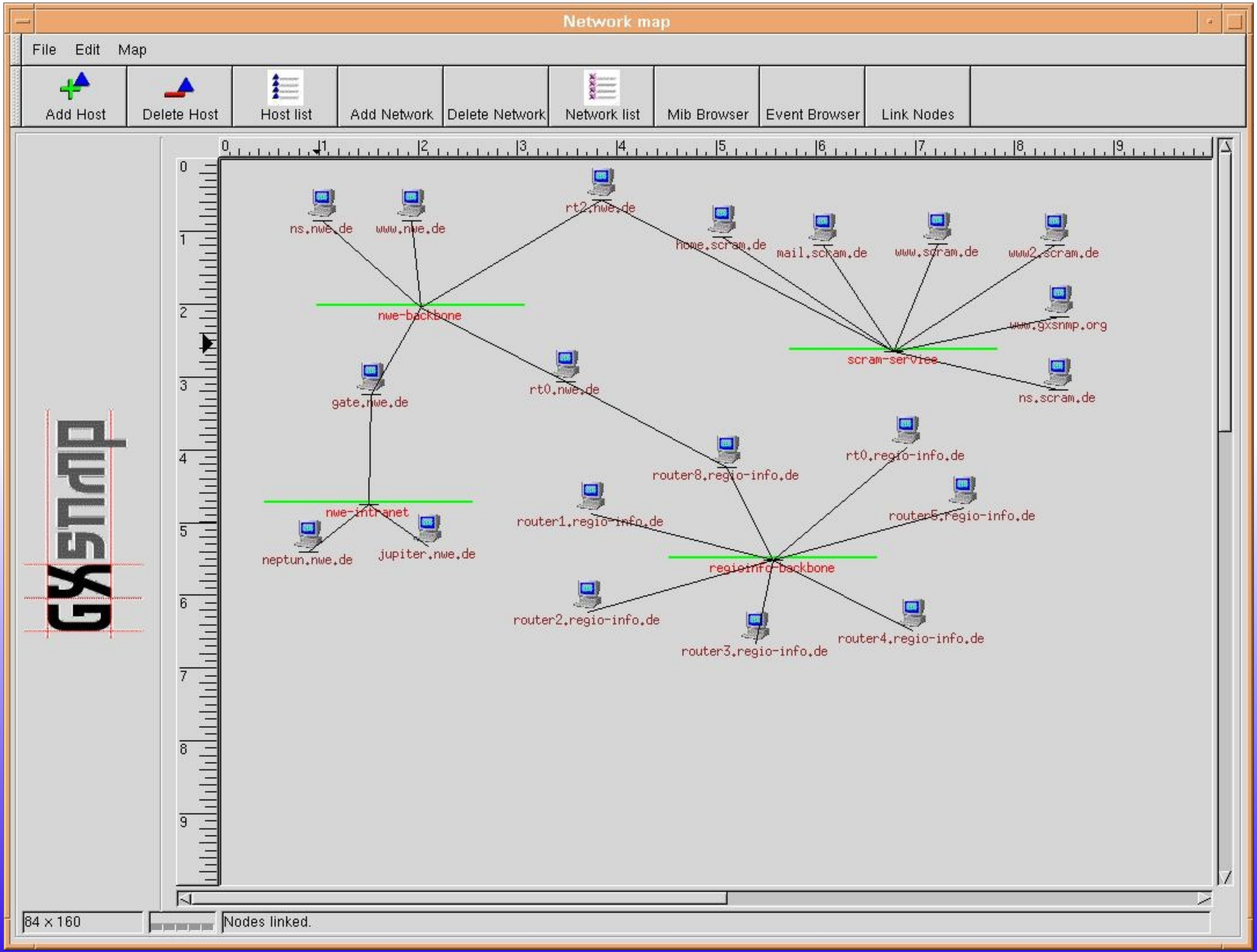
Provides a network discovery and mapping functionality

Functionality release has been somewhat slow, but very diligent

Very promising project

GxSNMP
SNMP Manager

A Screen Shot



Nodes linked.

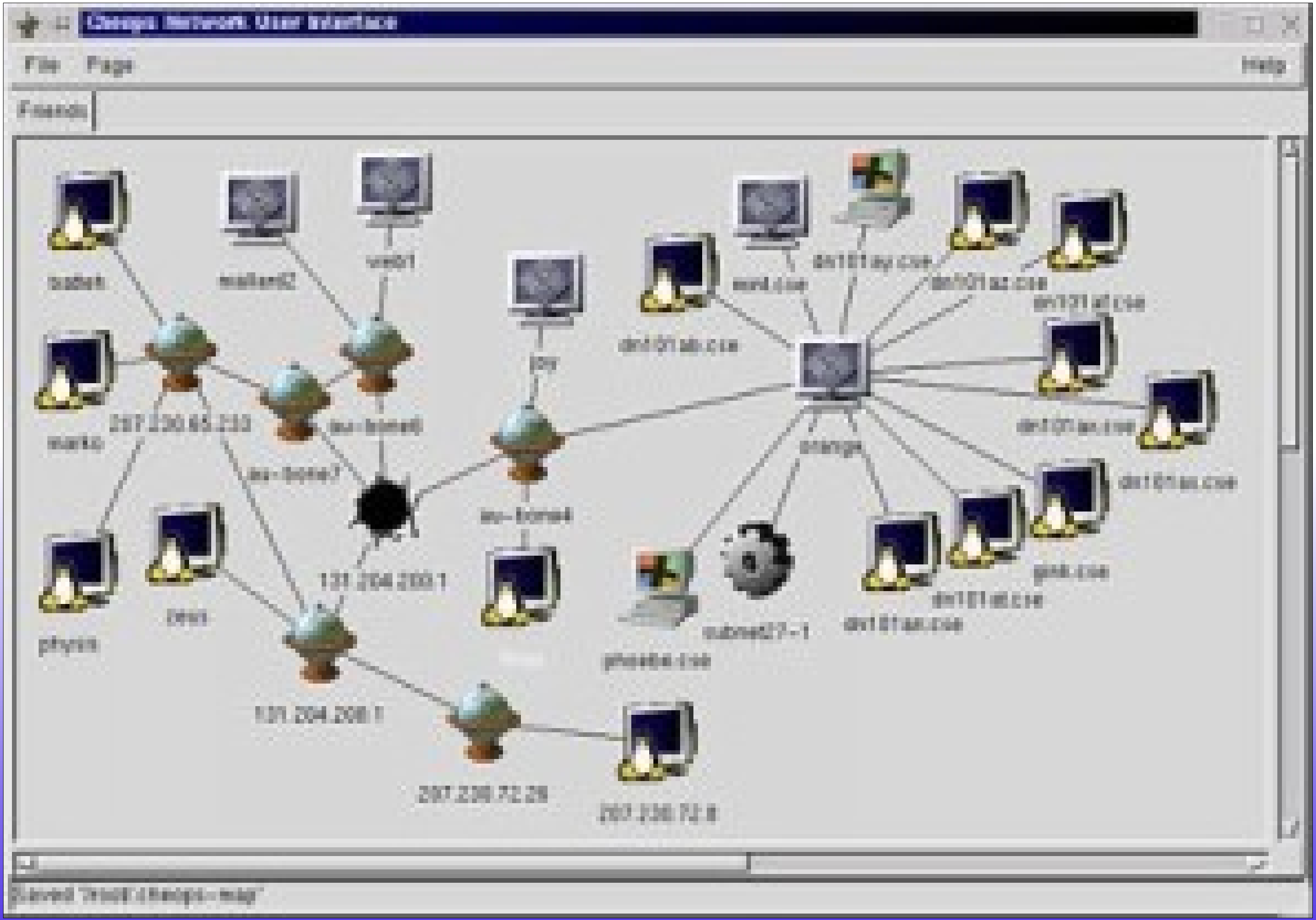
Cheops
Network User Interface

Cheops/Cheops-NG

- Written by Mark Spencer
- Marketed as "network user interface"
- Identification is manual, discovery is automatic
- SNMP and "service" monitoring are integrated
- Uses QueSO to determine target OS type
- Provides an event log for polling failures, with an integration point for email and upcoming integration to paging

Cheops
Network User Interface

Cheops/Cheops-NG



-MON-

- Written by Jim Trocki
- Provides polling and notification services
  - "Monitors" test a condition
  - "Alerts" instigate a communications tool (email/pager/reader board/etc)
- No GUI
- The product is the architectural framework. Alerts and Monitors are simply "plugged in"
- Excellent headless events/notification system

Big Sister

Written by Thomas Aeby

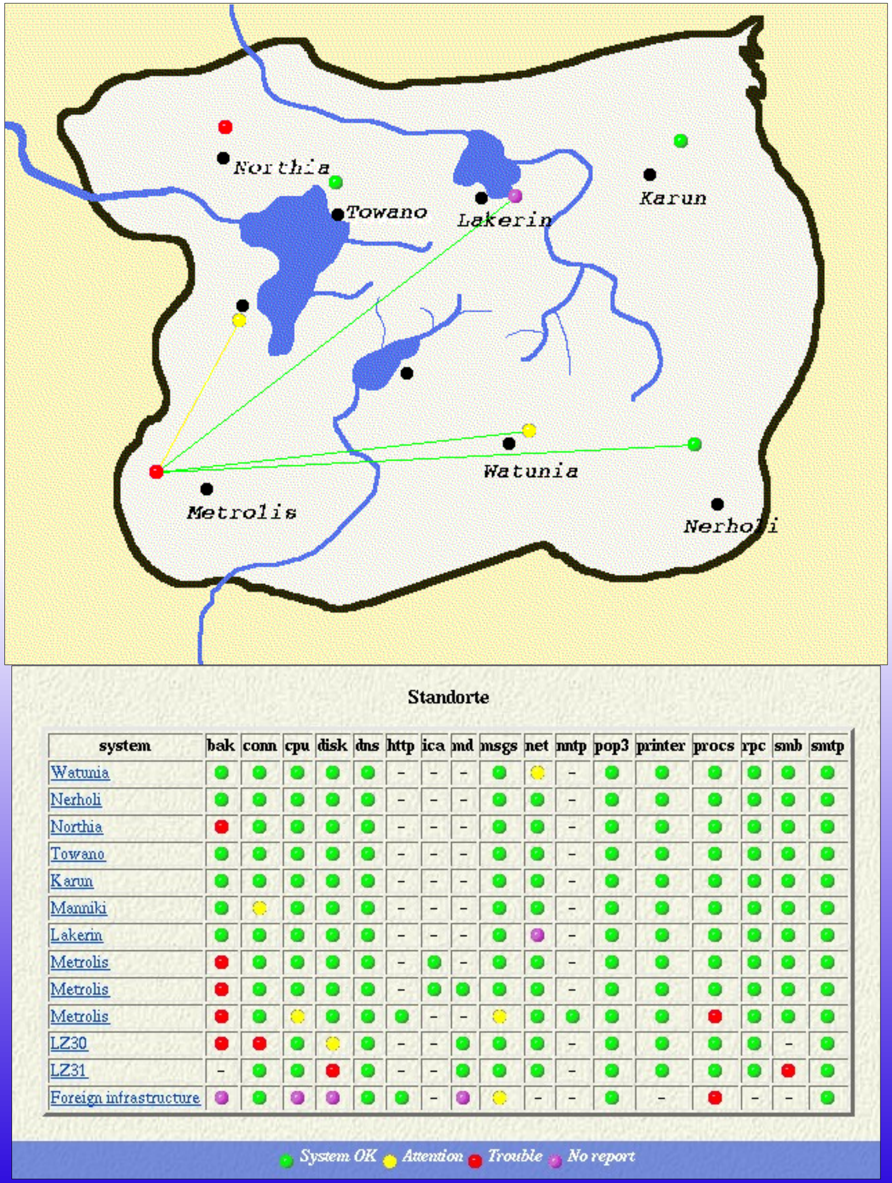
GPL-version of Big Brother (popular monitoring software under an unapproved open source license)

Excellent service monitor with Web frontend

Capable of receiving SNMP traps

Big Brother/Big Sister both very sound and functional, and now interoperable

A Screen Shot



Standorte

system	bak	conn	cpu	disk	dns	http	ica	md	msgs	net	nntp	pop3	printer	procs	rpc	smb	smtp
Watunia	🟢	🟢	🟢	🟢	🟢	-	-	-	🟢	🟡	-	🟢	🟢	🟢	🟢	🟢	🟢
Nerholi	🟢	🟢	🟢	🟢	🟢	-	-	-	🟢	🟢	-	🟢	🟢	🟢	🟢	🟢	🟢
Northia	🔴	🟢	🟢	🟢	🟢	-	-	-	🟢	🟢	-	🟢	🟢	🟢	🟢	🟢	🟢
Towano	🟢	🟢	🟢	🟢	🟢	-	-	-	🟢	🟢	-	🟢	🟢	🟢	🟢	🟢	🟢
Karun	🟢	🟢	🟢	🟢	🟢	-	-	-	🟢	🟢	-	🟢	🟢	🟢	🟢	🟢	🟢
Manniki	🟢	🟡	🟢	🟢	🟢	-	-	-	🟢	🟢	-	🟢	🟢	🟢	🟢	🟢	🟢
Lakerin	🟢	🟢	🟢	🟢	🟢	-	-	-	🟢	🟣	-	🟢	🟢	🟢	🟢	🟢	🟢
Metrolis	🔴	🟢	🟢	🟢	🟢	-	🟢	-	🟢	🟢	-	🟢	🟢	🟢	🟢	🟢	🟢
Metrolis	🔴	🟢	🟢	🟢	🟢	-	🟢	🟢	🟢	🟢	-	🟢	🟢	🟢	🟢	🟢	🟢
Metrolis	🔴	🟢	🟡	🟢	🟢	🟢	-	-	🟡	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢
LZ30	🔴	🔴	🟢	🟡	🟢	-	-	🟢	🟢	🟢	-	🟢	🟢	🟢	🟢	-	🟢
LZ31	-	🟢	🟢	🔴	🟢	-	-	🟢	🟢	🟢	-	🟢	🟢	🟢	🟢	🔴	🟢
Foreign infrastructure	🟣	🟢	🟣	🟣	🟢	🟢	-	🟣	🟡	-	-	🟢	-	🔴	-	-	🟢

🟢 System OK 🟡 Attention 🔴 Trouble 🟣 No report

Other Tools...

- Other Network Management Tools
  - NOCOL (Network Operations Center On-Line)/SNIPS
  - Emonitor
  - Scotty/Tkined
    - Development on Tkined abandoned
- Traffic Analyzers
  - tcpdump/Ethereal/snort/iptraf
- System Admin/Remote Admin Tools
  - PIKT (Problem Informant/Killer Tool)
  - GAP (GNU Administration Project)
  - Linuxconf

Some Limitations...

Usually, open source tools aren't considered at larger installations, for a few reasons:

- Limited professional support
- No concept of user views
- Scalability problems
- Performance problems
- Distribution problems
- Mandate non-standard enterprise platforms (Linux)
- Management concerns with open source in general

The Next Generation of Open Source Network Management Tools

New Versions of Existing Tools

- GxSNMP
  - Plans for distributed architecture
- Cheops
  - Constantly implementing workarounds for larger installations
- Mon
  - Addition of new functionality on regular basis
- Others
  - Tkined is slated for complete rewrite (unscheduled)

Emerging Tools

Disclaimer #1: I am biased

Disclaimer #2: I am right

OpenNMS' Bluebird

A next-generation network and systems management platform, built for the middleprise and enterprise markets

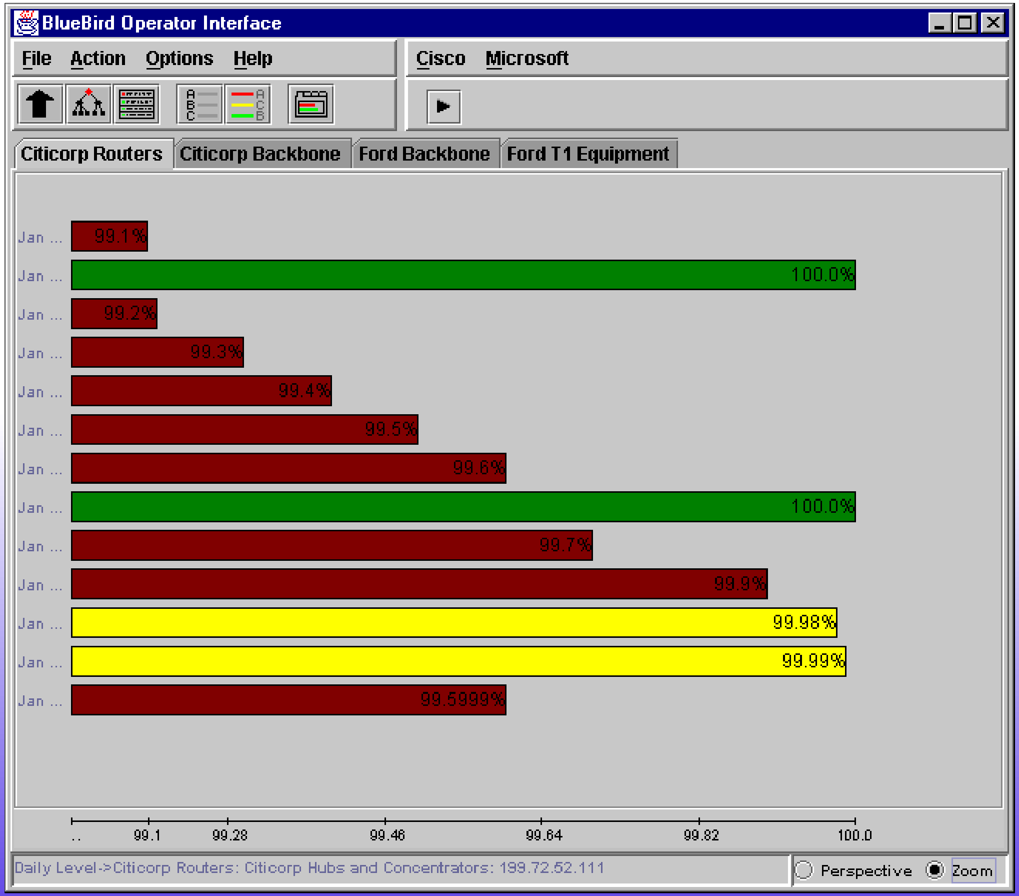
Includes distribution model to support localized polling, database synchronization to a centralized datastore, and user-specific views

Capable of handling overlapping IP address spaces (e.g, multiple "10." networks (RFC1918))

Built for extensibility and integration with other tools (e.g., trouble ticketing, notification, etc.)

7x24x265 Support Available

OpenNMS Timeline



Daily Level->Citicorp Routers: Citicorp Hubs and Concentrators: 199.72.52.111

○ Perspective ● Zoom

Jan 1999

- Design Begins

June 1999

- Defection Begins

November 1999

- Initial algorithm testing

May 2000

- jSNMP released

August 2000

- Project funded

November 2000

- Beta Test Begins

December 2000

- First Release

First Release Functionality

Network and Device Discovery

Ranging/Filtering

Service Polling

- Synthetic Transactions

Business Views in Real-Time

Historical Trending/Reporting

Rule-based Configuration

Bandwidth Trolls (self-limiting network usage)

The Critical Technologies

- Java
  - Native threads and development speed
- XML/XSL/FO
- RDBMS
  - Postgres & Oracle
- JDBC
- Synthetic Transactions
- SNMP (for discovery and event receipt)

The Synthetic Transaction

Example: The "Blue Screen of Death" problem

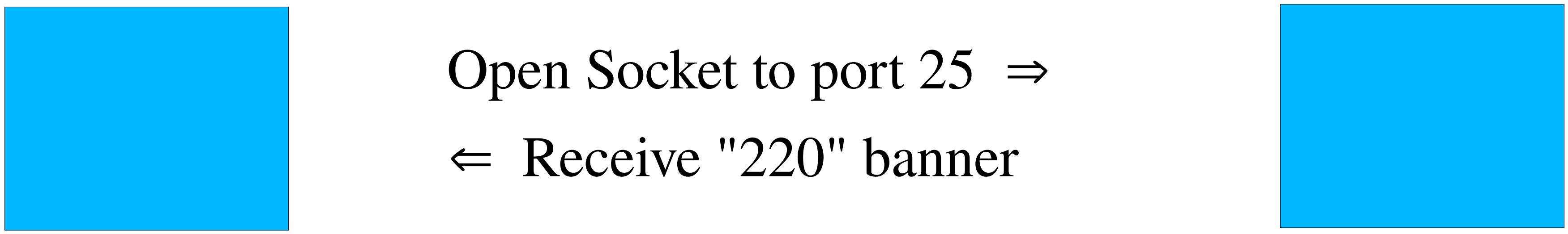
The Synthetic Transaction

- Prove the technology *using* the technology

Three "layers" of Synthetic Transactions

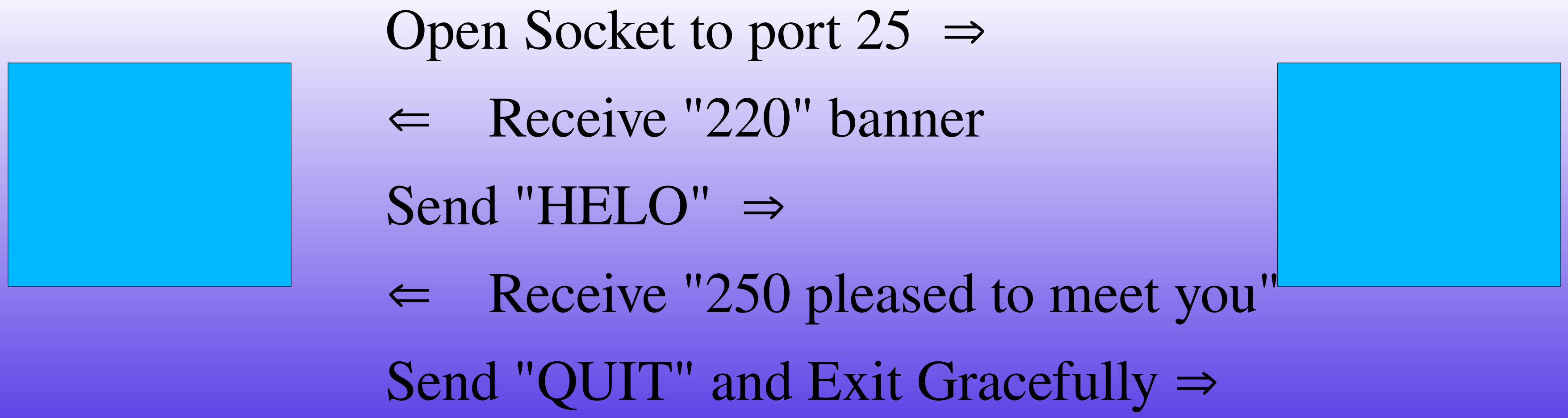
- Discovery (capsd)
- Pre-defined (poller)
- Custom (poller & XML)

Synthetic Transaction Example



Open Socket to port 25 ⇒

⇐ Receive "220" banner



Open Socket to port 25 ⇒

⇐ Receive "220" banner

Send "HELO" ⇒

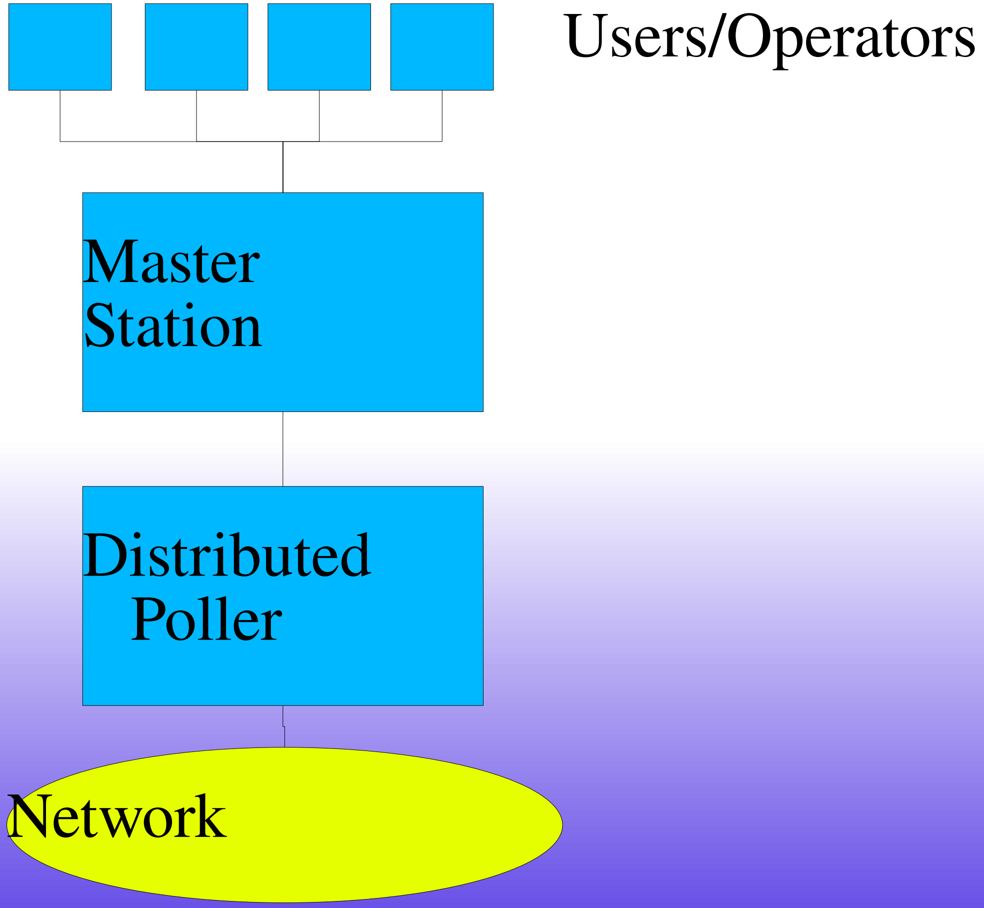
⇐ Receive "250 pleased to meet you"

Send "QUIT" and Exit Gracefully ⇒

Synthetic Transactions - Release 1

- TCP-based Monitoring
  - FTP
  - HTTP
  - SMTP
- UDP-based Monitoring
  - DNS
- Layer 3 (IP)-based Monitoring
  - ICMP

The Architecture



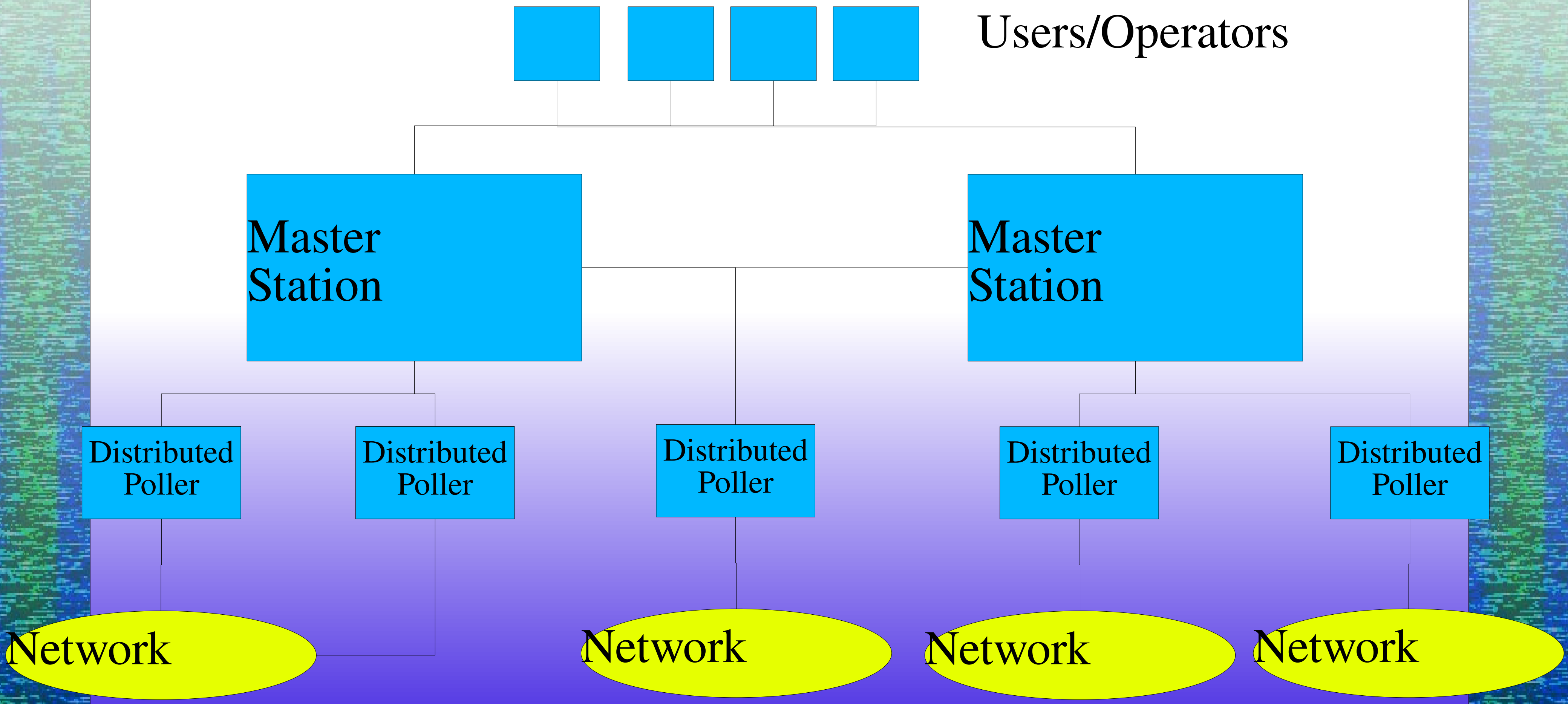
Users/Operators

Master Station

Distributed Poller

Network

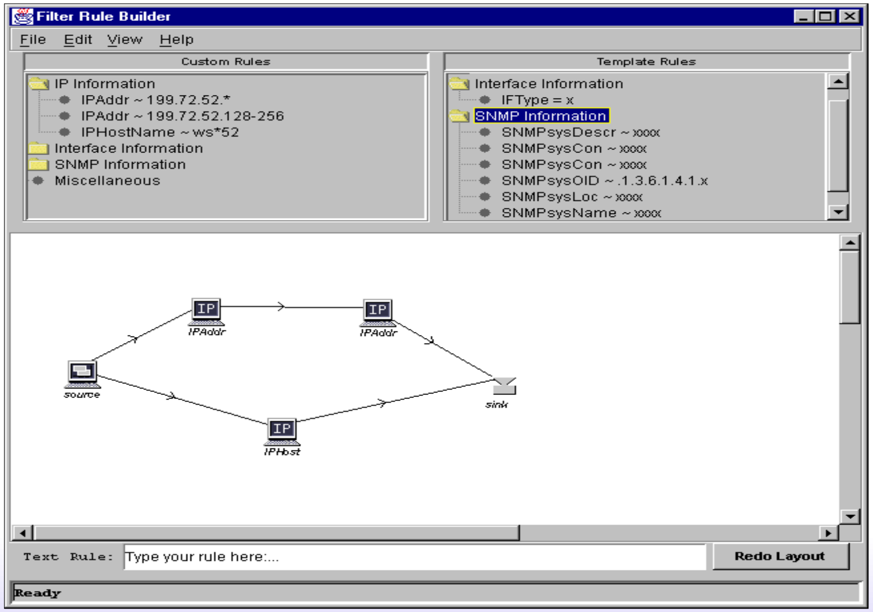
Distributed Architecture



OpenNMS' Bluebird Project Status

- On track for EOY release
- Discovery/Capsd are Available
- EUI complete and in testing
- Service Control Manager (start/stop/pause services on distributed platforms) in testing
- Transactions between MS and DP being constructed in XML over SOAP
- Filtering engine in testing

In Closing...



Custom Rules:

- IP Information
  - IPAddr ~ 199.72.52.*
  - IPAddr ~ 199.72.52.128-256
  - IPHostName ~ ws*52
- Interface Information
- SNMP Information
- Miscellaneous

Template Rules:

- Interface Information
  - IFType = x
- SNMP Information
  - SNMPsysDescr ~ xxxx
  - SNMPsysCon ~ xxxx
  - SNMPsysCon ~ xxxx
  - SNMPsysOID ~ .1.3.6.1.4.1.x
  - SNMPsysLoc ~ xxxx
  - SNMPsysName ~ xxxx

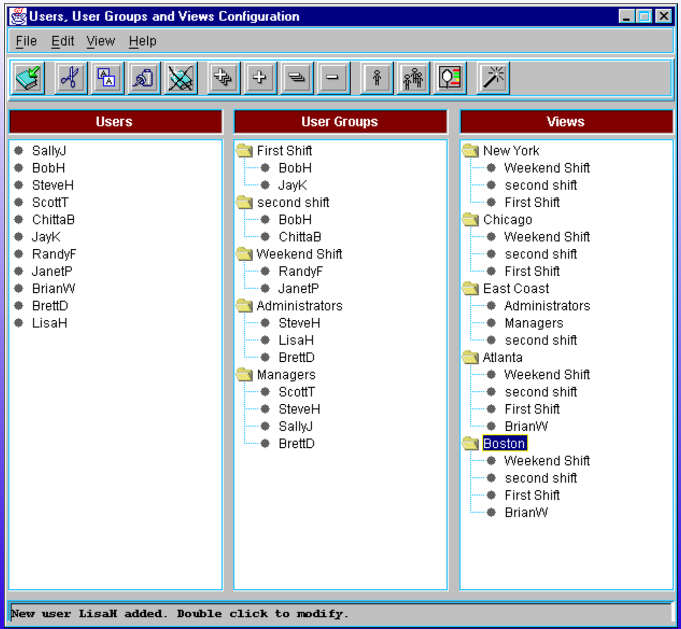
Text Rule: Type your rule here:...

Ready

Open source tools, if not already, are becoming a real option in network management.

Specific functionality in multiple tools is a good start.

Bluebird will help to change the industry.



Users:

- SallyJ
- BobH
- SteveH
- ScottT
- ChittaB
- JayK
- RandyF
- JanetP
- BrianW
- BrettD
- LisaH

User Groups:

- First Shift
  - BobH
  - JayK
- second shift
  - BobH
  - ChittaB
- Weekend Shift
  - RandyF
  - JanetP
- Administrators
  - SteveH
  - LisaH
  - BrettD
- Managers
  - ScottT
  - SteveH
  - SallyJ
  - BrettD

Views:

- New York
  - Weekend Shift
  - second shift
  - First Shift
- Chicago
  - Weekend Shift
  - second shift
  - First Shift
- East Coast
  - Administrators
  - Managers
  - second shift
- Atlanta
  - Weekend Shift
  - second shift
  - First Shift
  - BrianW
- Boston
  - Weekend Shift
  - second shift
  - First Shift
  - BrianW

New user LisaH added. Double click to modify.

openNMS.org

Open Network Management Software

RRDtool

GxSNMP

SNMP Manager

Thank You!

-MON-

Cheops

Network User Interface

MRTG

MULTI ROUTER TRAFFIC GRAPHER