Network-Monitoring using ntop and SNMP

Stephan Knabe
Student at Hochschule Harz, Wernigerode
Diploma Student at DESY Zeuthen, DV group
stephan.knabe@desy.de

26. November 2003

This is not only one topic:

SNMP and ntop - totally different things:

- ntop - a tool for Network-Monitoring
- SNMP - a Management-Networkprotocol

The power comes with the combination.

Inhalt

- Network-Monitoring using ntop
- Monitoring using SNMP
- Draft of an integrated Monitoring-Solution

Network-Monitoring using ntop

Stephan Knabe
Student at Hochschule Harz, Wernigerode, FB A/I
Diploma Student at DESY Zeuthen, DV group
stephan.knabe@desy.de

26. November 2003

In networks you'll get disturbances.

Possible causes are:

- Errors in hardware-, software- or configuration
- Bad design and bad scalability
- Unauthorized or not foreseen usage

Continued monitoring prevents you from this.

ntop overview (1)

- Monitoring of small and midsize networks
- OSI-Layers 2, 3, 4 and 5
- Comfortable Web-GUI
- Integrated webserver
- Extensive tabular and graphical overviews
- Open Source (GPL)

ntop overview (2)

- Supported media types:

  Loopback, Ethernet (including 802.11Q), Token Ring,

  PPP/PPPoE, FDDI, ...

- Supported Operating Systems:

  FreeBSD, Linux, Solaris, IRIX, AIX, MS Windows

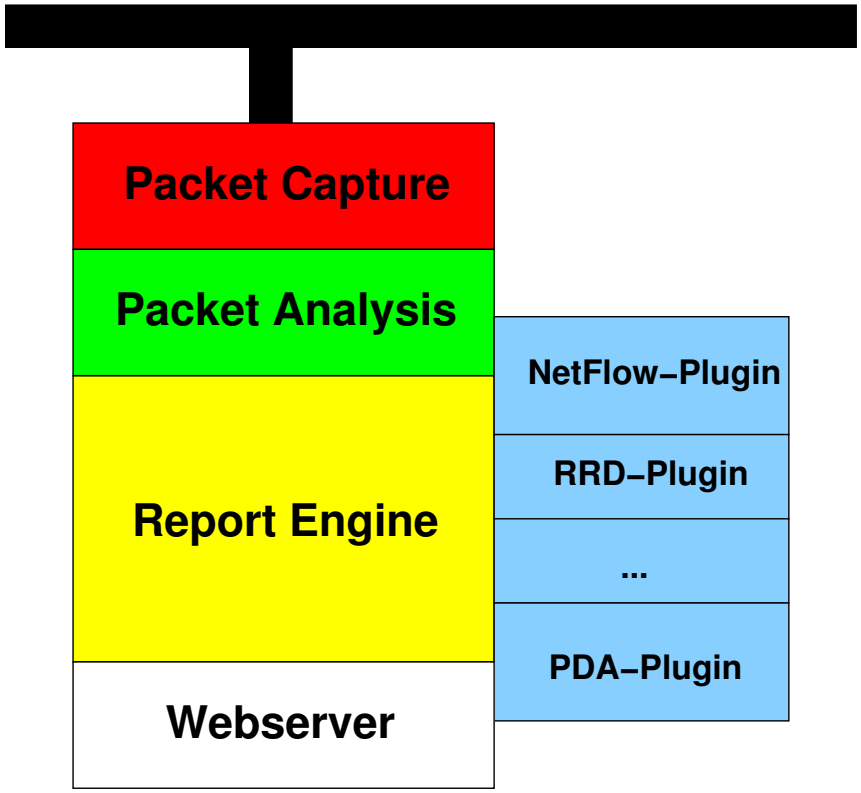
- Supported protocols :

  IP, IPX, DecNet, AppleTalk, Netbios, OSI, DLC ...

ntop overview (3)

- Mainly developed by Luca Deri (University of Pisa)
- Project-Homepage `www.ntop.org`
- CVS-Snapshots, FAQ, Forums at `snapshot.ntop.org`
- Mailinglists `ntop@unipi.it` and `ntop-dev@unipi.it`
- Actual version is 2.5c

Architecture



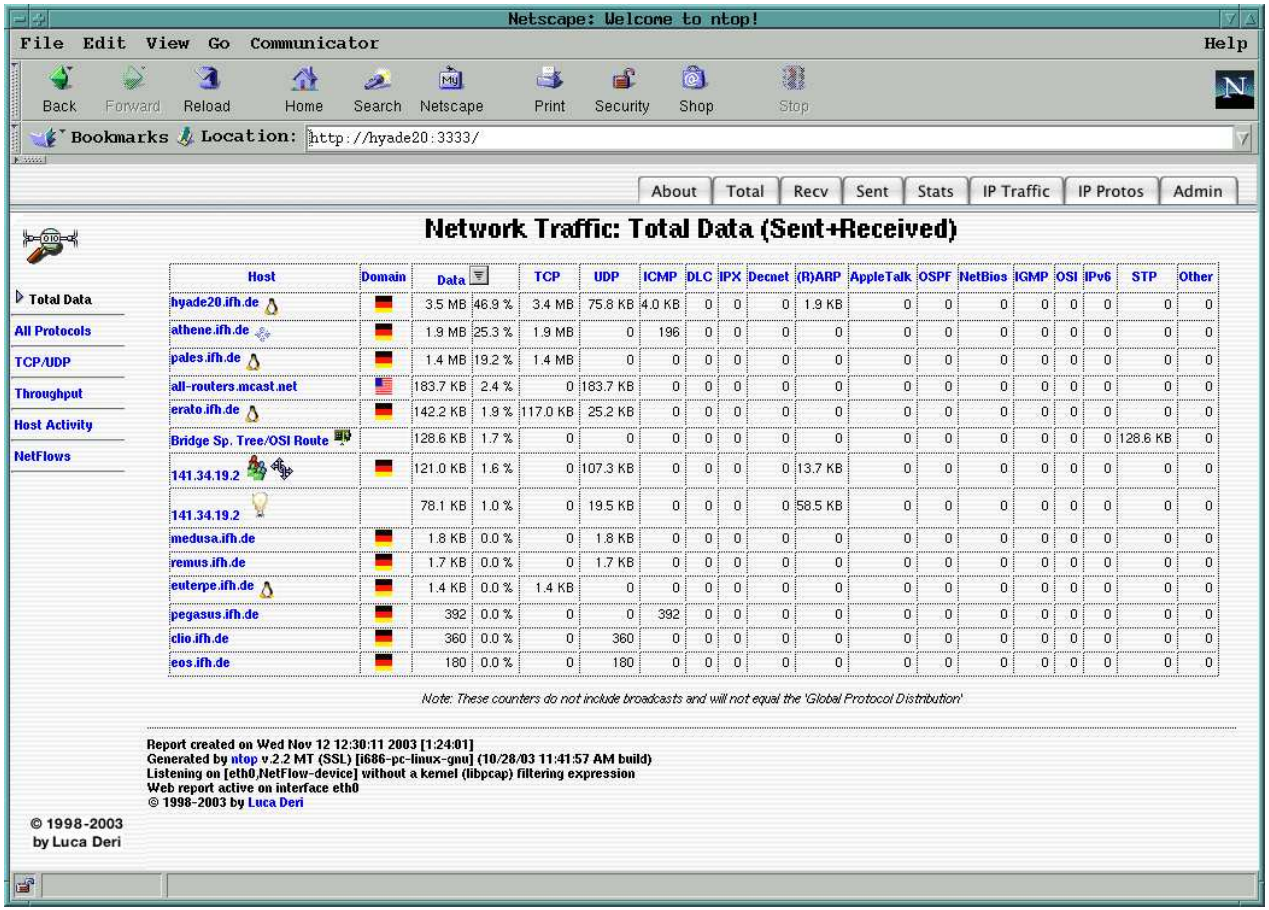
based on libpcap

Plugins

HTTP/HTTPS

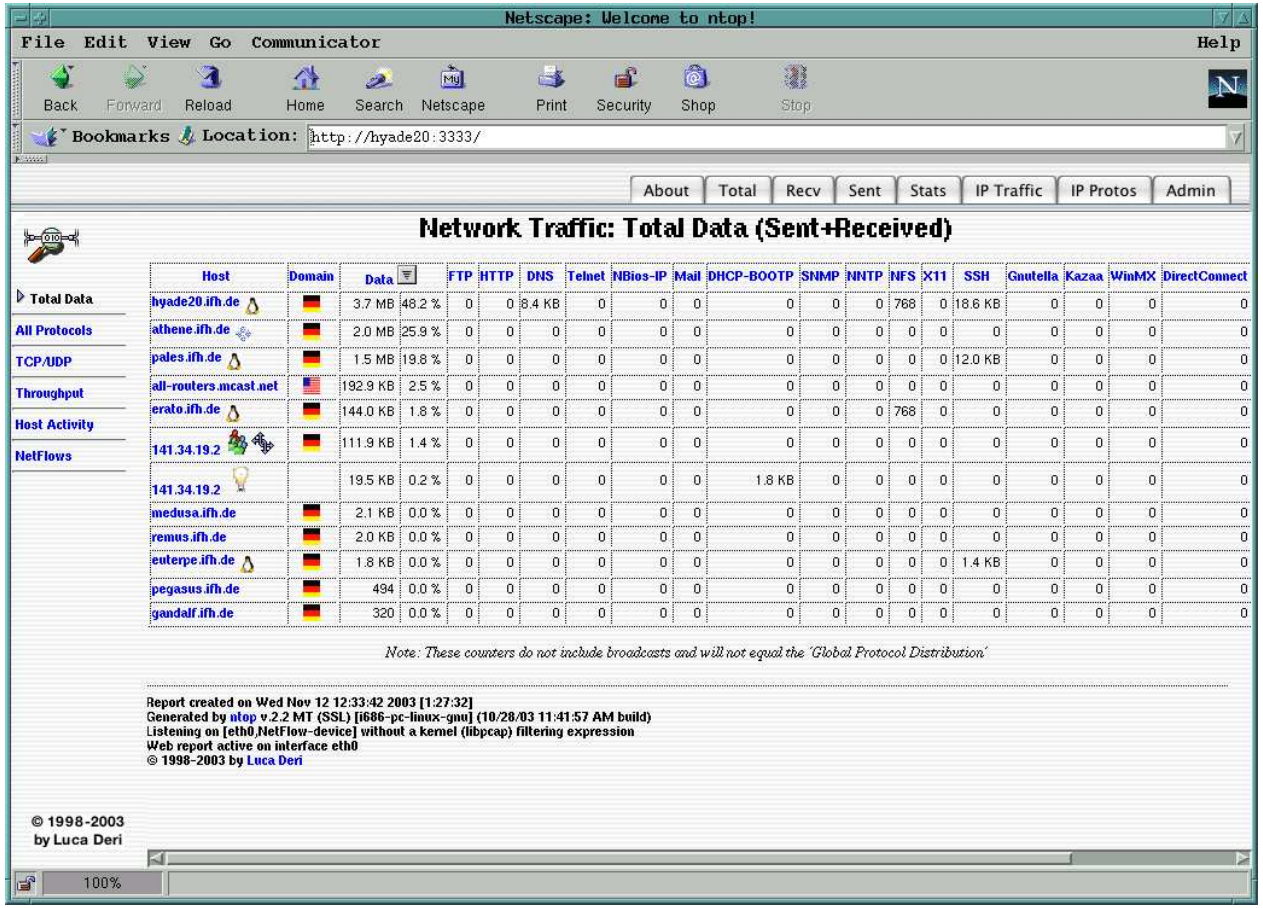
Basic-Features (1)

Total-Data-Statistic



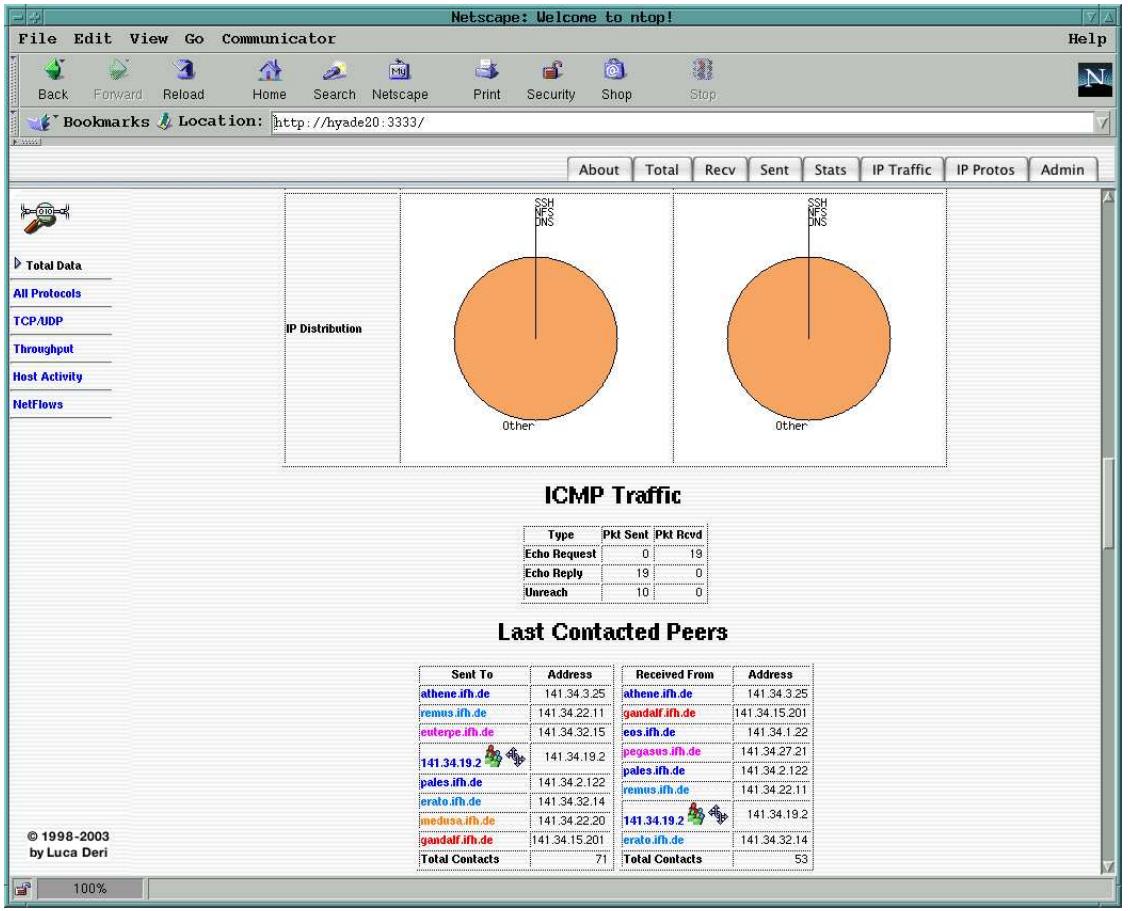
Basic-Features (2)

Detailed TCP/UDP-Statistic



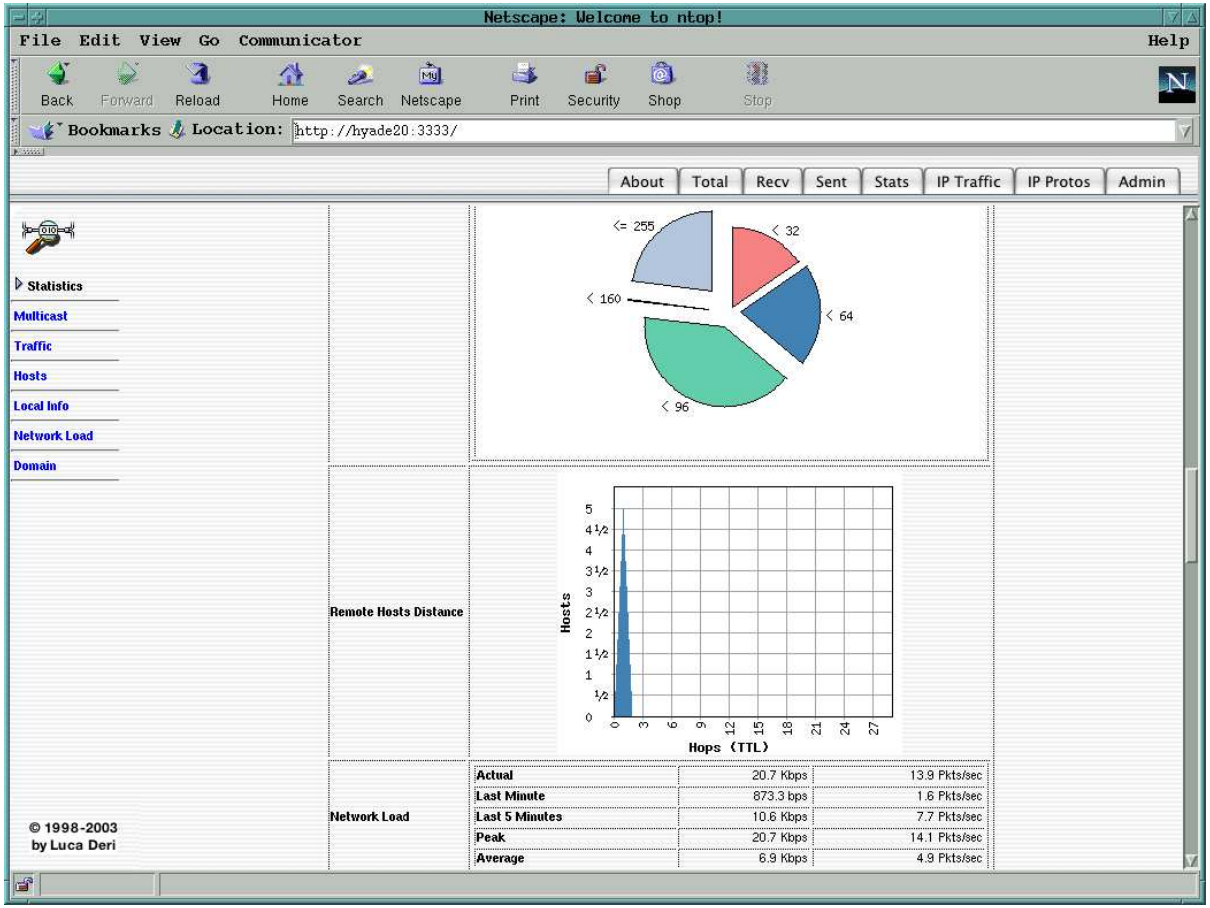
Basic-Features (3)

Host-Statistics



Basic-Features (4)

Network-Overview



Advanced Features

- TCP-Connection-Tracking
- Host-Matrix
- VLAN-Overview
- Basic IDS-Features

Administration

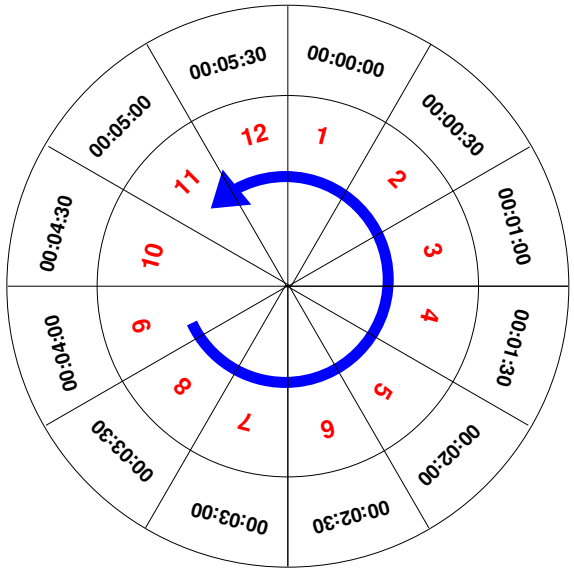
- Access control
- Reset of counters
- Setting filters
- Export of data (TXT, XML, PHP, Perl ...)
- Plugin-Configuration

Plugins

- NetFlow - Im- and export of Connection-Parameters
- rrdPlugin - Storage of data and creation of timebased trend graphics
- ICMP-Watch - Detailed monitoring of ICMP-Packets
- NFS-Watch - NFS-Statistics
- LastSeen - Stores time of first and last host activities

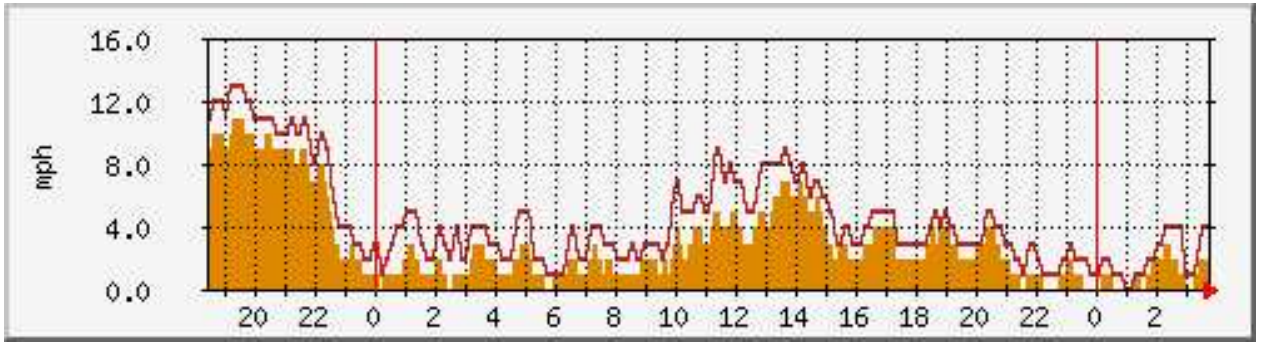
rrdPlugin (1)

- Medium-term archiving of collected data is necessary
- RDBMS needs manual service because of lots of data
- Alternatives are Round Robin Databases



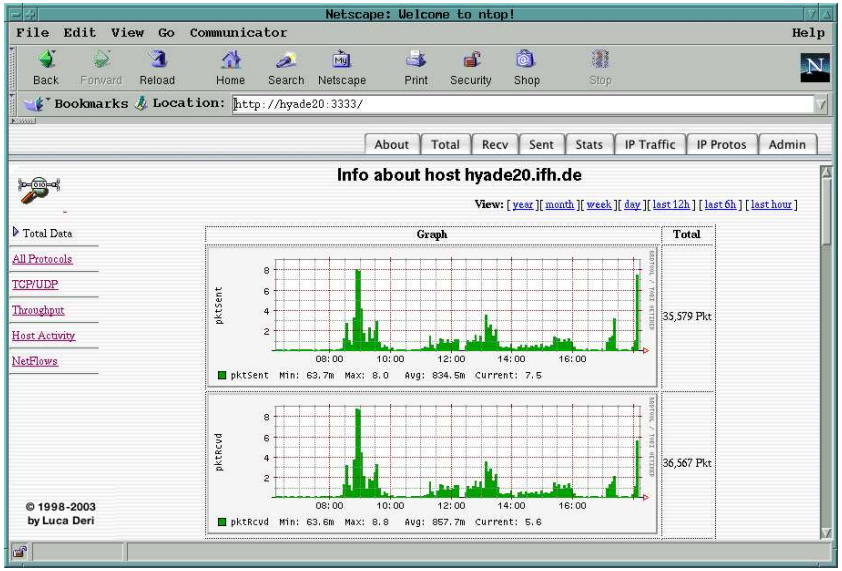
rrdPlugin (2)

- Based on rrdtools from mrtg
- Wide spread on Unix systems
- Packet includes graphic tool
- API's for Perl and C
- Interfaces to other tools



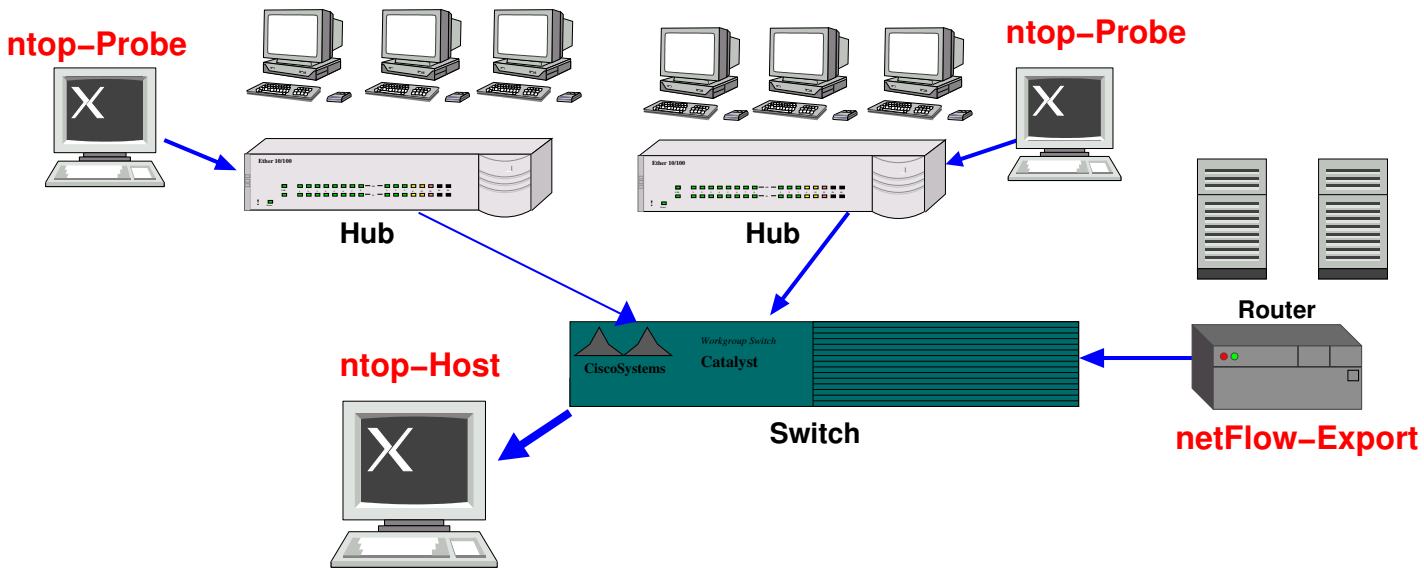
rrdPlugin (3)

- Configuration of storage path, data amount, data detail
- Creates graphical stats of host- and network-data



NetFlow-Plugin (1)

- In large networks and Switch-Environments distributed monitoring is a solution
- RMON/SMON only give insufficient data



NetFlow-Plugin (2)

- Plugin for im- and exporting of Flow-Data
- ntop supports NetFlow v5, sFlow, nFlow and NetFlow v9
- Interfaces to other applications are easy to implement

Summary

- Universal tool for daily practical use
- Works also with bigger networks
- Lot of interfaces to external (own) applications
- For long time data storage better use external tools
- No replacement for IDS or protocol analyzers

Ressources

- Project-Homepage `www.ntop.org` / `snapshot.ntop.org`
- Information about flow protocols: `www.cisco.com`, `www.sflow.org`
- RRD-Infos `www.mrtg.org`, `www.rrdtool.org`
- Feedback to `stephan.knabe@desy.de`

Monitoring using SNMP

Stephan Knabe
Student at Hochschule Harz, Wernigerode, FB A/I
Diploma Student at DESY Zeuthen, DV group
sknabe@ifh.de

November 26, 2003

In networks you'll get disturbances.

Possible causes are:

- Errors in hardware-, software- or configuration
- Bad design and bad scalability
- Unauthorized or not foreseen usage

Continued monitoring prevents you from this.

SNMP is good

- Platform-independent
- Open specification
- In fact THE standard for networking devices

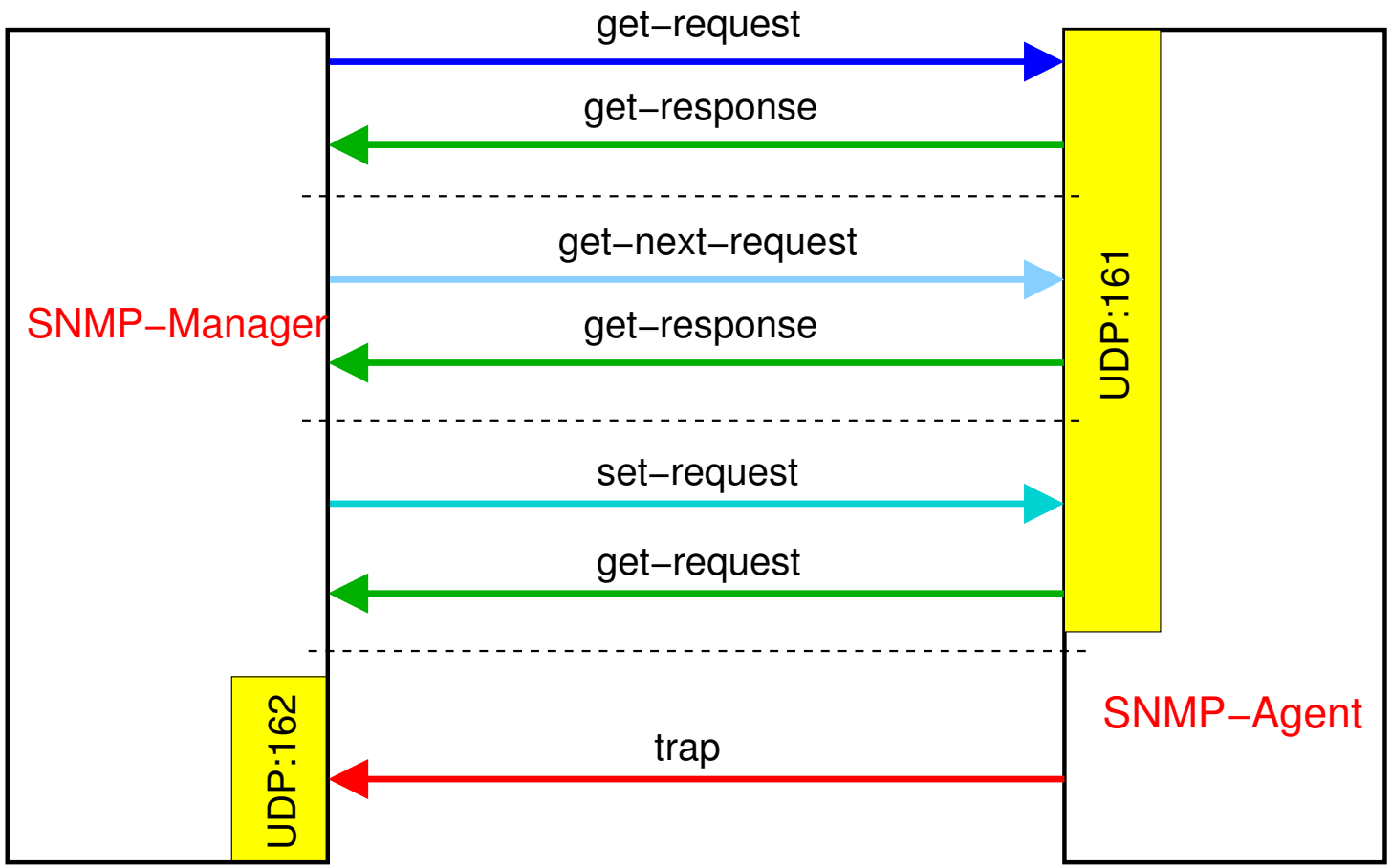
For a PC you can built your own protocol (i.e. like Big Brother, Scout).

The more protocols you use, the more stress you'll get (licensing, interfaces, security).

SNMP-Basics (1)

- Message-orientated networking protocol for managing distributed ressources
- SNMPv1: 1988, definition of basic operations
- SNMPv2: ca. 1996, 64Bit-Counters, support of IPX and AppleTalk, locking mechanisms
- SNMPv3: ca. 1999, security-features (i.e. authentication, encryption and better access control)

SNMP-Basics (2)

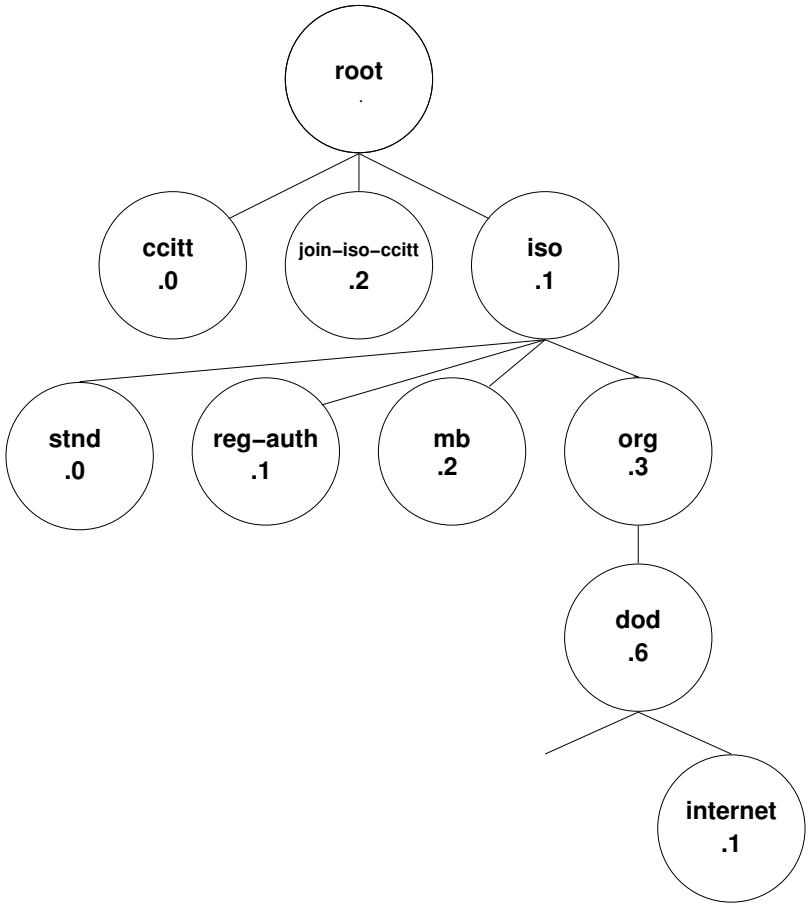


SNMP-Basics (3)

Management Information Bases

- Describe SNMP-Variables, using SMI-syntax
- Hierarchically structured
- Numerical and alphanumerical notation
- Registration of self made MIB's at IANA (`www.iana.org`

SNMP-Basics (4)




```
iso.org.dod.internet = .1.3.6.1
```

Management-Tools

- NetSNMP
- cheops
- cricket
- scotty/tkinet
- mrtg
- nagios

NetSNMP (1)

- Former UCD-SNMP
- Supports trend-setting featueres (SNMPv3, Kerberos,...)
- SNMP- and SNMP-Trap Agent
- management-tools
- SNMP Agent-API, C Library, Perl Modules
- Efficient UCD/NetSNMP-MIB
- Runs on Unix, MS Windows

NetSNMP (2)

NetSNMP-Agent

- Access control with VACM and USM
- Support of PC specific MIB2-Variables
- UCD/NetSNMP MIB for extended features (load, memory-usage, script-output etc.)
- Easy implementation of self implemented plugins (statically and dynamically loadable)

NetSNMP (3)

Management-Tools (command-line)

- snmptranslate - Management of different OID-Notations
- snmpget - Requests for single MIB-Variables
- snmpwalk - Browsing the MIB-Trees
- snmptable - Displaying tables
- snmptrap - Sending traps

...

scotty/tkined (1)

- Open Source Framework for Network-Management
- TCL based

TNM TCL-Extensions

- Extensions for accessing network ressources
- TCL-API for SNMP (v1 and v2, v3 soon)
- Functions for diagnosis of network services (ICMP, DNS, ...)
- Base for self implemented Management-Applications (syslog interface, netdb)

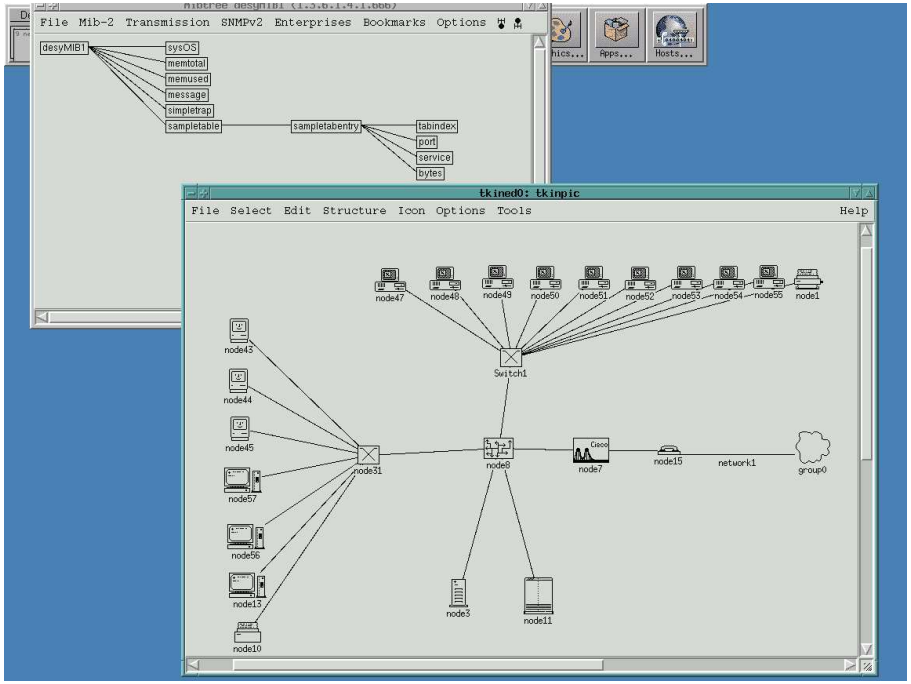
scotty/tkined (2)

tkined

- GUI-Tool for Network-Overview and -Monitoring
- Monitoring of availability and ressource usage
- Diagnosis und frontend for network services
- MIB-Browser
- Continuous or static SNMP-Monitor
- Own extensions, using TNM, possible

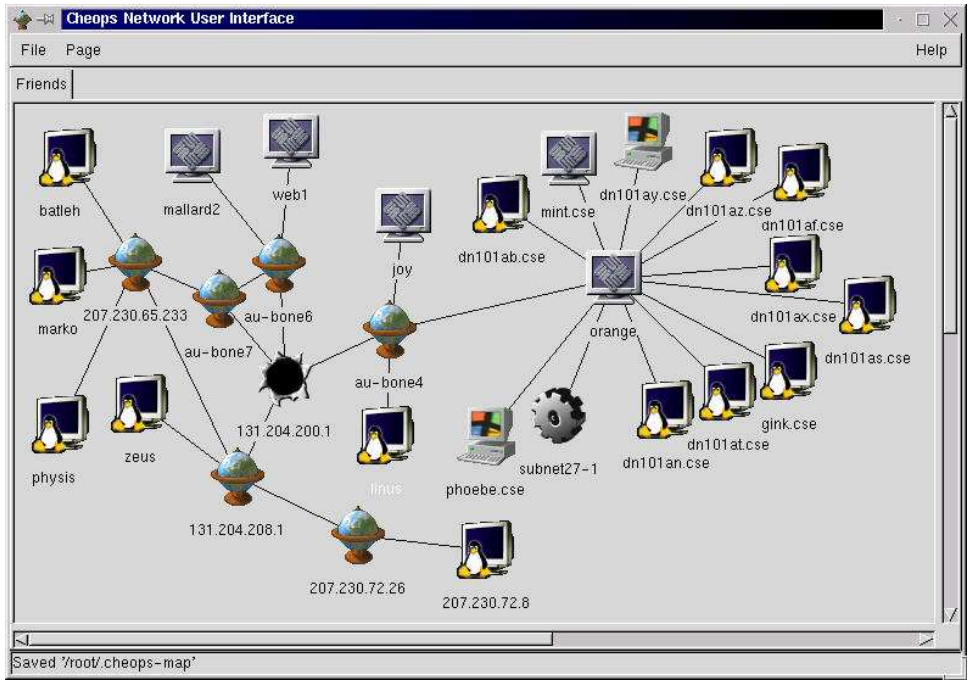
scotty/tkined (3)

- Comfortable GUI for designing graphical overviews



cheops

- Based on (old) GTK, uses NetSNMP-API
- Functionset similar to tkinetd

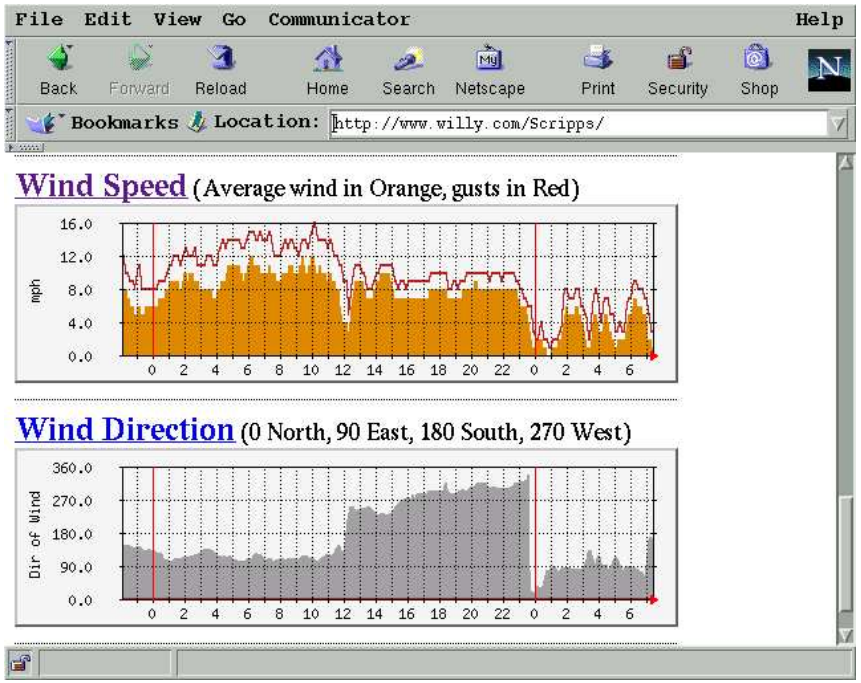


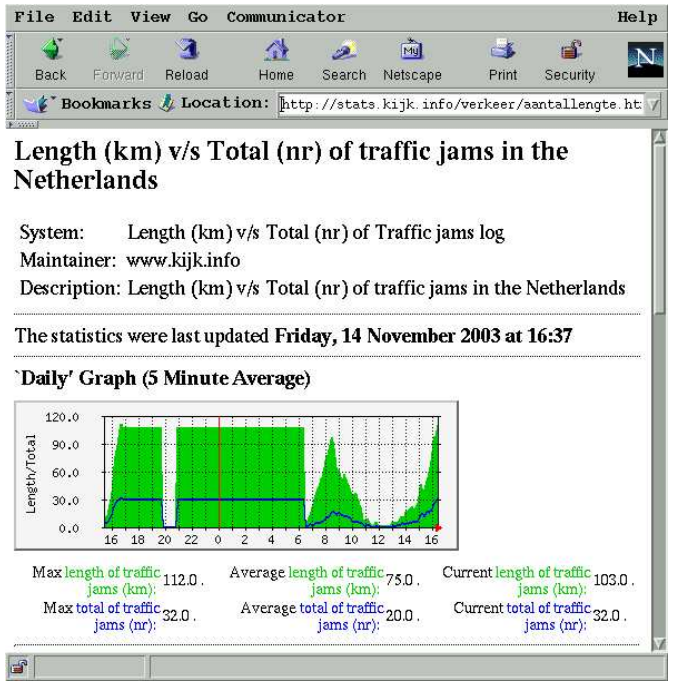
mrtg (1)

- Multi Router Traffic Grapher
- Runs on Unix and MS Windows
- Creates graphics for time-based trend views
- Output of HTML-Code, GIF- or PNG-Graphics
- Own SNMP-Implementation (v2)
- Datenbases are Round Robin Databases (RRD)
- CGI-API uses Embedded Perl

mrtg (2)

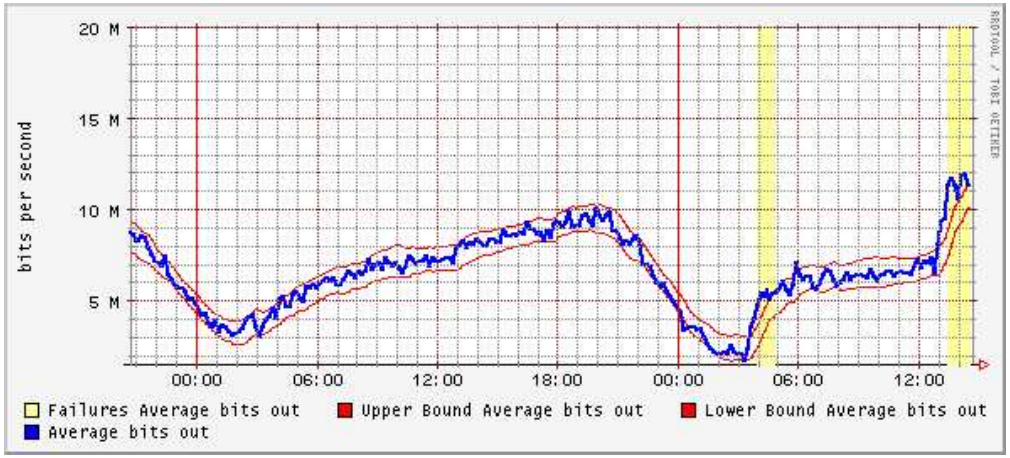
- Formerly used for network statistics
- Monitoring of any other data is possible





cricket

- Functionset like mrtg
- Better Performance
- Creates more complex graphics

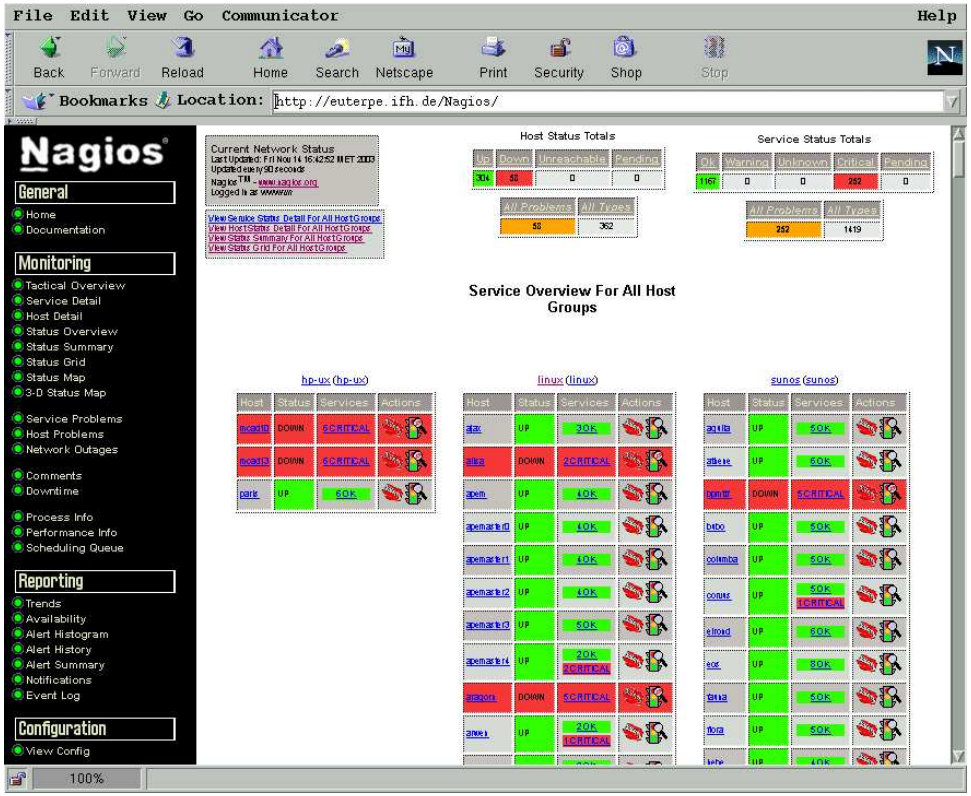


nagios (1)

- Complex Network-, Host- and Service-Monitoring
- Open Source (GPL)
- Formerly known as ”netsaint”
- Web-GUI with extensive statistics and diagrams
- Core only consists of Report-Engine
- Tests are implemented as Plugins
- API for implementing own Plugins

nagios (2)

nagios is already in use at DESY Zeuthen:



http://euterpe.ifh.de/Nagios

Summary (1)

- SNMP is a powerful, open Management-Protocol.
- (Serious) security-features can only be found in SNMPv3.
- Version 3 is not supported by every application.
- Integration into own solutions (i.e. SSH-Tunnel) is an alternative.

Summary (2)

- A lot of existing Monitoring-Tools
- Implementation of custom-made solutions using API's (C, Perl, Java, TCL,...) is not so difficult.
- Realization of own MIB's is no problem

Ressourcen

- www.net-snmp.org
- www.mrtg.org, www.rrdtool.org
- cricket.sourceforge.net
- wwwhome.cs.utwente.nl/~schoenw/scotty/
- www.marko.net/cheops/
- www.nagios.org, euterpe.ifh.de/Nagios/
- Feedback to stephan.knabe@desy.de

Draft of an integrated Network-Monitoring-Solution

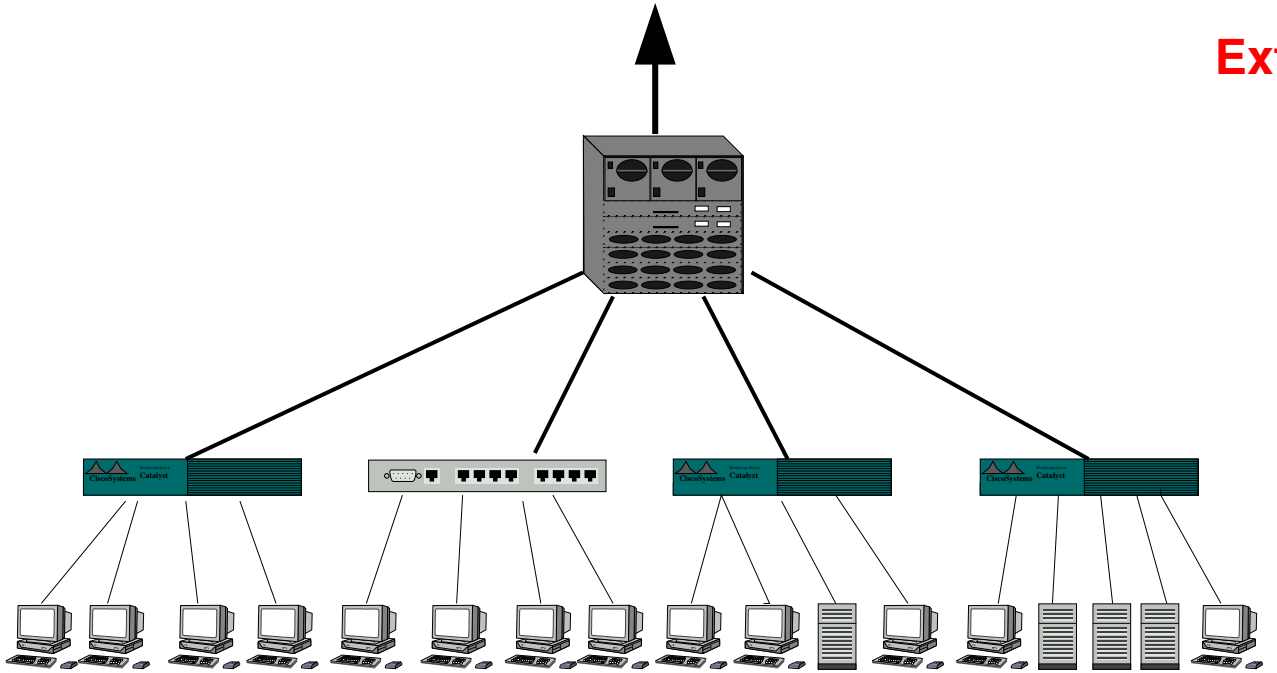
Stephan Knabe
Student at Hochschule Harz, Wernigerode
Diploma Student at DESY Zeuthen, DV group
stephan.knabe@desy.de

26. November 2003

The actual situation

- At this time, there is no efficient system for monitoring network traffic on OSI-Layer 3 and above.
- The objective is, to get and visualize traffic data in a mid-size time frame.
- Points of interest are on OSI-Layer 3, 4 and 5.

The Environment



Externer Zugang

Router

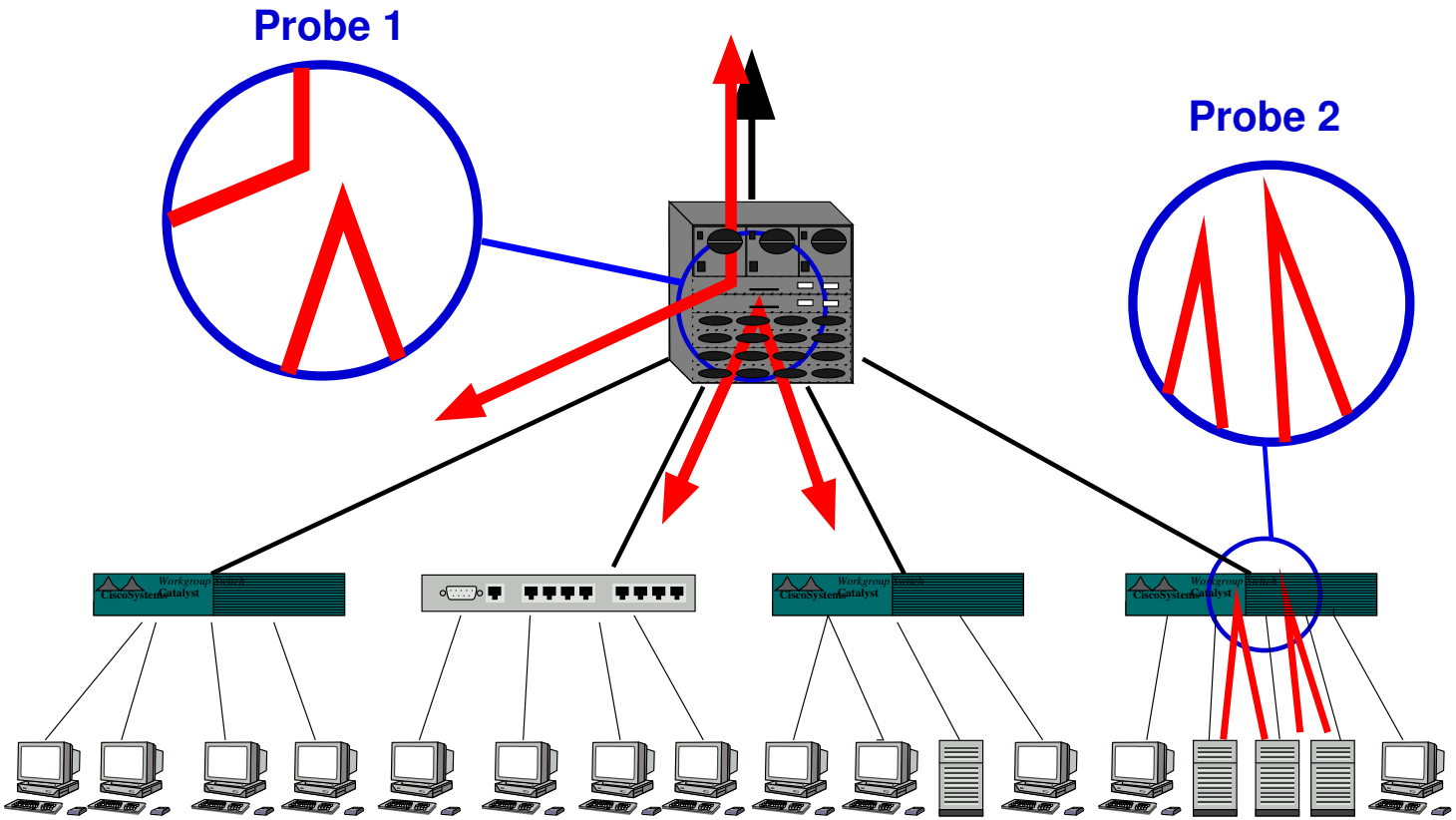
Switches

Workgroups

Using of Switches allows no central probe.

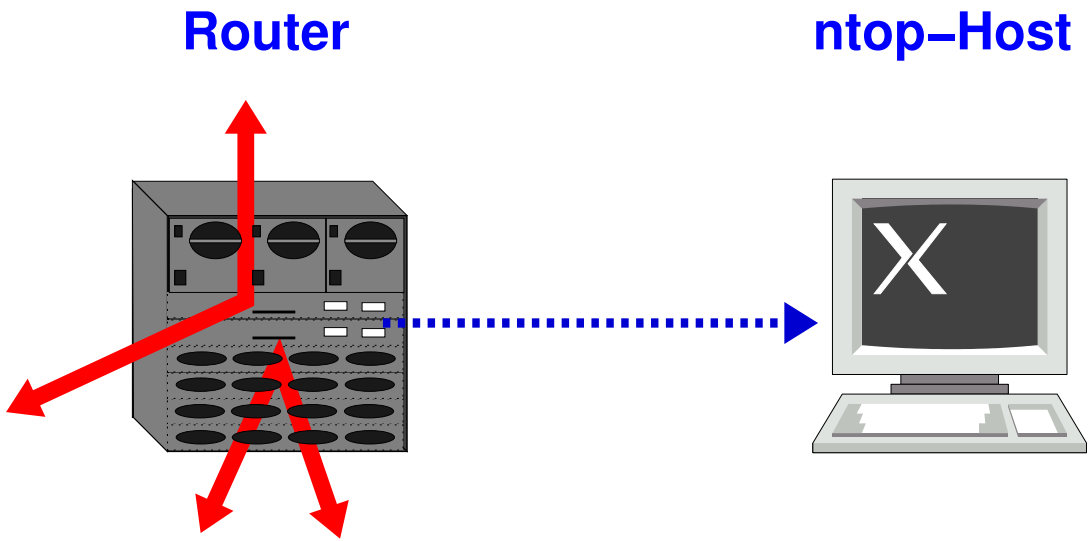
The Environment

We'll concentrate on spotting two points:



Probe 1

- Installation of a Mirror-Port
- Traffic from and into workgroups will be registered
- Data-Processing using ntop



Probe 2

- Port-Mirroring is impossible, because of technical reasons
- Switching on terminal-level allows no sub-probes
- Local probing with transmission of data to a central institution

Accounting using netFlow

netFlow gives us detailed connection information:

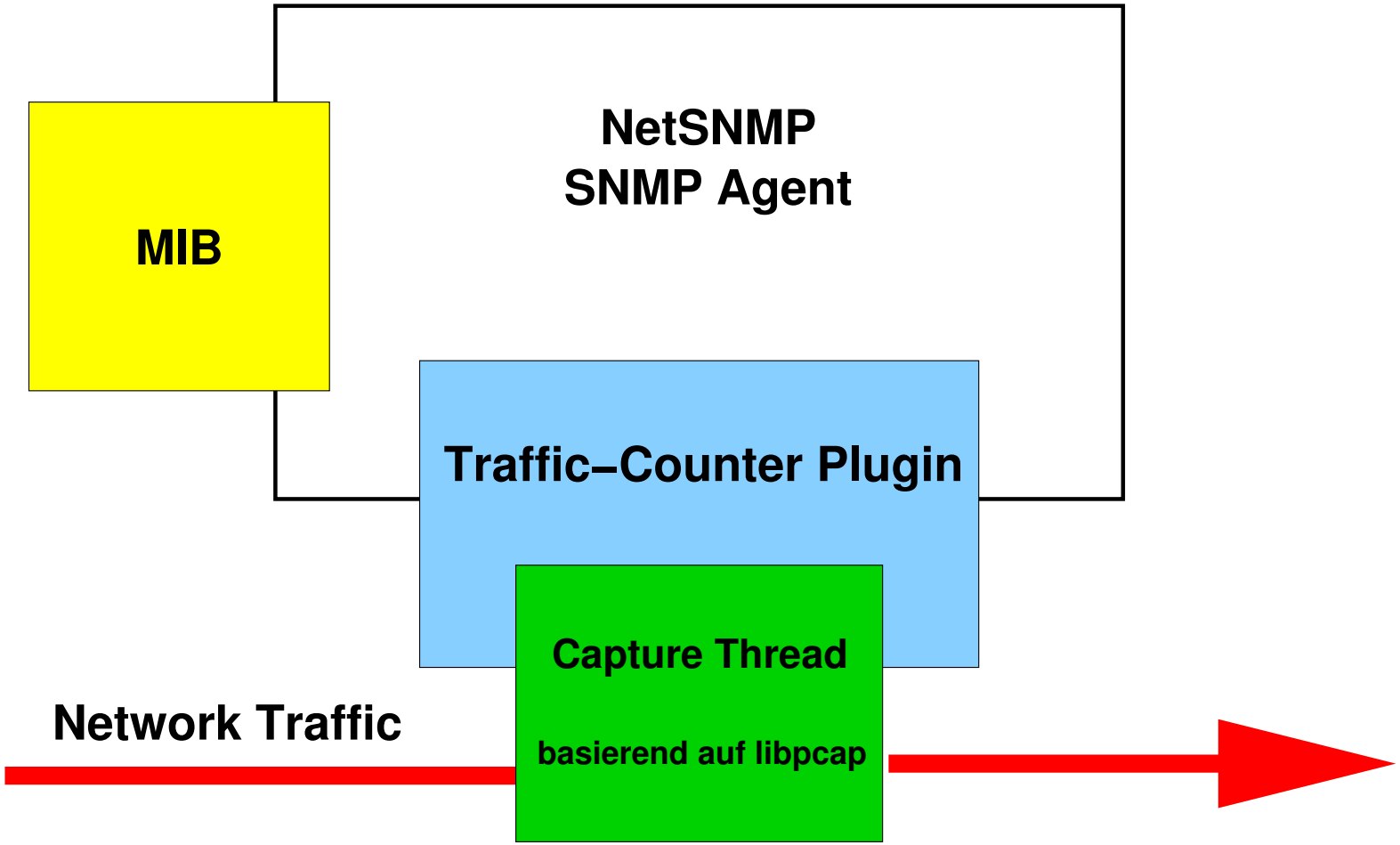
- Source- and destination address
- ULP, source and destination port
- Timestamp for opening and closing of a connection
- Transfered data volume

This results in an additional volume of network traffic.

Polling of SNMP Variables

- Within a workgroup, our interest is mostly on traffic volume and protocol distribution
- Traffic can be captured at the local network interface
- A local SNMP Agent will provide the traffic information
- Polling, storage and visualisation will be done by a central management-application

Design of the local SNMP Agent



Ressources

- www.ntop.org
- www.net-snmp.org
- www.tcpdump.org
- Feedback to stephan.knabe@desy.de

The End

Thanks for attending

Feedback is very much appreciated:

stephan.knabe@desy.de

The slides were made using LaTeX and seminar.sty.