

Netzwerkmanagement mit Linux und Open Source Werkzeugen



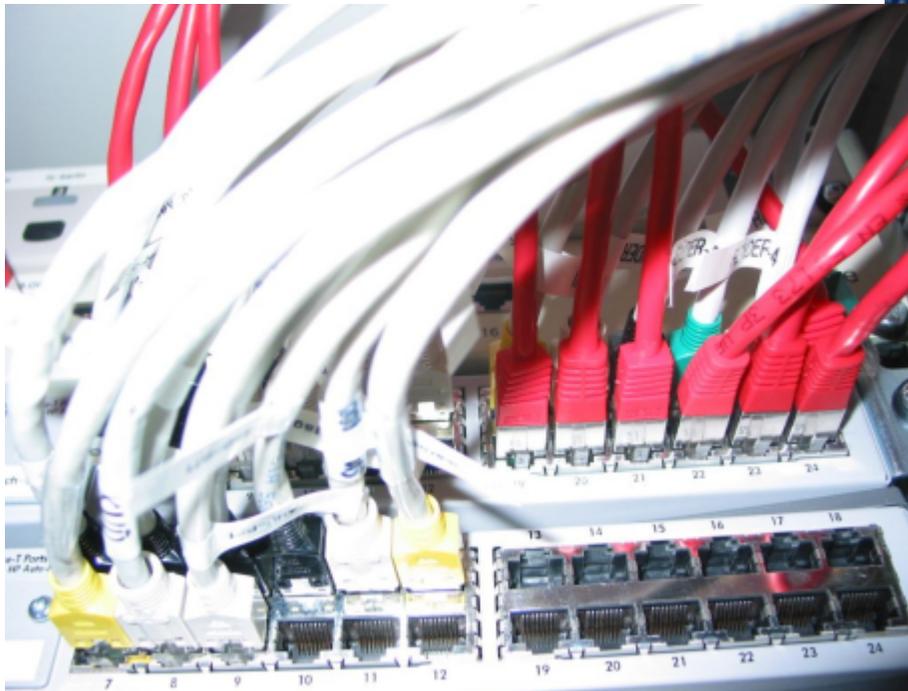
Wilhelm Dolle
Director Information Technology
interActive Systems GmbH



22. Oktober 2004, Berlin

Agenda

- **Netzwerküberwachung /
Netzwerkmanagement**
- **Nagios**
- **MRTG**
- **Ethereal**
- **ntop**



- **Andere Werkzeuge**
- **Fazit**

Wozu Netzwerküberwachung?

- **Status Quo von Netzwerk, Rechnern und Diensten**
- **Frühzeitige Warnungen, evtl. noch vor Ausfällen**
- **Entlastung der Administratoren durch automatische Überwachung**
- **Analyse von Unregelmäßigkeiten (Einbrüche, Fehlkonfigurationen, Hard-/Softwaredefekten, ...)**
- **Erkennen von langfristigen Trends**

Netzwerküberwachung und Geschäftsziele

- **Gewährleistung des reibungslosen und kontinuierlichen Betriebs des IT-Systems**
- **Verantwortliche sollten Probleme vor den Anwendern / Kunden erkennen können**
- **Kontrolle von SLA's (Service Level Agreements)**
- **Rechtzeitig Engpässe in der Infrastruktur erkennen und beheben**

Was kann / sollte man überwachen?

- Raumüberwachung (Temperatur, Feuchte, etc.)
- Computerhardware
- Peripherie (Drucker, TK, ...)
- Betriebssystem (RAM, Plattenplatz, Performance, ...)
- Middleware / Datenbanken
- Infrastrukturdienste (Routing, DNS, DHCP, ...)
- Anwendungen / Dienste

- Erste Releases als NetSaint (1999-2002)
- Namenskollision mit Security-Scanner NetSaint
- 2002 mit Version 1.0b6 in Nagios umbenannt (network + hagos, griechisch für heilig)
- Aktuelles Release: Nagios 1.2 (2.0 angekündigt)
- Logo und Name geschützt (Autor: Ethan Galstad)
- Lizenz: GNU GPL 2
- Homepage: <http://www.nagios.org>

- **Überwachungssystem für Server und Dienste**
- **Entwickelt für Linux und läuft auf Unix-Systemen**
- **Beliebige Zielplattformen überwachbar**
- **Flexible Benachrichtigungsfunktionen**
- **Plugin-Architektur**
- **Webinterface zur Präsentation und Bedienung**

- Keine vordefinierten Service Checks
- Konfiguration nicht webbasiert und schlecht skalierbar
- Relativ umfangreiche Konfigurationsdateien
- Konfigurationshilfen verfügbar (NagMIN, Nagat, NaWui)

- **Webinterface, Logdateien (automatisch rotiert)**
- **Konfiguration über Textdateien**
- **Scheduling (Zustand überwachter Objekte prüfen)**
 - Host erreichbar (ping)?
 - Plugin starten
 - Rückgabe des Plugins auswerten
 - Andere Datenquellen auswerten
- **Benachrichtigung (nach Host, Service, Kontakt, Zeit, ...) über Skripte per EMail, SMS, Pager, Instant Messaging, ...**
- **Zustandsinformationen werden persistent gehalten**
 - Textdateien (empfohlen)
 - MySQL, PostgreSQL (Fehler in Datenbankschnittstellen)

- **Service Checks als Plugins realisiert**
- **Einfache Erweiterbarkeit**
- **Ausführbares Script oder Binärdatei**
- **Seperates Projekt: nagios-plugins**
- **Kommunikation mit dem Daemon über**
 - Exitcodes (OK, Warning, Critical, Unknown)
 - Kurze Textmeldungen (z.B.
„HTTP CRITICAL: HTTP/1.1 500 Error WebObjects“
oder „DISK WARNING - [36907832 kB (9%) free on
/dev/sda8]“)

- **Linux / Unix**
 - Status von Prozessen
 - Verschiedene Server (NFS, Datenbank, Mail, Samba)
 - Syslog
 - CPU/Speicher/Swap Auslastung
 - Festplattenbelegung

- **Windows**
 - Status von Diensten und Prozessen
 - Uptime
 - Daten des Performance Monitors
 - CPU/Speicher Auslastung
 - Festplattenbelegung

- **„Clientzugriff“ (SSH, FTP, PING, DNS, HTTP(S), SMTP, LDAP, MySQL, Oracle, generisch auf TCP/UDP Ports, ...)**

Nagios®

General

- Home
- Documentation

Monitoring

- Tactical Overview
- Service Detail
- Host Detail
- Status Overview
- Status Summary
- Status Grid
- Status Map
- 3-D Status Map

- Service Problems
- Host Problems
- Network Outages

- Comments
- Downtime

- Process Info
- Performance Info
- Scheduling Queue

Reporting

- Trends
- Availability
- Alert Histogram
- Alert History
- Alert Summary
- Notifications
- Event Log

Configuration

- View Config

Nagios®

Copyright (c) 1999-2004 Ethan Galstad

Version 1.2

February 02, 2004

New Installations:

If you have just installed Nagios®, read the [documentation](#) for instructions on getting everything up and running.

Click [here](#) for a brief overview of new features that have been added in this release.

For More Information:

Visit the Nagios homepage at <http://www.nagios.org> for information on bug fixes, upgrades, support, etc.



Nagios and the Nagios logo are registered trademarks of Ethan Galstad.

Nagios is provided AS IS with NO WARRANTY OF ANY KIND, INCLUDING THE WARRANTY OF DESIGN, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE.

Nagios – Tactical Overview

Nagios®

Tactical Monitoring Overview

Last Updated: Thu Oct 21 21:11:52 CEST 2004
Updated every 90 seconds
Nagios® - www.nagios.org
Logged in as *wf*

Monitoring Performance

Check Execution Time: 0 / 16 / 3.435 sec
Check Latency: 0 / 14 / 5.022 sec
Active Checks: 186
Passive Checks: 0

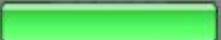
Network Outages

2 Outages

2 Blocking Outages

Network Health

Host Health: 

Service Health: 

Hosts

2 Down

0 Unreachable

72 Up

0 Pending

2 Unhandled Problems

Services

0 Critical

1 Warning

0 Unknown

185 Ok

0 Pending

1 Acknowledged

Monitoring Features

	Flap Detection	Notifications	Event Handlers	Active Checks	Passive Checks
Disabled	N/A	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled	Enabled All Services Enabled All Hosts Enabled	Disabled N/A

Nagios – Status Details



Current Network Status

Last Updated: Thu Oct 21 21:19:35 CEST 2004
 Updated every 90 seconds
 Nagios® - www.nagios.org
 Logged in as wdf

[View History For all hosts](#)
[View Notifications For All Hosts](#)
[View Host Status Detail For All Hosts](#)

Host Status Totals

Up	Down	Unreachable	Pending
72	2	0	0

All Problems	All Types
2	74

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
185	1	0	0	0

All Problems	All Types
1	186

Service Status Details For All Hosts

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑↓	Attempt ↑↓	Status Information
EuroPa-pf1	https-Zertifikat	OK	21-10-2004 21:17:37	1d 13h 51m 3s	1/3	Certificate will expire on 05/18/2006 14:1.
	https-proxy	OK	21-10-2004 21:18:32	1d 13h 53m 23s	1/3	HTTP ok: HTTP/1.1 200 OK - 0.612 second response time
	ssh	OK	21-10-2004 21:17:22	1d 13h 51m 53s	1/3	SSH ok - OpenSSH_3.9p1 (protocol 2.0)
EuroPa-pf2	https-proxy	OK	21-10-2004 21:18:27	1d 13h 50m 53s	1/3	HTTP ok: HTTP/1.1 401 Authorization Required - 0.489 second response time
EuroPa-sun	WebObjects (AdminTool)	OK	21-10-2004 21:18:37	1d 13h 52m 33s	1/3	HTTP ok: HTTP/1.1 200 Apple - 0.638 second response time
	WebObjects (AdminTool-Training)	OK	21-10-2004 21:18:37	1d 13h 51m 23s	1/3	HTTP ok: HTTP/1.1 200 Apple - 0.557 second response time
	WebObjects (DataCapture)	OK	21-10-2004 21:18:37	0d 19h 19m 33s	1/3	HTTP ok: HTTP/1.1 200 Apple - 0.565 second response time
	WebObjects (DataCapture-Training)	OK	21-10-2004 21:18:37	0d 19h 19m 33s	1/3	HTTP ok: HTTP/1.1 200 Apple - 0.590 second response time
	WebObjects (FormBuilder)	OK	21-10-2004 21:19:22	1d 13h 50m 58s	1/3	HTTP ok: HTTP/1.1 200 Apple - 0.529 second response time
	WebObjects (FormBuilder-Training)	OK	21-10-2004 21:18:37	1d 13h 50m 53s	1/3	HTTP ok: HTTP/1.1 200 Apple - 0.584 second response time
	WebObjects (RecruitmentTool)	OK	21-10-2004 21:18:51	1d 13h 52m 23s	1/3	HTTP ok: HTTP/1.1 200 Apple - 0.691 second response time

Nagios – Host Groups

Nagios®

DMZ der iAS in Berlin (DMZbln)

Host	Status	Services	Actions
bgpd	UP	1 OK	
extFW	UP	1 OK	
fax	UP	2 OK	
hp-switch-02	UP	2 OK	
ias-ipb	UP	1 OK	
ias1	UP	1 OK	
intFW	UP	2 OK	
mail	UP	1 OK	
proxy	UP	3 OK	
sw_dmz	UP	1 OK	
vpn-berlin	UP	1 OK	
web	UP	2 OK	

Drucker im LAN der iAS in Berlin
(Intranet-Berlin-Drucker)

Host	Status	Services	Actions
epson	UP	1 OK	
hp-black	UP	1 OK	
hp-color	UP	1 OK	
hp-lj2300	UP	1 OK	

Raids im LAN der iAS in Berlin
(Intranet-Berlin-raids)

Host	Status	Services	Actions
raid-bn	UP	1 OK	
raid-bne	UP	1 OK	

Server im LAN der iAS in Berlin
(Intranet-Berlin-server)

Host	Status	Services	Actions
cvs-berlin	UP	2 OK	
dc-berlin	UP	1 OK	
fs-berlin	UP	3 OK 1 WARNING	
intFW	UP	2 OK	

Nagios – Status Map

Nagios®

 **Render Slave**

Name: render4
Alias: render4.brainmedia.de
Address: 192.168.101.34
State: Up
Status Information: FPING OK - 192.168.101.34 (loss=0.000000%, rta=0.270000 ms)
State Duration: 7d 12h 39m 55s
Last Status Check: 20-10-2004 21:18:27
Last State Change: 14-10-2004 08:52:54
Parent Host(s): sw2
Immediate Child Hosts: 0

Services:
- 2 ok

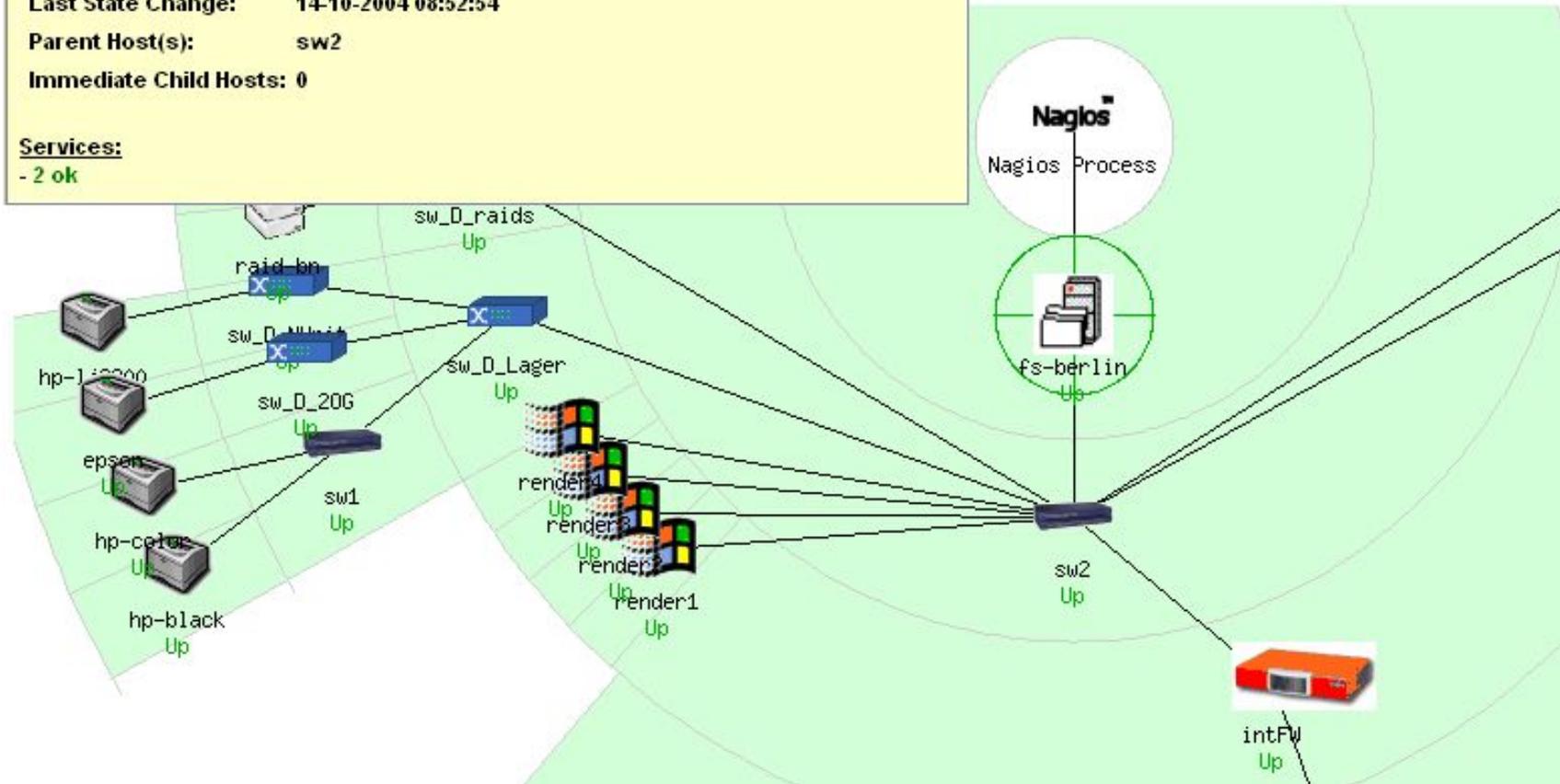
Method: (Marked Up) ▾

Layers:
IAS in Berlin
LAN der iAS in Berlin
Rechner LAN der iAS in Berlin
LAN der iAS in Berlin

Scaling factor: 0.0

Layer mode:
 Include
 Exclude

Buttons: Update



Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	6d 23h 42m 49s	99.830%	99.830%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	6d 23h 42m 49s	99.830%	99.830%
DOWN	Unscheduled	0d 0h 17m 11s	0.170%	0.170%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 17m 11s	0.170%	0.170%
UNREACHABLE	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	7d 0h 0m 0s	100.000%	100.000%

State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
KKS-AdminTool	99.859% (99.859%)	0.000% (0.000%)	0.000% (0.000%)	0.141% (0.141%)	0.000%
KKS-DataCapture	99.808% (99.808%)	0.000% (0.000%)	0.000% (0.000%)	0.192% (0.192%)	0.000%
KKS-ExportTool	99.808% (99.808%)	0.000% (0.000%)	0.000% (0.000%)	0.192% (0.192%)	0.000%
KKS-FormBuilder	99.884% (99.884%)	0.000% (0.000%)	0.000% (0.000%)	0.116% (0.116%)	0.000%
STP-AdminTool	99.883% (99.883%)	0.000% (0.000%)	0.000% (0.000%)	0.117% (0.117%)	0.000%
STP-DataCapture	99.808% (99.808%)	0.000% (0.000%)	0.000% (0.000%)	0.192% (0.192%)	0.000%
STP-ExportTool	99.854% (99.854%)	0.000% (0.000%)	0.000% (0.000%)	0.146% (0.146%)	0.000%
STP-FormBuilder	99.859% (99.859%)	0.000% (0.000%)	0.000% (0.000%)	0.141% (0.141%)	0.000%
https-Zertifikat	99.797% (99.797%)	0.000% (0.000%)	0.000% (0.000%)	0.203% (0.203%)	0.000%

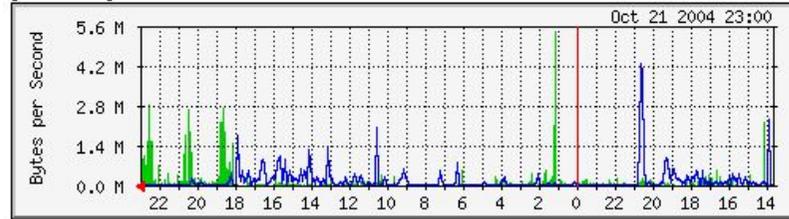
- **Aktive Servicetests (auf einem externen Host wird ein aktiver Test ausgeführt)**
 - Per SSH
 - Per NRPE (Nagios Remote Plugin Executor)
- **Passive Servicetests (externer Host liefert über NSCA-Client Daten an Nagios)**
 - Per NSCA (Nagios Service Check Acceptor)
- **Redundantes Monitoring (zweiter Slave-Nagios überwacht parallel und übernimmt die Benachrichtigung wenn Master down ist)**
- **Failover-Monitoring (Slave überwacht nur Master und beginnt mit kompletter Überwachung wenn Master down ist)**

- **MRTG (Multi Router Traffic Grapher)**
- **Autor: Tobias Oetiker**
- **Erste Version 1994 als Perl-Skript, heute geschwindigkeitsrelevante Teile in C**
- **Aktuelle Version: MRTG 2.10.15**
- **Lizenz: GNU GPL 2**
- **Homepage: <http://www.mrtg.org>**

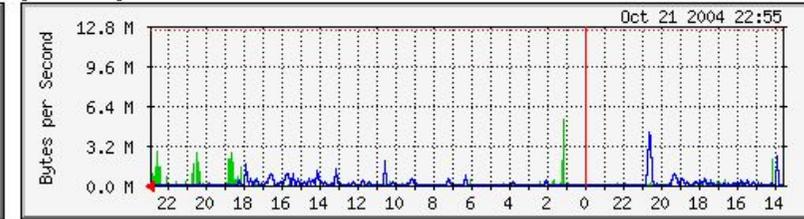
- **Überwacht Auslastung des Netzwerkes**
- **Fragt Daten von Rechnern, Routern und Switches über SNMP ab**
- **Daten in übersichtlichen Graphiken darstellen und in Webseiten einpacken**
- **Zusätzlich: andere Daten wie Festplattenausnutzung und CPU-Belastung abfragen**
- **Benötigt (neben Perl und C-Compiler): GD-, Libpng- und Zlib-Bibliothek**
- **Läuft unter Linux, Unix und Windows**
- **Kann RRD-Tool als Datenbasis benutzen**

MRTG – Überblick Server

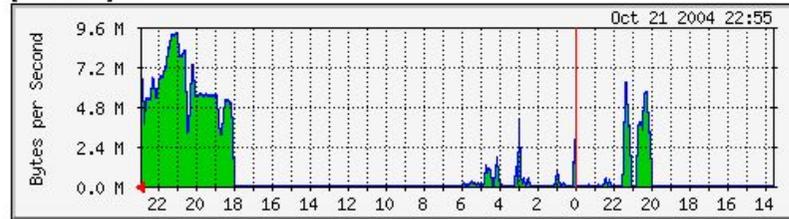
[fs-berlin] eth0



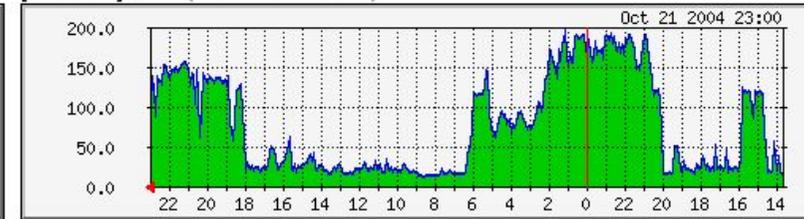
[fs-berlin] eth0 - unscaled



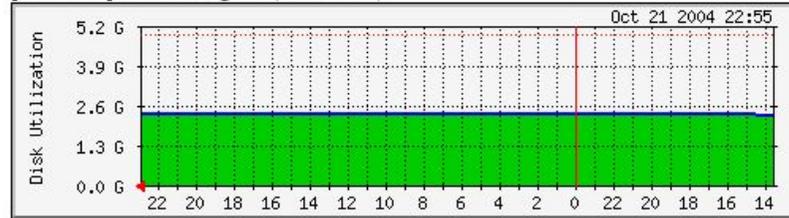
[fs-berlin] lo



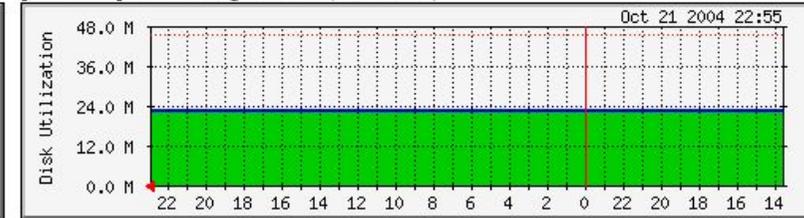
[fs-berlin] CPU (2x PIII 500 MHz)



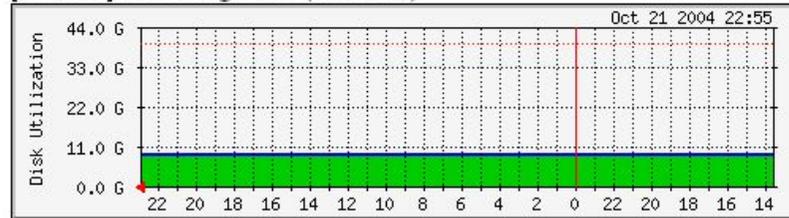
[fs-berlin] Disk Usage: / (/dev/sda2)



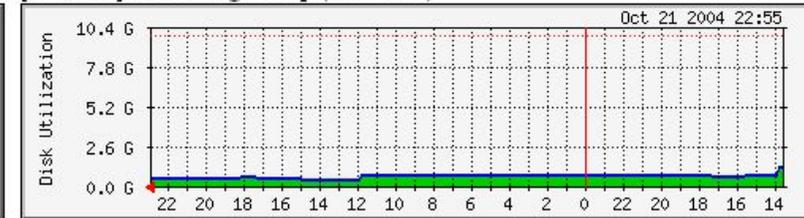
[fs-berlin] Disk Usage: /boot (/dev/sda1)



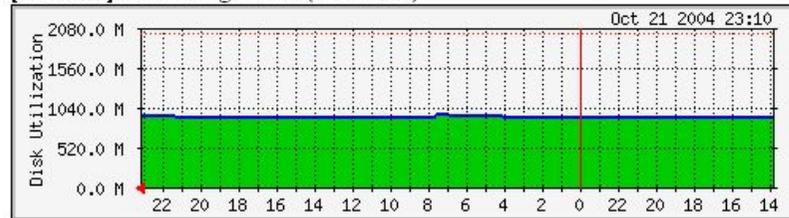
[fs-berlin] Disk Usage: /usr (/dev/sda5)



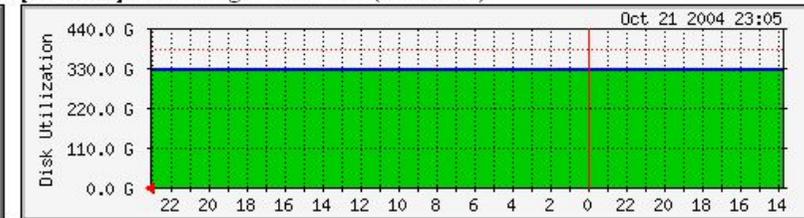
[fs-berlin] Disk Usage: /tmp (/dev/sda6)



[fs-berlin] Disk Usage: /var (/dev/sda7)



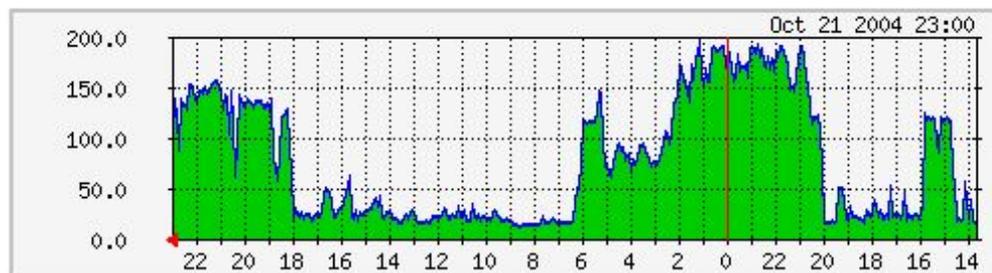
[fs-berlin] Disk Usage: /Network (/dev/sda8)



MRTG – CPU-Auslastung

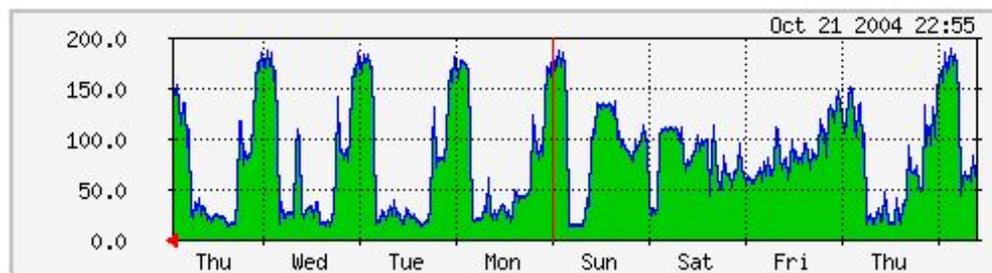
The statistics were last updated **Thursday, 21 October 2004 at 23:00**,
at which time 'fs-berlin' had been up for **11 days, 5:50:26**.

'Daily' Graph (5 Minute Average)



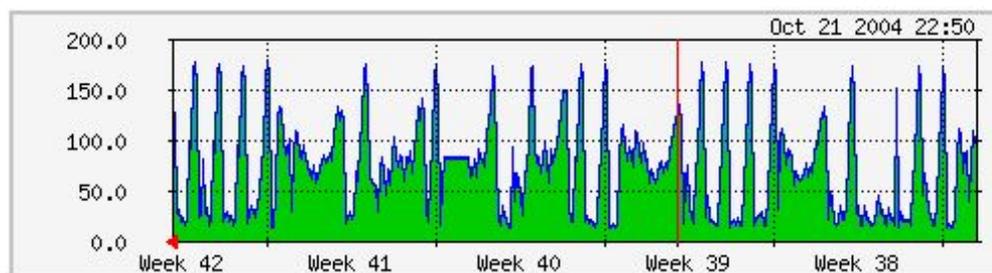
Max CPU Usage 196.0 % (98.0%) Average CPU Usage 78.0 % (39.0%) Current CPU Usage 103.0 % (51.5%)

'Weekly' Graph (30 Minute Average)



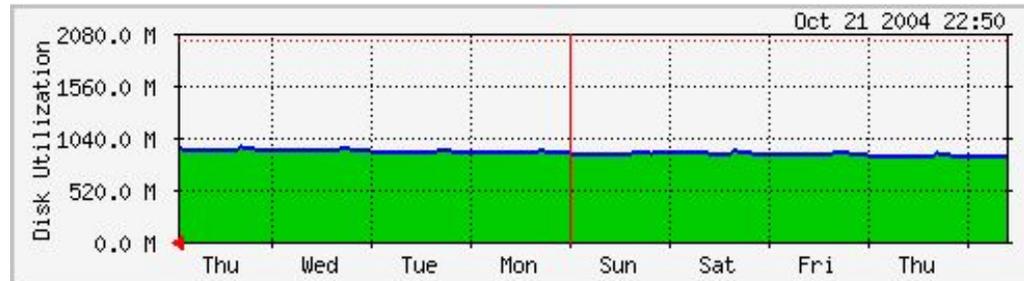
Max CPU Usage 188.0 % (94.0%) Average CPU Usage 80.0 % (40.0%) Current CPU Usage 142.0 % (71.0%)

'Monthly' Graph (2 Hour Average)



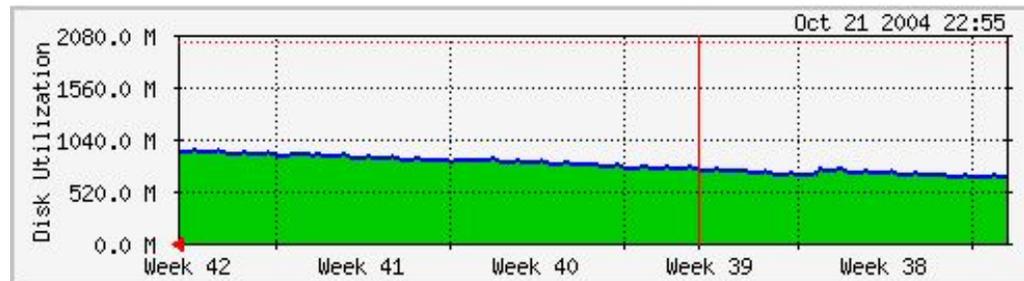
MRTG – Dateisystemauslastung

Weekly' Graph (30 Minute Average)



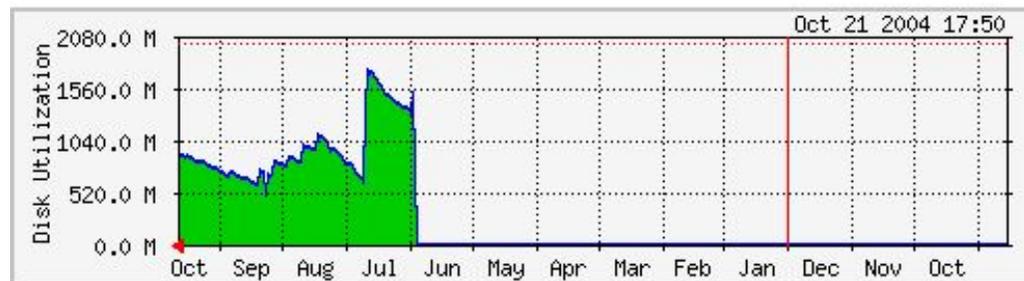
Max size 958.2 M B (47.6%) Average size 900.6 M B (44.7%) Current size 936.2 M B (46.5%)

Monthly' Graph (2 Hour Average)



Max size 951.4 M B (47.2%) Average size 796.4 M B (39.5%) Current size 935.9 M B (46.4%)

Yearly' Graph (1 Day Average)



Max size 1765.3 M B (87.6%) Average size 966.1 M B (47.9%) Current size 925.6 M B (45.9%)

Ethereal - Allgemeines

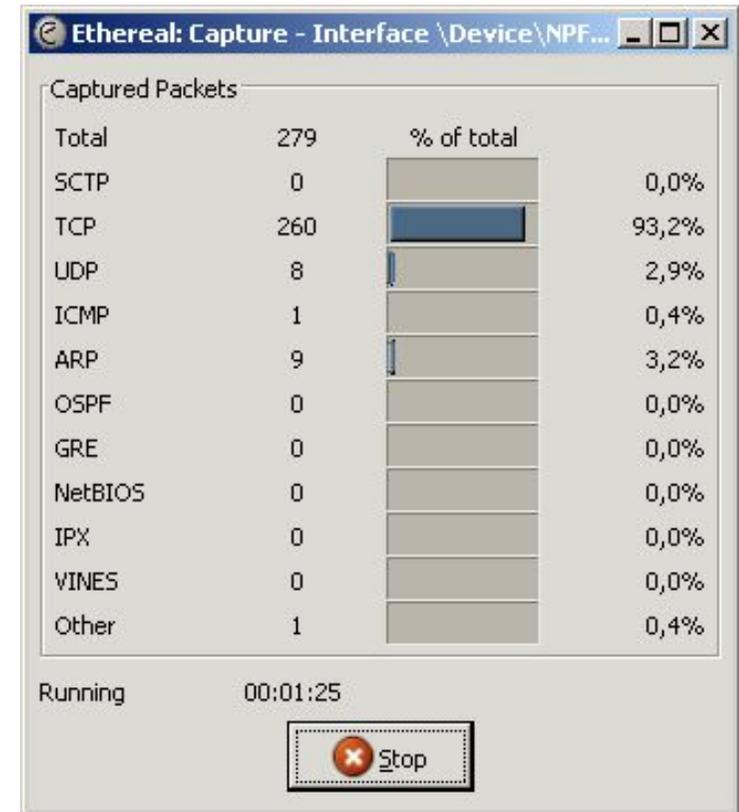


- **Ethereal (Analysewerkzeug für Netzwerkpakete)**
- **Originalautor: Gerald Combs**
- **Aktuelle Version: Ethereal 0.10.17**
- **Lizenz: GNU GPL 2**
- **Homepage: <http://www.ethereal.com>**

Ethereal - Features



- Live-Capture-Funktion
- Einlesen von sehr vielen Capturefile-Formaten, z.B. tcpdump
- Analyse per GUI oder im Textmodus
- Umfangreiche Filterfunktionen
- „Kennt“ zur Zeit 602 Netzwerkprotokolle



Ethereal - Analyse



(Untitled) - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: + Expression... Clear Apply

No. -	Time	Source	Destination	Protocol	Info
19	9.776595	192.168.101.5	Broadcast	ARP	who has 192.168.101.55? Tell 192.168.101.5
20	11.107709	192.168.101.66	194.146.160.1	TCP	4098 > 2000 [SYN] Seq=0 Ack=0 win=65535 Len=0
21	11.108114	194.146.160.1	192.168.101.66	TCP	2000 > 4098 [SYN, ACK] Seq=0 Ack=1 win=5840 Len=0
22	11.108138	192.168.101.66	194.146.160.1	TCP	4098 > 2000 [ACK] Seq=1 Ack=1 win=65535 [CHECKSUM] Len=0
23	11.111370	192.168.101.66	194.146.160.1	TCP	4098 > 2000 [PSH, ACK] Seq=1 Ack=1 win=65535 [CHECKSUM] Len=0
24	11.112012	194.146.160.1	192.168.101.66	TCP	2000 > 4098 [ACK] Seq=1 Ack=482 win=6432 Len=0
25	11.116488	194.146.160.1	192.168.101.66	TCP	2000 > 4098 [PSH, ACK] Seq=1 Ack=482 win=6432 Len=0
26	11.120078	194.146.160.1	192.168.101.66	TCP	2000 > 4098 [ACK] Seq=18 Ack=482 win=6432 Len=0

Frame 20 (62 bytes on wire, 62 bytes captured)

- Ethernet II, Src: 00:04:76:4c:23:5c, Dst: 00:10:4b:68:e3:2b
 - Destination: 00:10:4b:68:e3:2b (192.168.101.1)
 - Source: 00:04:76:4c:23:5c (192.168.101.66)
 - Type: IP (0x0800)
- Internet Protocol, Src Addr: 192.168.101.66 (192.168.101.66), Dst Addr: 194.146.160.1 (194.146.160.1)
 - Version: 4
 - Header length: 20 bytes
 - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
 - Total Length: 48
 - Identification: 0xf040 (61504)
 - Flags: 0x04 (Don't Fragment)
 - Fragment offset: 0
 - Time to live: 128
 - Protocol: TCP (0x06)
 - Header checksum: 0x0000 (incorrect, should be 0x8208)
 - Source: 192.168.101.66 (192.168.101.66)
 - Destination: 194.146.160.1 (194.146.160.1)
- Transmission Control Protocol, Src Port: 4098 (4098), Dst Port: 2000 (2000), Seq: 0, Ack: 0, Len: 0
 - Source port: 4098 (4098)
 - Destination port: 2000 (2000)
 - Sequence number: 0 (relative sequence number)
 - Header length: 28 bytes
 - Flags: 0x0002 (SYN)
 - window size: 65535
 - Checksum: 0x0c1f (correct)
 - Options: (8 bytes)

```
0000 00 10 4b 68 e3 2b 00 04 76 4c 23 5c 08 00 45 00  ..Kh.+.. vL#\..E.
0010 00 30 f0 40 40 00 80 06 00 00 c0 a8 65 42 c2 92  .0.@... ..eB..
0020 a0 01 10 02 07 d0 45 46 91 69 00 00 00 00 70 02  .....EF .i....p.
0030 ff ff 0c 1f 00 00 02 04 05 b4 01 01 04 02  .....
```

Internet Protocol (ip), 20 bytes | P: 502 D: 502 M: 0

Ethereal – Analyse (Follow Stream)



The screenshot displays the Ethereal network analysis tool interface. The main window shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Info. The selected packet (No. 2) is expanded to show its detailed structure, including Ethernet II, Internet Protocol (IP), and Transmission Control Protocol (TCP) layers. The TCP layer details show a sequence number of 0, acknowledgment number of 0, and flags for PSH and ACK.

No.	Time	Source	Destination	Protocol	Info
2	7.142678	192.168.101.66	195.37.132.70	TELNET	Telnet Data ...
3	7.142749	192.168.101.66	195.37.132.70	TELNET	Telnet Data ...
4	7.156731	195.37.132.70	192.168.101.66	TCP	telnet > 2443 [ACK] Seq=0 Ack=4 win=11792 Len=...
5	7.156888	195.37.132.70	192.168.101.66	TCP	telnet > 2443 [ACK] Seq=0 Ack=6 win=11792 Len=...
6	7.391535	195.37.132.70	192.168.101.66	TELNET	Telnet Data ...
7	7.538283	192.168.101.66	195.37.132.70	TCP	2443 > telnet [ACK] Seq=6 Ack=1024 win=64273 [c...
8	7.555493	195.37.132.70	192.168.101.66	TELNET	Telnet Data ...
9	7.738807	192.168.101.66	195.37.132.70	TCP	2443 > telnet [ACK] Seq=6 Ack=1633 win=65535 [c...
10	7.897268	192.168.101.66	195.37.132.70	TELNET	Telnet Data ...

Frame 2 (58 bytes on wire, 58 bytes captured)
Ethernet II, Src: 00:04:76:4c:23:5c, Dst: 00:10:4b:68:e3:2b
Destination: 00:10:4b:68:e3:2b (192.168.101.1)
Source: 00:04:76:4c:23:5c (192.168.101.66)
Type: IP (0x0800)
Internet Protocol, Src Addr: 192.168.101.66 (192.168.101.66), Dst Addr: 195.37.132.70 (195.37.132.70)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
Total Length: 44
Identification: 0xf018 (61464)
Flags: 0x04 (Don't Fragment)
Fragment offset: 0
Time to live: 128
Protocol: TCP (0x06)
Header checksum: 0x0000 (incorrect, should be 0x9d5c)
Source: 192.168.101.66 (192.168.101.66)
Destination: 195.37.132.70 (195.37.132.70)
Transmission Control Protocol, Src Port: 2443 (2443), Dst Port: telnet (23), Seq: 0, Ack: 0, Len: 4
Source port: 2443 (2443)
Destination port: telnet (23)
Sequence number: 0 (relative sequence number)
[Next sequence number: 4 (relative sequence number)]
Acknowledgement number: 0 (relative ack number)
Header length: 20 bytes
Flags: 0x0018 (PSH, ACK)
window size: 65297
checksum: 0x6d75 (incorrect, should be 0x20bb)

```
0000 00 10 4b 68 e3 2b 00 04 76 4c 23 5c 08 00 45 00  ..Kh+. .vL#\..E.
0010 00 2c f0 18 40 00 80 06 00 00 c0 a8 65 42 c3 25  ....@... ..eB.%
0020 84 46 09 8b 00 17 63 cd be 68 39 7b d1 76 50 18  .F....c. .h9{.vP.
0030 ff 11 6d 75 00 00 76 6f 6c 6b                    ..mu..vo lk
```

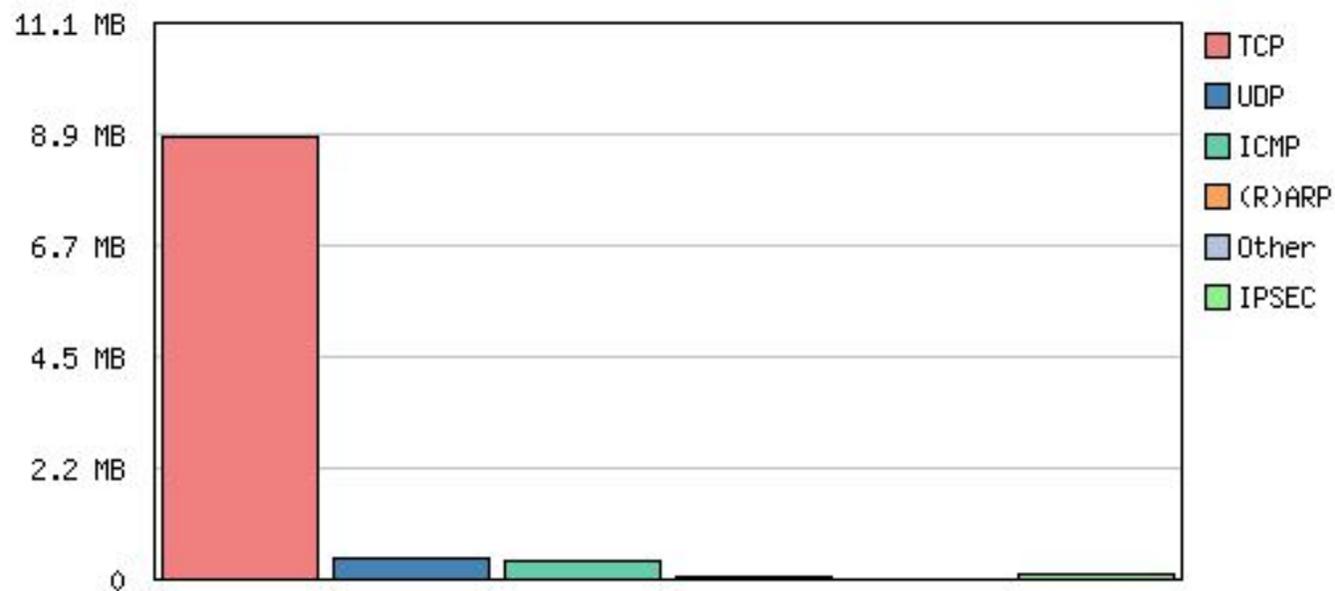
ntop - Allgemeines

- ntop (Überwacht Netzwerkauslastung)
- Autor: Luca Deri
- Aktuelle Version: ntop 3.0
- Lizenz: GNU GPL 2
- Homepage: <http://www.ntop.org>

ntop – Traffic-Analyse

Global Protocol Distribution

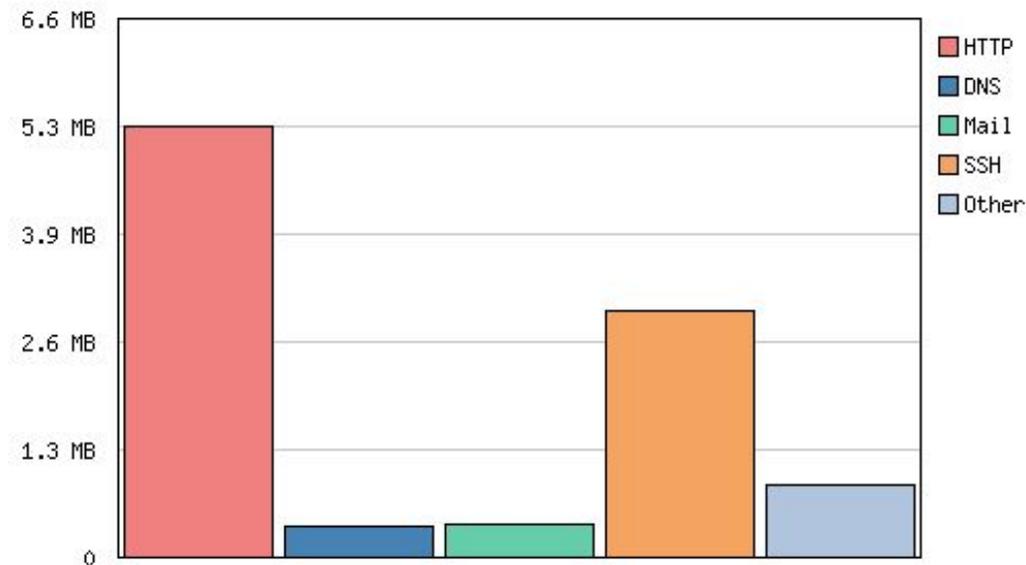
Protocol	Data	Percentage				
		Protocol	Data	Percentage	Visual	
IP	9.9 MB	98.8%	TCP	8.9 MB	90%	
			UDP	462.0 KB	4%	
			ICMP	395.3 KB	3%	
			IPSEC	156.1 KB	1%	
(R)ARP	85.9 KB	0%				
Other	9.3 KB	0%				



ntop – Traffic-Analyse

Global TCP/UDP Protocol Distribution

TCP/UDP Protocol	Data	Percentage
FTP	10.6 KB	0%
HTTP	5.3 MB	52%
DNS	405.9 KB	3%
Telnet	16.6 KB	0%
NBios-IP	8.6 KB	0%
Mail	426.8 KB	4%
SSH	3.0 MB	30%
Messenger	0.6 KB	0%
Other TCP/UDP-based Protocols	880.3 KB	8%



Andere Werkzeuge (Sicherheit)

- Nessus (Schwachstellenscanner)



- Snort (Intrusion Detection)



- Snort Inline (Intrusion Prevention)



- Nmap (Portscanner)



Fazit

- **Netzwerküberwachung und –management ist unter Linux mit Open Source Werkzeugen machbar**
- **Eine ganzheitliche Lösung muss / kann aus mehreren Einzelteilen bestehen**
- **Leistung und Konfigurationsmöglichkeiten stehen nicht hinter kommerziellen Systemen zurück**
- **Einheitlichkeit und Bequemlichkeit der Konfiguration ist oft deutlich schlechter und muss häufig mit externen Komponenten erledigt werden**

Diskussion

Vielen Dank für das Interesse!

**Wilhelm Dolle
Director Information Technology**

**iAS interActive Systems GmbH
Dieffenbachstrasse 33c
D-10967 Berlin**

**fon +49(0)30 69 004 - 100
fax +49(0)30 69 004 - 101
mail wilhelm.dolle@interActive-Systems.de
web http://www.interActive-Systems.de**