Nagios

- http://www.nagios.org/
- an enterprise-class network and server monitoring system.
- Useful for:
  - Monitoring of network services.
  - Monitoring of host resources (processor load, disk usage, system logs)
  - Contact notifications when service or host problems occur and get resolved (via e-mail, SMS).
  - You can define event handlers that execute when triggered by certain events. (Proactive problem resolution)

Nagios

Nagios®

General
- Home
- Documentation

Monitoring
- Tactical Overview
- Service Detail
- Host Detail
- Hostgroup Overview
- Hostgroup Summary
- Hostgroup Grid
- Servicegroup Overview
- Servicegroup Summary
- Servicegroup Grid
- Status Map
- 3-D Status Map
- Service Problems
  - Unhandled
- Host Problems
  - Unhandled
- Network Outages

Show Host:

- 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) 1999-2008 Ethan Galstad

Version 3.0rc1
December 17, 2007
Read what's new in Nagios 3

Need help with Nagios?

A variety of worldwide support options are available to help you get Nagios up and running quickly. Visit www.nagios.org/support/ for information on:

- Installation
- Configuration
- Performance Tuning
- Best Practices
- Integration

Nagios®
Enterprises

MONITORED BY
Nagios™
NETWORK MONITOR

Current Network Status

Current Network Status
Last Updated: Fri Jan 11 11:48:27 CST 2008
Updated every 90 seconds
Nagios® 3.0rc1 - www.nagios.org
Logged in as nagiosadmin

View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
17	0	0	0

All Problems	All Types
0	17

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
169	4	0	2	0

All Problems	All Types
6	175

Service Status Details For All Hosts

Host ↑↓	Service ↑↓	Status ↑↓	Last Check ↑↓	Duration ↑ ↓	Attempt ↓	Status Information
ayamon.com	DNS	OK	01-11-2008 11:45:08	2d 1h 48m 21s	1/3	DNS OK: 0.017 seconds response time. ayamon.com returns 208.64.136.202
	FTP	OK	01-11-2008 11:44:11	0d 0h 14m 16s	1/3	FTP OK - 10.261 second response time on port 21 [220 ProFTPD 1.3.0 Server (4Admin(tm) FTP Server) [208.64.136.202]]
	HTTP	OK	01-11-2008 11:48:06	0d 23h 0m 21s	1/3	HTTP OK HTTP/1.1 200 OK - 10363 bytes in 0.433 seconds
	IMAP	OK	01-11-2008 11:46:36	2d 1h 46m 51s	1/3	IMAP OK - 0.202 second response time on port 143 [* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNION STARTTLS] Courier-IMAP ready. Copyright 1998-2004 Double Precision, Inc. See COPYING for distribution information.]
	PING	OK	01-11-2008 11:46:34	0d 1h 42m 21s	1/3	OK - 208.64.136.202 rta 97.770ms, lost 0%
	SMTP	OK	01-11-2008 11:44:37	1d 18h 58m 51s	1/3	SMTP OK - 0.401 sec. response time
dev1	/ Disk Usage	OK	01-11-2008 11:47:35	1d 23h 42m 21s	1/3	DISK OK - free space: / 6497 MB (60% inode=88%):
	//dev1/html	OK	01-11-2008 11:48:08	1d 23h 40m 46s	1/3	Disk ok - 6.34G (57%) free on \\DEV1\HTML
	/boot Disk Usage	OK	01-11-2008 11:48:02	1d 23h 41m 21s	1/3	DISK OK - free space: /boot 223 MB (91% inode=99%):
	/dev/sda S.M.A.R.T.	OK	01-11-2008 11:47:36	1d 23h 40m 51s	1/3	Id=1, Status=11 {PreFailure , OnLine}, Value=200, Threshold= 51, Passed
	/home Disk Usage	OK	01-11-2008 11:48:09	1d 23h 40m 19s	1/3	DISK OK - free space: /home 2437 MB (84% inode=93%):
	/store Disk Usage	OK	01-11-2008 11:45:23	1d 23h 44m 19s	1/3	DISK OK - free space: /store 683 MB (28% inode=99%):
	/tmp Disk Usage	OK	01-11-2008 11:45:23	1d 23h 44m 19s	1/3	DISK OK - free space: /tmp 1109 MB (97% inode=99%):
	Backups Home Dirs	OK	01-11-2008 11:44:40	1d 23h 43m 49s	1/3	/store/backups/homedirs/root.tar.gz is OK (0d 5h 41m 40s old, 184094422 bytes)
	Backups Mondo Rescue	OK	01-11-2008 11:45:08	1d 23h 43m 19s	1/3	/store/backups/mondo/mondorescue-1.iso is OK (4d 8h 22m 2s old, 736595328 bytes)
	Backups MySQL	CRITICAL	01-11-2008 11:47:18	2d 1h 45m 50s	3/3	CRITICAL: mysql_2008-01-02_07h00m.Wednesday.sql.gz is too old (9d 4h 47m 15s old)
	Backups	OK	01-11-2008 11:46:08	1d 23h 42m 20s	1/3	/store/backups/system/etc.tar.gz is OK (0d 6h 45m 52s

Nagios Availability

Service Availability Report
Last Updated: Fr Jan 11 12:08:47 CST 2008
Nagios® 3.0rc1 - www.nagios.org
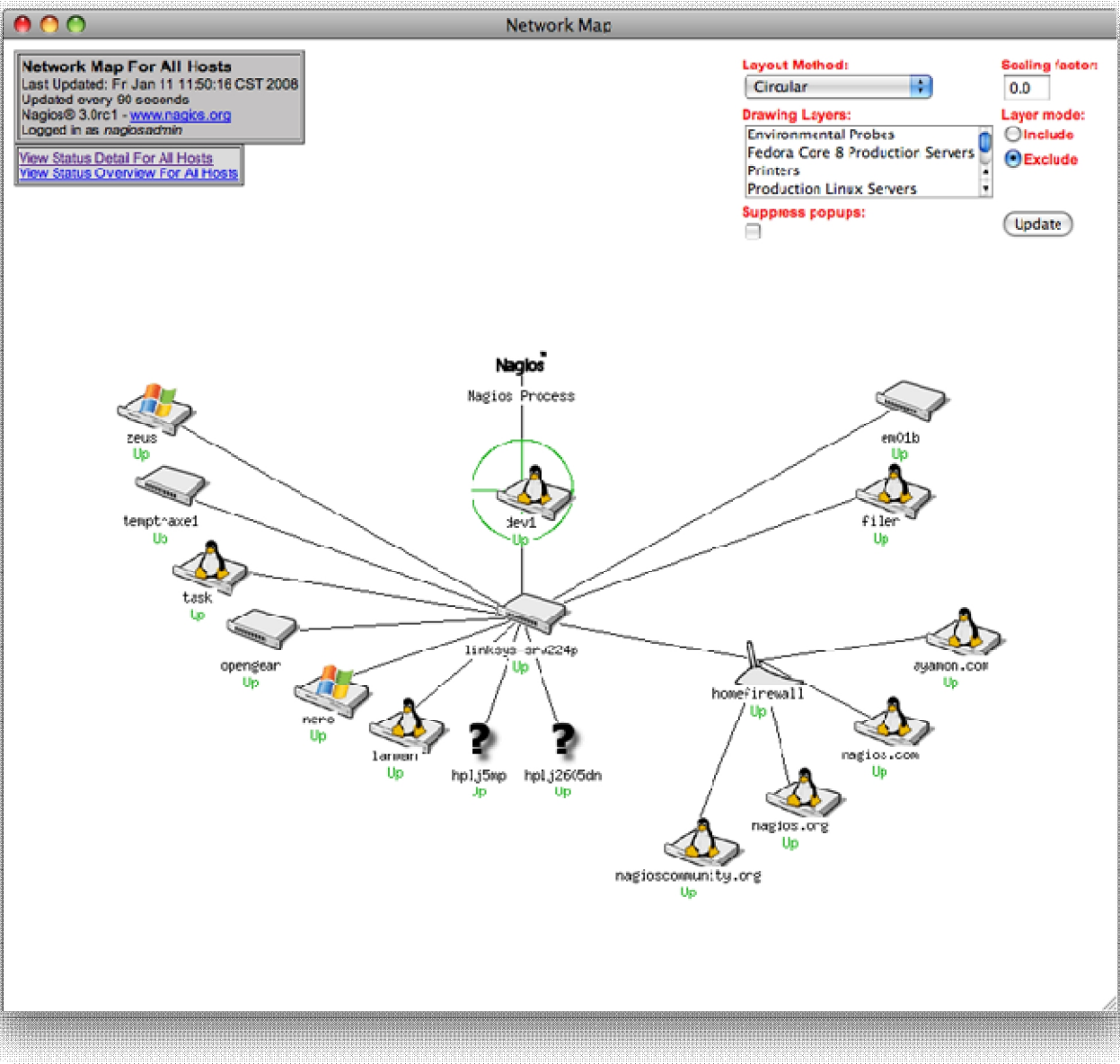Logged in as nagiosadmin

All Services

01-10-2008 12:08:47 to 01-11-2008 12:08:47
Duration: 1d 0h 0m 0s

First assured service state:
Unspecified

Report period:
Last 24 Hours

Backtracked archives:
4

(Update)

[Availability report completed in 0 min 0 sec]

Service State Breakdowns:

Host	Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
ayamon.com	DNS	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	FTP	98.927% (98.927%)	0.000% (0.000%)	0.000% (0.000%)	1.073% (1.073%)	0.000%
	HTTP	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	IMAP	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	PING	96.876% (96.876%)	3.124% (3.124%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	SMTP	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
dev1	/ Disk Usage	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	//dev1/html	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	/boot Disk Usage	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	/dev/sda S.M.A.R.T.	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	/home Disk Usage	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	/store Disk Usage	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	/tmp Disk Usage	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Backups: Home Dirs	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Backups: Mondo Rescue	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
	Backups: MySQL	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	100.000% (100.000%)	0.000%

All Hosts and Services

View Status Detail For All Hosts
View Notifications For All Hosts

Latest Archive

Log File Navigation
Fri Jan 11 00:00:00
CST 2008
to
Present...

File: /usr/local/nagios/var/nagios.log

State type options:

All state types

History detail level for all hosts:

All alerts

☐ Hide Flapping Alerts

☐ Hide Downtime Alerts

☐ Hide Process Messages

☐ Older Entries First

Update

January 11, 2008 12:00

OK [01-11-2008 12:02:16] SERVICE ALERT: filer;Yum Updates;OK;SOFT;2;YUM OK: O/S is up to date.

[01-11-2008 12:00:16] SERVICE ALERT: filer;Yum Updates;CRITICAL;SOFT;1;CHECK_NRPE: Socket timeout after 10 seconds.

January 11, 2008 11:00

OK [01-11-2008 11:52:56] SERVICE ALERT: hplj2605dn;PING;OK;SOFT;2;OK - 192.168.1.30: rta 0.268ms, lost 0%

OK [01-11-2008 11:52:26] HOST ALERT: hplj2605dn;UP;SOFT;2;PING CK - Packet loss = 0%, RTA = 0.62 ms

[01-11-2008 11:51:06] HOST ALERT: hplj2605dn;DOWN;SOFT;1;CRITICAL - Host Unreachable (192.168.1.30)

[01-11-2008 11:50:56] SERVICE ALERT: hplj2605dn;PING;CRITICAL;SOFT;1;CRITICAL - 192.168.1.30: rta nan, lost 100%

OK [01-11-2008 11:45:56] SERVICE ALERT: hplj2605dn;PING;OK;HARD;1;OK - 192.168.1.30: rta 0.650ms, lost 0%

OK [01-11-2008 11:45:06] SERVICE ALERT: filer;Yum Updates;OK;HARD;3;YUM OK: O/S is up to date.

OK [01-11-2008 11:42:56] SERVICE ALERT: filer;Memory Usage;OK;HARD;3;OK - 308 / 756 MB (40%) Free Memory, Used: 448 MB, Shared: 0 MB, Buffers: 59 MB, Cached: 274 MB

OK [01-11-2008 11:42:26] SERVICE ALERT: hplj2605dn;Printer Status;OK;SOFT;2;Printer ok - ("Ready")

OK [01-11-2008 11:42:06] HOST ALERT: hplj2605dn;UP;SOFT;3;PING CK - Packet loss = 0%, RTA = 0.46 ms

[01-11-2008 11:40:56] SERVICE ALERT: hplj2605dn;PING;CRITICAL;HARD;1;CRITICAL - 192.168.1.30: rta nan, lost 100%

[01-11-2008 11:40:56] HOST ALERT: hplj2605dn;DOWN;SOFT;2;CRITICAL - Host Unreachable (192.168.1.30)

[01-11-2008 11:40:36] HOST ALERT: hplj2605dn;DOWN;SOFT;1;CRITICAL - Host Unreachable (192.168.1.30)

[01-11-2008 11:40:26] SERVICE ALERT: hplj2605dn;Printer Status;CRITICAL;SOFT;1;Timeout: No Response from 192.168.1.30. : Timeout from host 192.168.1.30

[01-11-2008 11:36:54] Nagios 3.0rc1 starting... (PID=24137)

[01-11-2008 11:36:54] Caught SIGTERM, shutting down...

OK [01-11-2008 11:34:31] SERVICE ALERT: ayamon.com;FTP;OK;HARD;3;FTP OK - 10.753 second response time on port 21 [220 ProFTPD 1.3.0 Server (4Admin(tm) FTP Server) [208.64.136.202]]

⚠ [01-11-2008 11:32:51] SERVICE ALERT: filer;Memory Usage;WARNING;HARD;3;WARNING - 8 / 756 MB (1%) Free Memory, Used: 748 MB, Shared: 0 MB, Buffers: 46 MB, Cached: 434 MB

[01-11-2008 11:31:48] Nagios 3.0rc1 starting... (PID=22265)

[01-11-2008 11:31:48] Caught SIGTERM, shutting down...

OpenNMS

- http://www.opennms.org
- Functionalities
  - High performance
    - A single instance of OpenNMS supports monitoring of a large number of nodes.
  - Automation
    - OpenNMS minimizes the amount of manual configuration.
  - Rule-based configuration
    - Flexible rules can be used to specify what services are polled on what devices.

openNMS

Web Console

Home | Search | Outages | Events | Notification | Assets | Reports | Admin | Help

Nodes with Outages

192.168.23.38

Categories	Outages	24hr Avail
Network Interfaces	0 of 1	100.000%
Web Servers	0 of 0	100.000%
Email Servers	0 of 0	100.000%
DNS & DHCP Servers	0 of 0	100.000%
Database Servers	0 of 0	100.000%
Other Servers	0 of 0	100.000%
Total	**Outages**	**24hr Avail**
Overall Service Availability	0 of 2	100.000%
Percentage over last 24 hours		

Notification

Check Your Notices
Check All Open Notices
No outstanding notices

Performance

No performance data has been gathered yet

ZABBIX

- http://www.zabbix.com
- Functionalities
  - Performance monitoring
  - User alerts
  - Monitoring of log files
  - Logging services
  - Capacity planning
  - Assuring and monitoring of SLA
  - High level view of IT resources and services
  - Graphical representation of collected information
  - Network maps

Cacti

- http://www.cacti.net
- Similar to MRTG.
- Based on RRDtool.
- Offers excellent graphing capabilities.
- Has extensive templates.

File Edit View Go Bookmarks Tools Help

http://www.lbigspring.k12.pa.us/cacti-0.8.6/graph_view.php?action=preview&host_id=21&filter=

Week 28 Week 29 Week 30 Week 31 Week 32 Week 33 Week 34 Week 35
From 2004/06/28 22:51:02 To 2004/08/28 22:51:02

■ Inbound   Current: 793.56   Average: 721.17   Maximum: 2.64 k
■ Outbound Current: 374.33   Average: 3.80 k   Maximum: 22.04 k

Traffic - WWW - 216.37.141.11

From 2004/06/28 22:51:02 To 2004/08/28 22:51:02

■ Inbound   Current: 89.60   Average: 1.4t k   Maximum: 516.66 k
■ Outbound Current: 683.46   Average: 4.79 k   Maximum: 151.38 k

WWW - CPU Usage

From 2004/06/28 22:51:02 To 2004/08/28 22:51:02

■ System Current: 932.77 m   Average: 835.63 m   Maximum: 3.153
■ User   Current: 6.25   Average: 5.54   Maximum: 26.47
■ Nice   Current: 0.00   Average: 566.72 u   Maximum: 3.196 m
■ Total   Current: 7.19   Average: 6.38   Maximum: 30.20

WWW - Load Average

From 2004/06/28 22:51:02 To 2004/08/28 22:51:02

■ 1 Minute Average   Current: 0.76
■ 5 Minute Average   Current: 0.60
■ 15 Minute Average Current: 0.39

WWW - Logged in Users

Done

File   Edit   View   Go   Bookmarks   Tools   Help

http://www.bigspring.k12.pa.us/cacti-0.8.6/graph.php?action=zoom&local_graph_id=10&rra_id=0&graph_sta

console   graphs   settings

Graphs -> Preview Mode -> Traffic - WWW - 216.37.141.11 -> Zoom   Logged in as lberry (Logout)

Zooming Graph 'Traffic - WWW - 216.37.141.11'

Traffic - WWW - 216.37.141.11

From 2004/06/28 22:53:33 To 2004/08/28 22:53:33

■ Inbound	Current:	89.60	Average:	1.41 k	Maximum:	55.66 k
■ Outbound	Current:	683.46	Average:	4.70 k	Maximum:	151.36 k

Done

NTop

- http://ntop.org
- Network probe that shows network activity just like "top".

| About | Total | Recv | Sent | Stats | IP Traffic | IP Protos | Admin |

Network Traffic: Data Received

▷ Data
Received

All Protocols

TCP/UDP

Throughput

Host Activity

Host ▦	Domain	Data			Packets		
		Current	**Avg**	**Peak**	**Current**	**Avg**	**Peak**
10.0.0.2 ✛ 🌐		0.0 bps	0.0 bps	117.6 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.2 Pkts/sec
barney		1.7 Kbps	0.0 bps	8.5 Kbps	2.2 Pkts/sec	0.1 Pkts/sec	10.7 Pkts/sec
bart		9.3 Kbps	0.0 bps	9.3 Kbps	2.4 Pkts/sec	0.0 Pkts/sec	2.4 Pkts/sec
gnasher		112.6 bps	0.0 bps	44.9 Kbps	0.2 Pkts/sec	0.0 Pkts/sec	11.9 Pkts/sec
penfold		0.0 bps	0.0 bps	0.0 bps	0.0 Pkts/sec	0.0 Pkts/sec	0.0 Pkts/sec

Peak values are the maximum value for any 10 second interval.
Average values are recomputed each 60 seconds, using values accumulated since this run of ntop was started.

Note: Both values are reset each time ntop is restarted.

Report created on Tue Dec 09 16:08:04 2003 [1 day(s) 1:11:23]
Generated by ntop v.2.2 MT [WinNT/2K/XP] (2003-04-14 build)
Listening on [\Device\NPF_EI90x1] without a kernel (libpcap) filtering expression
Web report active on interface 3Com EtherLink PCI
© 1998-2003 by Luca Deri

© 1998-2003
by Luca Deri

🔷 Done   🖳 Local intranet
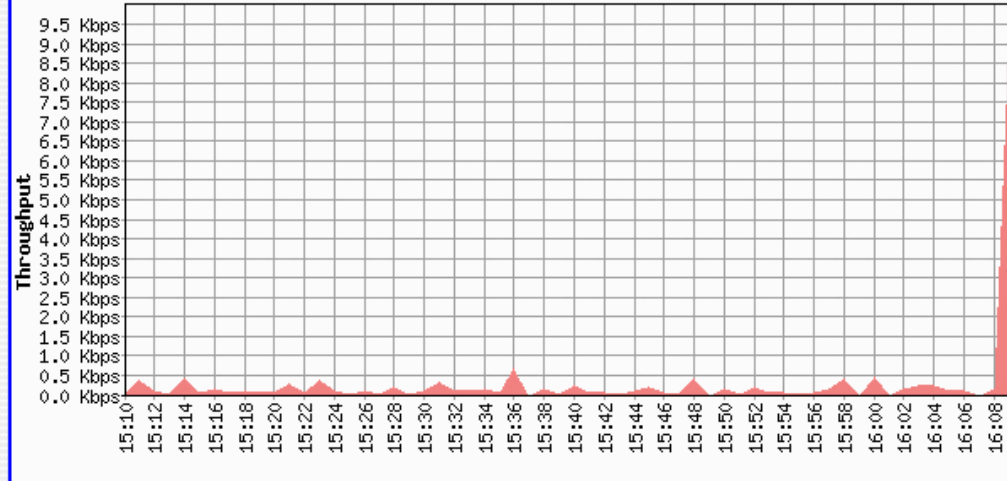
File   Edit   View   Favorites   Tools   Help

⇐ Back ▾ ⇒ ▾ ⊗ �ⅸ ⌂ | ⊛Search ⋇Favorites ⊛Media ⊛ | ⊟▾ ⊜ ⊠ ▾ ⊠

Address | http://barney:3000

Google ▾ | | ⊛Search Web ▾ | ⊛ | PageRank ⊕ ▾ ⊟388 blocked ⊟AutoFill ⊟ ⊟Options ✎

Links

| About | Total | Recv | Sent | Stats | IP Traffic | IP Protos | Admin |

Network Load Statistics

▷ Statistics

Multicast

Traffic

Hosts

Local Info

Network Load

Domain

© 1998-2003
by Luca Deri

Last 60 Minutes Average Throughput

Throughput

9.5 Kbps
9.0 Kbps
8.5 Kbps
8.0 Kbps
7.5 Kbps
7.0 Kbps
6.5 Kbps
6.0 Kbps
5.5 Kbps
5.0 Kbps
4.5 Kbps
4.0 Kbps
3.5 Kbps
3.0 Kbps
2.5 Kbps
2.0 Kbps
1.5 Kbps
1.0 Kbps
0.5 Kbps
0.0 Kbps

15:10 15:12 15:14 15:16 15:18 15:20 15:22 15:24 15:26 15:28 15:30 15:32 15:34 15:36 15:38 15:40 15:42 15:44 15:46 15:48 15:50 15:52 15:54 15:56 15:58 16:00 16:02 16:04 16:06 16:08

Time [now - Tue Dec 09 15:09:04 2003]

Last 24 Hours Average Throughput

1.4 Kbps
1.3 Kbps
1.1 Kbps
1.0 Kbps

Local intranet

| About | Total | Recv | Sent | Stats | IP Traffic | IP Protos | Admin |
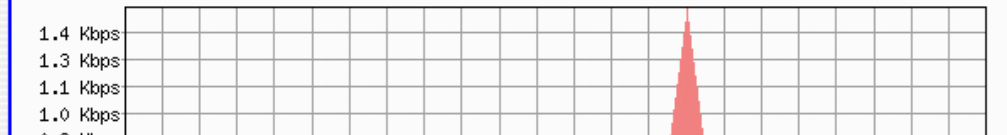
Protocol Distribution
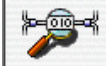
▷ **Data Sent**

All Protocols

TCP/UDP

Throughput

Host Activity

© 1998-2003
by Luca Deri

Protocol	Data Sent	Data Rcvd
TCP	1.4 MB	461.8 KB
UDP	473.4 KB	17.4 KB
ICMP	0.0 KB	195.6 KB
(R)ARP	26.6 KB	22.8 KB
Protocol Distribution		
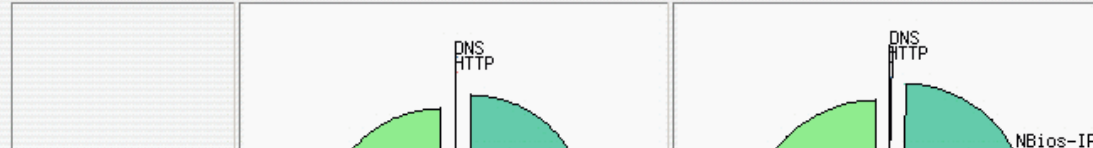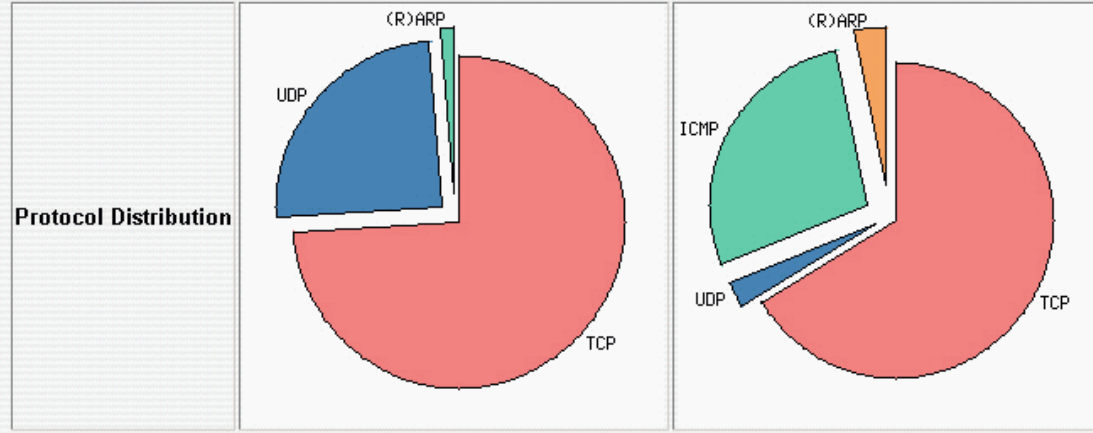
Request Tracker

- http://bestpractical.com/rt/
- Tracks data/conversations/requests.
- Convenient for end users.
- Highly customizable.
- Easy to install (hmm…)

RT for example.com

RT at a glance

| Home |
| Simple Search |
| Tickets |
| Tools |
| Configuration |
| Preferences |
| Approval |

New ticket in   General ▾   [_____]   Search

Edit

10 highest priority tickets I own   Edit

#	Subject	Priority	Queue	Status
1	Office has run out of coffee	0	General	(pending 1 other ticket)
2	order more coffee	0	General	(pending 1 other ticket)

10 newest unowned tickets   Edit

#	Subject	Queue	Status	Created	
3	Obtain Series-C funding	General	new	16 min ago	Take

Bookmarked Tickets   Edit

#	Subject	Priority	Queue	Status	
1	Office has run out of coffee	0	General	(pending 1 other ticket)	☆

Quick ticket creation

Subject: [_____]

Queue: General ▾   Owner: root ▾

Content:
[
                                          ]

Create

Reminders

Quick search   Edit

Queue	new	open	stalled
General	3	0	0

Dashboards   Edit

Name	Subscription
SLA Performance	daily at 06:00

Refresh

Don't refresh this page. ▾

Go!

Logged in as root | Preferences | Logout

SLA Performance

| New ticket in | General ⬍ | | Search |

Basics · Queries · Subscription · **Show**

Home
Simple Search
Tickets
Tools
  Dashboards
    Select dashboard
    New dashboard
    SLA Performance
    Offline
    Reports
    My Day
  Configuration
  Preferences
  Approval

^

| **New, unresolved tickets** | | | | | Edit |

#	Subject Requestors	Status Created	Queue Told	Owner Last Updated	Priority Time Left
1	Office has run out of coffee jesse@bestpractical.com	new 15 min ago	General	root 7 min ago	0 0
2	order more coffee jesse@bestpractical.com	new 12 min ago	General	root 7 min ago	0 0
3	Obtain Series-C funding jesse@bestpractical.com	new 11 min ago	General	Nobody 10 min ago	0 0

^

| **20 newest unowned tickets** | | | | Edit |

#	Subject	Queue	Status	Created	
3	Obtain Series-C funding	General	new	11 min ago	Take

RT for example.com

Create a new ticket

New ticket in | General ▲▼ | | Search |

- Home
- Simple Search
- Tickets
- Tools
- Configuration
- Preferences
- Approval

Show basics · Show details

Create a new ticket

Queue: General	Status:	new ▲▼	Owner: Nobody ▲▼

Requestors: je-sse@bestpractical.com

Cc: _____ (Sends a carbon-copy of this update to a comma-delimited list of email addresses. These people will receive future updates.)

Admin Cc: _____ (Sends a carbon-copy of this update to a comma-delimited list of administrative email addresses. These people will receive future updates.)

Subject: Office has run out of coffee

Operating System
Combobox: Select or enter one value

Filterfresh ▲▼
Linux
Mac OS X
Solaris

Attach file: _____ ore Files

Describe the issue below:

| Source | | | | | | | | | | | | | |

| **B** *I* U ABC ₓ² Style | Format Normal | Font | Size | |

The worst has happened.

There's no coffee to be found anywhere in the office.

Productivity is at an all-time low!

| Create |

BEST

Security Tools

- Some security tools to consider:
  - NetFilter IP Tables – Firewall
  - WireShark – Protocol analyzer
  - Snort – Intrusion detection
  - Netcat – Feature rich tool. Great for debugging.
  - Nessus – Vulnerability scanner
  - Many many more…

Recommended Reading

- Practice of System and Network administration by Thomas A. Limoncelli

- How to accelerate your Internet E-book http://bwmo.net/

- Red Hat Linux Network Management Tools (CD-ROM included) (Paperback) By Steven Maxwell.