# Stager

## Web-based Statistics Display

NANOG35

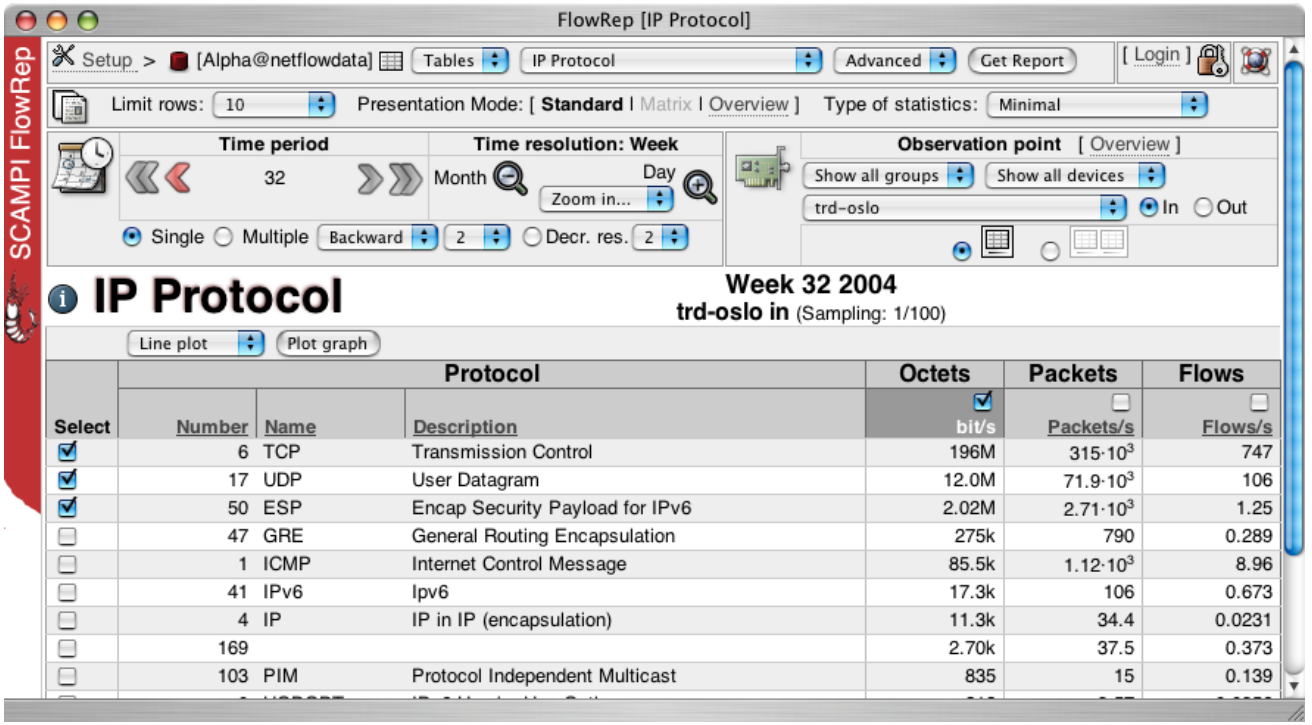
23-25 October 2005

Arne Øslebø

arneos@uninett.no

# What is Stager?

- A web-based tool for aggregating and presenting most types of network statistics
- GPL
- 100+ people on public mailinglist

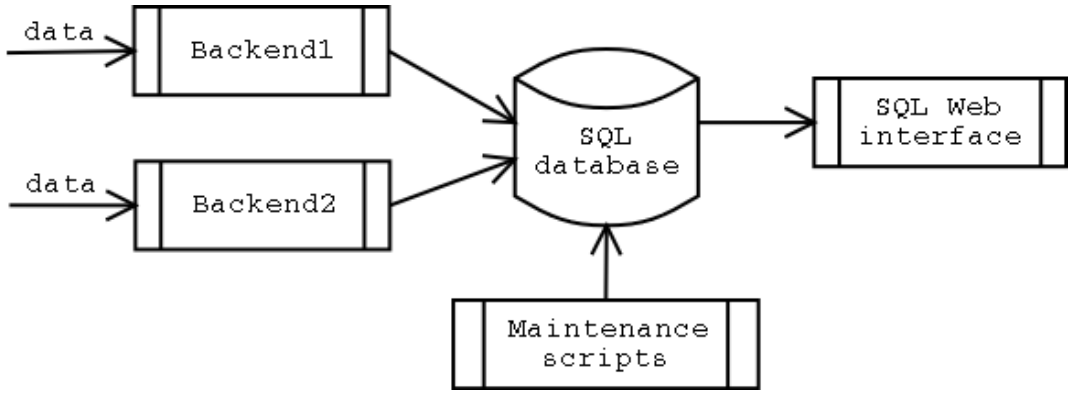


# Main features

- Easy to use web frontend
  - Text based reports and graphs
- Support for different types of network statistics
  - Netflow
  - SNMP
  - Mping
- Easy to add new reports
  - Templates and plugins
- Access control
  - Observation points and reports

# Stager design

- One or more backends for collecting data
- Database for storing and aggregating reports
- Web frontend



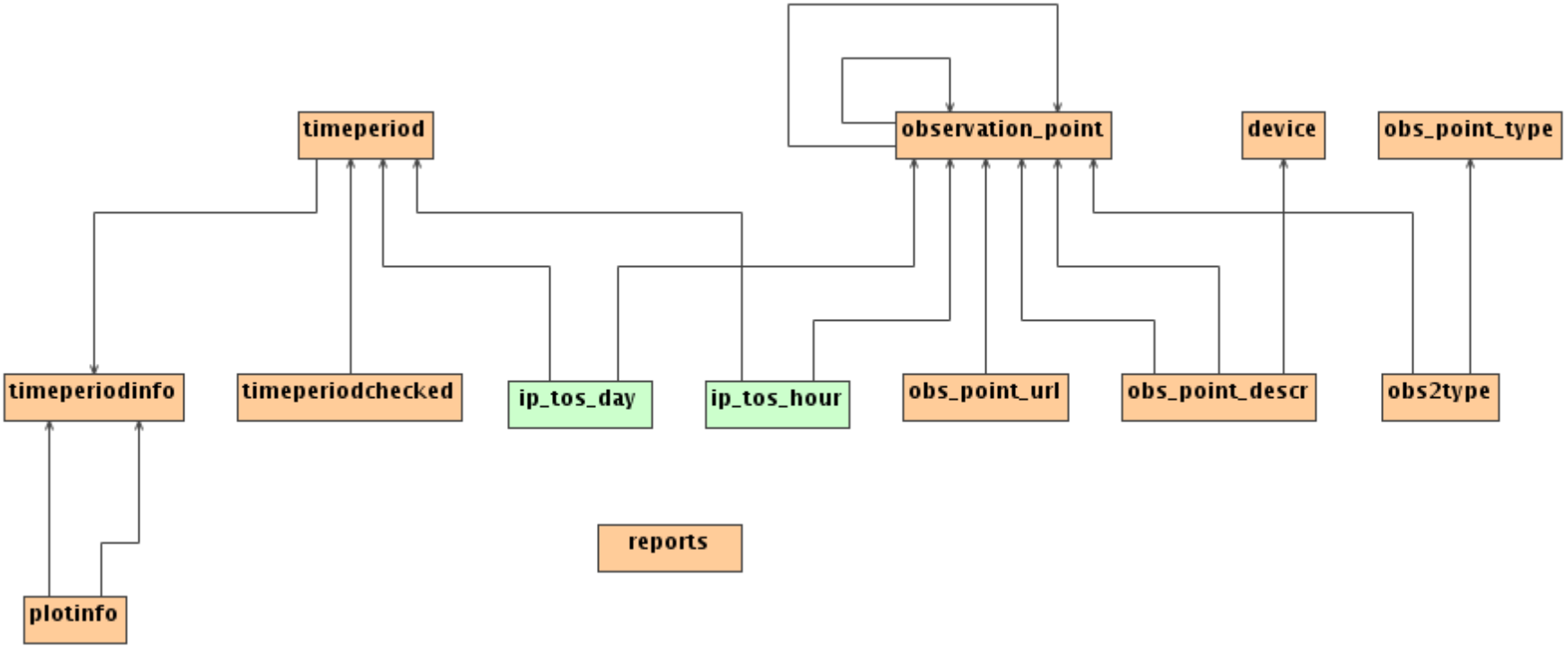
# Backend

- Collects raw data from some source, processes it and inserts reports into the database
  - most commonly used IP protocols
  - the top 100 source IP addresses with the highest traffic
  - Router CPU load
- Robustness
  - Detects deadlocks
  - Inserts missing data automatically after DB problems
- Generic aggregation

# Report templates

- Specifies how to present a report in the frontend.
  - bps, pps, % etc.
- Multiple views for the same report type.
  - Overview, packet details, flows details etc.
- Report transformations
  - Table, matrix, overview and global
- Specifies where to collect report data from
  - Database
  - Raw netflow files
  - etc.

# Database ER diagram

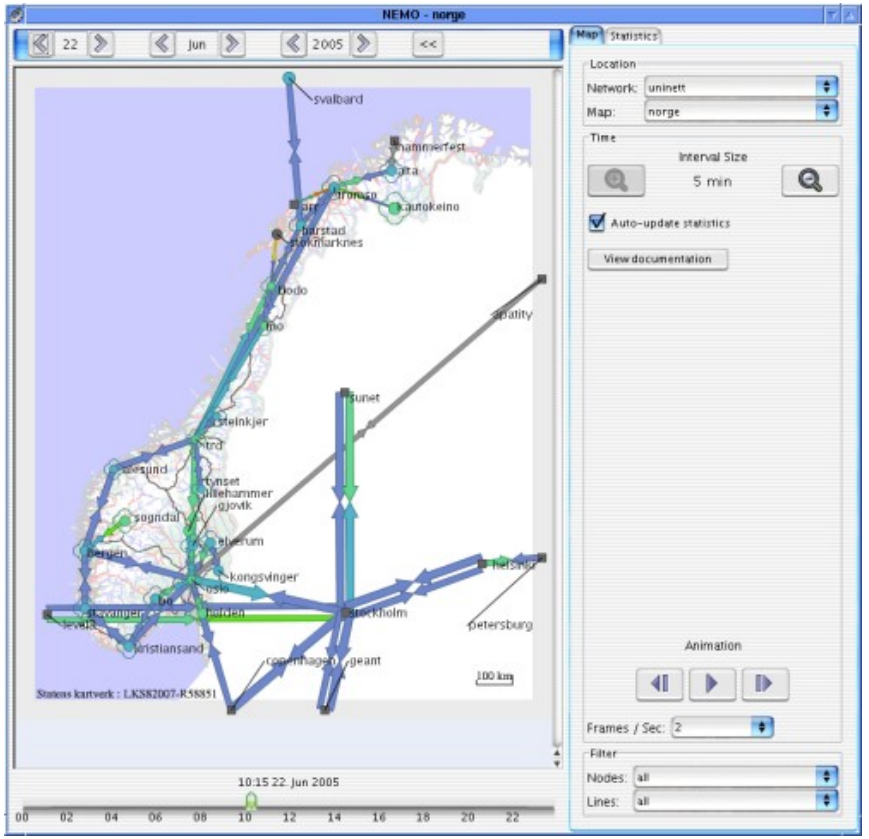


# What do you need to run Stager?

- Linux or BSD
- Perl
  - DBI – database interface module
- PostgreSQL
- HTTP server
  - PHP
    - Smarty – template engine
    - JpGraph – graph creating library
- Stager
  - http://software.uninett.no/

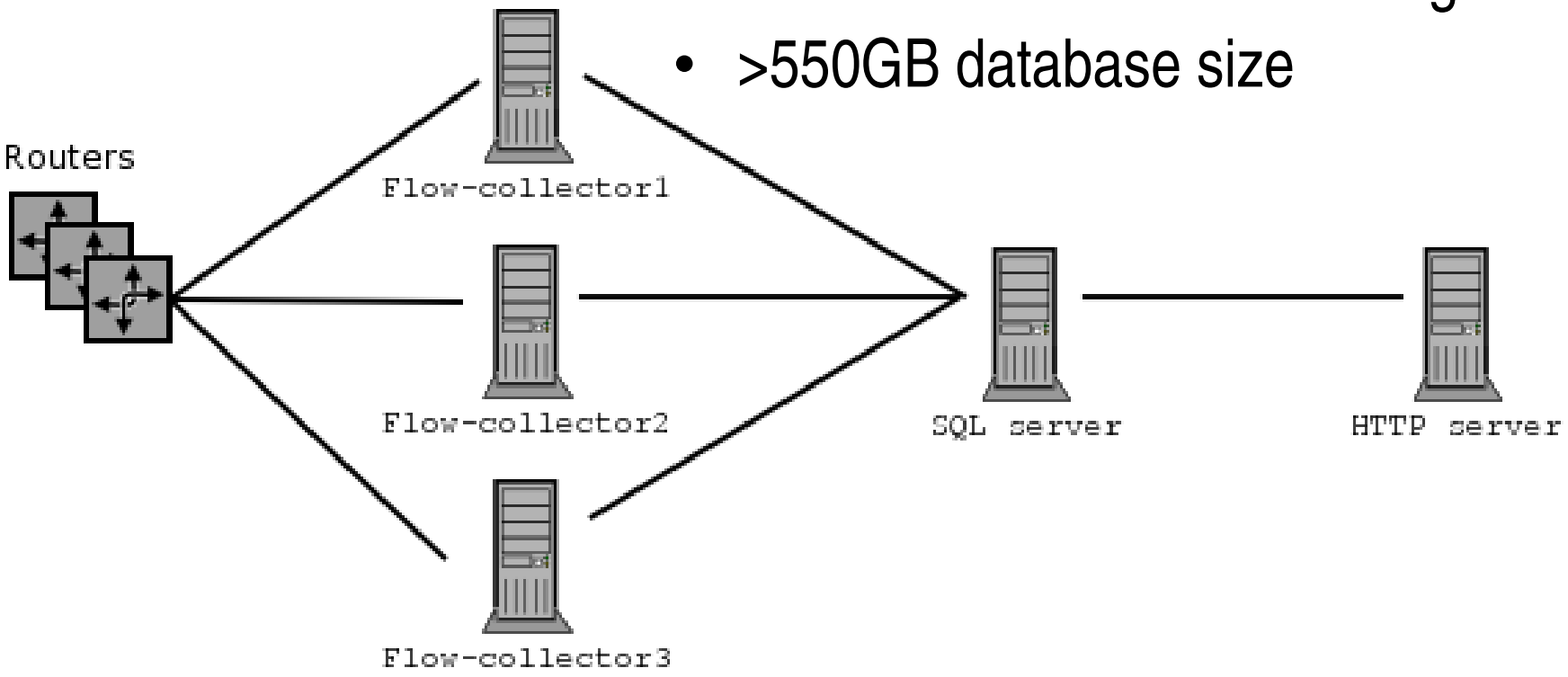
# Nemo

- Java application that can show animated maps with network statistics
- Can read and animate data from the Stager database
- Animates links and routers
- Geographic maps
- Topology
- Zooming



# Our netflow setup

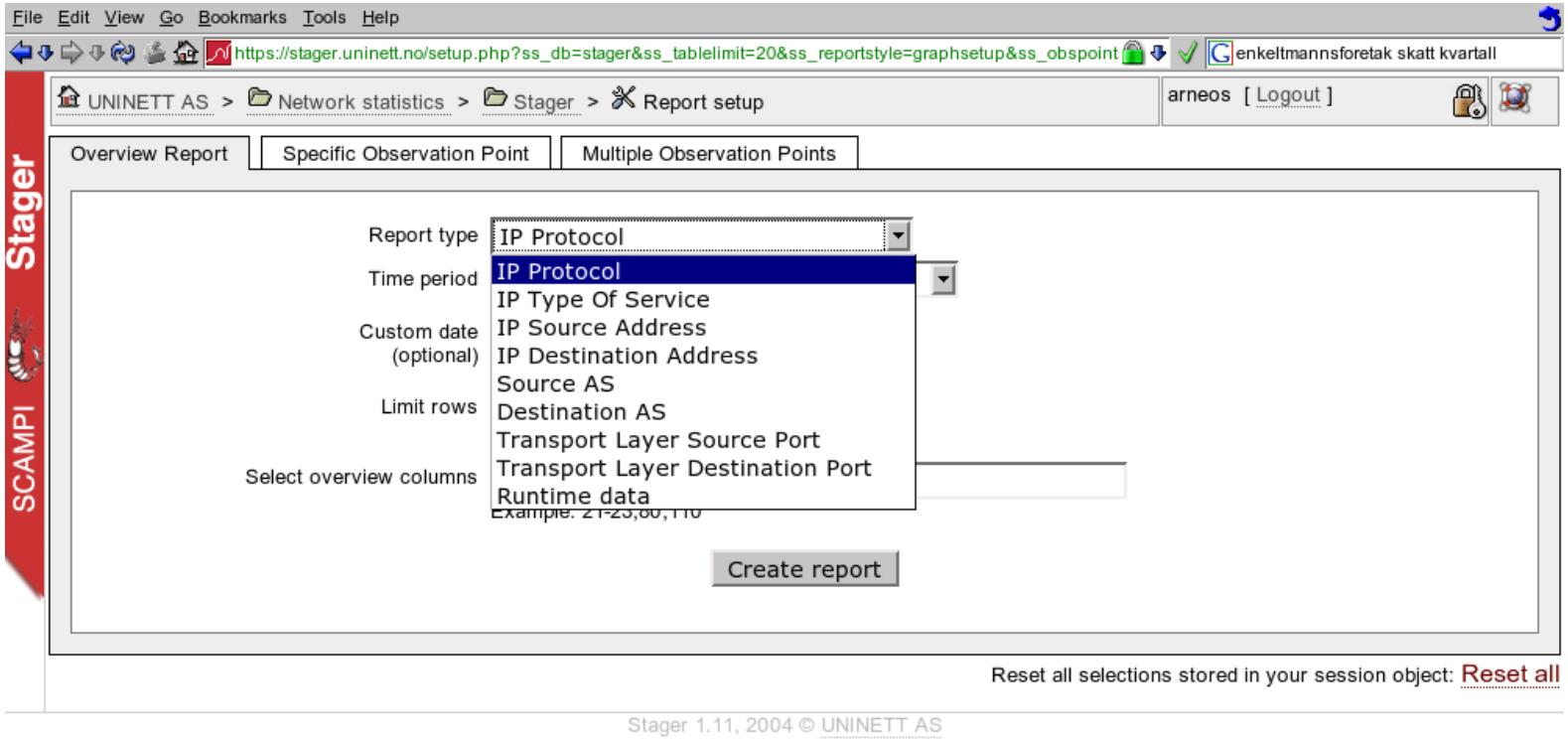
- 31 routers, 175 interfaces
  - 1/100 sampling on most routers
- ~30GB of raw netflow data per day
- peak hours: 100 inserts per second
- >300 millions entries in a single table
- >550GB database size



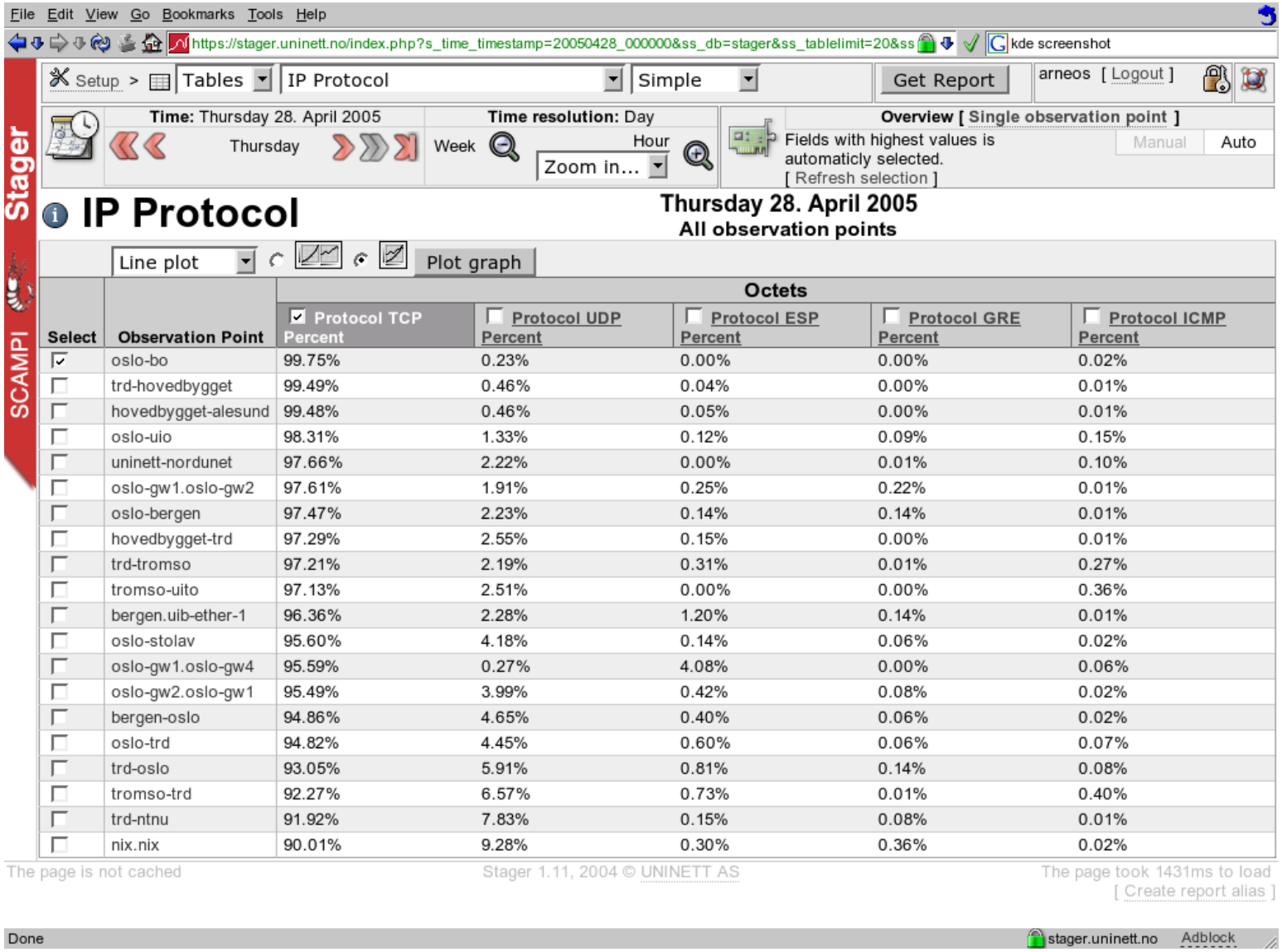
# Live demo

https://stager.uninett.no

# Start page


File Edit View Go Bookmarks Tools Help
https://stager.uninett.no/setup.php?ss_db=stager&ss_tablelimit=20&ss_reportstyle=graphsetup&ss_obspoint
enkeltmannsforetak skatt kvartall
UNINETT AS > Network statistics > Stager > Report setup
arneos [ Logout ]
Stager
SCAMPI
Overview Report
Specific Observation Point
Multiple Observation Points
Report type
IP Protocol
Time period
Custom date (optional)
Limit rows
Select overview columns
IP Protocol
IP Type Of Service
IP Source Address
IP Destination Address
Source AS
Destination AS
Transport Layer Source Port
Transport Layer Destination Port
Runtime data
Create report
Reset all selections stored in your session object: Reset all
Stager 1.11, 2004 © UNINETT AS
Done
stager.uninett.no
Adblock

# Overview report



File Edit View Go Bookmarks Tools Help

https://stager.uninett.no/index.php?s_time_timestamp=20050428_000000&ss_db=stager&ss_tablelimit=20&ss

kde screenshot

Stager

SCAMPI

Setup > Tables | IP Protocol | Simple | Get Report | arneos [ Logout ]

**Time:** Thursday 28. April 2005 — Thursday — Week — Hour — Zoom in...

**Time resolution:** Day

**Overview [ Single observation point ]**

Fields with highest values is automaticly selected.

[ Refresh selection ]

Manual | Auto

## IP Protocol

**Thursday 28. April 2005**

**All observation points**

Line plot | Plot graph

| Select | Observation Point | Octets | | | | |
|---|---|---|---|---|---|---|
| | | Protocol TCP Percent | Protocol UDP Percent | Protocol ESP Percent | Protocol GRE Percent | Protocol ICMP Percent |
| ☑ | oslo-bo | 99.75% | 0.23% | 0.00% | 0.00% | 0.02% |
| ☐ | trd-hovedbygget | 99.49% | 0.46% | 0.04% | 0.00% | 0.01% |
| ☐ | hovedbygget-alesund | 99.48% | 0.46% | 0.05% | 0.00% | 0.01% |
| ☐ | oslo-uio | 98.31% | 1.33% | 0.12% | 0.09% | 0.15% |
| ☐ | uninett-nordunet | 97.66% | 2.22% | 0.00% | 0.01% | 0.10% |
| ☐ | oslo-gw1.oslo-gw2 | 97.61% | 1.91% | 0.25% | 0.22% | 0.01% |
| ☐ | oslo-bergen | 97.47% | 2.23% | 0.14% | 0.14% | 0.01% |
| ☐ | hovedbygget-trd | 97.29% | 2.55% | 0.15% | 0.00% | 0.01% |
| ☐ | trd-tromso | 97.21% | 2.19% | 0.31% | 0.01% | 0.27% |
| ☐ | tromso-uito | 97.13% | 2.51% | 0.00% | 0.00% | 0.36% |
| ☐ | bergen.uib-ether-1 | 96.36% | 2.28% | 1.20% | 0.14% | 0.01% |
| ☐ | oslo-stolav | 95.60% | 4.18% | 0.14% | 0.06% | 0.02% |
| ☐ | oslo-gw1.oslo-gw4 | 95.59% | 0.27% | 4.08% | 0.00% | 0.06% |
| ☐ | oslo-gw2.oslo-gw1 | 95.49% | 3.99% | 0.42% | 0.08% | 0.02% |
| ☐ | bergen-oslo | 94.86% | 4.65% | 0.40% | 0.06% | 0.02% |
| ☐ | oslo-trd | 94.82% | 4.45% | 0.60% | 0.06% | 0.07% |
| ☐ | trd-oslo | 93.05% | 5.91% | 0.81% | 0.14% | 0.08% |
| ☐ | tromso-trd | 92.27% | 6.57% | 0.73% | 0.01% | 0.40% |
| ☐ | trd-ntnu | 91.92% | 7.83% | 0.15% | 0.08% | 0.01% |
| ☐ | nix.nix | 90.01% | 9.28% | 0.30% | 0.36% | 0.02% |

The page is not cached

Stager 1.11, 2004 © UNINETT AS

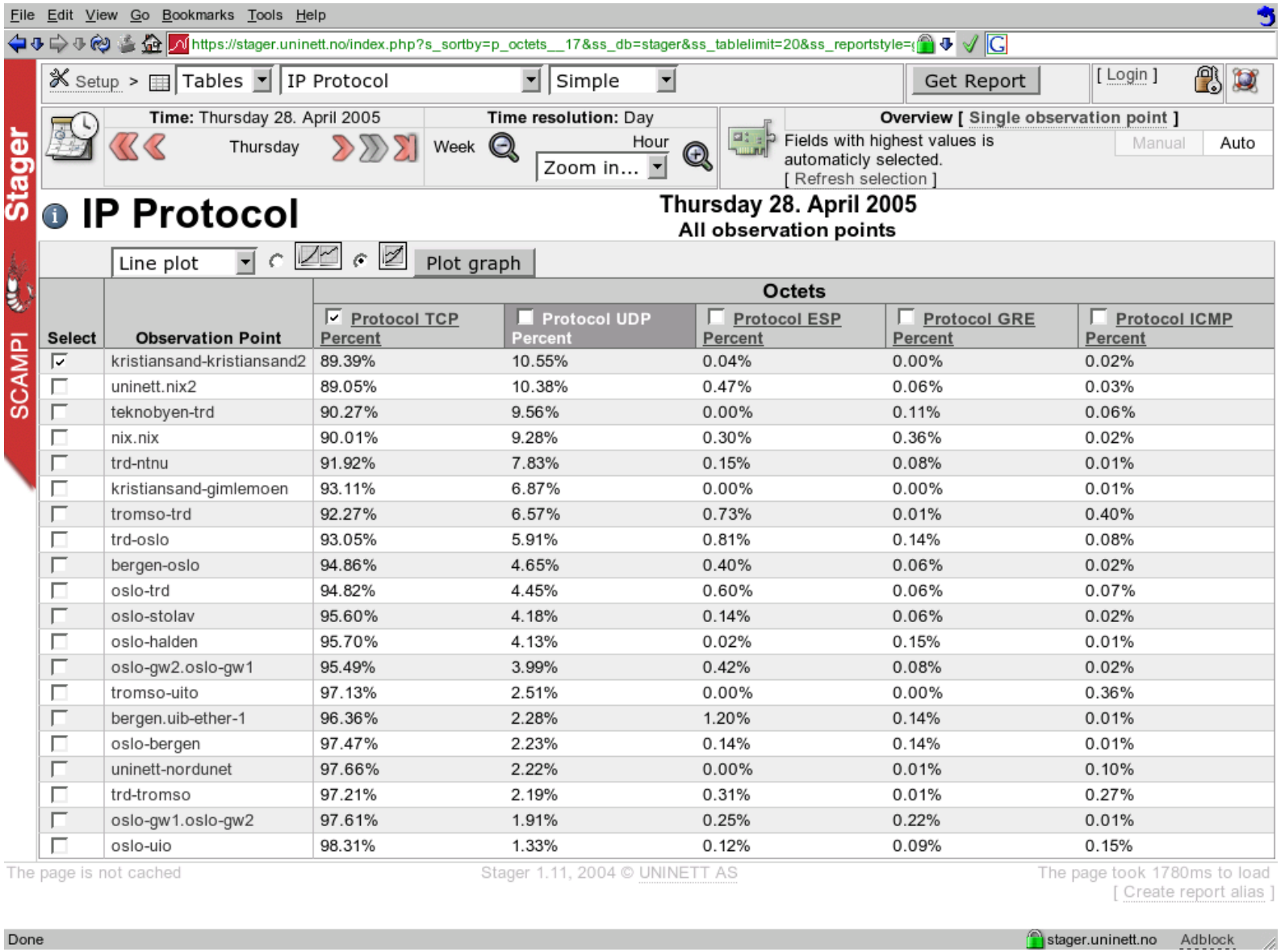
The page took 1431ms to load

[ Create report alias ]

Done

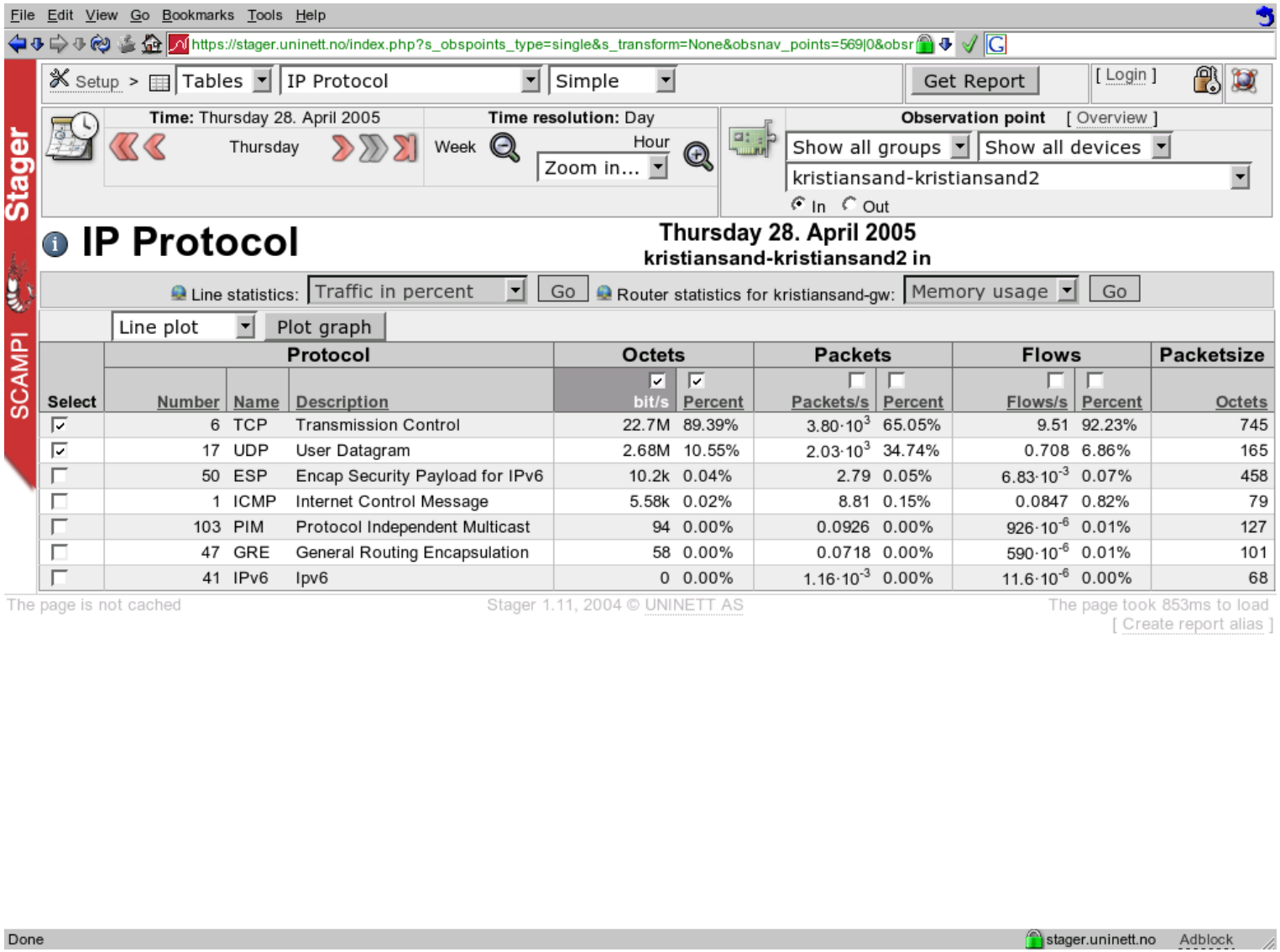
stager.uninett.no Adblock

# Overview – sorted on UDP



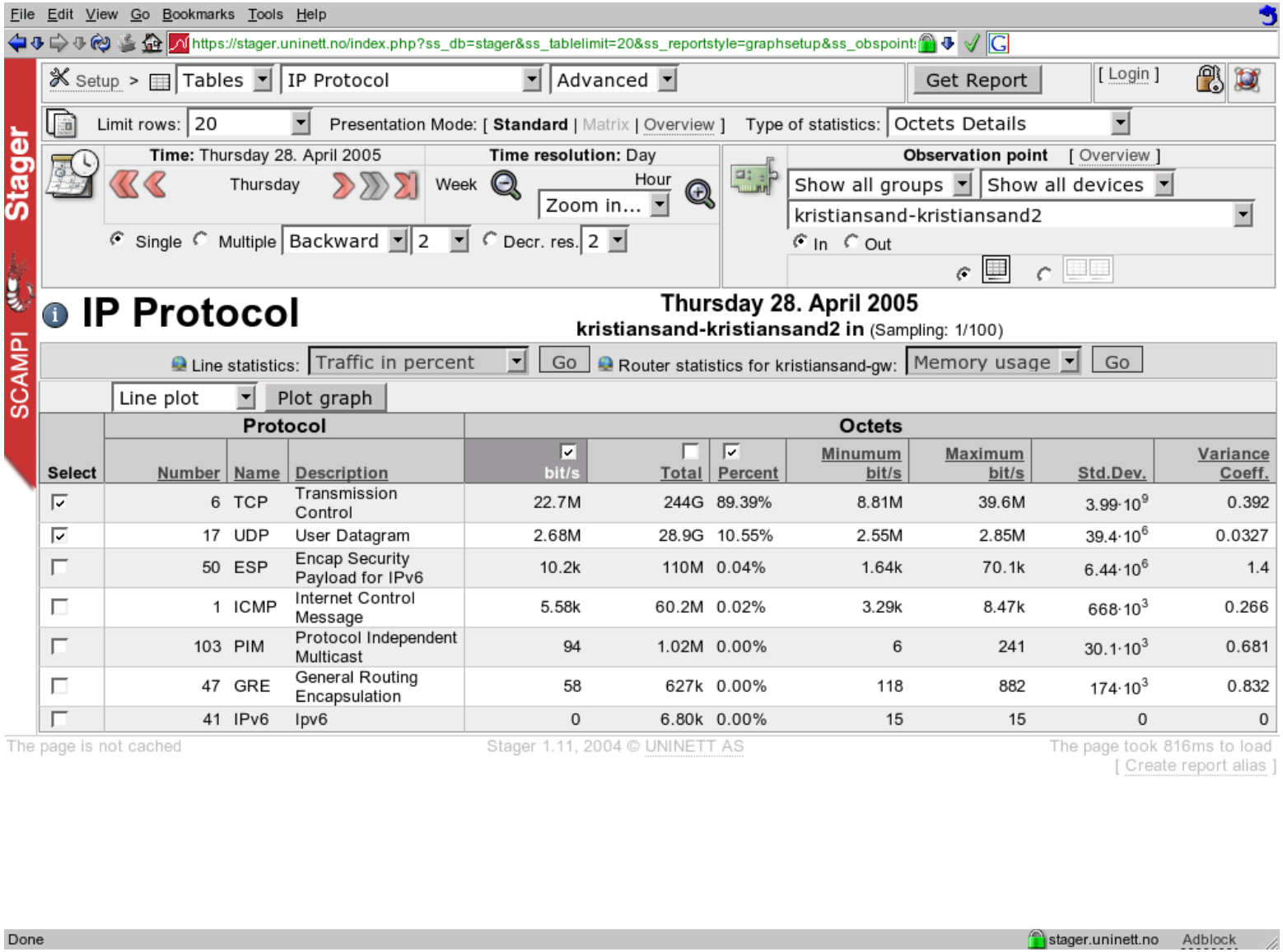

| Select | Observation Point | Octets | | | | |
|---|---|---|---|---|---|---|
| | | Protocol TCP Percent | Protocol UDP Percent | Protocol ESP Percent | Protocol GRE Percent | Protocol ICMP Percent |
| ☑ | kristiansand-kristiansand2 | 89.39% | 10.55% | 0.04% | 0.00% | 0.02% |
| ☐ | uninett.nix2 | 89.05% | 10.38% | 0.47% | 0.06% | 0.03% |
| ☐ | teknobyen-trd | 90.27% | 9.56% | 0.00% | 0.11% | 0.06% |
| ☐ | nix.nix | 90.01% | 9.28% | 0.30% | 0.36% | 0.02% |
| ☐ | trd-ntnu | 91.92% | 7.83% | 0.15% | 0.08% | 0.01% |
| ☐ | kristiansand-gimlemoen | 93.11% | 6.87% | 0.00% | 0.00% | 0.01% |
| ☐ | tromso-trd | 92.27% | 6.57% | 0.73% | 0.01% | 0.40% |
| ☐ | trd-oslo | 93.05% | 5.91% | 0.81% | 0.14% | 0.08% |
| ☐ | bergen-oslo | 94.86% | 4.65% | 0.40% | 0.06% | 0.02% |
| ☐ | oslo-trd | 94.82% | 4.45% | 0.60% | 0.06% | 0.07% |
| ☐ | oslo-stolav | 95.60% | 4.18% | 0.14% | 0.06% | 0.02% |
| ☐ | oslo-halden | 95.70% | 4.13% | 0.02% | 0.15% | 0.01% |
| ☐ | oslo-gw2.oslo-gw1 | 95.49% | 3.99% | 0.42% | 0.08% | 0.02% |
| ☐ | tromso-uito | 97.13% | 2.51% | 0.00% | 0.00% | 0.36% |
| ☐ | bergen.uib-ether-1 | 96.36% | 2.28% | 1.20% | 0.14% | 0.01% |
| ☐ | oslo-bergen | 97.47% | 2.23% | 0.14% | 0.14% | 0.01% |
| ☐ | uninett-nordunet | 97.66% | 2.22% | 0.00% | 0.01% | 0.10% |
| ☐ | trd-tromso | 97.21% | 2.19% | 0.31% | 0.01% | 0.27% |
| ☐ | oslo-gw1.oslo-gw2 | 97.61% | 1.91% | 0.25% | 0.22% | 0.01% |
| ☐ | oslo-uio | 98.31% | 1.33% | 0.12% | 0.09% | 0.15% |

# Details



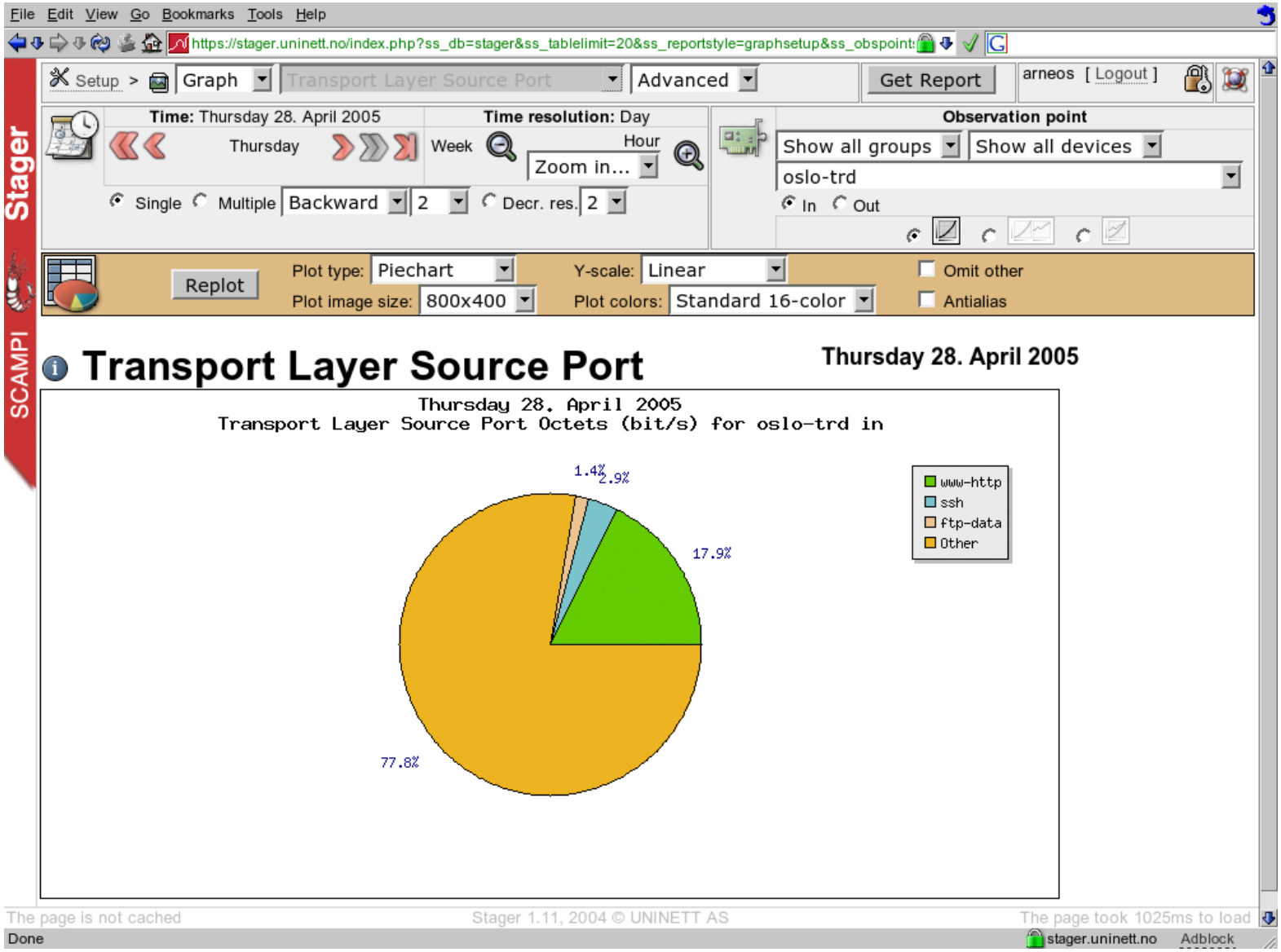

| Select | Protocol Number | Name | Description | Octets bit/s | Octets Percent | Packets Packets/s | Packets Percent | Flows Flows/s | Flows Percent | Packetsize Octets |
|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | 6 | TCP | Transmission Control | 22.7M | 89.39% | $3.80 \cdot 10^{3}$ | 65.05% | 9.51 | 92.23% | 745 |
| ☑ | 17 | UDP | User Datagram | 2.68M | 10.55% | $2.03 \cdot 10^{3}$ | 34.74% | 0.708 | 6.86% | 165 |
| ☐ | 50 | ESP | Encap Security Payload for IPv6 | 10.2k | 0.04% | 2.79 | 0.05% | $6.83 \cdot 10^{-3}$ | 0.07% | 458 |
| ☐ | 1 | ICMP | Internet Control Message | 5.58k | 0.02% | 8.81 | 0.15% | 0.0847 | 0.82% | 79 |
| ☐ | 103 | PIM | Protocol Independent Multicast | 94 | 0.00% | 0.0926 | 0.00% | $926 \cdot 10^{-6}$ | 0.01% | 127 |
| ☐ | 47 | GRE | General Routing Encapsulation | 58 | 0.00% | 0.0718 | 0.00% | $590 \cdot 10^{-6}$ | 0.01% | 101 |
| ☐ | 41 | IPv6 | Ipv6 | 0 | 0.00% | $1.16 \cdot 10^{-3}$ | 0.00% | $11.6 \cdot 10^{-6}$ | 0.00% | 68 |

# Detailed statistics

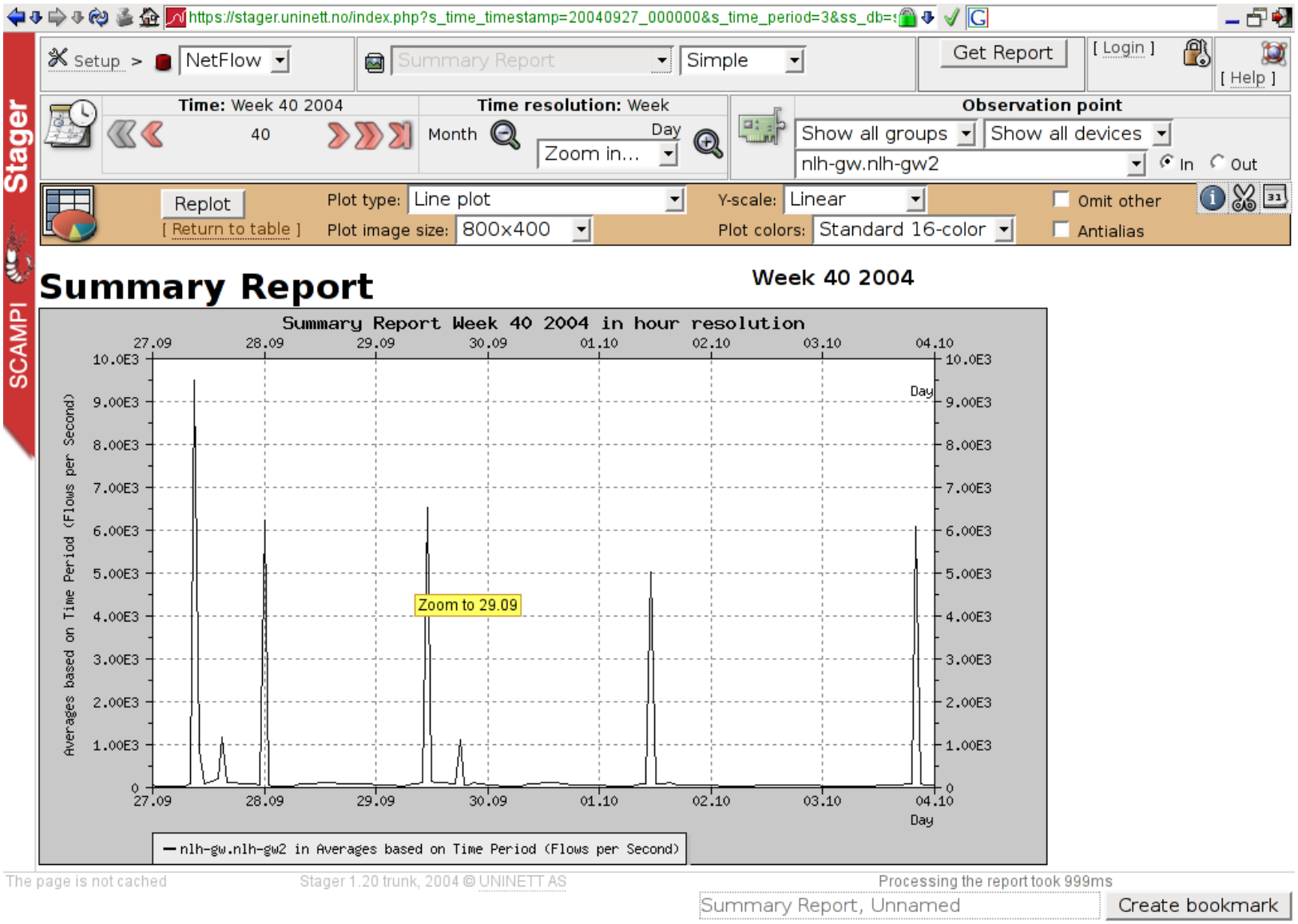



| Select | Protocol Number | Name | Description | Octets bit/s | Total | Percent | Minumum bit/s | Maximum bit/s | Std.Dev. | Variance Coeff. |
|---|---|---|---|---|---|---|---|---|---|---|
| ☑ | 6 | TCP | Transmission Control | 22.7M | 244G | 89.39% | 8.81M | 39.6M | $3.99 \cdot 10^9$ | 0.392 |
| ☑ | 17 | UDP | User Datagram | 2.68M | 28.9G | 10.55% | 2.55M | 2.85M | $39.4 \cdot 10^6$ | 0.0327 |
| ☐ | 50 | ESP | Encap Security Payload for IPv6 | 10.2k | 110M | 0.04% | 1.64k | 70.1k | $6.44 \cdot 10^6$ | 1.4 |
| ☐ | 1 | ICMP | Internet Control Message | 5.58k | 60.2M | 0.02% | 3.29k | 8.47k | $668 \cdot 10^3$ | 0.266 |
| ☐ | 103 | PIM | Protocol Independent Multicast | 94 | 1.02M | 0.00% | 6 | 241 | $30.1 \cdot 10^3$ | 0.681 |
| ☐ | 47 | GRE | General Routing Encapsulation | 58 | 627k | 0.00% | 118 | 882 | $174 \cdot 10^3$ | 0.832 |
| ☐ | 41 | IPv6 | Ipv6 | 0 | 6.80k | 0.00% | 15 | 15 | 0 | 0 |

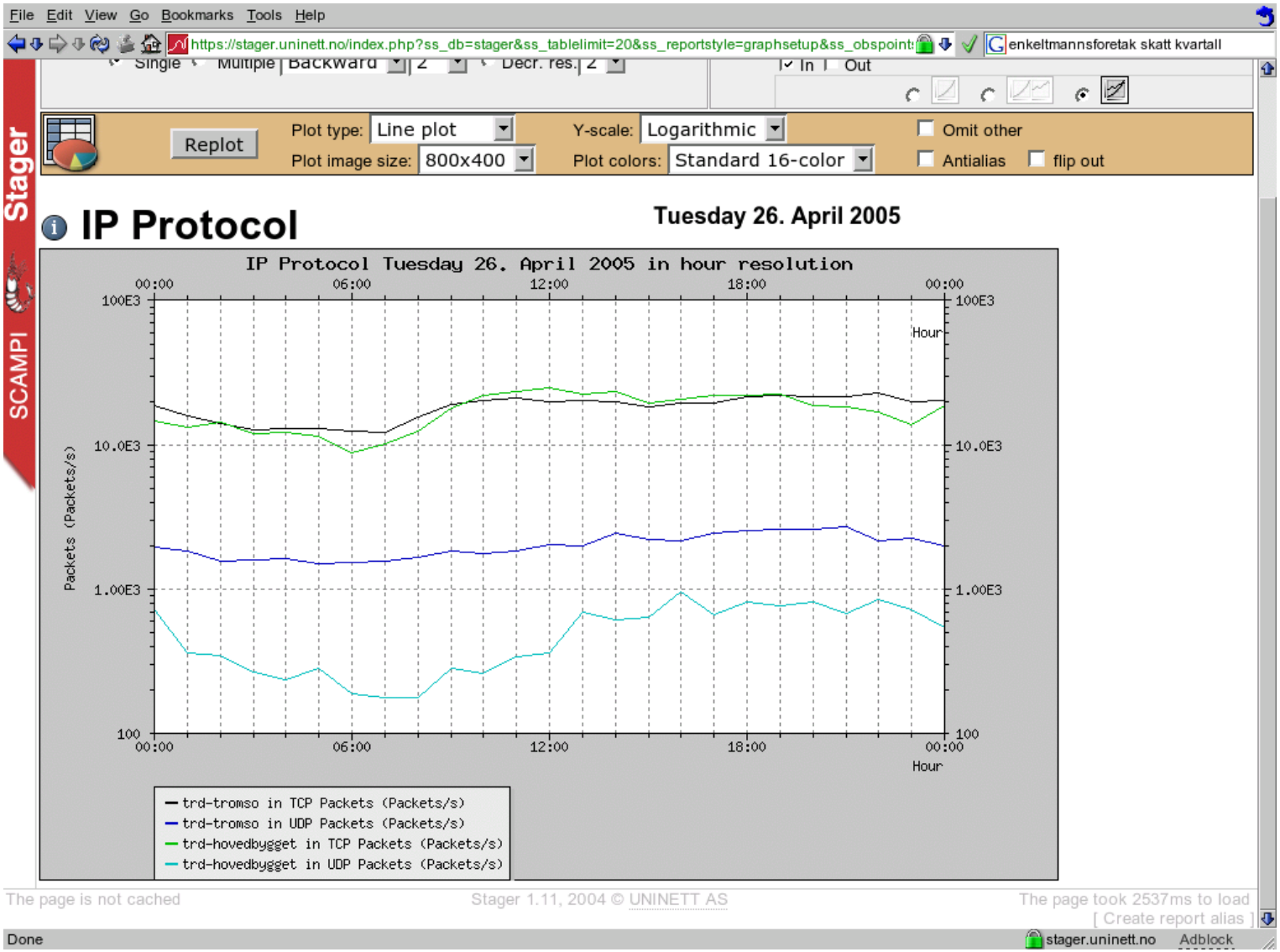
# Piechart


File Edit View Go Bookmarks Tools Help
https://stager.uninett.no/index.php?ss_db=stager&ss_tablelimit=20&ss_reportstyle=graphsetup&ss_obspoint
Stager
SCAMPI
Setup > Graph
Transport Layer Source Port
Advanced
Get Report
arneos [ Logout ]
Time: Thursday 28. April 2005
Thursday
Time resolution: Day
Week
Hour
Zoom in...
Single Multiple Backward 2 Decr. res. 2
Observation point
Show all groups
Show all devices
oslo-trd
In Out
Replot
Plot type: Piechart
Y-scale: Linear
Omit other
Plot image size: 800x400
Plot colors: Standard 16-color
Antialias
Transport Layer Source Port
Thursday 28. April 2005
Thursday 28. April 2005
Transport Layer Source Port Octets (bit/s) for oslo-trd in
1.4%
2.9%
17.9%
77.8%
www-http
ssh
ftp-data
Other
The page is not cached
Stager 1.11, 2004 © UNINETT AS
The page took 1025ms to load
Done
stager.uninett.no
Adblock

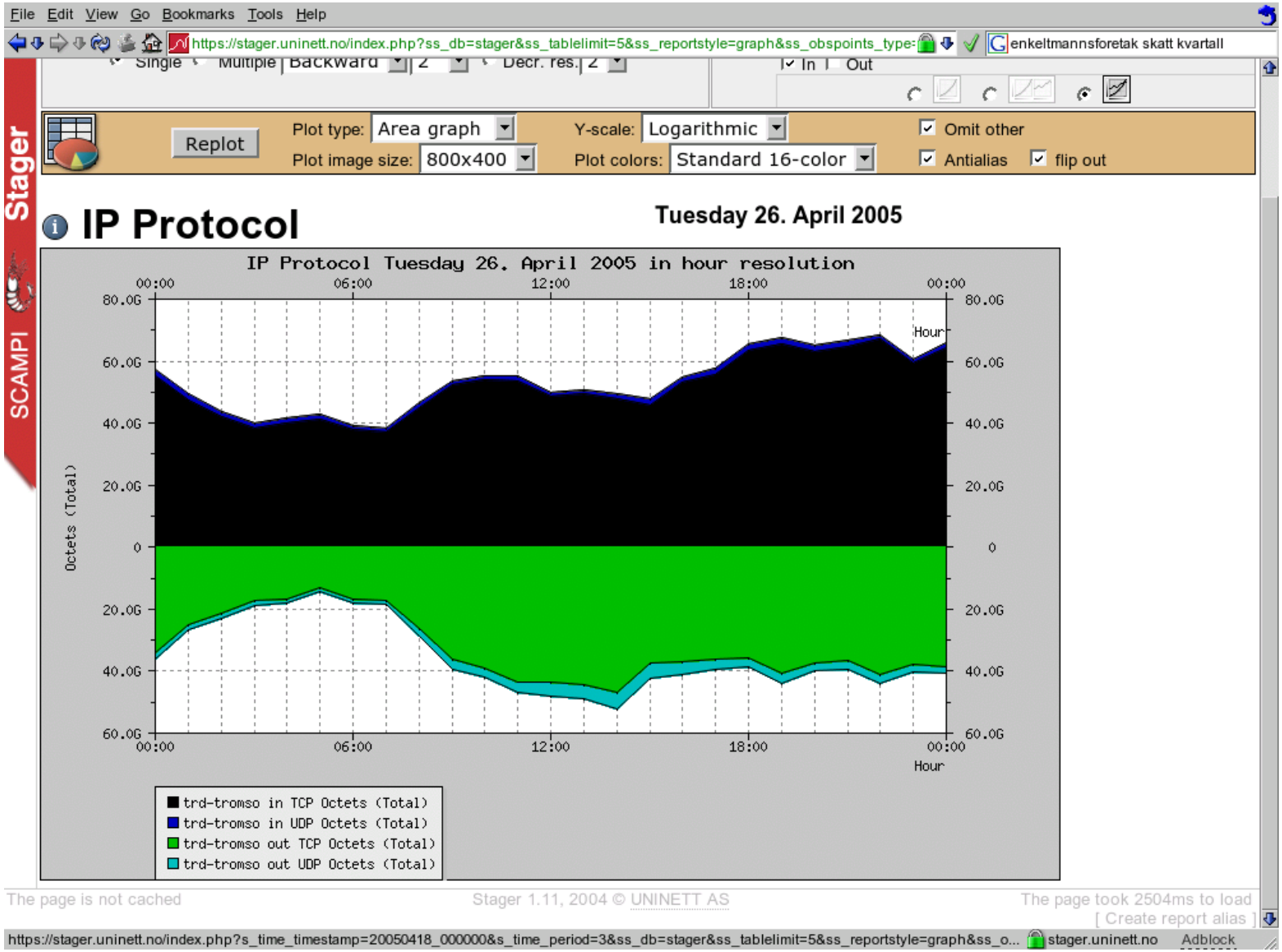
# Line plot of a DOS attack



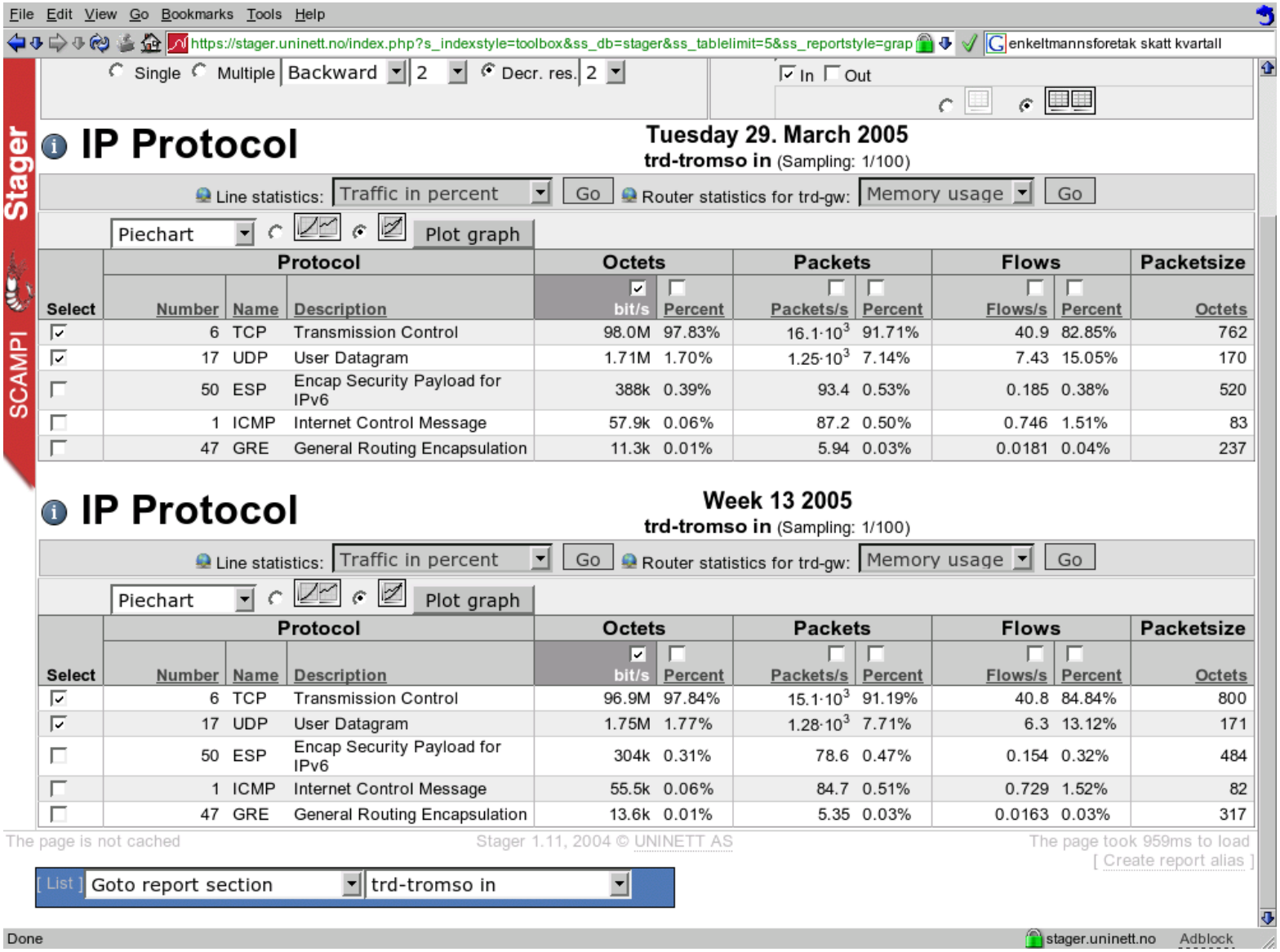
# Multiple observation points



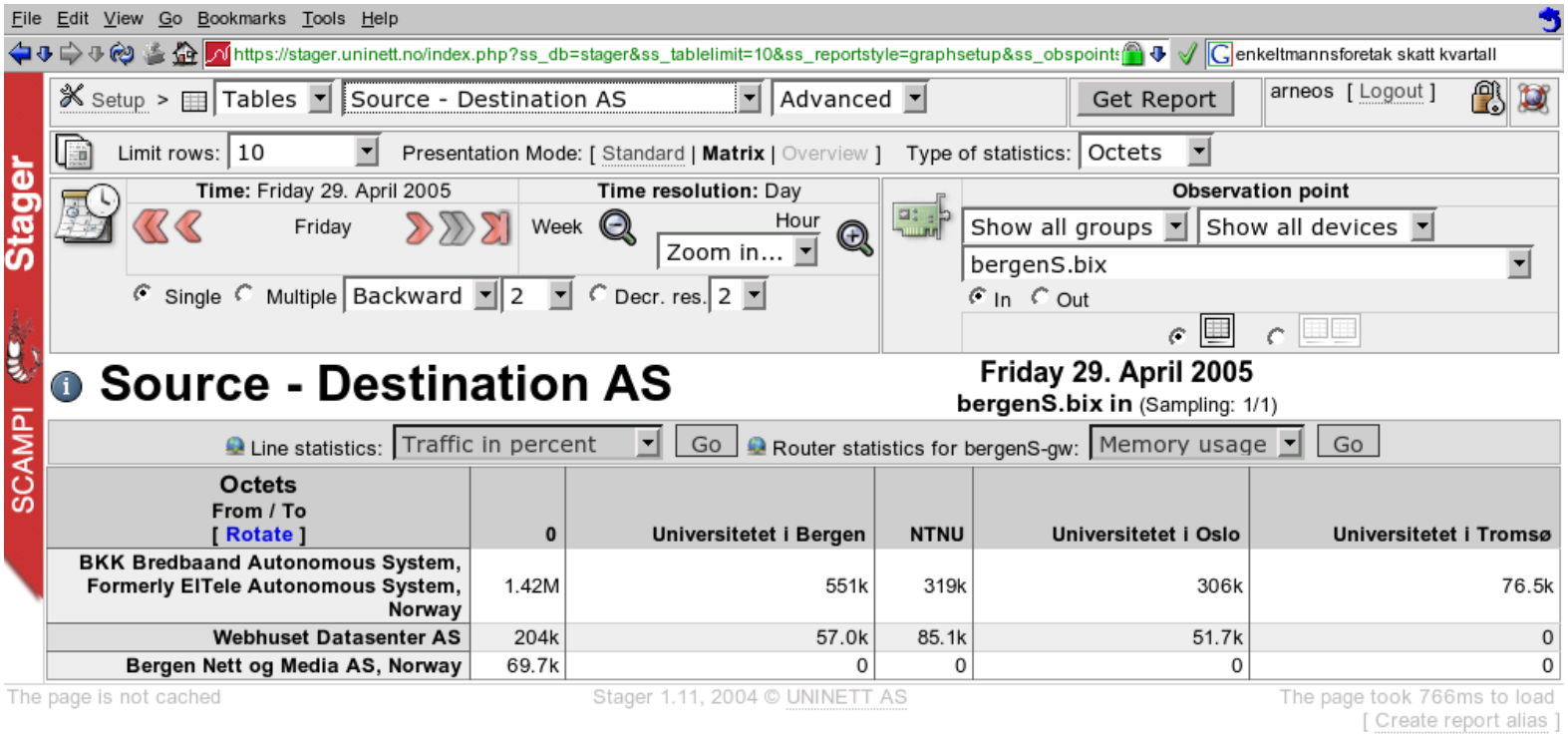
# Area graph


File Edit View Go Bookmarks Tools Help
https://stager.uninett.no/index.php?ss_db=stager&ss_tablelimit=5&ss_reportstyle=graph&ss_obspoints_type:
enkeltmannsforetak skatt kvartall
Single Multiple Backward 2 Decr. res. 2
In Out
Stager
SCAMPI
Replot
Plot type: Area graph
Y-scale: Logarithmic
Omit other
Plot image size: 800x400
Plot colors: Standard 16-color
Antialias
flip out
IP Protocol
Tuesday 26. April 2005
IP Protocol Tuesday 26. April 2005 in hour resolution
Octets (Total)
Hour
80.0G
60.0G
40.0G
20.0G
0
00:00
06:00
12:00
18:00
trd-tromso in TCP Octets (Total)
trd-tromso in UDP Octets (Total)
trd-tromso out TCP Octets (Total)
trd-tromso out UDP Octets (Total)
The page is not cached
Stager 1.11, 2004 © UNINETT AS
The page took 2504ms to load
[ Create report alias ]
https://stager.uninett.no/index.php?s_time_timestamp=20050418_000000&s_time_period=3&ss_db=stager&ss_tablelimit=5&ss_reportstyle=graph&ss_o...
stager.uninett.no
Adblock

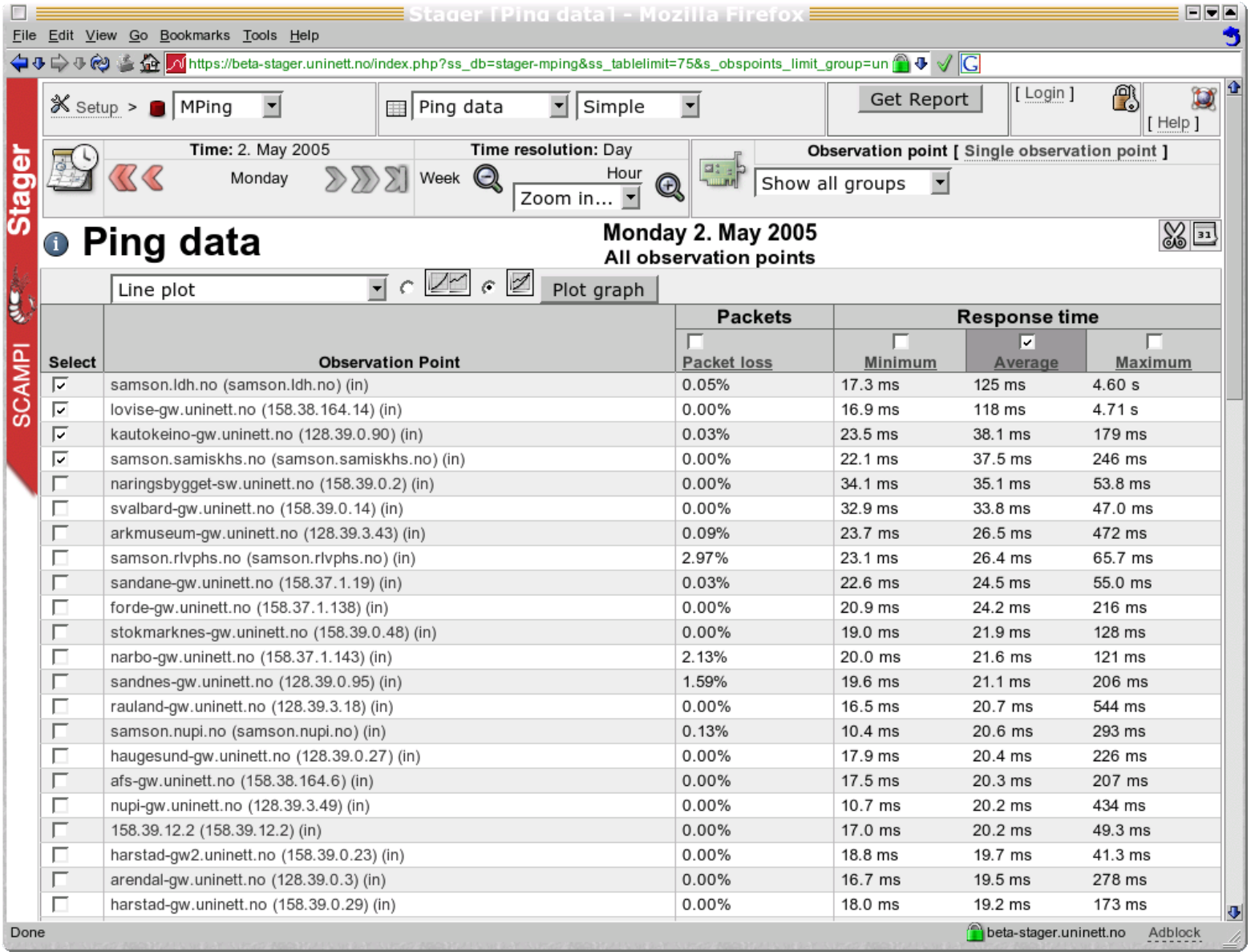
# Multiple time periods



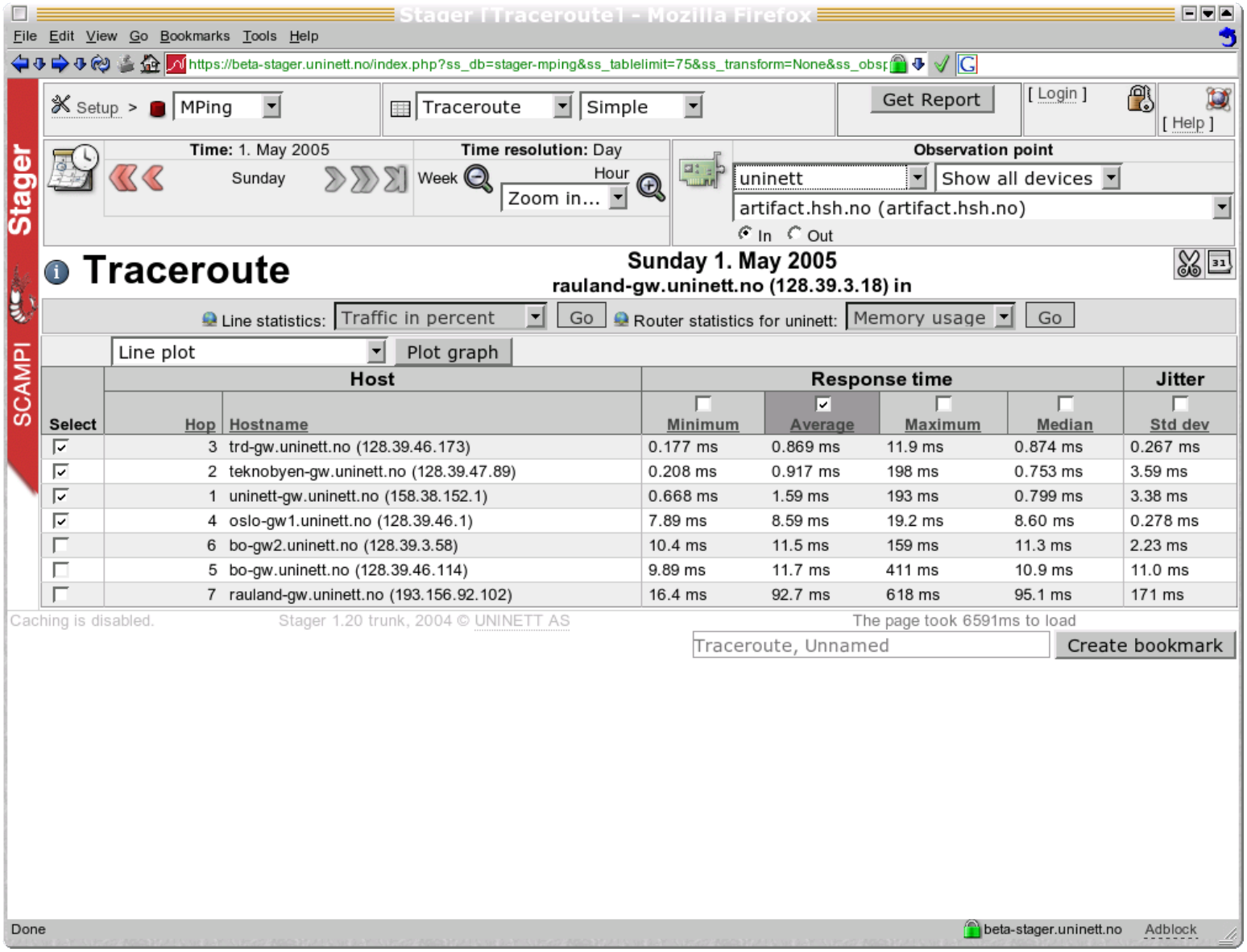
# Matrix


File Edit View Go Bookmarks Tools Help
https://stager.uninett.no/index.php?ss_db=stager&ss_tablelimit=10&ss_reportstyle=graphsetup&ss_obspoints
enkeltmannsforetak skatt kvartall
Stager
SCAMPI
Setup > Tables Source - Destination AS Advanced Get Report
arneos [ Logout ]
Limit rows: 10 Presentation Mode: [ Standard | Matrix | Overview ] Type of statistics: Octets
Time: Friday 29. April 2005 Time resolution: Day
Friday Week Hour Zoom in...
Single Multiple Backward 2 Decr. res. 2
Observation point
Show all groups Show all devices
bergenS.bix
In Out
Source - Destination AS
Friday 29. April 2005
bergenS.bix in (Sampling: 1/1)
Line statistics: Traffic in percent Go Router statistics for bergenS-gw: Memory usage Go
Octets
From / To
[ Rotate ]
0
Universitetet i Bergen
NTNU
Universitetet i Oslo
Universitetet i Tromsø
BKK Bredbaand Autonomous System, Formerly ElTele Autonomous System, Norway
1.42M
551k
319k
306k
76.5k
Webhuset Datasenter AS
204k
57.0k
85.1k
51.7k
0
Bergen Nett og Media AS, Norway
69.7k
0
0
0
0
The page is not cached
Stager 1.11, 2004 © UNINETT AS
The page took 766ms to load
[ Create report alias ]
Done
stager.uninett.no
Adblock

# Mping


Stager [Ping data] - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://beta-stager.uninett.no/index.php?ss_db=stager-mping&ss_tablelimit=75&s_obspoints_limit_group=un
Setup > MPing
Ping data
Simple
Get Report
[ Login ]
[ Help ]
Time: 2. May 2005
Monday
Time resolution: Day
Week
Hour
Zoom in...
Observation point [ Single observation point ]
Show all groups
Stager
SCAMPI
Ping data
Monday 2. May 2005
All observation points
Line plot
Plot graph
Select
Observation Point
Packets
Packet loss
Response time
Minimum
Average
Maximum
samson.ldh.no (samson.ldh.no) (in) 0.05% 17.3 ms 125 ms 4.60 s
lovise-gw.uninett.no (158.38.164.14) (in) 0.00% 16.9 ms 118 ms 4.71 s
kautokeino-gw.uninett.no (128.39.0.90) (in) 0.03% 23.5 ms 38.1 ms 179 ms
samson.samiskhs.no (samson.samiskhs.no) (in) 0.00% 22.1 ms 37.5 ms 246 ms
naringsbygget-sw.uninett.no (158.39.0.2) (in) 0.00% 34.1 ms 35.1 ms 53.8 ms
svalbard-gw.uninett.no (158.39.0.14) (in) 0.00% 32.9 ms 33.8 ms 47.0 ms
arkmuseum-gw.uninett.no (128.39.3.43) (in) 0.09% 23.7 ms 26.5 ms 472 ms
samson.rlvphs.no (samson.rlvphs.no) (in) 2.97% 23.1 ms 26.4 ms 65.7 ms
sandane-gw.uninett.no (158.37.1.19) (in) 0.03% 22.6 ms 24.5 ms 55.0 ms
forde-gw.uninett.no (158.37.1.138) (in) 0.00% 20.9 ms 24.2 ms 216 ms
stokmarknes-gw.uninett.no (158.39.0.48) (in) 0.00% 19.0 ms 21.9 ms 128 ms
narbo-gw.uninett.no (158.37.1.143) (in) 2.13% 20.0 ms 21.6 ms 121 ms
sandnes-gw.uninett.no (128.39.0.95) (in) 1.59% 19.6 ms 21.1 ms 206 ms
rauland-gw.uninett.no (128.39.3.18) (in) 0.00% 16.5 ms 20.7 ms 544 ms
samson.nupi.no (samson.nupi.no) (in) 0.13% 10.4 ms 20.6 ms 293 ms
haugesund-gw.uninett.no (128.39.0.27) (in) 0.00% 17.9 ms 20.4 ms 226 ms
afs-gw.uninett.no (158.38.164.6) (in) 0.00% 17.5 ms 20.3 ms 207 ms
nupi-gw.uninett.no (128.39.3.49) (in) 0.00% 10.7 ms 20.2 ms 434 ms
158.39.12.2 (158.39.12.2) (in) 0.00% 17.0 ms 20.2 ms 49.3 ms
harstad-gw2.uninett.no (158.39.0.23) (in) 0.00% 18.8 ms 19.7 ms 41.3 ms
arendal-gw.uninett.no (128.39.0.3) (in) 0.00% 16.7 ms 19.5 ms 278 ms
harstad-gw.uninett.no (158.39.0.29) (in) 0.00% 18.0 ms 19.2 ms 173 ms
Done
beta-stager.uninett.no
Adblock

# Mping traceroute




| Select | Hop | Hostname | Response time: Minimum | Response time: Average | Response time: Maximum | Response time: Median | Jitter: Std dev |
|---|---|---|---|---|---|---|---|
| ☑ | 3 | trd-gw.uninett.no (128.39.46.173) | 0.177 ms | 0.869 ms | 11.9 ms | 0.874 ms | 0.267 ms |
| ☑ | 2 | teknobyen-gw.uninett.no (128.39.47.89) | 0.208 ms | 0.917 ms | 198 ms | 0.753 ms | 3.59 ms |
| ☑ | 1 | uninett-gw.uninett.no (158.38.152.1) | 0.668 ms | 1.59 ms | 193 ms | 0.799 ms | 3.38 ms |
| ☑ | 4 | oslo-gw1.uninett.no (128.39.46.1) | 7.89 ms | 8.59 ms | 19.2 ms | 8.60 ms | 0.278 ms |
| ☐ | 6 | bo-gw2.uninett.no (128.39.3.58) | 10.4 ms | 11.5 ms | 159 ms | 11.3 ms | 2.23 ms |
| ☐ | 5 | bo-gw.uninett.no (128.39.46.114) | 9.89 ms | 11.7 ms | 411 ms | 10.9 ms | 11.0 ms |
| ☐ | 7 | rauland-gw.uninett.no (193.156.92.102) | 16.4 ms | 92.7 ms | 618 ms | 95.1 ms | 171 ms |