Stager – A Generic Tool for Presenting Network Statistics

FloCon 2010
January 11-14, 2010

Arne Øslebø
arne.oslebo@uninett.no

What is Stager?

- A web based tool for presenting and aggregating most types of network statistics
- Store high level reports in database
- Detailed reports from other sources
- Access control
- Stable version
  - NetFlow
  - Qflow - IPFIX probe with extra QoS attributes
- Development version
  - Qstream, Mping, Asmping, Rude/Crude, SNMP
- http://software.uninett.no/stager/
  - GPL license

UNINETT

Overview report

Setup Back | Protocol | overview | Octets percent | 10 | Show | Add

All interfaces | vpn-gw.uio.no | In | none | 1

Protocol

Thursday 15. October 2009, 21:00

All observation points (in)

Pie chart | Other | Plot graph

Select	Observation Point	Octets - percent							
		TCP	UDP	GRE	ESP	IPv6	ICMP	PIM	IPv6-ICMP
	elverum-gw.elverum-gw2-1	0.00%	0.00%	0.00%	0.00%	0.00%	100.00%	0.00%	0.00%
	oslo-trd2	0.00%	0.00%	0.00%	0.00%	0.00%	100.00%	0.00%	0.00%
	trd-tromso2	0.00%	0.00%	0.00%	0.00%	0.00%	75.68%	24.32%	0.00%
	elverum-gw.elverum-gw2-2	0.00%	36.36%	0.00%	0.00%	0.00%	63.64%	0.00%	0.00%
	hoytek-niva	0.64%	65.75%	0.00%	0.00%	0.00%	33.61%	0.00%	0.00%
	trd-niva	3.86%	66.29%	0.00%	0.00%	0.00%	29.84%	0.00%	0.00%
	oslo-oslomsh	19.42%	53.90%	0.00%	0.00%	0.00%	26.68%	0.00%	0.00%
	teknobyen2-teknobyen	5.89%	3.82%	0.00%	0.00%	0.00%	23.70%	66.59%	0.00%
	nhh2-nhh	7.41%	69.95%	0.00%	0.00%	0.00%	22.64%	0.00%	0.00%
	nhh-gw2.nhh-gw	7.41%	69.95%	0.00%	0.00%	0.00%	22.64%	0.00%	0.00%

Processing the report took 486.82ms

UNINETT

Global report

Setup Back | Source port | global | Standard | 10 | Show | Add | Bookmarks..

All interfaces | uninett.uninett-wlan_ans | In | none | 1

Source port

Tuesday 12. January 2010, 3:00
All observation points (in)

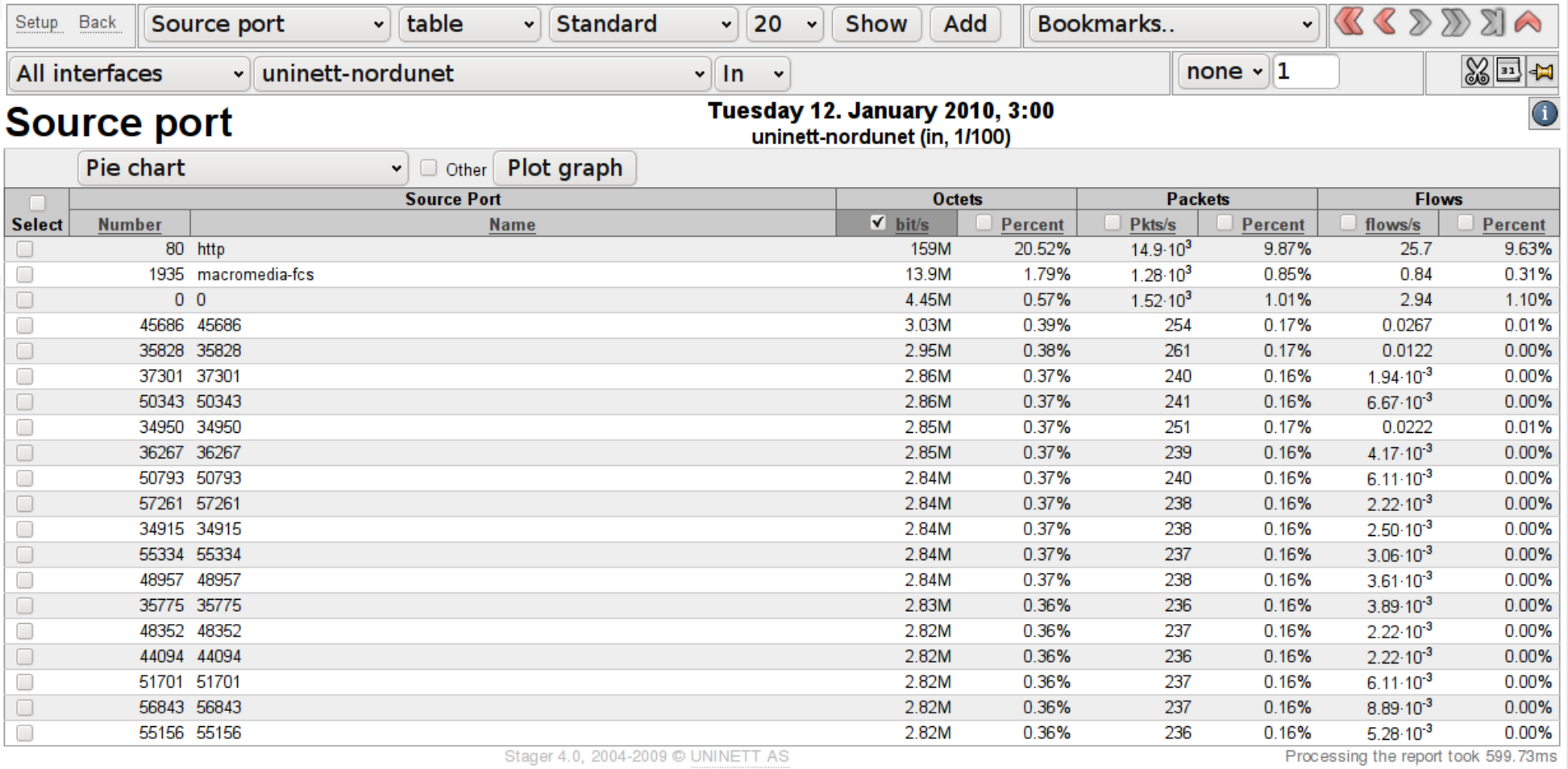
Select	Port number	Port name	Observation point	Octets		Packets		Flows	
				bit/s	Percent	Pkts/s	Percent	flows/s	Percent
	80	http	uninett-nordunet	159M	20.52%	$14.9 \cdot 10^3$	9.87%	25.7	9.63%
	80	http	uninett-nordunet4	127M	17.12%	$12.1 \cdot 10^3$	9.93%	22.3	11.04%
	80	http	trd-oslo	117M	19.04%	$11.2 \cdot 10^3$	10.45%	23.7	11.90%
	80	http	oslo-dnmi	92.3M	92.03%	$8.92 \cdot 10^3$	66.50%	13.1	88.40%
	33661	33661	uninett.uninett-nett	85.5M	93.45%	$7.38 \cdot 10^3$	81.17%	$5.83 \cdot 10^{-3}$	0.03%
	80	http	oslo-gw.stolav-gw1	85.0M	14.92%	$8.08 \cdot 10^3$	8.93%	19.2	12.24%
	49152	49152	nix.nix	78.6M	44.92%	$7.31 \cdot 10^3$	24.25%	0.188	0.39%
	80	http	oslo-trd	73.4M	9.06%	$6.61 \cdot 10^3$	5.97%	10.6	5.24%
	80	http	bergen-oslo	68.6M	19.68%	$7.05 \cdot 10^3$	12.18%	17.8	21.07%
	48959	48959	trofast-gw1	65.3M	54.92%	$5.79 \cdot 10^3$	54.89%	$4.17 \cdot 10^{-3}$	0.05%

Processing the report took 681.74ms

4

UNINETT

Detailed report



Select	Source Port		Octets		Packets		Flows	
	Number	Name	bit/s	Percent	Pkts/s	Percent	flows/s	Percent
	80	http	159M	20.52%	$14.9 \cdot 10^{3}$	9.87%	25.7	9.63%
	1935	macromedia-fcs	13.9M	1.79%	$1.28 \cdot 10^{3}$	0.85%	0.84	0.31%
	0	0	4.45M	0.57%	$1.52 \cdot 10^{3}$	1.01%	2.94	1.10%
	45686	45686	3.03M	0.39%	254	0.17%	0.0267	0.01%
	35828	35828	2.95M	0.38%	261	0.17%	0.0122	0.00%
	37301	37301	2.86M	0.37%	240	0.16%	$1.94 \cdot 10^{-3}$	0.00%
	50343	50343	2.86M	0.37%	241	0.16%	$6.67 \cdot 10^{-3}$	0.00%
	34950	34950	2.85M	0.37%	251	0.17%	0.0222	0.01%
	36267	36267	2.85M	0.37%	239	0.16%	$4.17 \cdot 10^{-3}$	0.00%
	50793	50793	2.84M	0.37%	240	0.16%	$6.11 \cdot 10^{-3}$	0.00%
	57261	57261	2.84M	0.37%	238	0.16%	$2.22 \cdot 10^{-3}$	0.00%
	34915	34915	2.84M	0.37%	238	0.16%	$2.50 \cdot 10^{-3}$	0.00%
	55334	55334	2.84M	0.37%	237	0.16%	$3.06 \cdot 10^{-3}$	0.00%
	48957	48957	2.84M	0.37%	238	0.16%	$3.61 \cdot 10^{-3}$	0.00%
	35775	35775	2.83M	0.36%	236	0.16%	$3.89 \cdot 10^{-3}$	0.00%
	48352	48352	2.82M	0.36%	237	0.16%	$2.22 \cdot 10^{-3}$	0.00%
	44094	44094	2.82M	0.36%	236	0.16%	$2.22 \cdot 10^{-3}$	0.00%
	51701	51701	2.82M	0.36%	237	0.16%	$6.11 \cdot 10^{-3}$	0.00%
	56843	56843	2.82M	0.36%	237	0.16%	$8.89 \cdot 10^{-3}$	0.00%
	55156	55156	2.82M	0.36%	236	0.16%	$5.28 \cdot 10^{-3}$	0.00%

Processing the report took 599.73ms

UNINETT

Graph

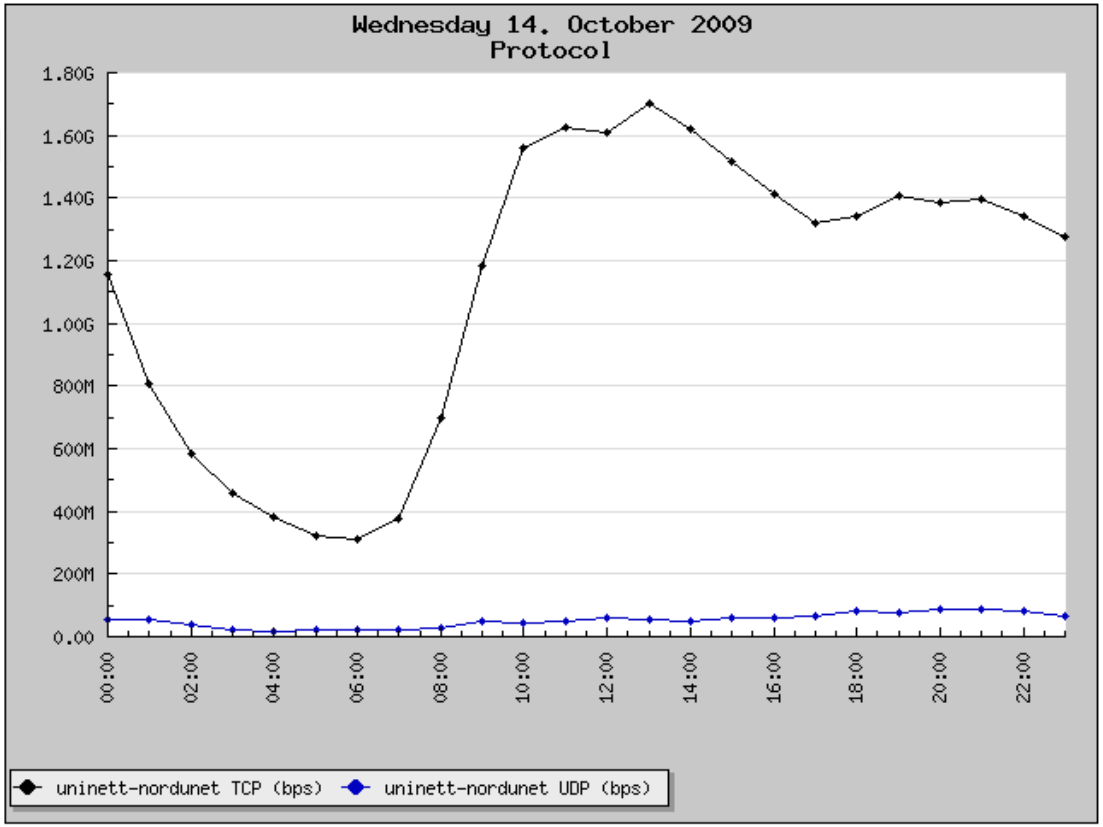
Setup Back | Protocol | table | Octet details | 20 | Show | Add | hour...

oslo-gw | uninett-nordunet | In | none | 1

Protocol

Wednesday 14. October 2009

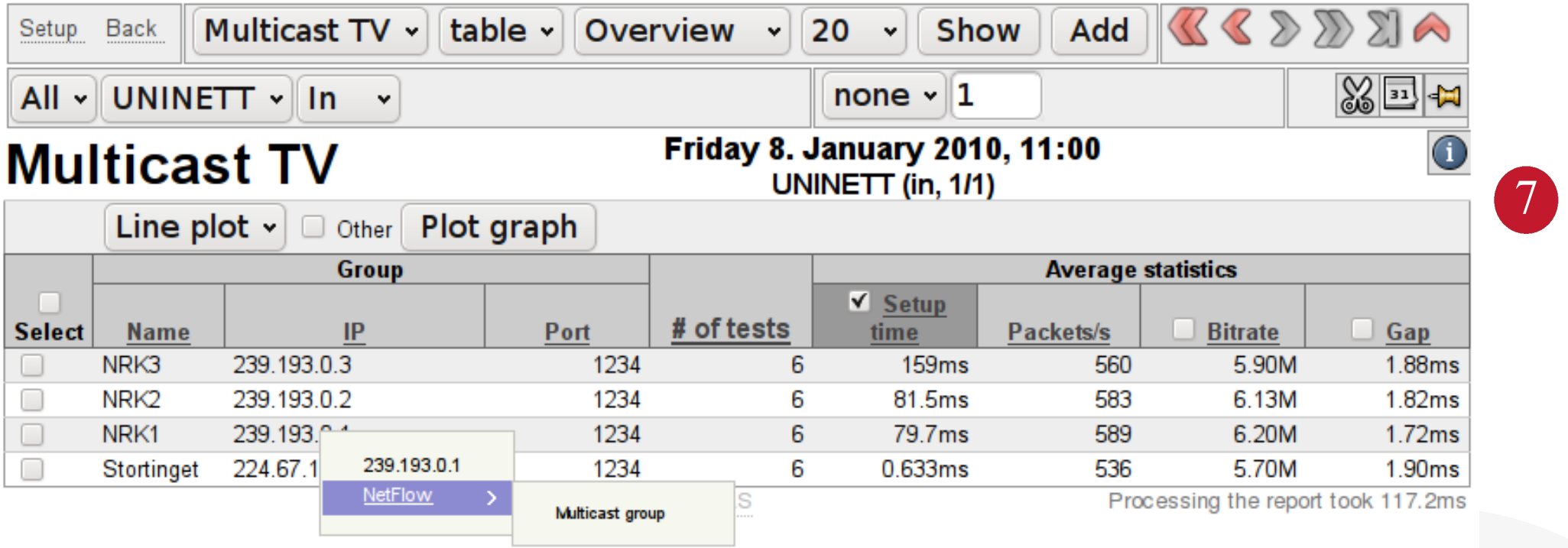
[Return to table] | Line plot | Linear | Other | Replot



Processing the report took 168.55ms

UNINETT

Context menus



Multiple reports

Setup Back | Protocol | table | Standard | 5 | Show | Add | Bookmarks.. | hour...

All interfaces | trd-teknobyen | In | none | 1

Protocol

Wednesday 14. October 2009
trd-teknobyen (in, 1/100)

Line plot | Other | Plot graph

Select	Protocol Number	Protocol Name	Octets bit/s	Octets Percent	Packets Pkts/s	Packets Percent	Flows flows/s	Flows Percent
	6	TCP	75.9M	98.70%	$7.62 \cdot 10^3$	93.33%	4.95	64.15%
	17	UDP	915k	1.19%	442	5.41%	2.04	26.42%
	1	ICMP	52.0k	0.07%	71.4	0.87%	0.691	8.96%
	47	GRE	28.2k	0.04%	26.3	0.32%	0.0178	0.23%
	103	PIM	2.46k	0.00%	5.22	0.06%	0.0178	0.23%

Protocol

Tuesday 13. October 2009
trd-teknobyen (in, 1/100)

Line plot | Other | Plot graph

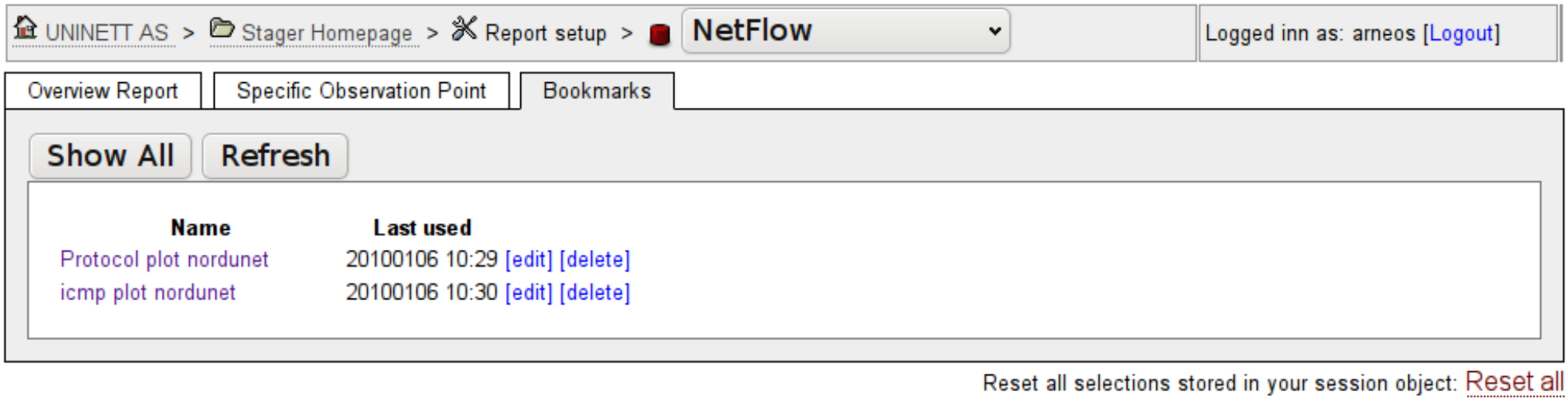
Select	Protocol Number	Protocol Name	Octets bit/s	Octets Percent	Packets Pkts/s	Packets Percent	Flows flows/s	Flows Percent
	6	TCP	152M	99.10%	$14.3 \cdot 10^3$	95.46%	5.94	66.18%
	17	UDP	1.17M	0.76%	545	3.63%	2.23	24.79%
	50	ESP	92.8k	0.06%	14.1	0.09%	$3.98 \cdot 10^{-3}$	0.04%
	47	GRE	62.4k	0.04%	37.8	0.25%	0.0183	0.20%
	1	ICMP	57.3k	0.04%	79.4	0.53%	0.77	8.57%

Processing the report took 265.77ms

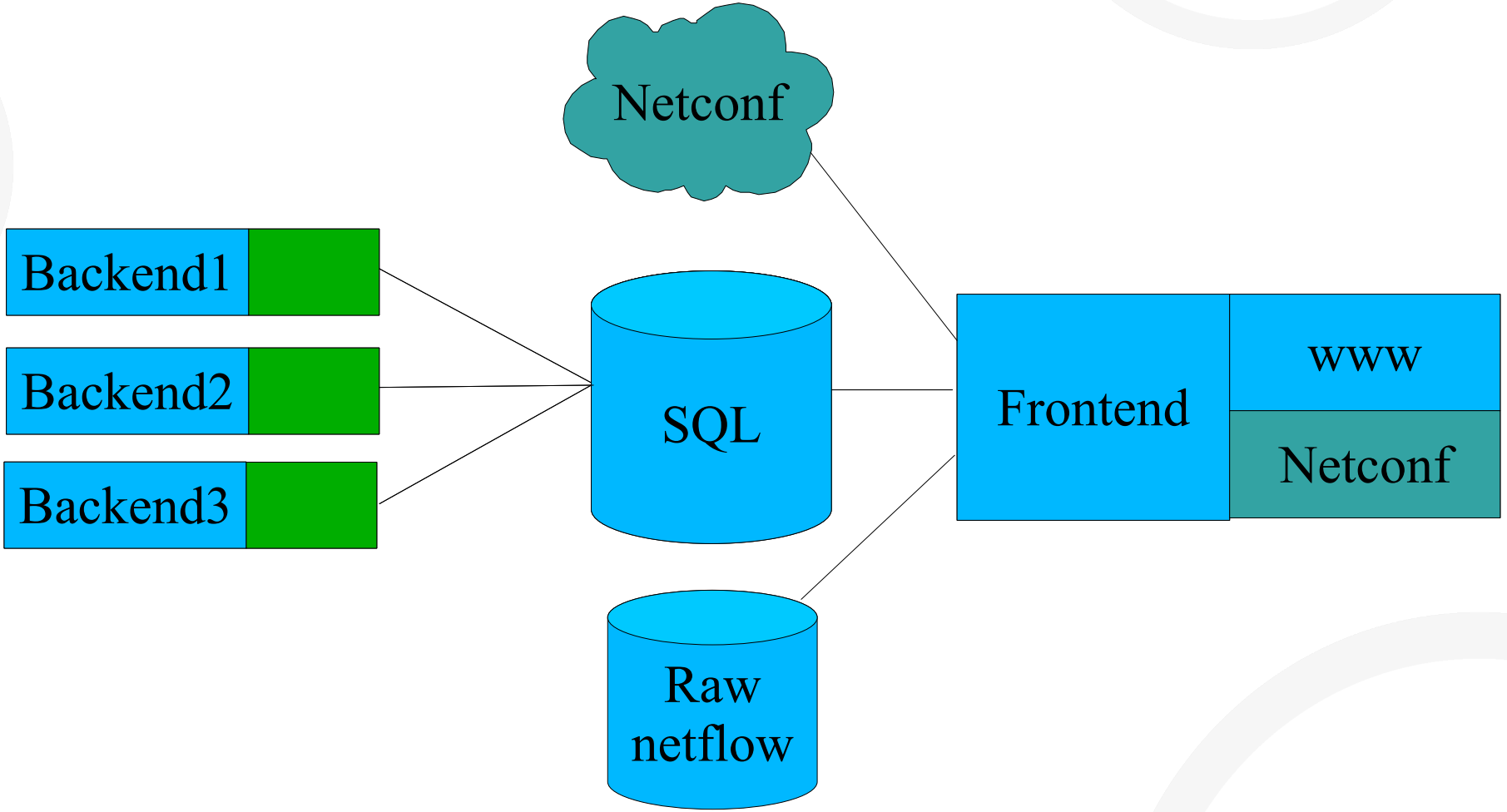
UNINETT

Bookmarks

- Setting up multiple reports can involve a lot of clicking
- Possible to create bookmarks with relative time
  - Always show last hour, day, week etc.



Stager architecture



UNINETT

Template based

- All data for a report is stored in a database or collected from other sources
- XML based template specifies how the frontend should present the data
  - bps, pps, %, temperature, IP address etc.
- Built in functions
  - divideandmultiply, persec, bitpersec, concat etc.
- Transformations
  - Table, overview, global (and matrix).
- Multiple views for each transformation.
  - Specifies which data types should be visible
- New reports can be added without code changes to the frontend

UNINETT

Backend robustness

- Graceful handling of database downtime
  - Store reports to files
  - Insert into database when possible
- Avoid multiple instances of the same backend
  - Wait for previous instances that are still processing the raw data
  - Detect dead locks and memory starvations
- Supports anycast for NetFlow
  - Raw NetFlow data automatically processed by active collector

UNINETT

Anycast support

- All collectors are configured to collect data from all routers
- Script automatically detects which routers a collector actually collects data from
  - Development version: raw NetFlow data automatically copied to one server
- Collectors run Linux
- Loopback interface configured with anycast IP address
- Runs Quagga routing software
  - BGP peering
- Sanity check scripts
  - Takes down BGP peering if problems

UNINETT

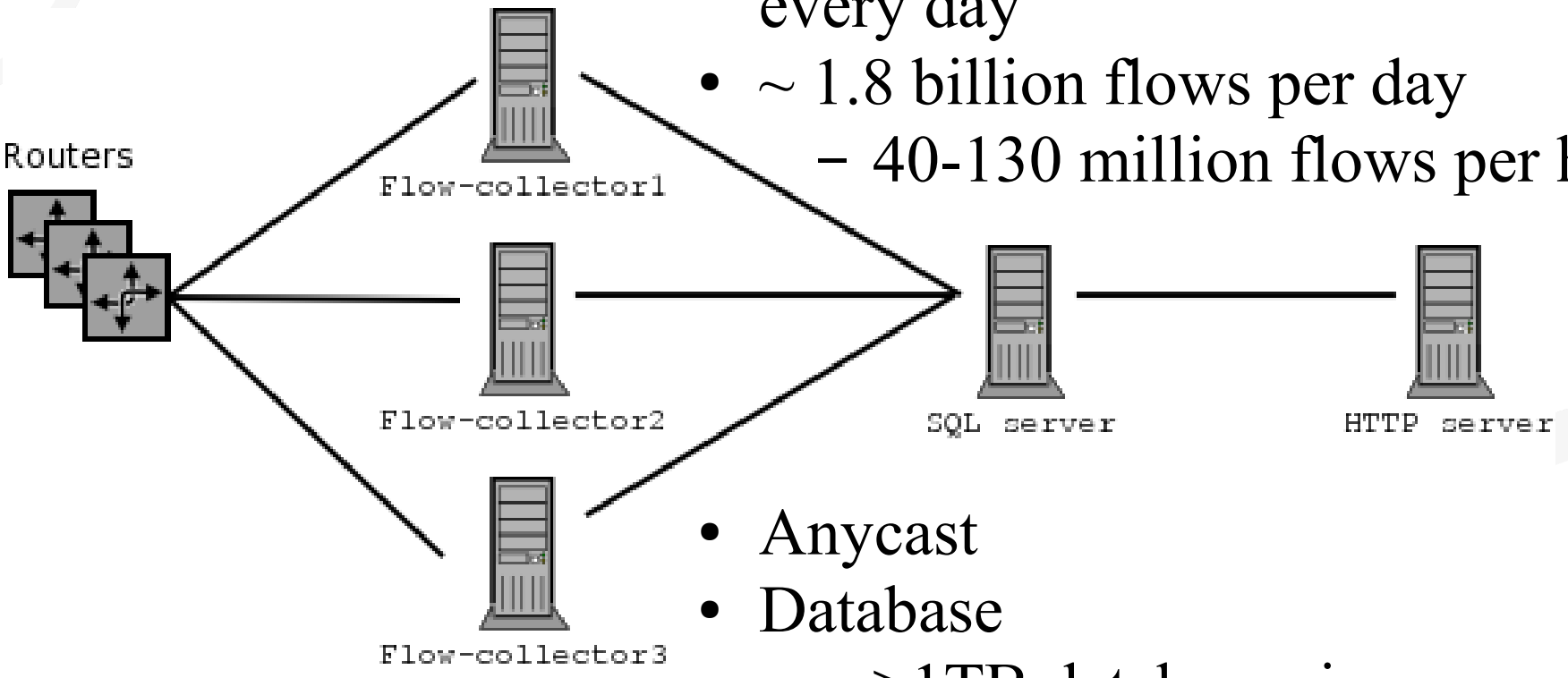
Netflow in Stager

- Runs nfdump
- Reports generated every hour
- Aggregated to day, week, month and year
- Available reports
  - Summary
  - Interface
  - Src/Dst AS/IP/Port (Top X)
  - Protocol
  - Mulicast
    - Src AS
    - Src IP
    - Groups (Dst IP)
- Possible to view raw NetFlow data for more details
- Reports follow links, not interfaces

UNINETT

Our NetFlow setup

- 34 routers
- 439 interfaces
- 1/100 sampling rate on most routers
- ~25Gb of compressed raw Netflow data every day
- ~ 1.8 billion flows per day
  - 40-130 million flows per hour



- Anycast
- Database
  - >1TB database size
  - >800 millions entries in a single table

UNINETT

NetFlow performance

Backend

Data from January 5 between 12:00-13:00

	Col1	Col2	Col3	Total
Netflow size	470MB	62MB	654MB	1186MB
Sequentially	3min 33s	1min 36s	6min 5s	11min 14s
Simultaneously	3min 36s	1min 38s	6min 17s	11min 31s

Frontend

Report	Time
IP Protocol overview	1540ms
IP Protocol overview (previous timeperiod)	487ms
IP Protocol detailed report	223ms
Top Src Port overview	1068ms
Top Src Port overview (previous timeperiod)	507ms
Top Src Port details	442ms
Top Src IP address from raw NetFlow	3220ms

UNINETT

Upcoming features

- Improved anycast support
- Improved visualization
  - Today only simple graphs and pie charts are supported
- Better integration between different data sources
  - Shows reports from different sources on the same screen
- Anomaly detection
  - Today we only have simple threshold alerts
- Improved NetFlow reports
  - Top X + specified ports/IP addresses/AS numbers

UNINETT

Questions?

Arne Oslebo
arne.oslebo@uninett.no

http://software.uninett.no/stager

UNINETT