Appflow - categorizing network traffic at 10Gbps using commodity hardware

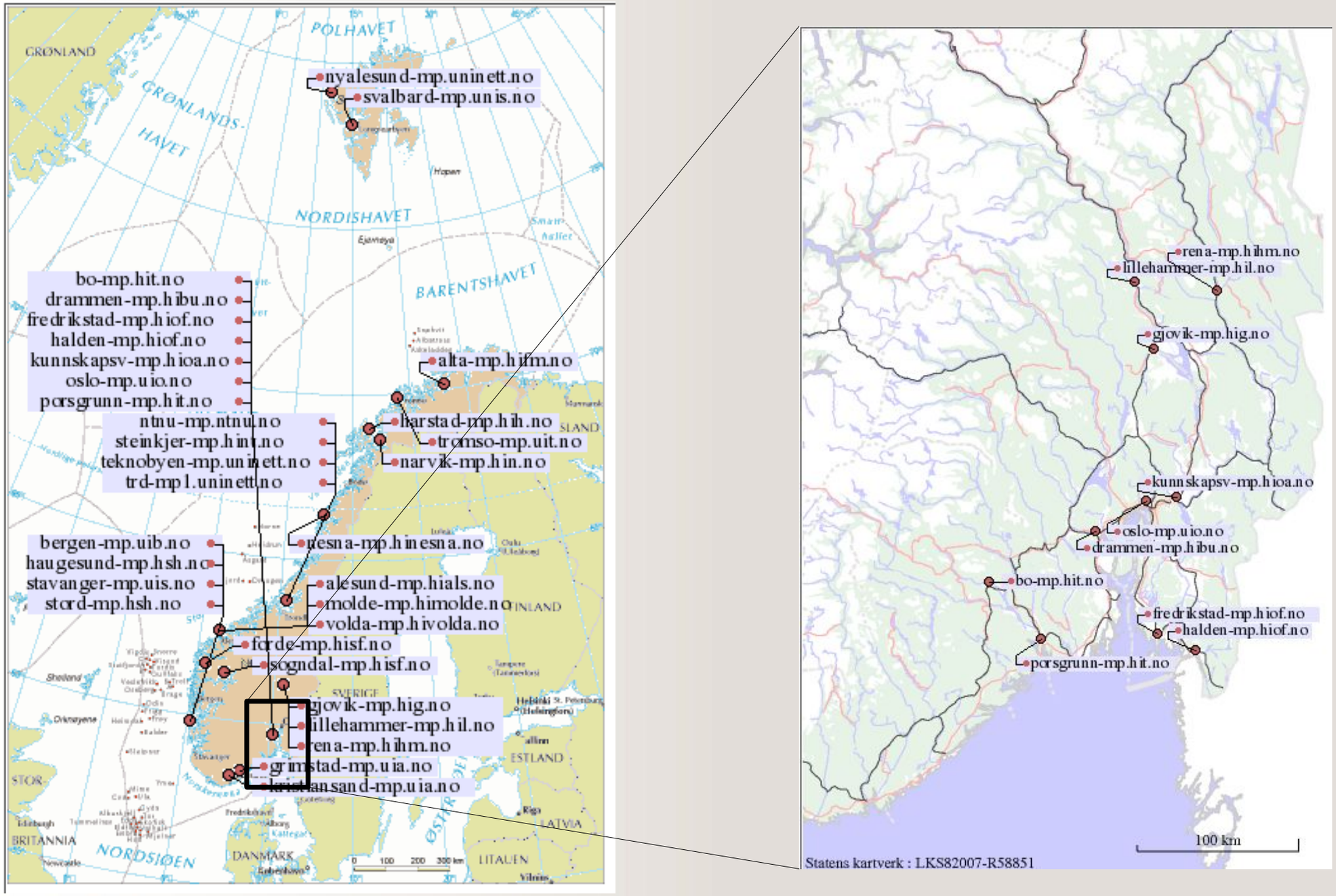
TNC2014

May 21, 2014

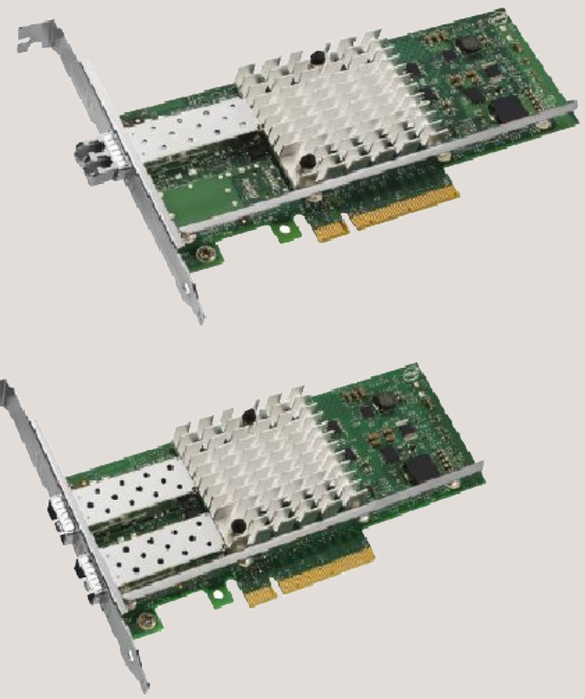
Arne Øslebø, arne.oslebo@uninett.no

UNINETT

UNINETT monitoring infrastructure

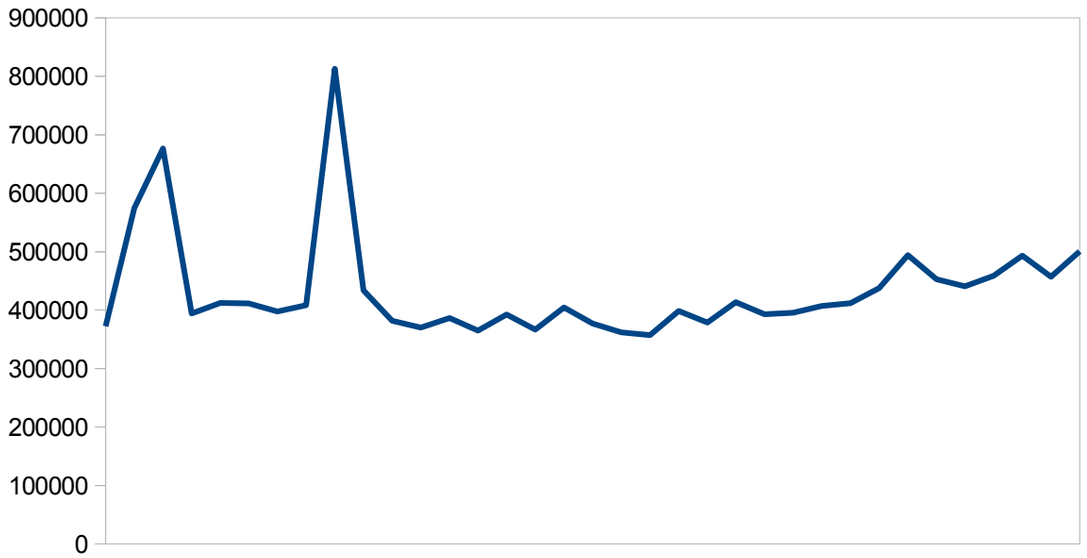


Intel X520 family of NICs

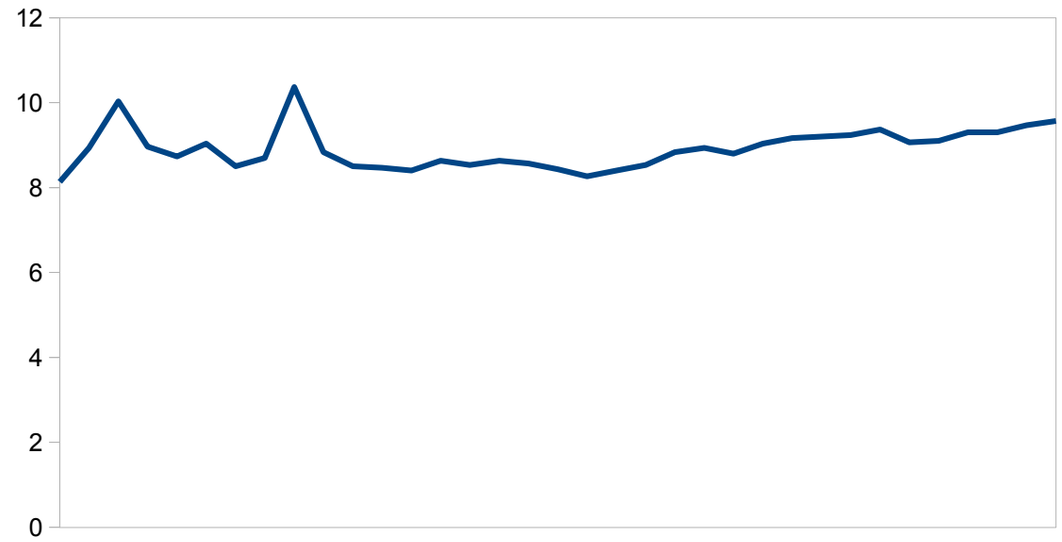


- Support multi-core processors
  - Hardware based load balancing
- DMA transfer of captured packets
- pf_ring driver

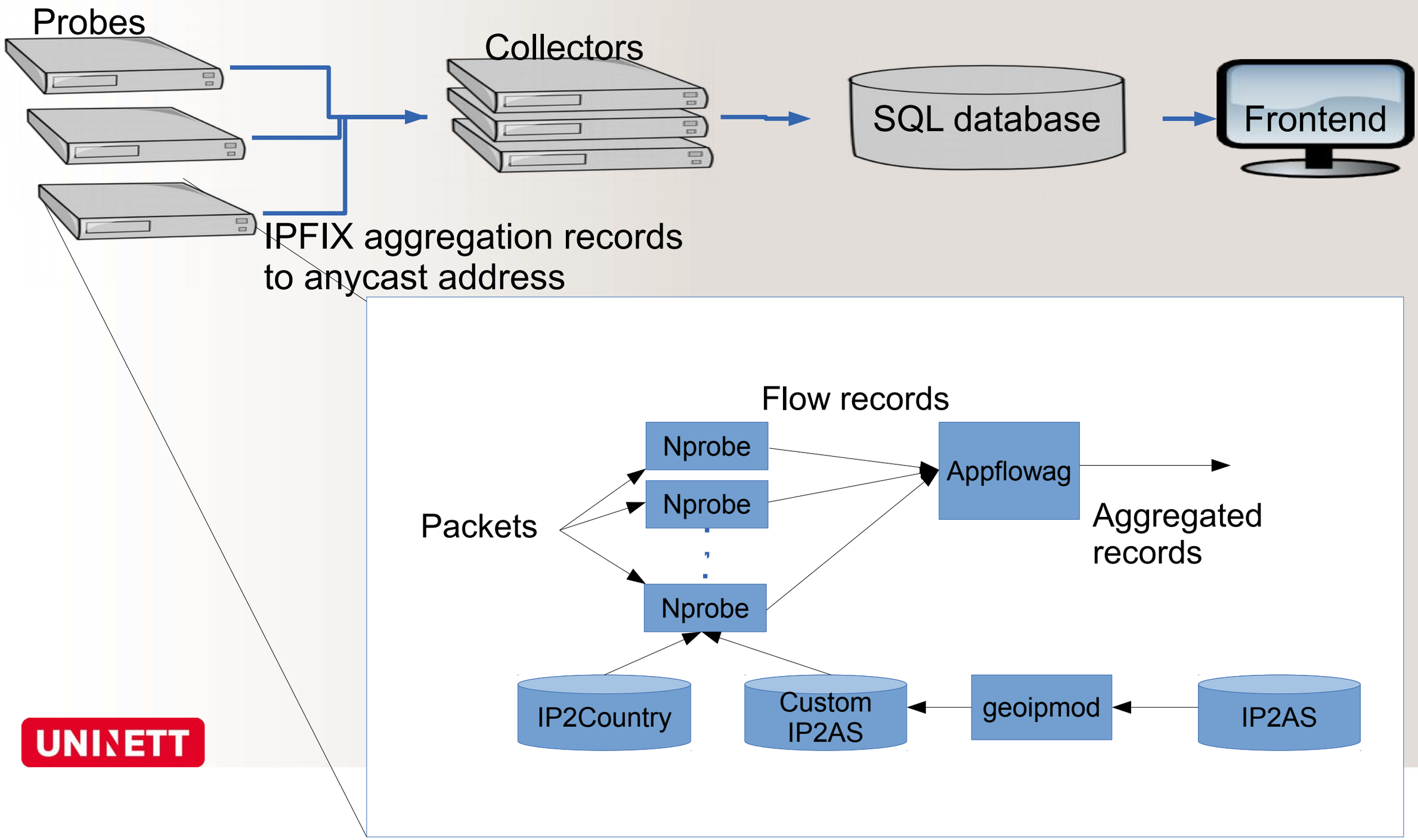
Packets per second



Total CPU usage
8 cores is use

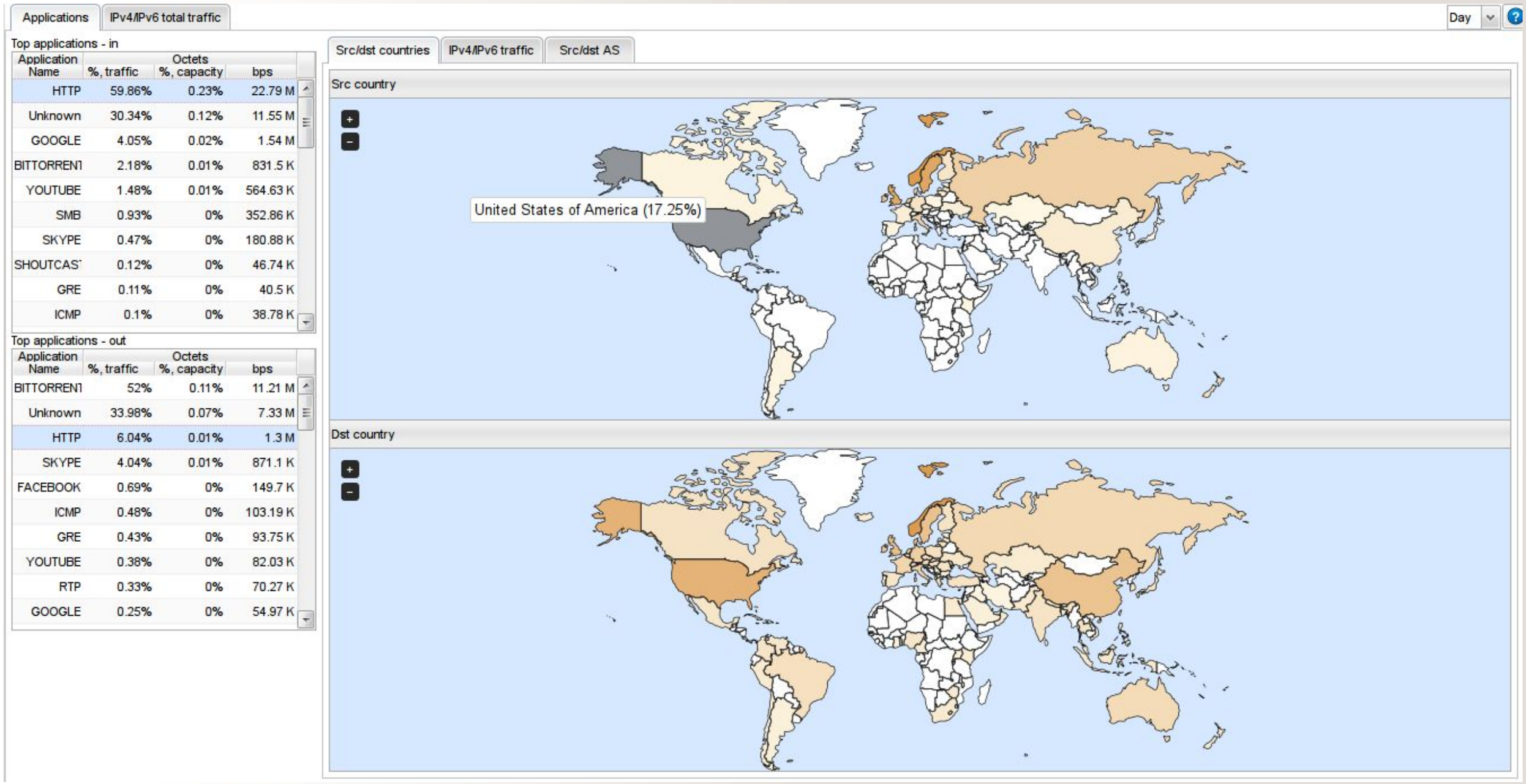


Appflow architecture

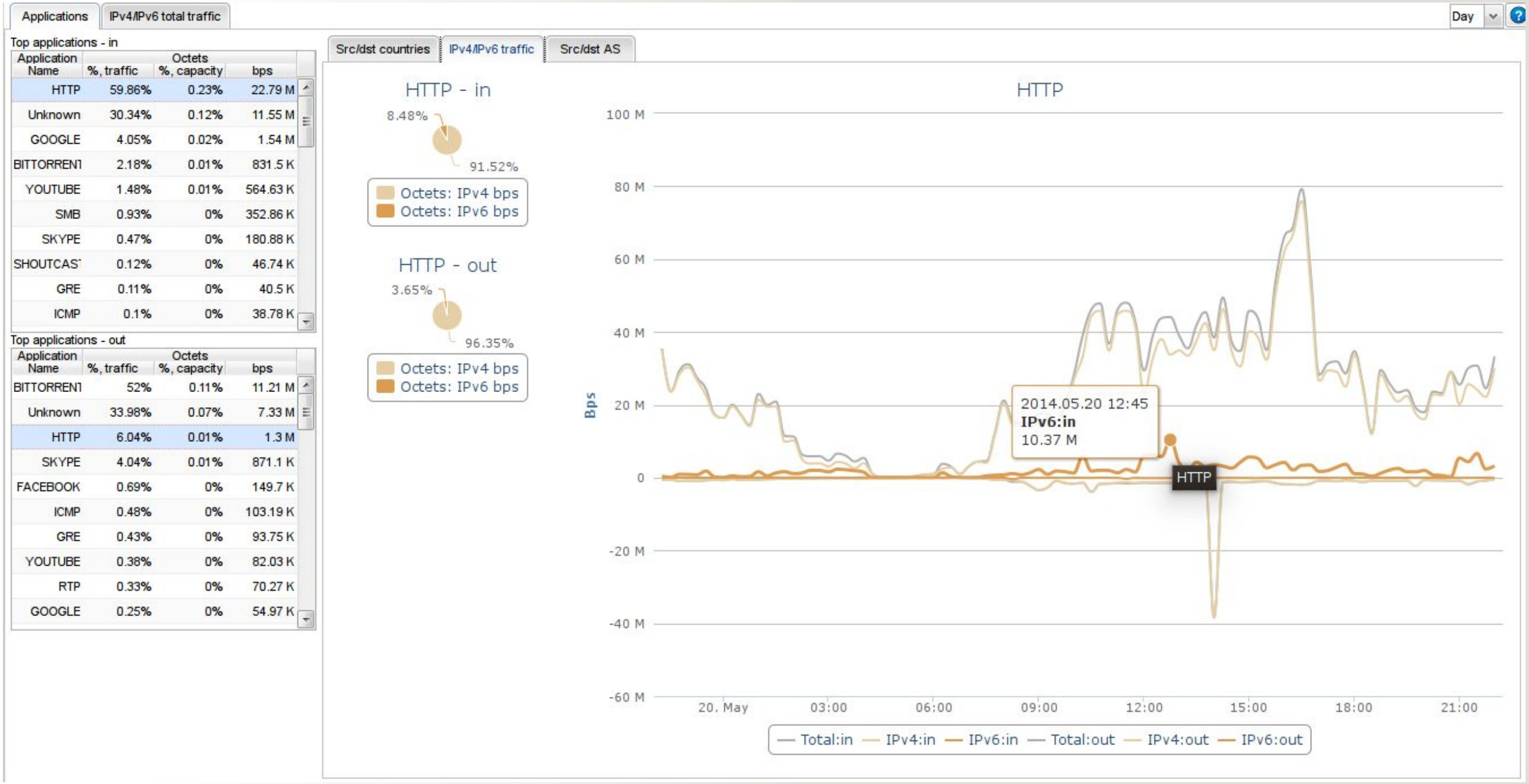


UNINETT

Appflow web interface



Appflow web interface (2)



Appflow web interface (3)

Applications | IPv4/IPv6 total traffic

Day

Top applications - in

Application Name	Octets %, traffic	%, capacity	bps
HTTP	59.86%	0.23%	22.79 M
Unknown	30.34%	0.12%	11.55 M
GOOGLE	4.05%	0.02%	1.54 M
BITTORRENT	2.18%	0.01%	831.5 K
YOUTUBE	1.48%	0.01%	564.63 K
SMB	0.93%	0%	352.86 K
SKYPE	0.47%	0%	180.88 K
SHOUTCAST	0.12%	0%	46.74 K
GRE	0.11%	0%	40.5 K
ICMP	0.1%	0%	38.78 K

Top applications - out

Application Name	Octets %, traffic	%, capacity	bps
BITTORRENT	52%	0.11%	11.21 M
Unknown	33.98%	0.07%	7.33 M
HTTP	6.04%	0.01%	1.3 M
SKYPE	4.04%	0.01%	871.1 K
FACEBOOK	0.69%	0%	149.7 K
ICMP	0.48%	0%	103.19 K
GRE	0.43%	0%	93.75 K
YOUTUBE	0.38%	0%	82.03 K
RTP	0.33%	0%	70.27 K
GOOGLE	0.25%	0%	54.97 K

Src/dst countries | IPv4/IPv6 traffic | Src/dst AS

IPv4 src AS/prefix

AS Name	Octets bps	% of app traffic
uninett.no	7.14 M	34.23%
NORDUNET	3.4 M	16.3%
JUSTINTV	2.45 M	11.73%
NETFLIX	1.99 M	9.52%
GBLX	1.1 M	5.28%
EDGECAST	575.28 K	2.76%
GOOGLE	424.94 K	2.04%
TELIANET	258.66 K	1.24%
QBRICK-AS	189.51 K	0.91%
LEASEWEB-US	164.6 K	0.79%
SCHIBSTED	154.28 K	0.74%
FASTHOST-AS	140.05 K	0.67%

IPv4 dst AS/prefix

AS Name	Octets bps	% of app traffic
moreforsk.no	473.85 K	37.78%
uninett.no	81.8 K	6.52%
NETFLIX	38.41 K	3.06%
JUSTINTV	34.81 K	2.78%
TELENOR-NEXTEL	24.23 K	1.93%
NORDUNET	24.21 K	1.93%
ASN-CATCHCOM	23.83 K	1.9%
MICROSOFT-CORP-MSN-A	22.08 K	1.76%
AMAZON-02	20.2 K	1.61%
PORT80-GLOBALTRANSI	19.78 K	1.58%
LEVEL3	16.73 K	1.33%
SCHIBSTED	16.02 K	1.28%

IPv6 src AS/prefix

AS Name	Octets bps	% of app traffic
NETFLIX	674.67 K	34.91%
NORDUNET	354.15 K	18.33%
GOOGLE	341.43 K	17.67%
UNINETT	137.84 K	7.13%
REDPILL-LINPRO	122.93 K	6.36%
AKAMAI-ASN1	60.28 K	3.12%
CLOUDFLARENET	39.78 K	2.06%
VIDEOPLAZA-AS	16.79 K	0.87%
AKAMAI-LON	14.75 K	0.76%
ITSJEFEN-AS	12.78 K	0.66%
FACEBOOK	9.77 K	0.51%
WIKIMEDIA-EU	7.26 K	0.38%

IPv6 dst AS/prefix

AS Name	Octets bps	% of app traffic
REDPILL-LINPRO	12.97 K	27.3%
ITSJEFEN-AS	8.71 K	18.34%
NETFLIX	7.9 K	16.63%
GOOGLE	7.17 K	15.1%
AKAMAI-ASN1	3.33 K	7.02%
BASEFARM-ASN	1.05 K	2.21%
CLOUDFLARENET	1.01 K	2.13%
AKAMAI-LON	0.08	1.65%
WIKIMEDIA-EU	0.07	1.57%
VIDEOPLAZA-AS	0.01	0.3%
AMAZON-02	0.01	0.3%
FACEBOOK	0.01	0.28%

UNINETT

Code availability

- pf_ring and nprobe
  - http://www.ntop.org
  - Not everything is open source
  - Free for academic and nonprofit use
- So far no web page for our own code
  - is available as open source if anyone is interested

arne.oslebo@uninett.no

UNINETT