

Monitoring IPv4 address utilization/depletion in UNINETT

Campus network monitoring and
security workshop
24 April 2014, Prague

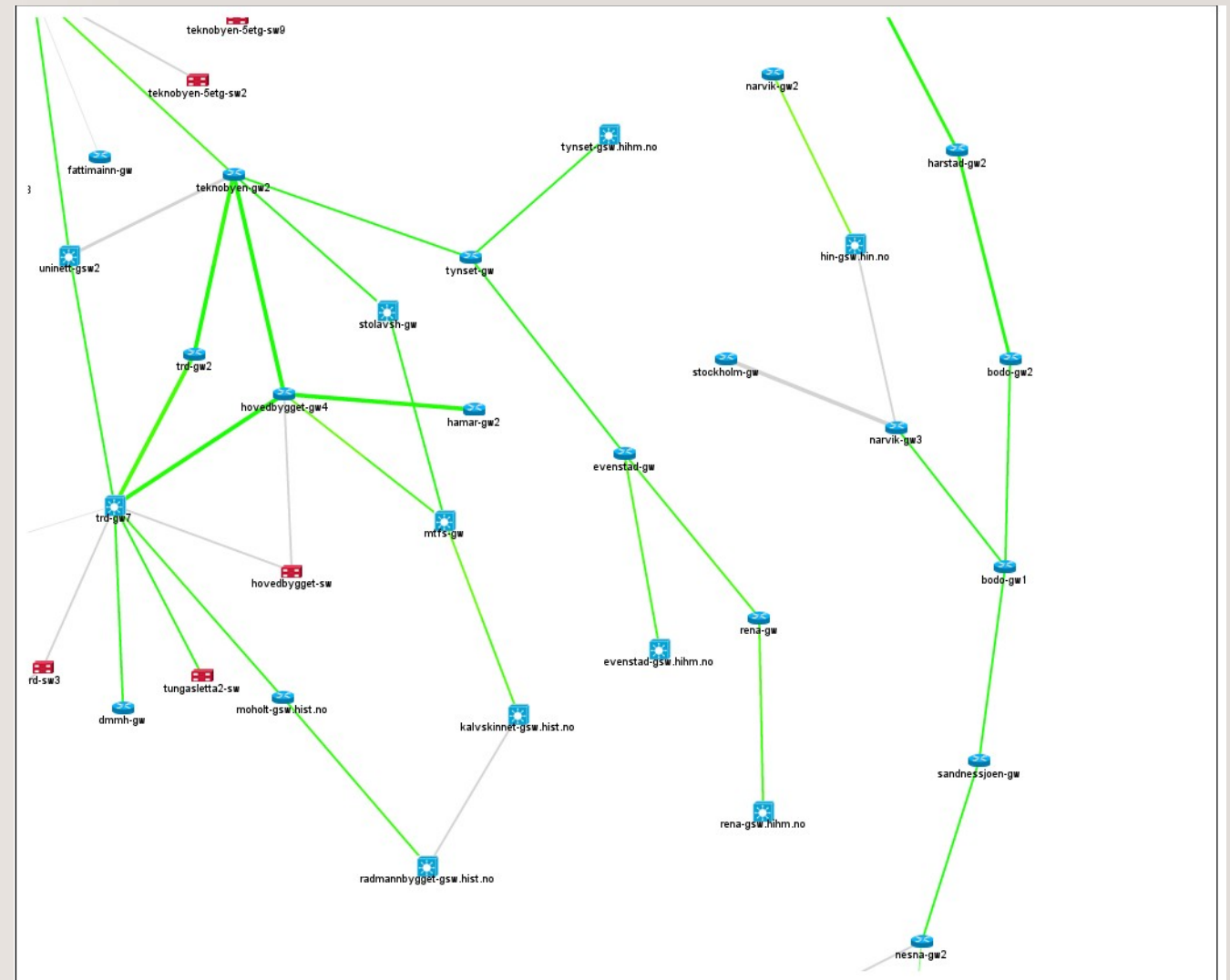
Morten Brekkevold
Engineer

UNINETT



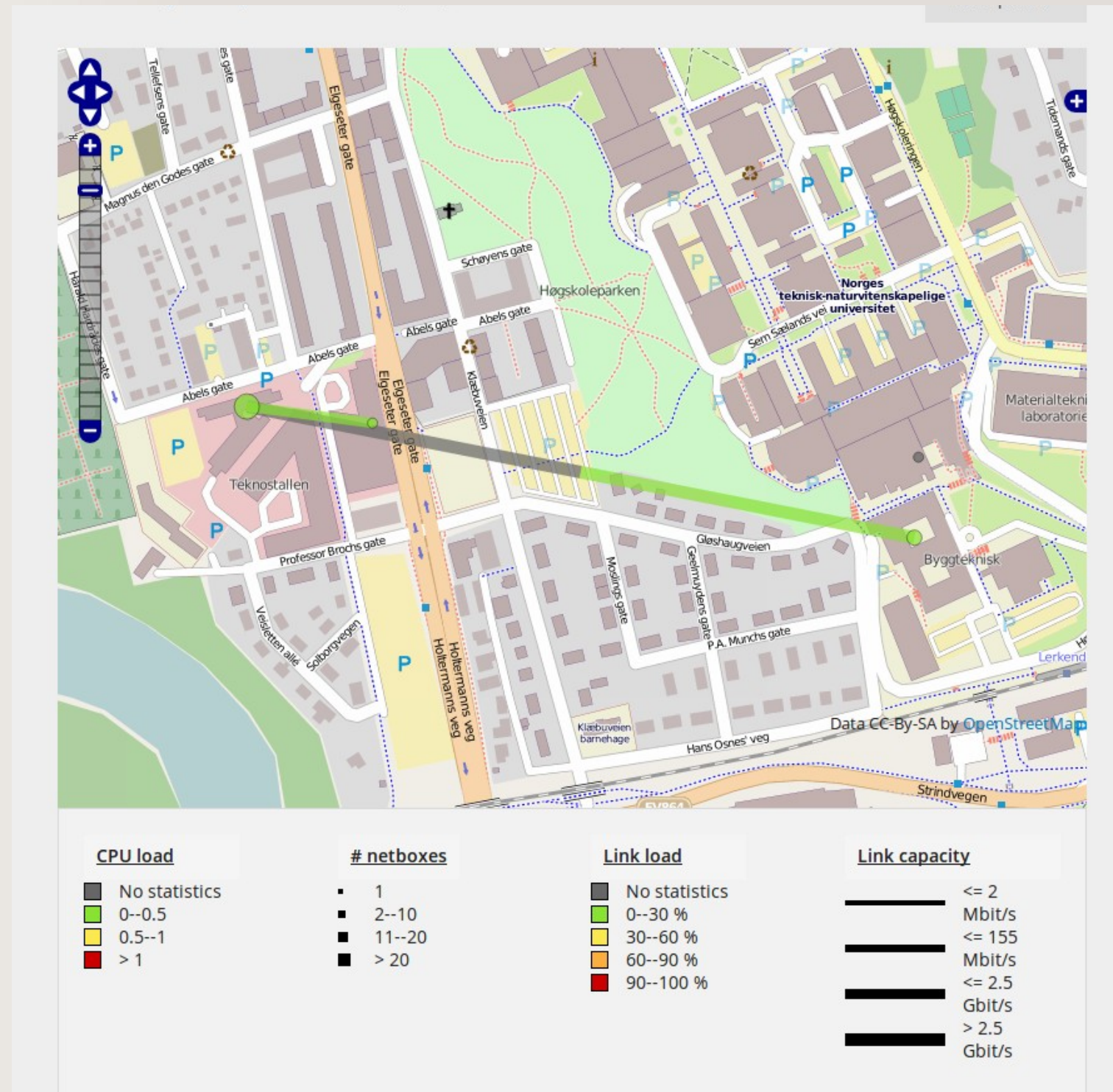
Birth of Network Administration Visualized

- A network monitoring system
- Initially built by NTNU in 1999
- Did for them what HP OpenView couldn't



NAV

- Alerts
- Automatic inventory & topology
- Statistics and graphs
- Simple port configuration



A brief history of NAV

- 2001 - 50% UNINETT funding
- 2004 - Open sourced
- 2006 - UNINETT takeover



IP Devices down					History
Sysname	IP	Down since	Downtime	History	
weathergoose.uninett.no	158.38.129.146	2014-04-07 13:34:48	16 days, 0:41:45	history	Put on maintenance
teknobyen-4etg-sw1.uninett.no	158.38.129.41	2014-04-06 20:23:33	16 days, 17:52:59	history	Put on maintenance
ebony-bay6.uninett.no	158.38.179.17	2014-03-20 10:17:03	34 days, 2:59:29	history	Put on maintenance
ebony-bay5.uninett.no	158.38.179.16	2014-03-20 10:17:03	34 days, 2:59:29	history	Put on maintenance
ebony-bay2.uninett.no	158.38.179.13	2014-03-20 10:17:03	34 days, 2:59:29	history	Put on maintenance
ebony-bay1.uninett.no	158.38.179.12	2014-03-20 10:17:03	34 days, 2:59:29	history	Put on maintenance
fattimainn-gw.uninett.no	128.39.3.21	2014-03-06 12:23:34	48 days, 0:52:59	history	Put on maintenance
oldsmobile.lab.uninett.no	158.38.152.163	2014-01-04 15:33:22	108 days, 21:43:10	history	Put on maintenance

NAV's unique position in Norway

- 94% deployment rate at higher education institutions
- Many of these installations are operated by UNINETT
 - A result of the 2006-2009 GigaCampus program
 - Which again inspired the GN3 Campus Best Practices task
- Continued development to meet HE customer's demands
 - While still remaining all free and open source

Upshots for UNINETT

- An intimately familiar monitoring tool at 94% HE customers
- Can we use this data to improve the research network?

ARP and ND

- Timestamped logs of routers' ARP (IPv4) and ND (IPv6) records
 - Enables tracking of individual clients
- All routed subnet prefixes collected from routers
 - Enables usage statistics per subnet/VLAN

Machine Tracker

Search NAV's logs of IP and MAC address activity to find where and when hosts in your network have been active.

IP Search

MAC Search

Switch Search

Netbios Search

128.39.60.72

Search

Help

Filters

☒ Active☐ Inactive☐ Both

Period

Days

7

☐ Only Active

Columns

☐ Netbios☒ Dns

IP search results – From 128.39.60.72 to 128.39.60.72

1 hit

DNS	↕	IP	↕	MAC	↕	Start time	↕	End time	↕
voip-dhcp-72.uninett.no		128.39.60.72		00:04:13:27:b0:4f		2014-04-07 19:40:56		Still active	

1 hit

Machine Tracker

Search NAV's logs of IP and MAC address activity to find where and when hosts in your network have been active.

IP Search

MAC Search

Switch Search

Netbios Search

00:04:13:27:b0:4f

Search

Help

Period

Days

7

Only active ☐

Columns

Dns ☒Netbios ☐

MAC Search results

1 hit

Switch	Module	Interface	Start time	End time	Mac
teknobyen-5etg-sw1.uninett.no		C2	2013-03-21 09:10	Still active	00:04:13:27:b0:4f

1 hit

IP search results

1 hit

DNS	IP	MAC	Start time	End time
voip-dhcp-72.uninett.no	128.39.60.72	00:04:13:27:b0:4f	2014-04-07 19:40:56	Still active

1 hit

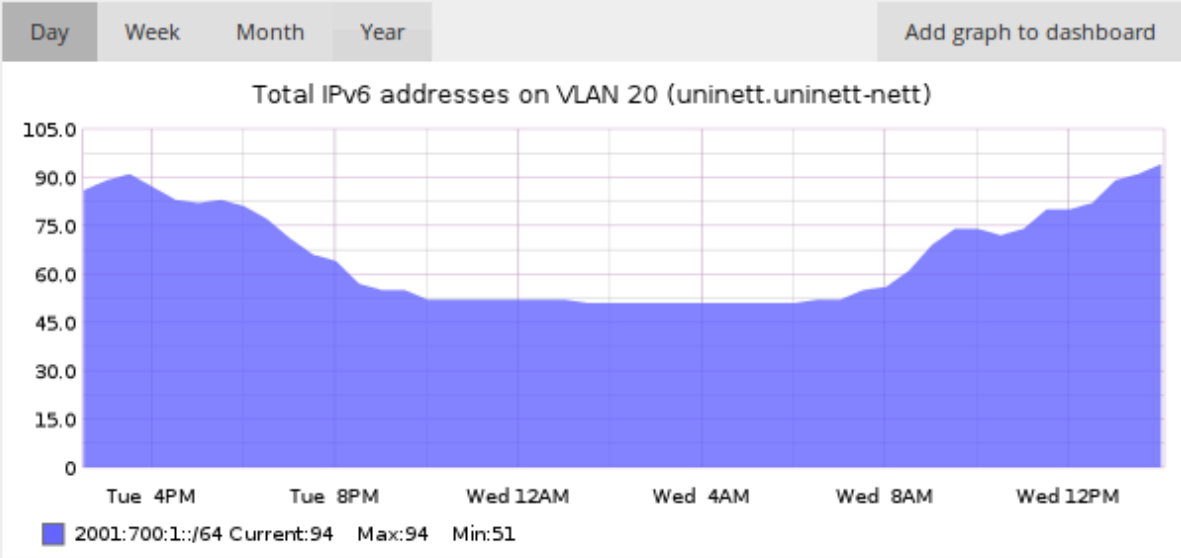
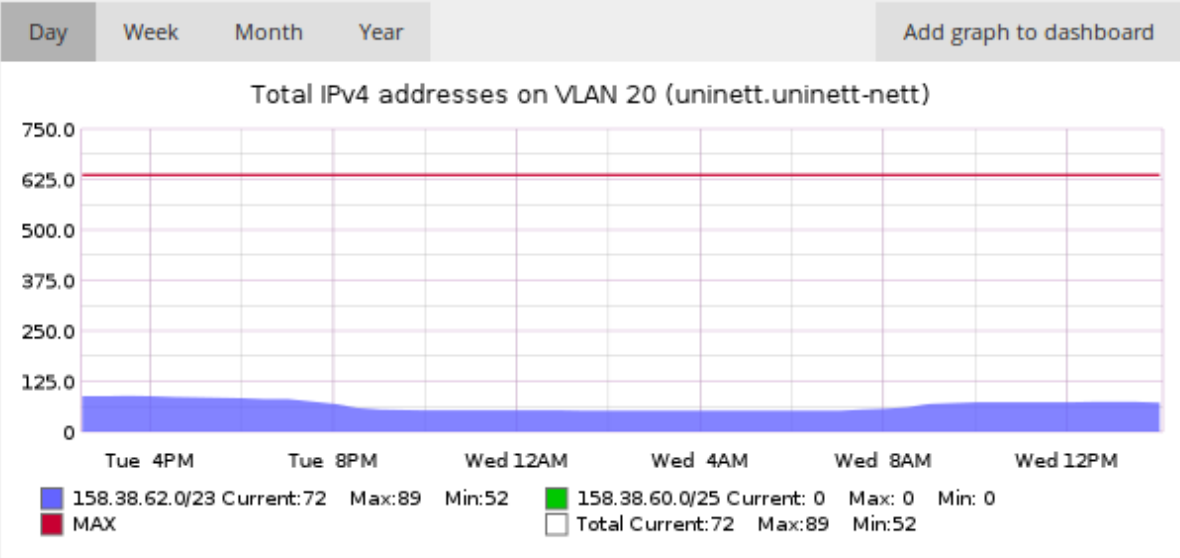
VLAN search

Vlan 20 (uninett.uninett-nett)	
Vlan	20
Type	lan
Organization	
Net Ident	uninett.uninett-nett
Description	lokal vlan

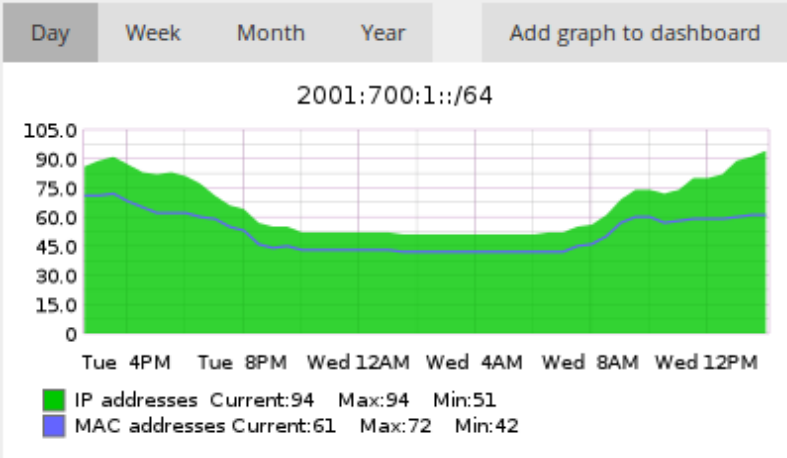
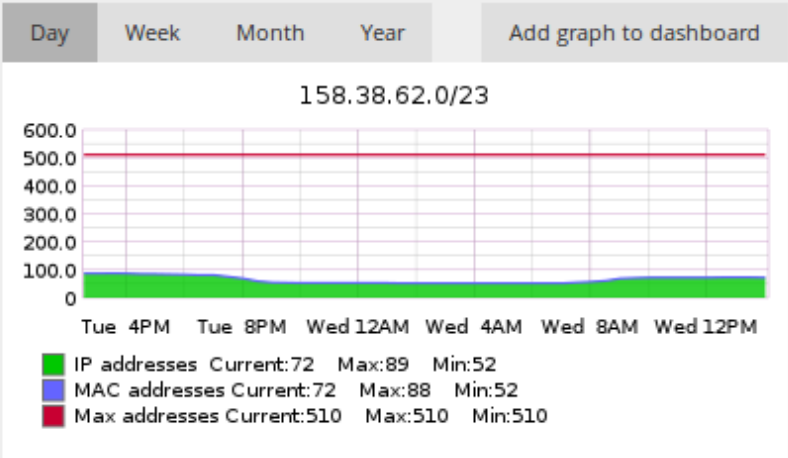
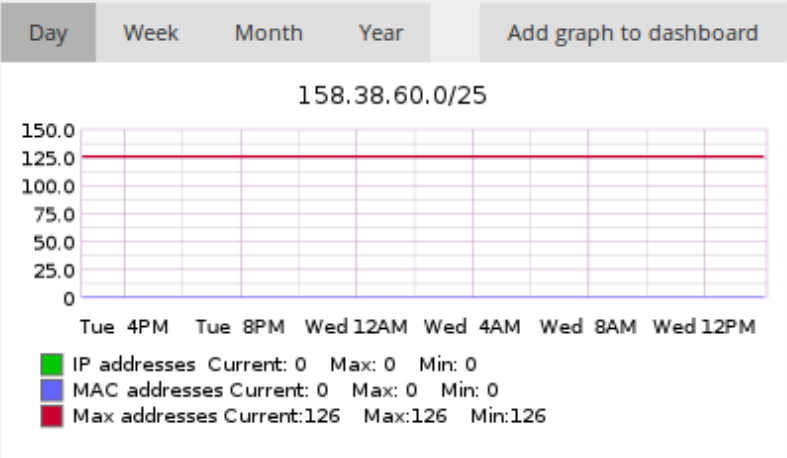
Router ports		
Netbox	Address	Interface
uninett-gw.uninett.no	158.38.62.1	VI20
uninett-gw.uninett.no	2001:700:1::1	VI20

Prefixes	
Net address	
158.38.60.0/25	
158.38.62.0/23	
2001:700:1::/64	

Vlan graphs

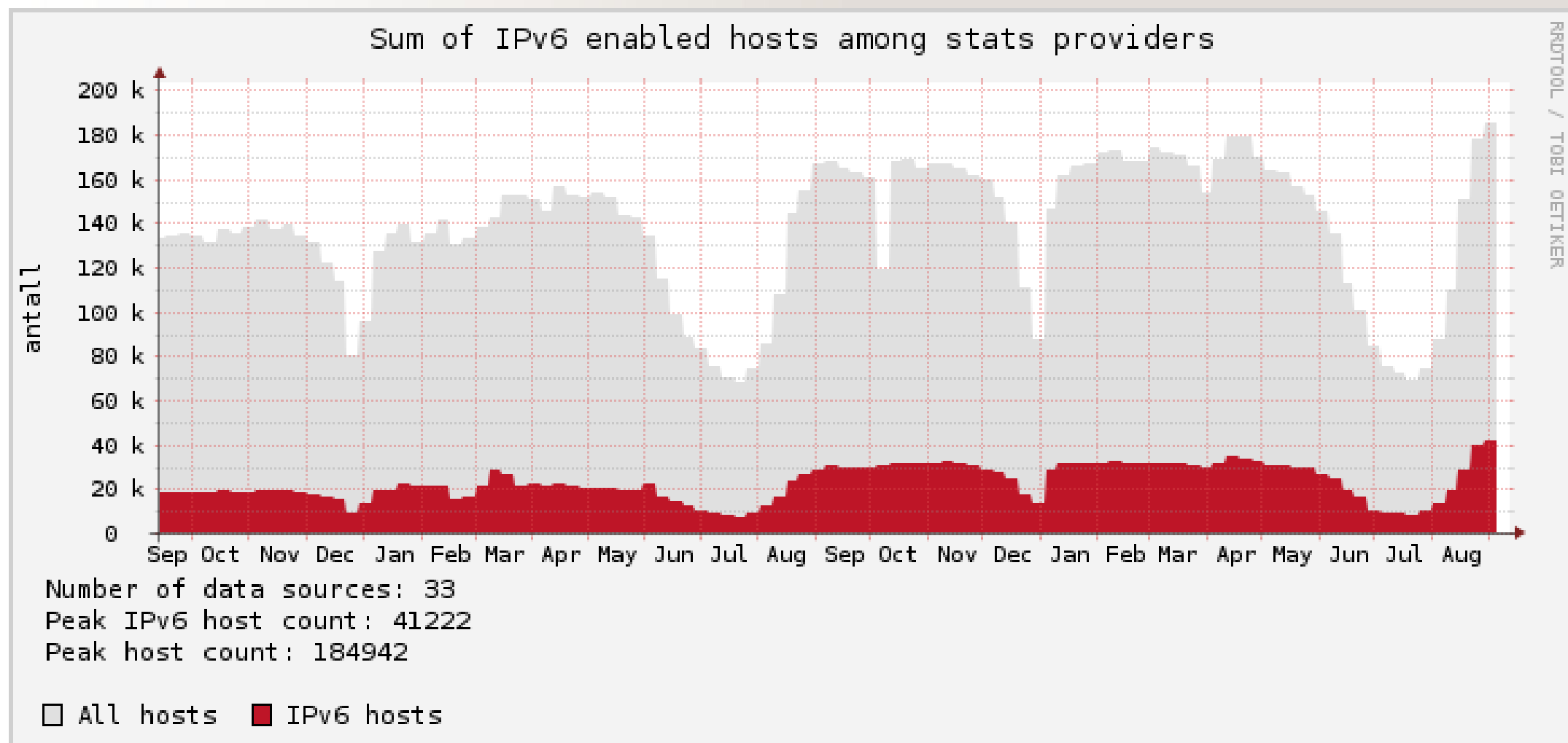


Prefix graphs



Stage 1: IPv6 usage stats

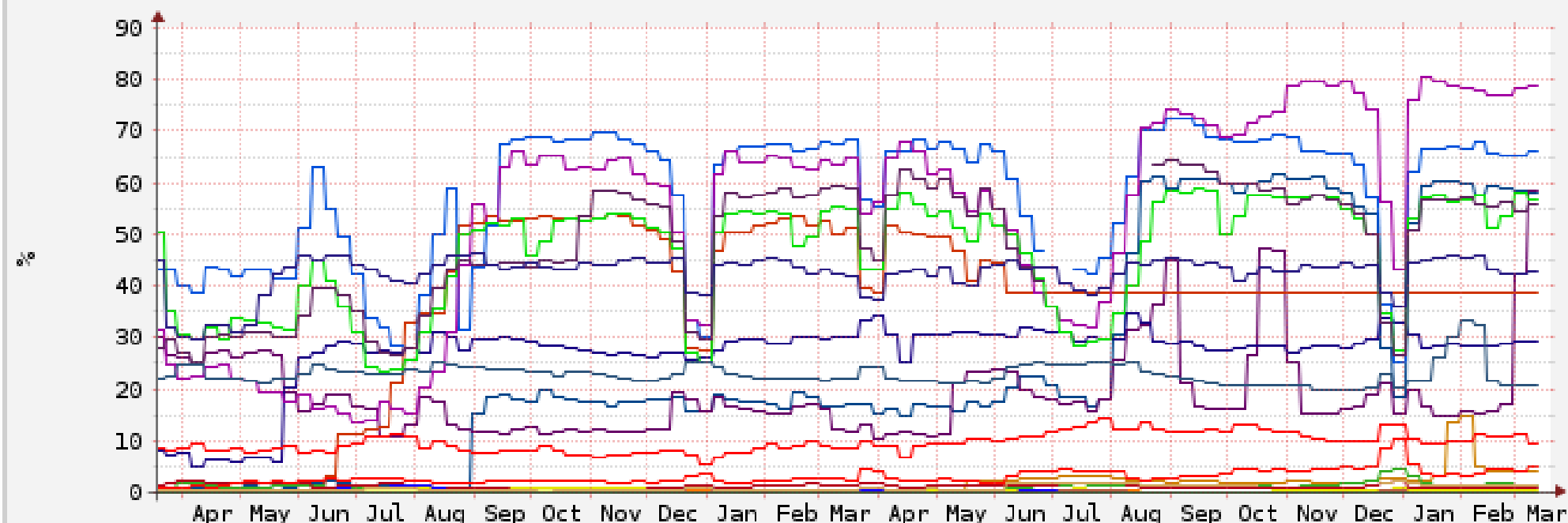
- Collected from campus NAV installations since 2009



Hack hack hack

- The data collection system is less than optimal
 - Requires installation of extension script
 - Appends to log file once every 24h
 - Log files collected nightly over HTTP from all known NAV installs
 - Log files parsed and data entered into RRD files

IPv6 enabled hosts per domain



RRDTOOL / TOBI OETIKER

Høgskolen i Oslo og Akershus (hiak.no)	peak: 0.64%
Høgskolen i Ålesund (hials.no)	peak: 61.53%
Høgskolen i Buskerud (hibu.no)	peak: 58.70%
Høgskolen i Gjøvik (hig.no)	peak: 54.03%
Høgskolen i Hedmark (hihm.no)	peak: 14.94%
Høgskolen i Molde (himolde.no)	peak: 4.52%
Høgskolen i Narvik (hin.no)	peak: 34.58%
Høgskolen i Nesna (hinesna.no)	peak: 2.44%
Høgskolen i Nord-Trøndelag (hint.no)	peak: 0.89%
Høgskolen i Oslo og Akershus (hioa.no)	peak: 72.25%
Høgskolen i Østfold (hiof.no)	peak: 80.54%
Høgskolen i Sør-Trøndelag (hist.no)	peak: 10.42%
Høgskolen i Telemark (hit.no)	peak: 0.47%
Høgskolen i Vestfold (hive.no)	peak: 58.92%
Høgskolen i Volda (hivolda.no)	peak: 1.21%
Høgskolen Stord/Haugesund (hsh.no)	peak: 14.38%
Kunsthøgskolen i Oslo (khio.no)	peak: 0.32%
Meteorologisk Institutt (met.no)	peak: 0.29%
NTNU (ntnu.no)	peak: 33.42%
Universitetet i Agder (uia.no)	peak: 64.39%
Universitetet i Oslo (uio.no)	peak: 2.11%
Universitetet i Stavanger (uis.no)	peak: 0.20%
UNINETT AS (uninett.no)	peak: 46.31%

Stage 2: IPv4 usage stats

- What about utilization of the existing IPv4 address space?
- We have a limited number of subnets to delegate to customers
 - Are they using them reasonably?
- Do the right thing™: Build a REST API for NAV, no more hacks

Challenges

- Are customers even routing all the assigned address space?
- Are they monitoring them?
- Number of IPv6-enabled users might be «gamified»
 - But who cares to compete for best utilization of remaining IPv4 space?

Preliminary numbers

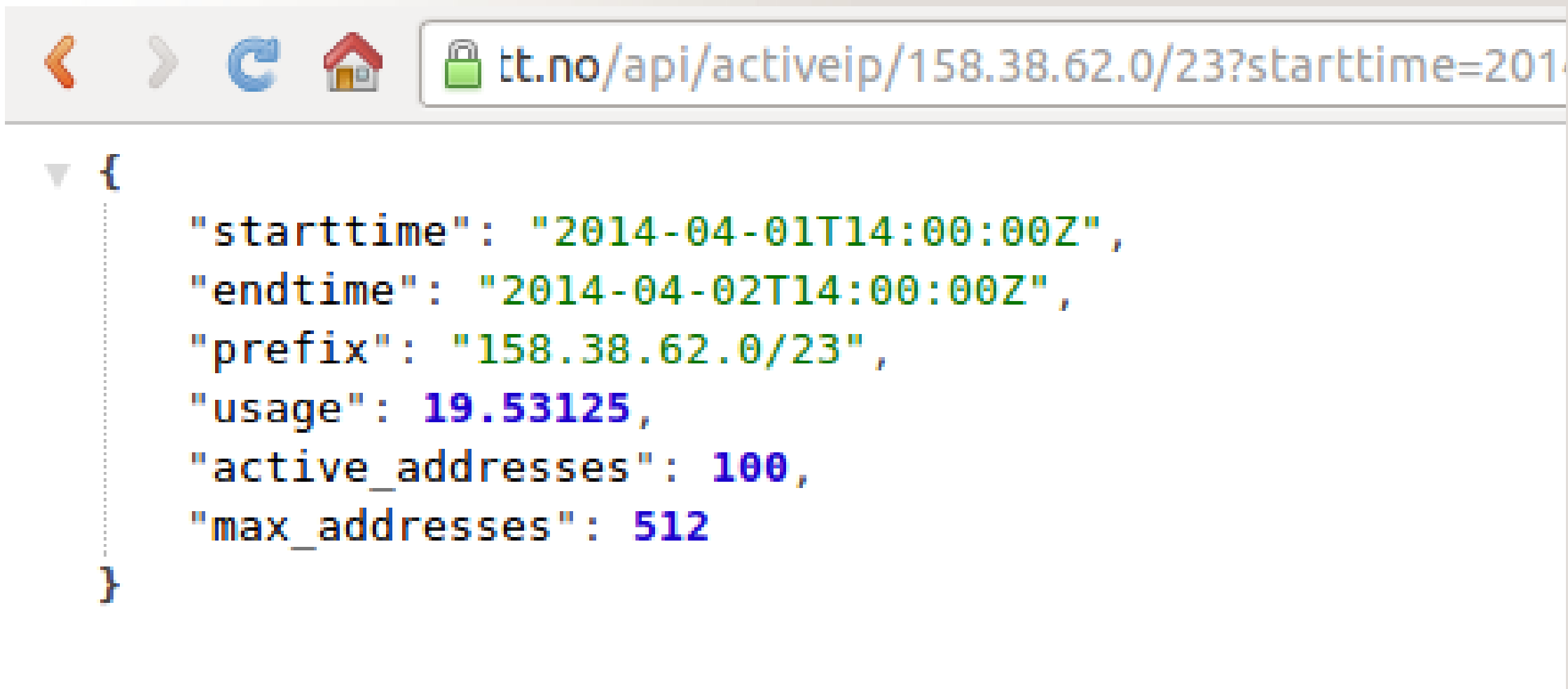
- Many sources of errors
- Demonstrates the need to measure coverage

Domain	Address	Pct
rocketrange.no	0/1088	0.0%
unis.no	0/1896	0.00%
met.no	1988/65632	3.00%
hihm.no	587/16164	3.60%
uninett.no	1596/19880	8.00%
uis.no	12935/65536	19.70%
nmh.no	258/1160	22.20%
khib.no	546/2176	25.10%
hinesna.no	540/1744	31.00%
samiskhs.no	728/2304	31.60%
hive.no	2626/8000	32.80%
himolde.no	1817/5312	34.20%
ntnu.no	32068/87808	36.50%
khio.no	1297/3264	39.70%
hisf.no	3541/8888	39.80%
hint.no	3990/9840	40.50%
hsh.no	2897/6880	42.10%
hih.no	1068/2496	42.80%
hibu.no	4322/9528	45.40%
hials.no	3259/7056	46.20%
hiof.no	3941/8472	46.50%
hin.no	2116/4288	49.30%
hit.no	5997/10952	54.80%
uia.no	11640/20984	55.50%
hivolda.no	3025/5440	55.60%
hist.no	7229/12712	56.90%
aho.no	1216/2088	58.20%
hil.no	3405/5640	60.40%
hioa.no	10436/15864	65.80%

Building an API, v1

- Simple, time-limited, revokeable API access token
 - We generate one on each NAV install we have access to
 - Using OAuth2-derived mechanisms
- API calls for
 - Getting the number of uniquely active addresses on an arbitrary network prefix
 - Getting the complete list of routed network prefixes

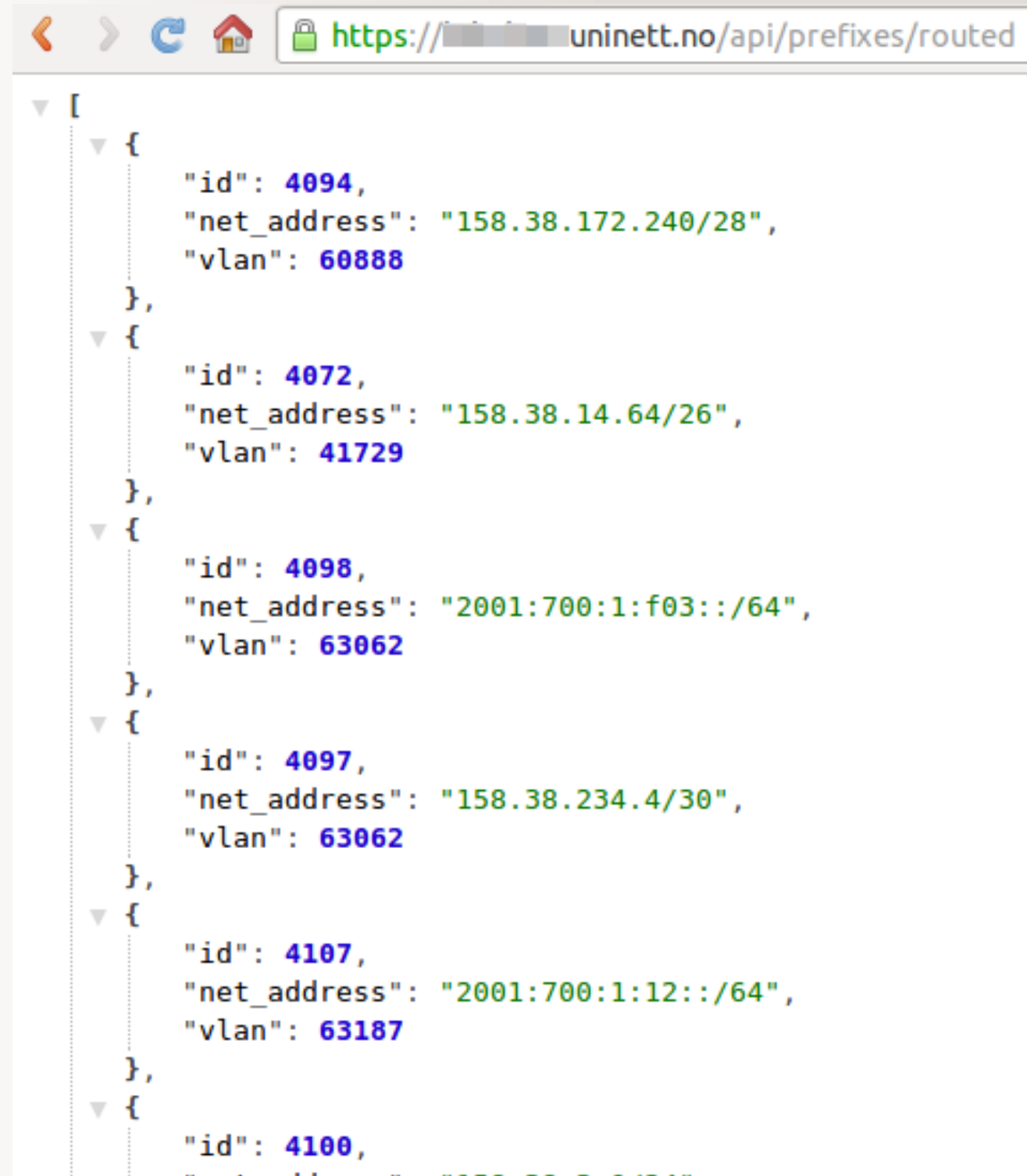
A simple API query



The screenshot shows a web browser window with the address bar displaying the URL `tt.no/api/activeip/158.38.62.0/23?starttime=2014-04-01T14:00:00Z`. Below the address bar, a JSON object is displayed, representing the API response. The JSON object contains the following fields: `starttime`, `endtime`, `prefix`, `usage`, `active_addresses`, and `max_addresses`. The values for `usage`, `active_addresses`, and `max_addresses` are highlighted in blue.

```
{
  "starttime": "2014-04-01T14:00:00Z",
  "endtime": "2014-04-02T14:00:00Z",
  "prefix": "158.38.62.0/23",
  "usage": 19.53125,
  "active_addresses": 100,
  "max_addresses": 512
}
```

Another simple API query



The screenshot shows a web browser window with the address bar displaying `https://[redacted]uninett.no/api/prefixes/routed`. The main content area shows a JSON array of five objects, each representing a network prefix. The objects are expanded to show their details. The JSON is as follows:

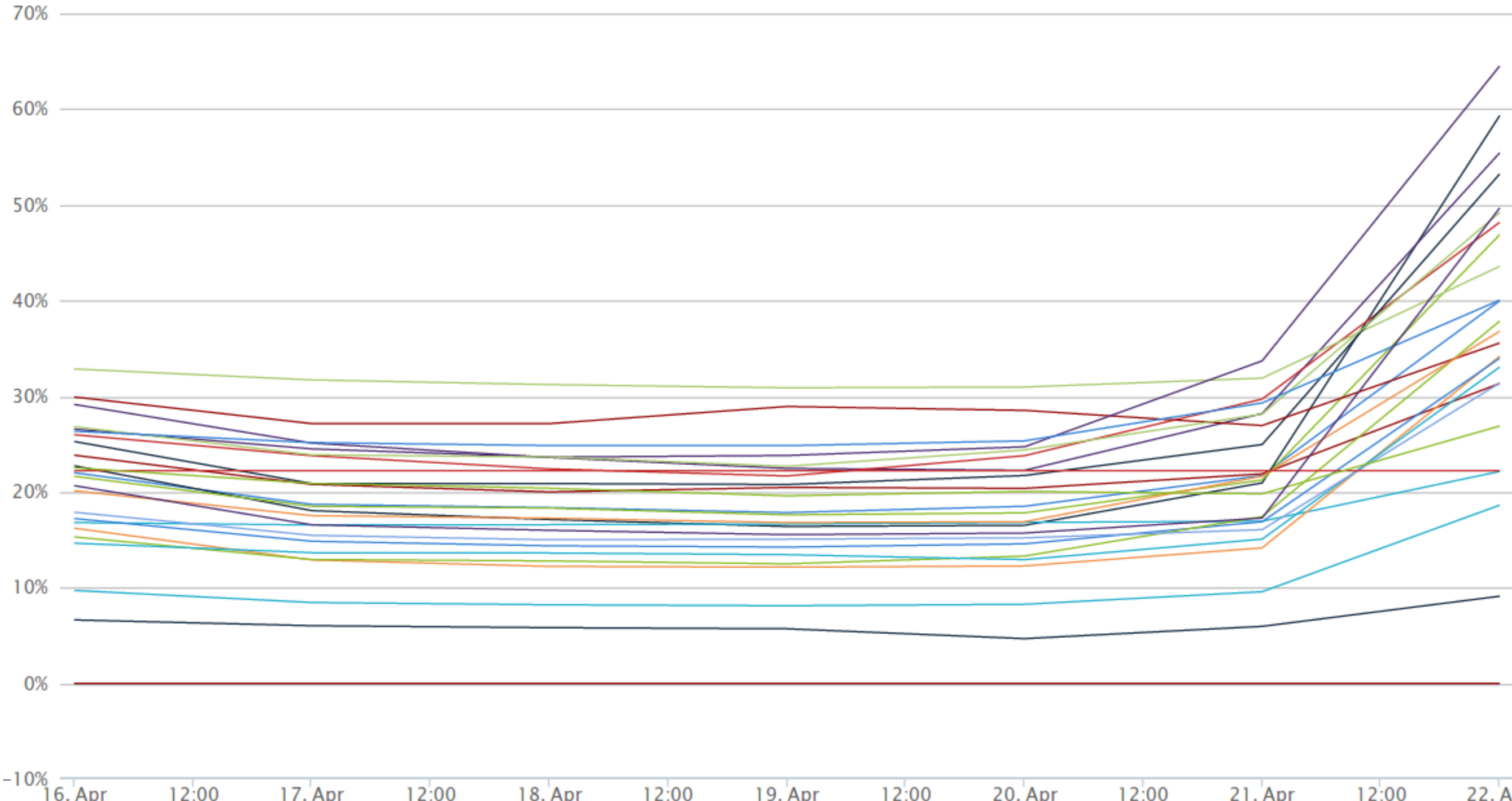
```
[
  {
    "id": 4094,
    "net_address": "158.38.172.240/28",
    "vlan": 60888
  },
  {
    "id": 4072,
    "net_address": "158.38.14.64/26",
    "vlan": 41729
  },
  {
    "id": 4098,
    "net_address": "2001:700:1:f03::/64",
    "vlan": 63062
  },
  {
    "id": 4097,
    "net_address": "158.38.234.4/30",
    "vlan": 63062
  },
  {
    "id": 4107,
    "net_address": "2001:700:1:12::/64",
    "vlan": 63187
  },
  {
    "id": 4100,
    "net_address": "158.38.2.0/24",
    "vlan": 63187
  }
]
```

Calculating coverage

- Adjoining delegations may be routed as a single prefix
 - 192.168.86.0/24 + 192.168.87.0/24 delegated to single customer
 - Customer may route single 192.168.86.0/23 prefix
- Delegations may be split into multiple routed prefixes
 - 192.168.100.0/20 delegated to customer
 - Customer routes 192.168.100.0/22 and 192.168.104.0/22 and reserves the rest for future use

	Domain	#Services on IPv6	NAV Monitoring Co	IPv4 Subnet Usage	IPv6
▶	hil.no	2	95	65	
▶	hiof.no	3	77	59	
▶	aho.no	2	96	55	
▶	hih.no	2	76	53	
▶	hioa.no	3	94	50	
▶	khio.no	2	84	49	
▶	hit.no	1	98	48	
▶	hist.no	2	92	47	
▶	hive.no	2	75	44	
▶	hisf.no	1	86	40	
▶	ntnu.no	1	85	40	
▶	hsh.no	1	96	38	
▶	himolde.no	2	93	37	
▶	samiskhs.no	1	88	36	
▶	hials.no	2	100	34	
▶	hibu.no	1	97	34	
▶	hint.no	1	92	33	
▶	hin.no	2	94	31	
▶	hinesna.no	1	85	31	
▶	khib.no	2	93	27	
▶	nmh.no	2	100	22	
▶	uninett.no	3	22	22	
▶	uia.no	2	90	19	
▶	uia.no	4	100	0	

IPv4 Subnet Usage



Moving forward

- Front-end still not in production
 - Maybe add graph of how much free address space is left
 - Filter non-UNINETT delegated address space
- Encourage customers to not waste precious IPv4 addresses
- Maybe (threaten to) reclaim addresses from squatters?
 - But better to assist in migration to IPv6

References

- <https://nav.uninett.no/>
- <https://stats.uninett.no/ipv6stat>
- https://openwiki.uninett.no/gigacampus:ipv6status_english
- morten.brekkevold@uninett.no