Sikt

The Microdep project

GNA-G talk, September 20th 2022

Otto J Wittner, Sikt (Norwegian NREN)

Outline

- Motivation: Relevance of end-to-end monitoring
  - Resulting improvements
- The Microdep system
  - Components and functionality
  - Analysis and events
  - Relations to perfSONAR
  - How to contribute
  - Demo

Relevance of end-to-end monitoring

- **Continuous end-to-end measurements** have significant importance
  - May compensate for "end-to-end blindness" due to only (traditional) per-device monitoring
- Enable NOCs to
  - Better understand how customers experienced delivered networking services
    - **Also, interdomain QoS**
    - **Early problem-awareness**, e.g. always before customer calls service centre
  - Evaluate and improve routing and forwarding
  - Faster discover and "debug" interdomain issues
- Enable customers to
  - Monitor network QoS towards critical application service providers
  - Easier differentiate between external- and internal-network issues

Routing configuration requires care

Routing configurations are often complex

- ISIS's, OSPF's and BGP's myriad of config-options
- Increased demand for security measures
- Increased demand for reliability (by multihoming)
- Growing no of peering partners

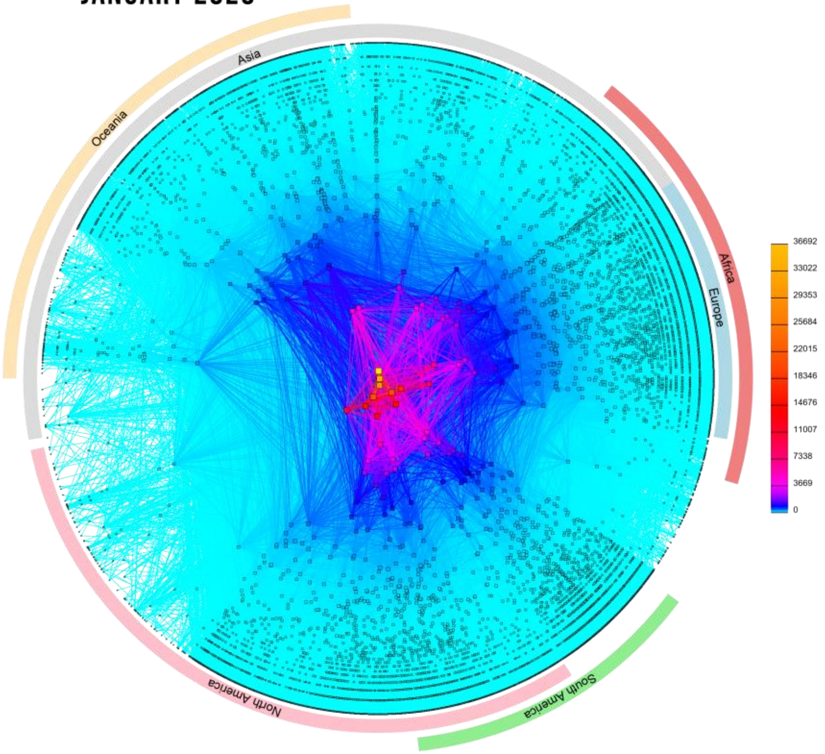
Running configs need careful maintenance

- Regular routing OS update
- Adjustments when customer leave/join
- Adjustments on network topology alterations
- Adjustments on security incidents
- Route deflection before planned reboots

Verification of successful re-configs are required

- Via device monitoring
- **Via end-to-end monitoring**

CAIDA'S IPV4 AS CORE GRAPH
JANUARY 2020

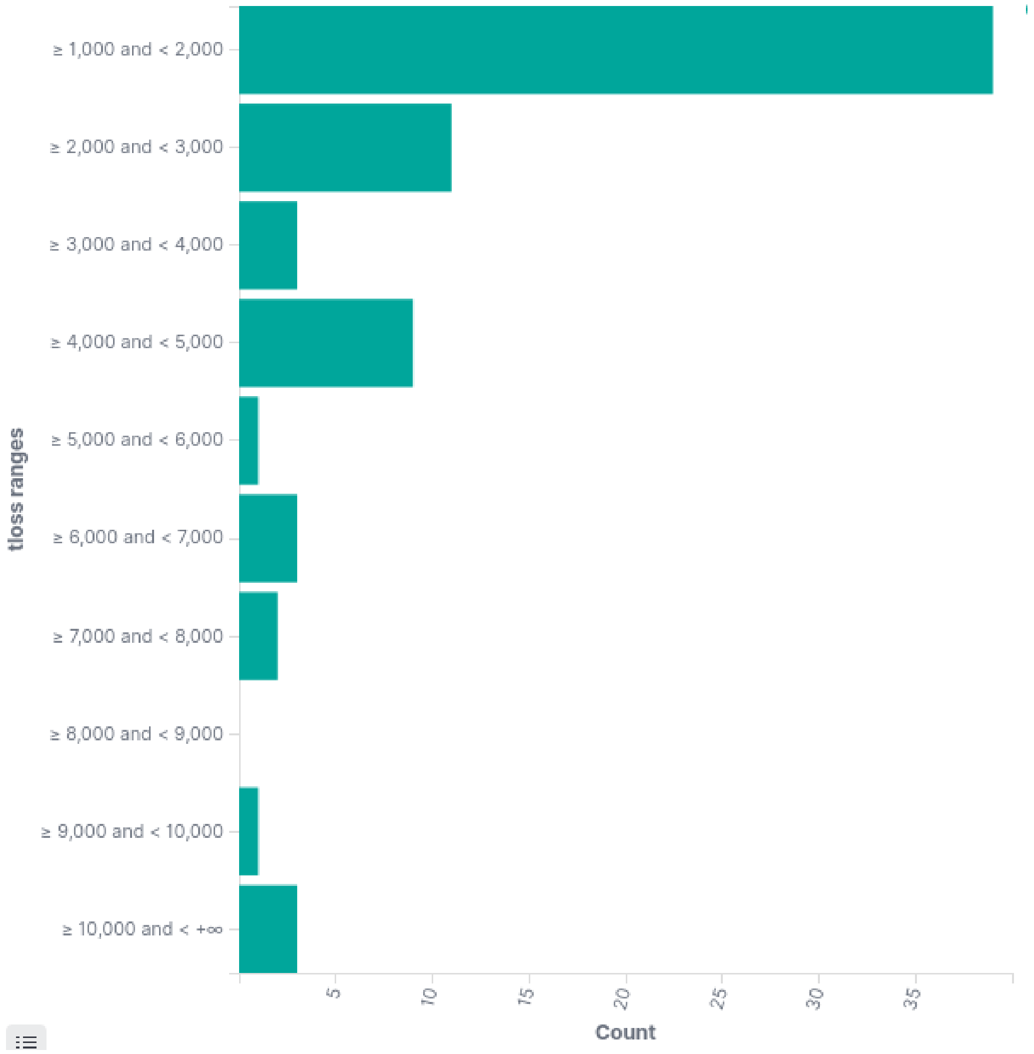


Some end-to-end observations and resulting improvements

- **Periodic 2 min outage** in NORDUnet
  - MPLS-transporter in USA required to optimize configurations
- **Routing stopped for 30 min** in Geant network
  - Caused by upgrade failure
- **2 min BGP failover time** between customer's primary and secondary connections in Uninett/Sikt
  - Optimization in BGP and IS-IS configurations required
- **Down-time due to planned maintenance** in Uninett/Sikt
  - Routines for route deflection updated
- **Fine-grained understanding of load and queues** on customer access links in Uninett/Sikt
  - Enabled timely and well documented capacity upgrade warnings to customers (no longer "gut feeling based").
- … and "die hard" packets
  - 2 week old packets traversing the Geant network,
  - 2 hour old packets in the Uninett/Sikt network

May 2022 findings

- *May 22 09:04*
  Several route-changes in both NORDUnet and Geant
  30 seconds downtime between Copenhagen and Zurich
- *May 22 09:02*
  Route-change in Geant
  16 seconds downtime between Copenhagen and Madrid
- *May 16 19:11*
  Route-change in Geant
  22 second downtime between Stockholm and Madrid
- *May 17, 19, 24, 26 and 29 between 8-10 and 14-17 o'clock*
  Route-change in NORDUnet
  6-8 seconds downtimes

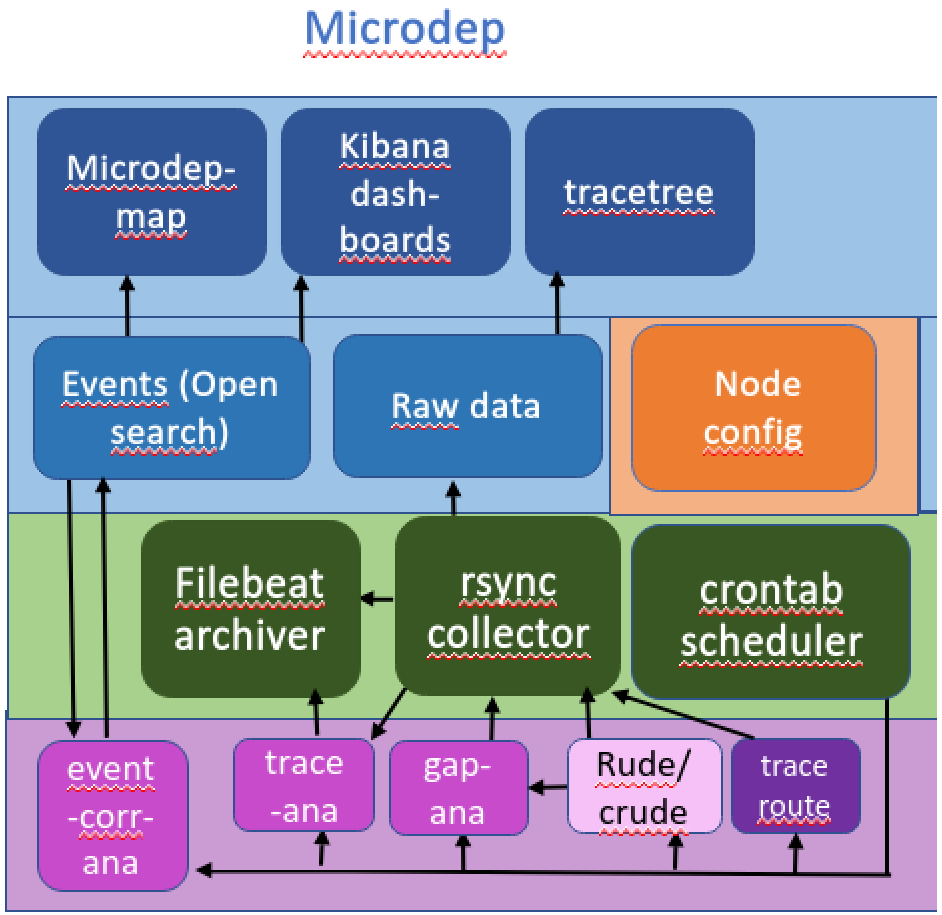


Downtime (ms) due to route-changes in Geant or NORDUnet May 11-30 2022

Sikt

Microdep funamentals

- ınitially a measurement project (since 2010)
- Today a measurement system and a project
- Objectives
  - **Improve routing** in NRENs and **the global Internet**
  - Reveal network **dependability issues** at **fine grained** level by **end-to-end measurements**



Sikt

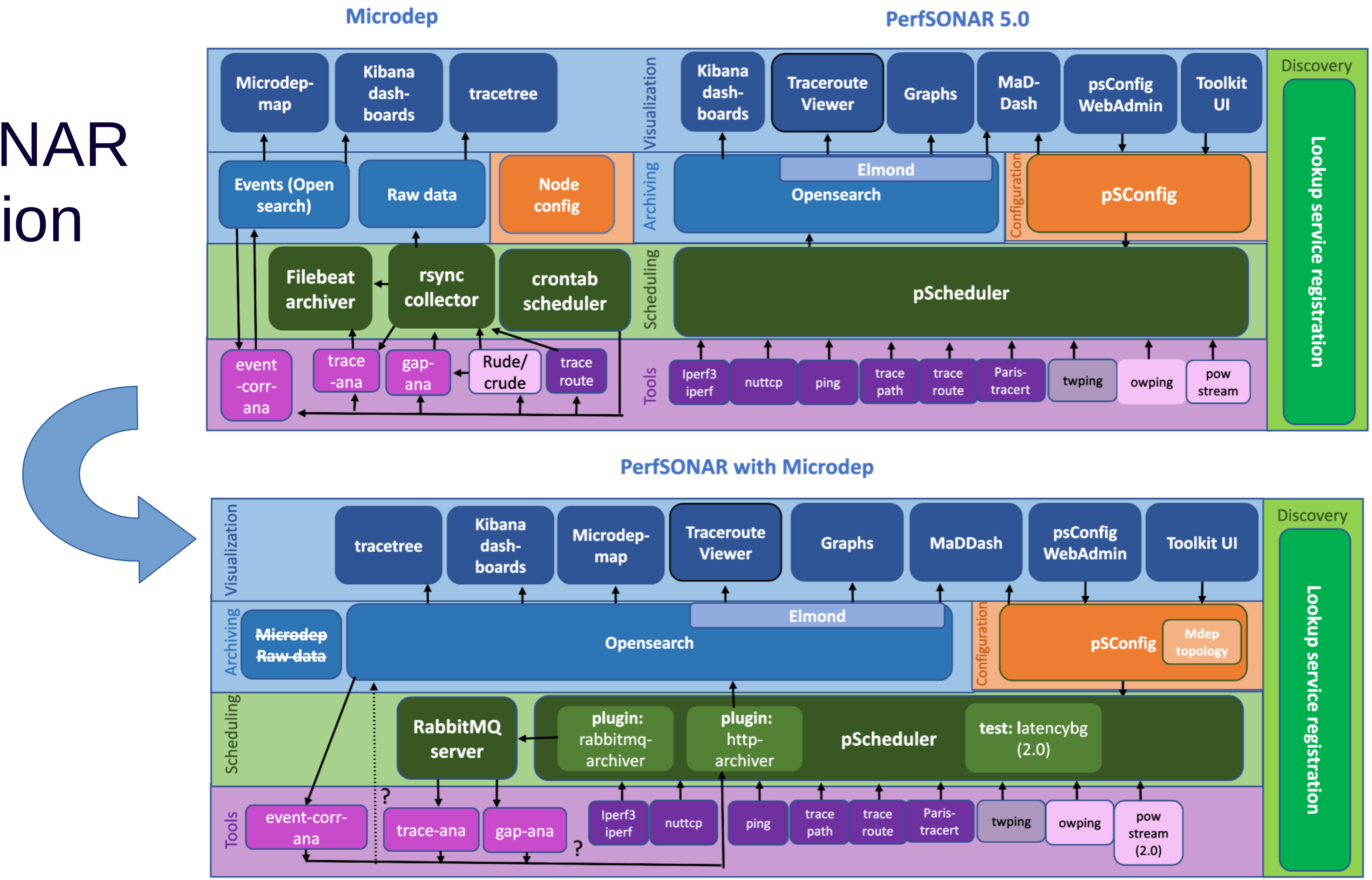
Microdep system details

- End-to-end measurements 24/7
  - 100 packets/s probe traffic
  - 60 per hour traceroutes
  - ICMP response monitoring
- 51 nodes, 212 flows in Norway
- 24 nodes, 238 flows globally
  - 8 DC-nodes (amazon, azure, google)

- Realtime event analysis
  - Packet-loss (gaps)
  - Queues (jitter)
  - Route failures and changes (traceroute)
  - Correlated events
- ML based joint event anomality planned.
- perfSONAR integration in progress

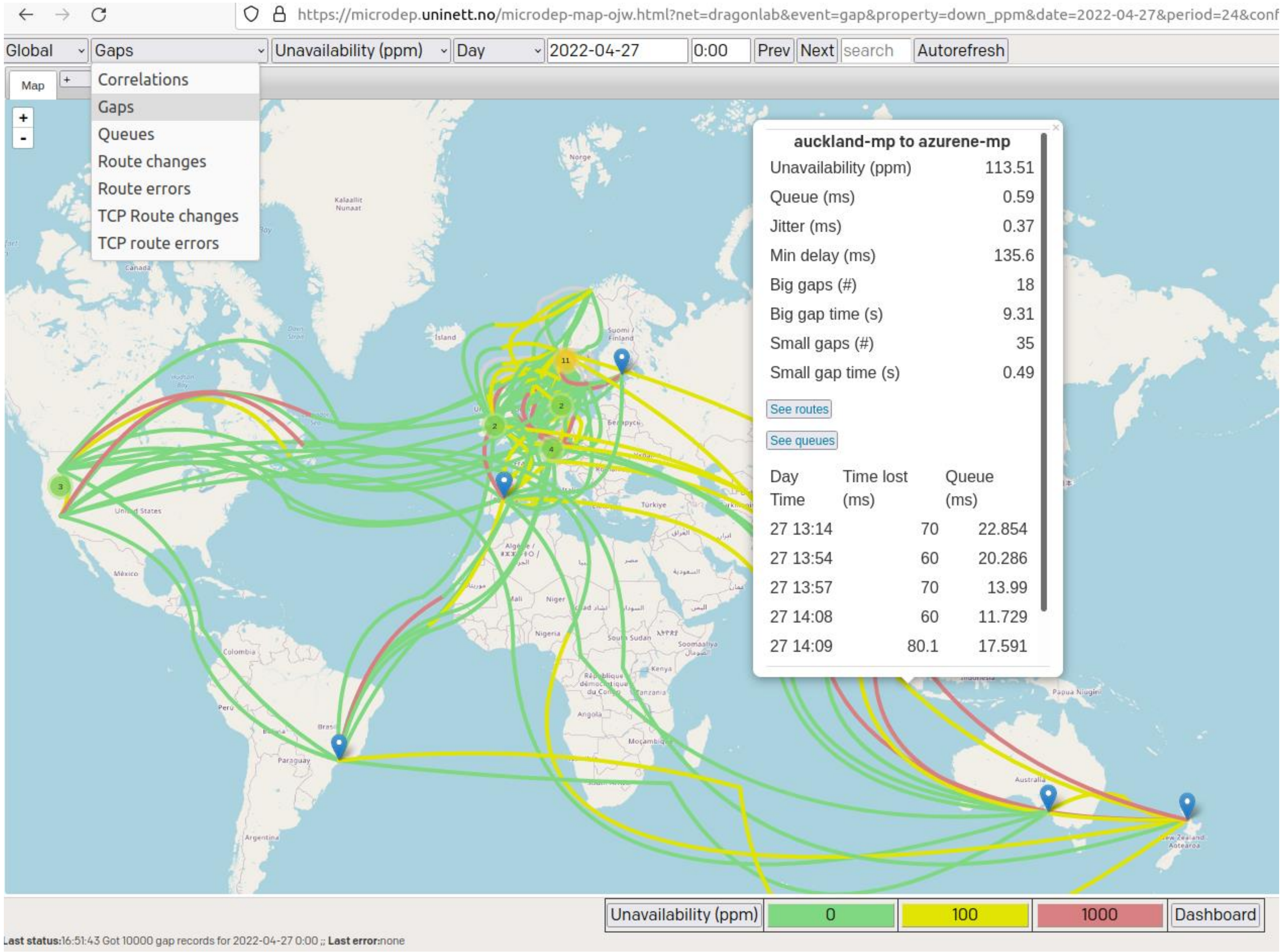
Sikt

PerfSONAR integration



Map view and flow status

https://microdep.uninett.no



https://microdep.uninett.no/microdep-map-ojw.html?net=dragonlab&event=gap&property=down_ppm&date=2022-04-27&period=24&conf

Global | Gaps | Unavailability (ppm) | Day | 2022-04-27 | 0:00

auckland-mp to azurene-mp

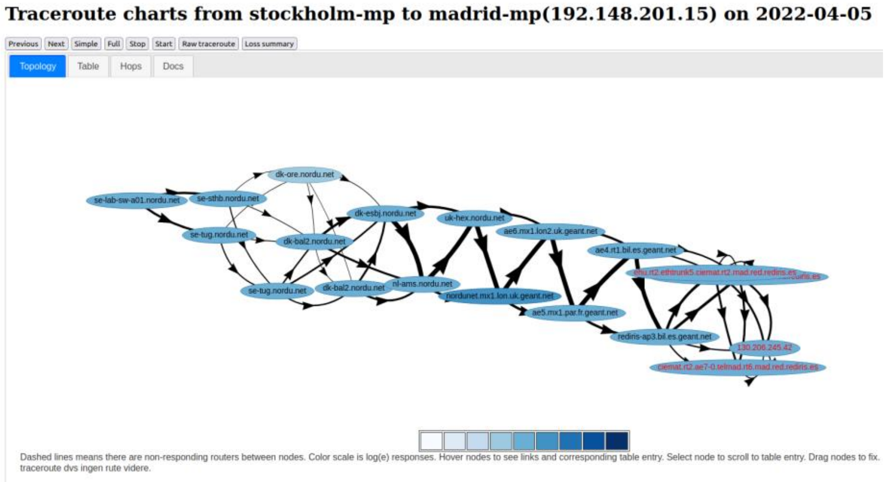
Unavailability (ppm)	113.51
Queue (ms)	0.59
Jitter (ms)	0.37
Min delay (ms)	135.6
Big gaps (#)	18
Big gap time (s)	9.31
Small gaps (#)	35
Small gap time (s)	0.49

Day Time	Time lost (ms)	Queue (ms)
27 13:14	70	22.854
27 13:54	60	20.286
27 13:57	70	13.99
27 14:08	60	11.729
27 14:09	80.1	17.591

Last status:16:51:43 Got 10000 gap records for 2022-04-27 0:00 ;; **Last error:**none

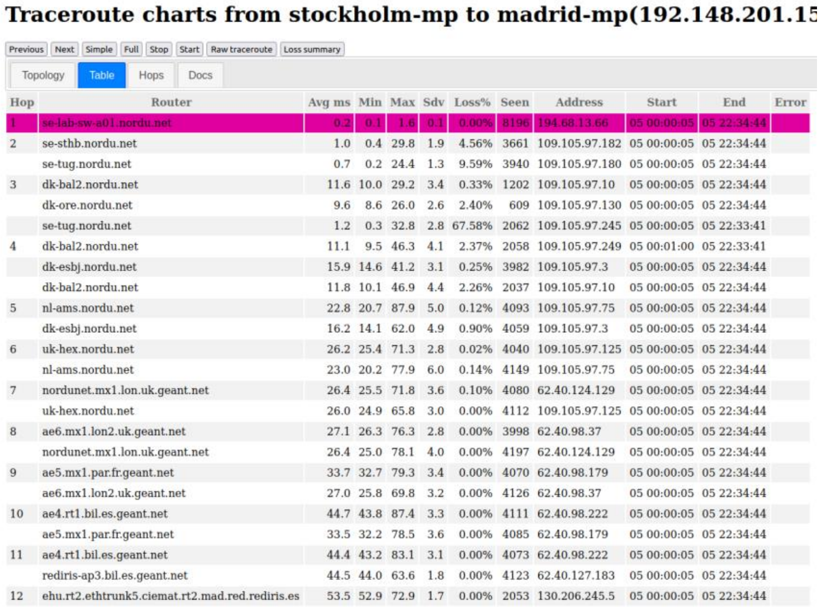
Sikt

Other views



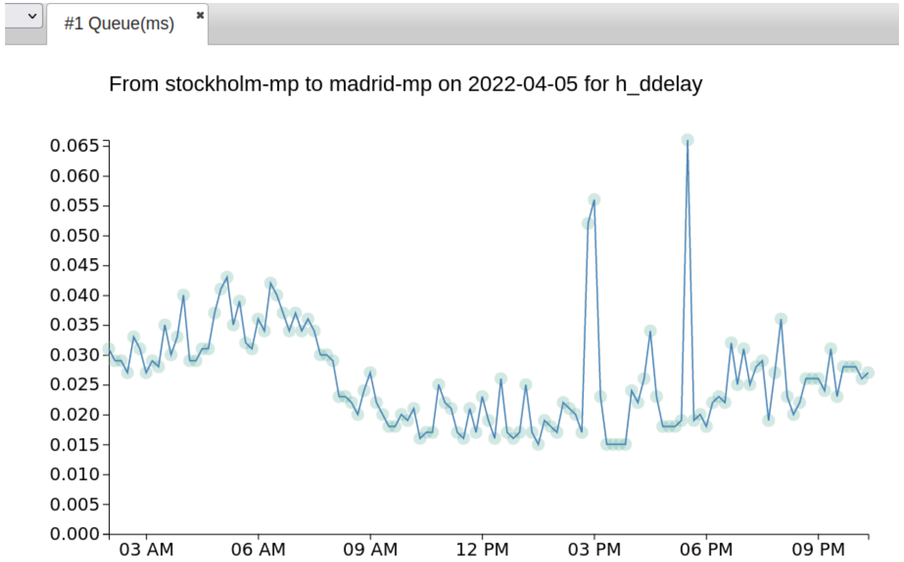
Traceroute charts from stockholm-mp to madrid-mp(192.148.201.15) on 2022-04-05

Dashed lines means there are non-responding routers between nodes. Color scale is log(e) responses. Hover nodes to see links and corresponding table entry. Select node to scroll to table entry. Drag nodes to fix. traceroute dvs ingen rute videre.

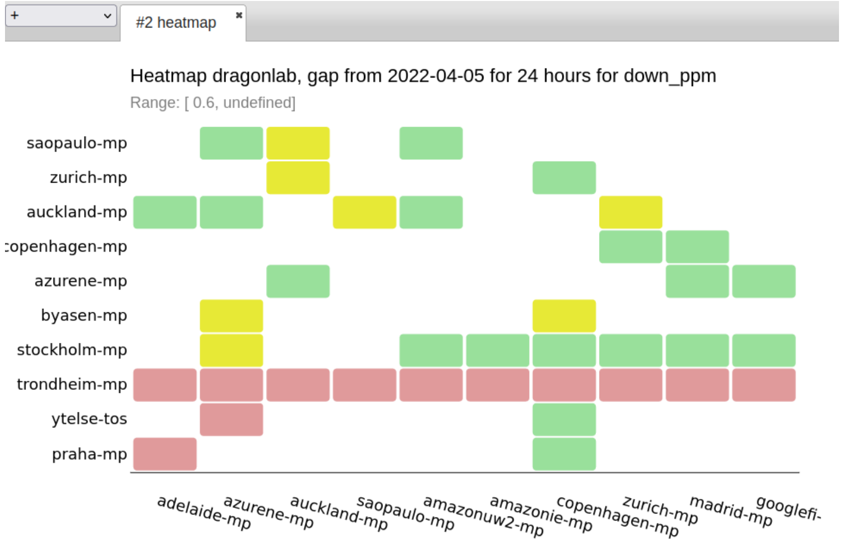


Traceroute charts from stockholm-mp to madrid-mp(192.148.201.15

Hop	Router	Avg ms	Min	Max	Sdv	Loss%	Seen	Address	Start	End	Error
1	se-lab-sw-a01.nordu.net	0.2	0.1	1.6	0.1	0.00%	8196	194.68.13.66	05 00:00:05	05 22:34:44	
2	se-sthb.nordu.net	1.0	0.4	29.8	1.9	4.56%	3661	109.105.97.182	05 00:00:05	05 22:34:44	
	se-tug.nordu.net	0.7	0.2	24.4	1.3	9.59%	3940	109.105.97.180	05 00:00:05	05 22:34:44	
3	dk-bal2.nordu.net	11.6	10.0	29.2	3.4	0.33%	1202	109.105.97.10	05 00:00:05	05 22:34:44	
	dk-ore.nordu.net	9.6	8.6	26.0	2.6	2.40%	609	109.105.97.130	05 00:00:05	05 22:34:44	
	se-tug.nordu.net	1.2	0.3	32.8	2.8	67.58%	2062	109.105.97.245	05 00:00:05	05 22:33:41	
4	dk-bal2.nordu.net	11.1	9.5	46.3	4.1	2.37%	2058	109.105.97.249	05 00:01:00	05 22:33:41	
	dk-esbj.nordu.net	15.9	14.6	41.2	3.1	0.25%	3982	109.105.97.3	05 00:00:05	05 22:34:44	
	dk-bal2.nordu.net	11.8	10.1	46.9	4.4	2.26%	2037	109.105.97.10	05 00:00:05	05 22:34:44	
5	nl-ams.nordu.net	22.8	20.7	87.9	5.0	0.12%	4093	109.105.97.75	05 00:00:05	05 22:34:44	
	dk-esbj.nordu.net	16.2	14.1	62.0	4.9	0.90%	4059	109.105.97.3	05 00:00:05	05 22:34:44	
6	uk-hex.nordu.net	26.2	25.4	71.3	2.8	0.02%	4040	109.105.97.125	05 00:00:05	05 22:34:44	
	nl-ams.nordu.net	23.0	20.2	77.9	6.0	0.14%	4149	109.105.97.75	05 00:00:05	05 22:34:44	
7	nordunet.mx1.lon.uk.geant.net	26.4	25.5	71.8	3.6	0.10%	4080	62.40.124.129	05 00:00:05	05 22:34:44	
	uk-hex.nordu.net	26.0	24.9	65.8	3.0	0.00%	4112	109.105.97.125	05 00:00:05	05 22:34:44	
8	ae6.mx1.lon2.uk.geant.net	27.1	26.3	76.3	2.8	0.00%	3998	62.40.98.37	05 00:00:05	05 22:34:44	
	nordunet.mx1.lon.uk.geant.net	26.4	25.0	78.1	4.0	0.00%	4197	62.40.124.129	05 00:00:05	05 22:34:44	
9	ae5.mx1.par.fr.geant.net	33.7	32.7	79.3	3.4	0.00%	4070	62.40.98.179	05 00:00:05	05 22:34:44	
	ae6.mx1.lon2.uk.geant.net	27.0	25.8	69.8	3.2	0.00%	4126	62.40.98.37	05 00:00:05	05 22:34:44	
10	ae4.rt1.bil.es.geant.net	44.7	43.8	87.4	3.3	0.00%	4111	62.40.98.222	05 00:00:05	05 22:34:44	
	ae5.mx1.par.fr.geant.net	33.5	32.2	78.5	3.6	0.00%	4085	62.40.98.179	05 00:00:05	05 22:34:44	
11	ae4.rt1.bil.es.geant.net	44.4	43.2	83.1	3.1	0.00%	4073	62.40.98.222	05 00:00:05	05 22:34:44	
	rediris-ap3.bil.es.geant.net	44.5	44.0	63.6	1.8	0.00%	4123	62.40.127.183	05 00:00:05	05 22:34:44	
12	ehu.rt2.ethtrunk5.ciemat.rt2.mad.red.rediris.es	53.5	52.9	72.9	1.7	0.00%	2053	130.206.245.5	05 00:00:05	05 22:34:44	



From stockholm-mp to madrid-mp on 2022-04-05 for h_ddelay



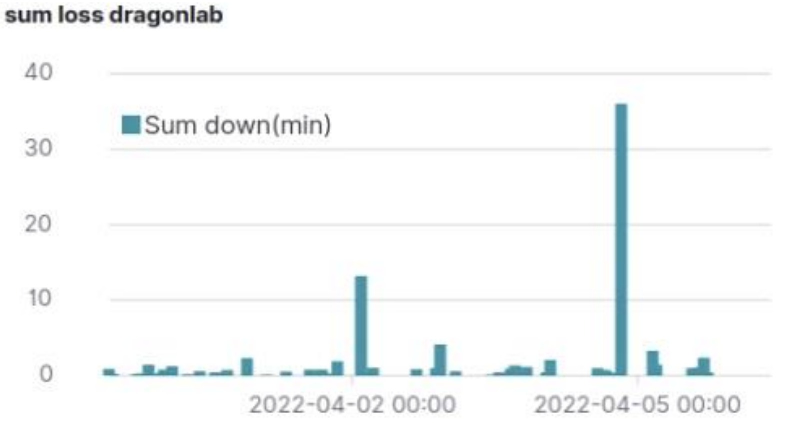
Heatmap dragonlab, gap from 2022-04-05 for 24 hours for down_ppm

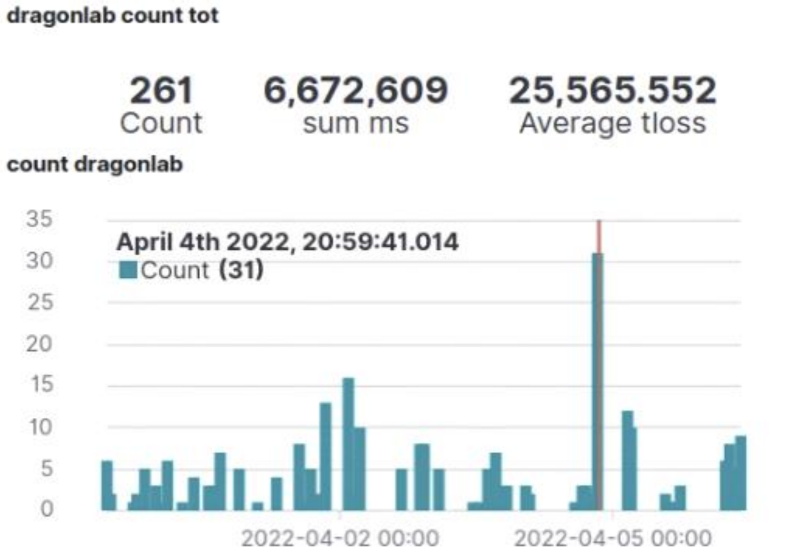
Range: [0.6, undefined]

	adelaide-mp	azurene-mp	auckland-mp	saopaulo-mp	amazonuw2-mp	amazonie-mp	copenhagen-mp	zurich-mp	madrid-mp	googlefi-
saopaulo-mp		🟩	🟨		🟩					
zurich-mp			🟨				🟩			
auckland-mp	🟩	🟩		🟨	🟩			🟨		
copenhagen-mp								🟩	🟩	
azurene-mp			🟩						🟩	🟩
byasen-mp		🟨					🟨			
stockholm-mp		🟨			🟩	🟩	🟩	🟩	🟩	🟩
trondheim-mp	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
ytelse-tos		🟥					🟩			
praha-mp	🟥						🟩			

Gaps / packet loss events

- Windows of 2000 pkts -> min one-way delay
- Gap event = 5 or more pkts lost, i.e. 50 ms downtime
  - 5 successfull pkts ends gap
- Stats on head and tail of gaps (50 pkts)
- Smaller gaps + other stats in daily summary reports




dragonlab count tot

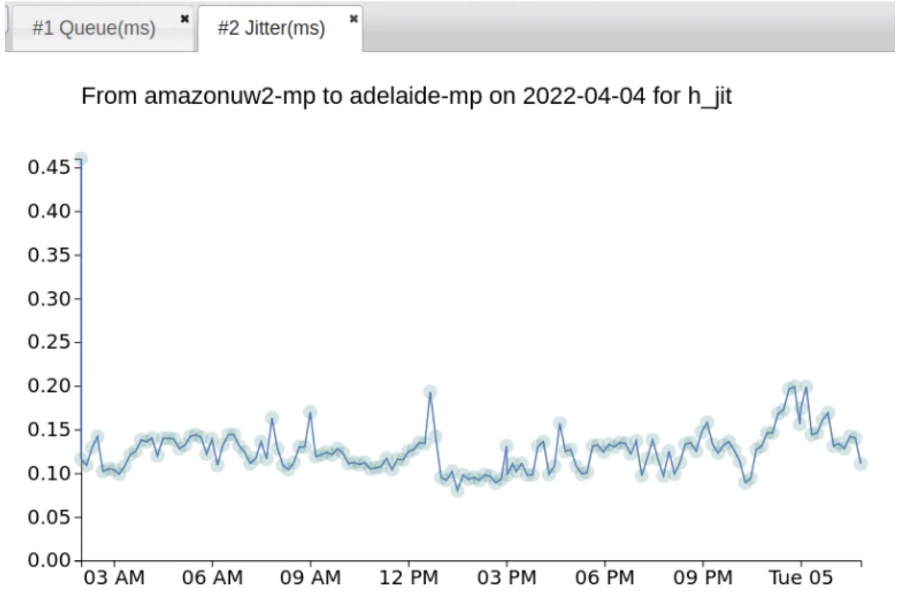
261 Count

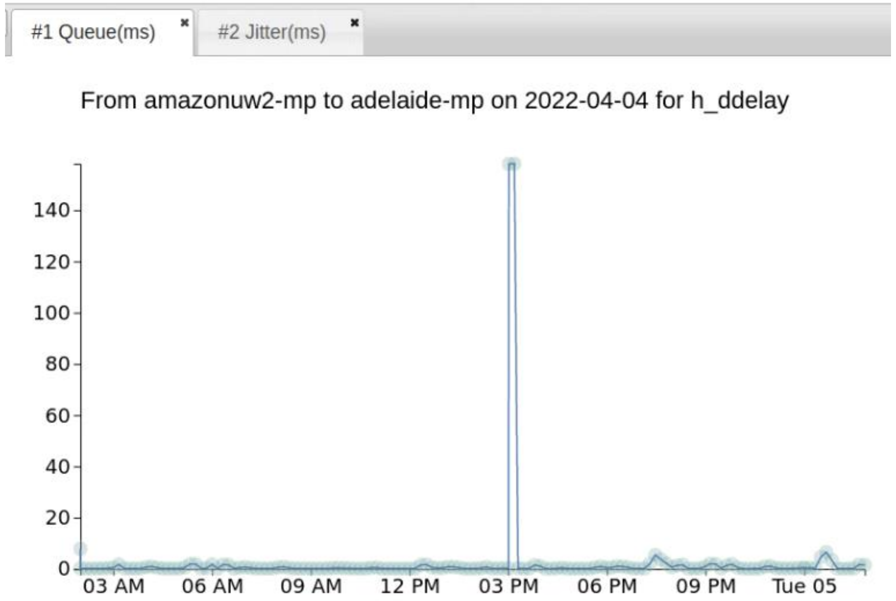
6,672,609 sum ms

25,565.552 Average tloss

Queues / Jitter events

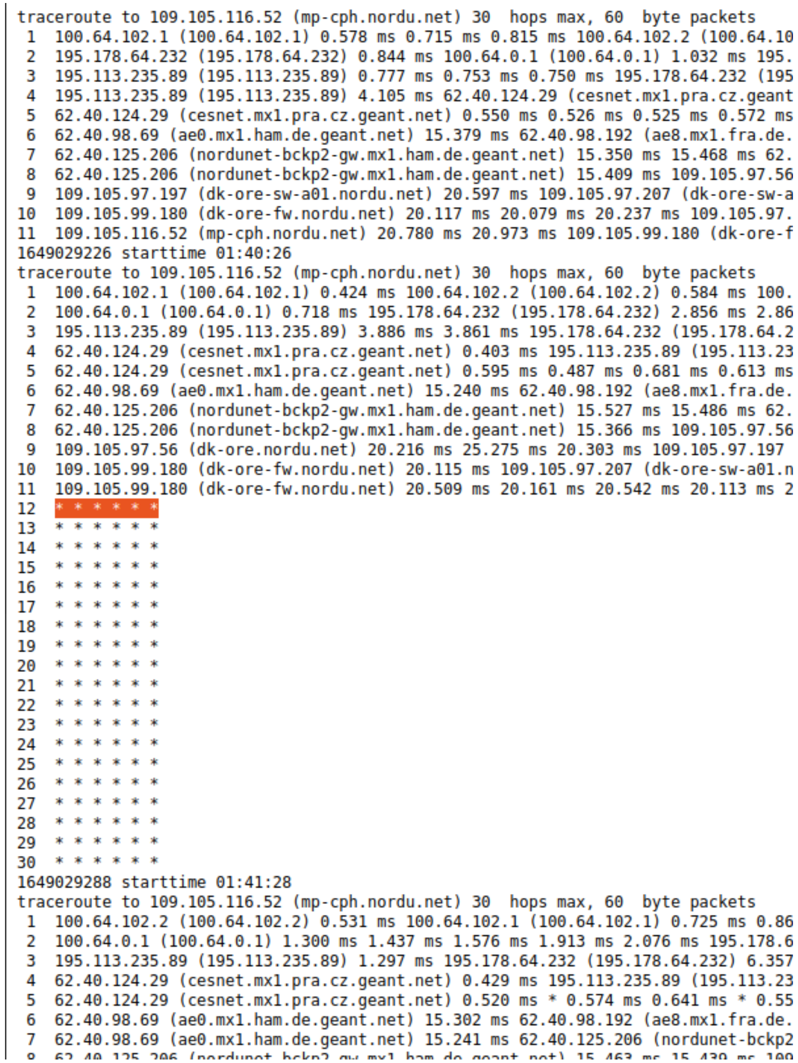
- Jitter definition from RTCP (rfc3550)
  - ... but show only minor variances
  - Order of few ms
- Queue-buildup events by change in differential one-way delay
  - (delayB – delayA) – mindelay
  - Order of 10-100 ms


From amazonuw2-mp to adelaide-mp on 2022-04-04 for h_jit


From amazonuw2-mp to adelaide-mp on 2022-04-04 for h_ddelay

Route failure events

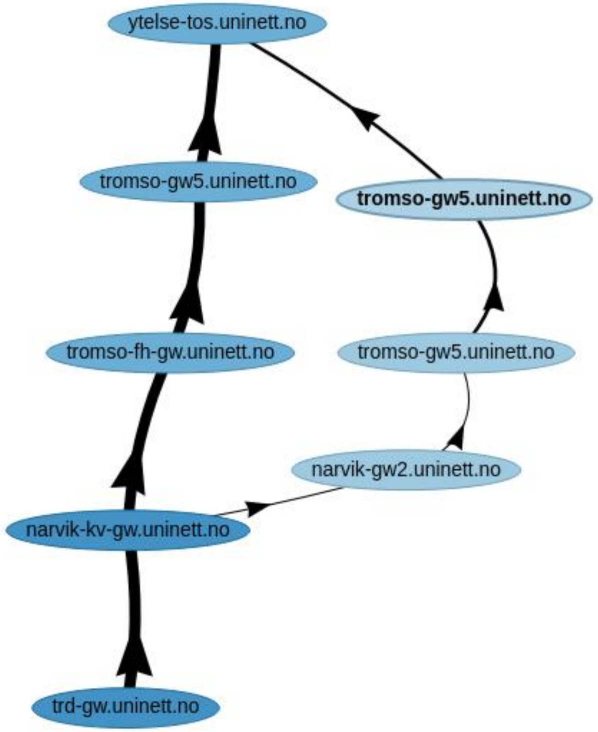
- Route failure = «never ending» traceroute
- Detect periodes with route failures
  - Find «* * * * * *» at max-hops
- Report ICMP errors
  - Network unreachable (N!)
  - ...



```
traceroute to 109.105.116.52 (mp-cph.nordu.net) 30  hops max, 60  byte packets
 1  100.64.102.1 (100.64.102.1) 0.578 ms 0.715 ms 0.815 ms 100.64.102.2 (100.64.10
 2  195.178.64.232 (195.178.64.232) 0.844 ms 100.64.0.1 (100.64.0.1) 1.032 ms 195.
 3  195.113.235.89 (195.113.235.89) 0.777 ms 0.753 ms 0.750 ms 195.178.64.232 (195
 4  195.113.235.89 (195.113.235.89) 4.105 ms 62.40.124.29 (cesnet.mx1.pra.cz.geant
 5  62.40.124.29 (cesnet.mx1.pra.cz.geant.net) 0.550 ms 0.526 ms 0.525 ms 0.572 ms
 6  62.40.98.69 (ae0.mx1.ham.de.geant.net) 15.379 ms 62.40.98.192 (ae8.mx1.fra.de.
 7  62.40.125.206 (nordunet-bckp2-gw.mx1.ham.de.geant.net) 15.350 ms 15.468 ms 62.
 8  62.40.125.206 (nordunet-bckp2-gw.mx1.ham.de.geant.net) 15.409 ms 109.105.97.56
 9  109.105.97.197 (dk-ore-sw-a01.nordu.net) 20.597 ms 109.105.97.207 (dk-ore-sw-a
10  109.105.99.180 (dk-ore-fw.nordu.net) 20.117 ms 20.079 ms 20.237 ms 109.105.97.
11  109.105.116.52 (mp-cph.nordu.net) 20.780 ms 20.973 ms 109.105.99.180 (dk-ore-f
1649029226 starttime 01:40:26
traceroute to 109.105.116.52 (mp-cph.nordu.net) 30  hops max, 60  byte packets
 1  100.64.102.1 (100.64.102.1) 0.424 ms 100.64.102.2 (100.64.102.2) 0.584 ms 100.
 2  100.64.0.1 (100.64.0.1) 0.718 ms 195.178.64.232 (195.178.64.232) 2.856 ms 2.86
 3  195.113.235.89 (195.113.235.89) 3.886 ms 3.861 ms 195.178.64.232 (195.178.64.2
 4  62.40.124.29 (cesnet.mx1.pra.cz.geant.net) 0.403 ms 195.113.235.89 (195.113.23
 5  62.40.124.29 (cesnet.mx1.pra.cz.geant.net) 0.595 ms 0.487 ms 0.681 ms 0.613 ms
 6  62.40.98.69 (ae0.mx1.ham.de.geant.net) 15.240 ms 62.40.98.192 (ae8.mx1.fra.de.
 7  62.40.125.206 (nordunet-bckp2-gw.mx1.ham.de.geant.net) 15.527 ms 15.486 ms 62.
 8  62.40.125.206 (nordunet-bckp2-gw.mx1.ham.de.geant.net) 15.366 ms 109.105.97.56
 9  109.105.97.56 (dk-ore.nordu.net) 20.216 ms 25.275 ms 20.303 ms 109.105.97.197
10  109.105.99.180 (dk-ore-fw.nordu.net) 20.115 ms 109.105.97.207 (dk-ore-sw-a01.n
11  109.105.99.180 (dk-ore-fw.nordu.net) 20.509 ms 20.161 ms 20.542 ms 20.113 ms 2
12  * * * * * *
13  * * * * * *
14  * * * * * *
15  * * * * * *
16  * * * * * *
17  * * * * * *
18  * * * * * *
19  * * * * * *
20  * * * * * *
21  * * * * * *
22  * * * * * *
23  * * * * * *
24  * * * * * *
25  * * * * * *
26  * * * * * *
27  * * * * * *
28  * * * * * *
29  * * * * * *
30  * * * * * *
1649029288 starttime 01:41:28
traceroute to 109.105.116.52 (mp-cph.nordu.net) 30  hops max, 60  byte packets
 1  100.64.102.2 (100.64.102.2) 0.531 ms 100.64.102.1 (100.64.102.1) 0.725 ms 0.86
 2  100.64.0.1 (100.64.0.1) 1.300 ms 1.437 ms 1.576 ms 1.913 ms 2.076 ms 195.178.6
 3  195.113.235.89 (195.113.235.89) 1.297 ms 195.178.64.232 (195.178.64.232) 6.357
 4  62.40.124.29 (cesnet.mx1.pra.cz.geant.net) 0.429 ms 195.113.235.89 (195.113.23
 5  62.40.124.29 (cesnet.mx1.pra.cz.geant.net) 0.520 ms * 0.574 ms 0.641 ms * 0.55
 6  62.40.98.69 (ae0.mx1.ham.de.geant.net) 15.302 ms 62.40.98.192 (ae8.mx1.fra.de.
 7  62.40.98.69 (ae0.mx1.ham.de.geant.net) 15.241 ms 62.40.125.206 (nordunet-bckp2
 8  62.40.125.206 (nordunet-bckp2-gw.mx1.ham.de.geant.net) 15.463 ms 15.439 ms 109
```

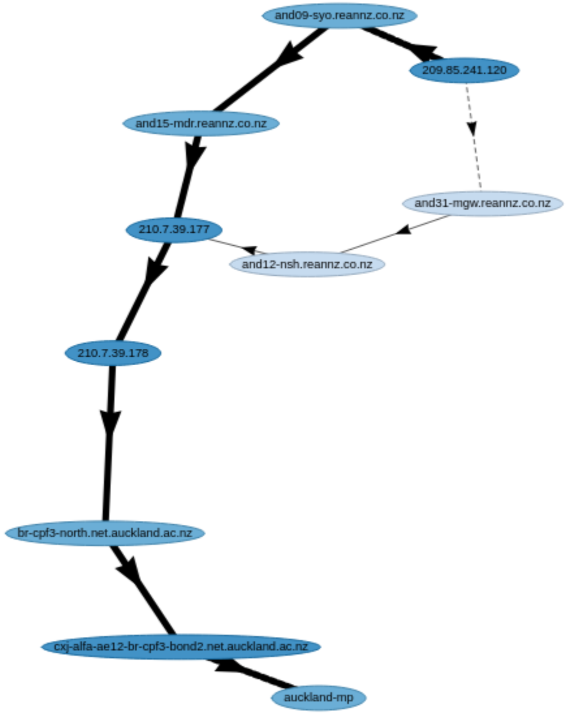
Route change events

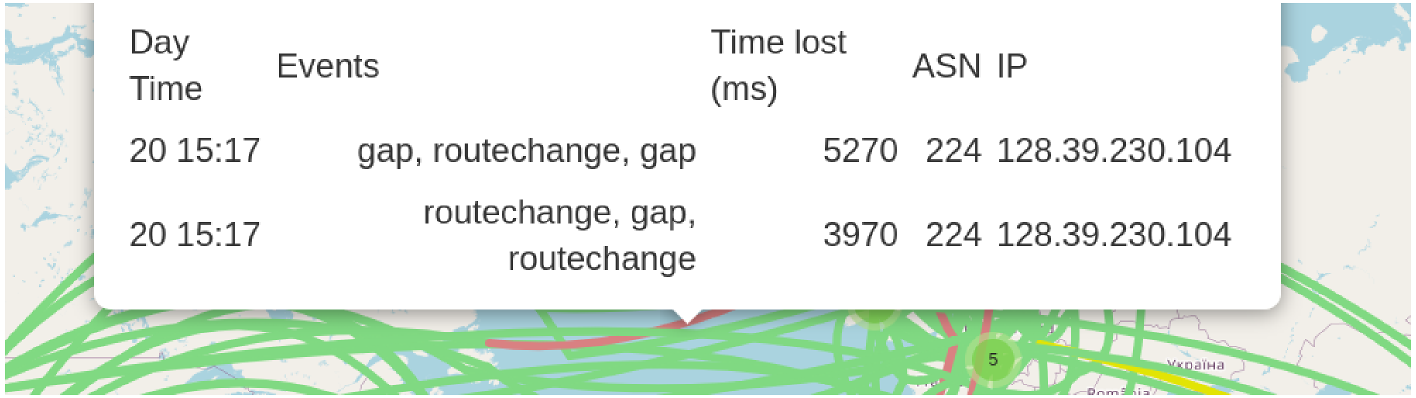
- Route change = **significant** new route
- Detects **change in distribution of seen ip** addresses for each traceroute hop
  - Differential cross entropy
- «Learns» which route changes are normal



Correlated events

- Gap and routechange in same time window
- Downtime + path anomality
- Identity and ASN of responsible router





Day Time	Events	Time lost (ms)	ASN	IP
20 15:17	gap, routechange, gap	5270	224	128.39.230.104
20 15:17	routechange, gap, routechange	3970	224	128.39.230.104

Join the Microdep project !

- Access the Microdep online tool via **https://microdep.uninett.no**
- Add a node to the topology
  - Prepare a Debian or Ubuntu system (VM, container, physical)
  - Open some ports:
    - UDP 10001 and 34464-34564
    - TCP 22 and 80.
  - Run
    - wget -O- http://apt.uninett.no/uninett_apt.gpg | apt-key add -
    - apt-add-repository 'deb [arch=amd64] http://apt.uninett.no/debian buster main'
    - apt update && apt install mp-dragonlab
  - Email IP-address of node and other questions to **microdep@sikt.no**

Demo time...