Microdep-based network analysis

2nd Geant Telemetry and Data Workshop
April 6, 2022

Otto J Wittner - Sikt (Uninett)

Sikt

Microdep funamental

- Initially a measurement project (since 2010)

- Today a measurement system and a project

- Objectives

  - Reveal network **dependability issues** at **fine grained** level by **end-to-end measurements**

  - **Improve routing** in NRENs and **the global Internet**

Sikt

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)
- Joint event anomality and alarms via ELK (potentially ML based)

- perfSONAR integration in progress

Sikt

Results from analysis

https://microdep.uninett.no
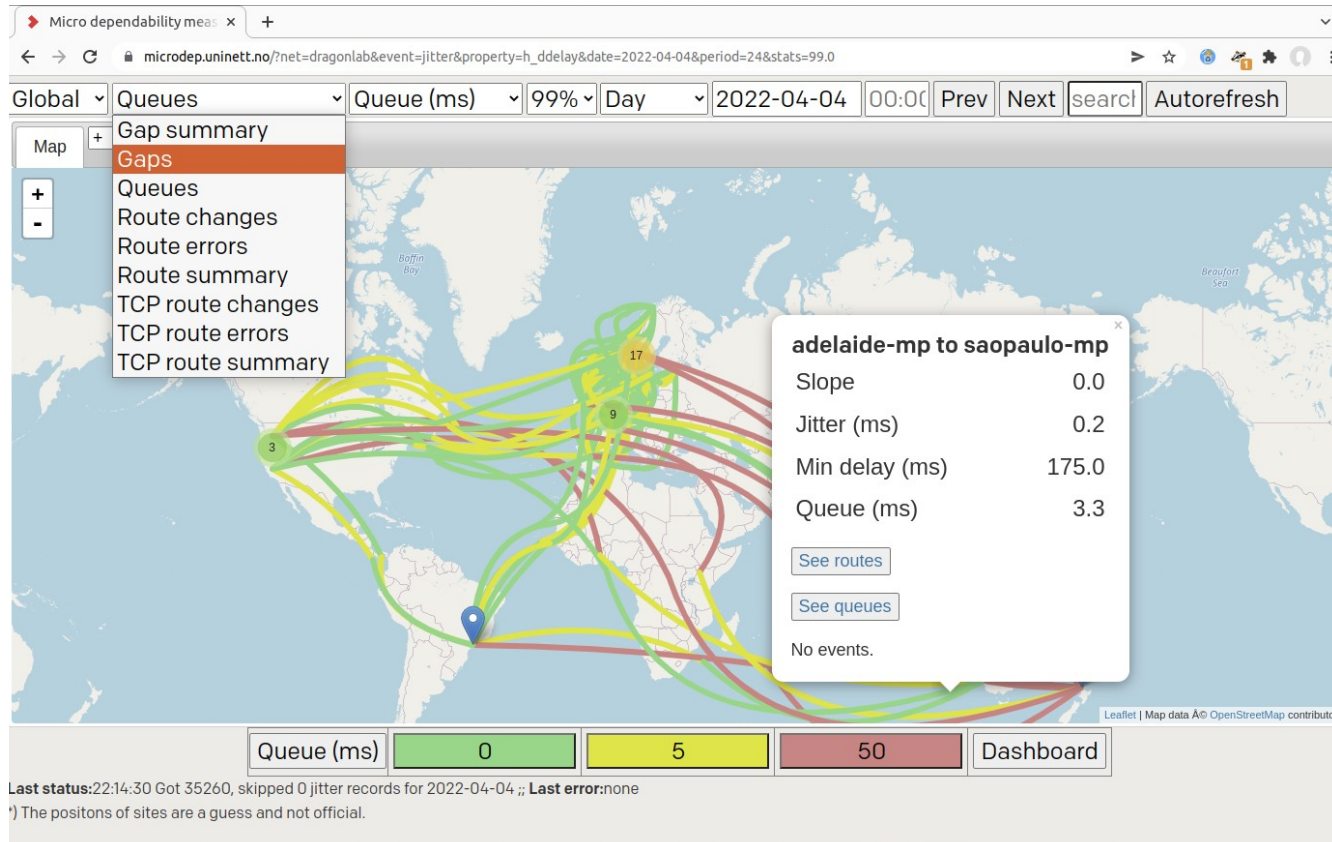
Other results views

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

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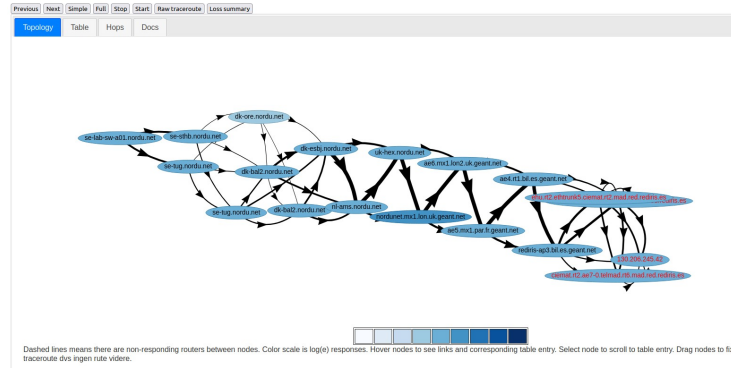
Traceroute charts from stockholm-mp to madrid-mp(192.148.201.15)

| 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%	4047	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	
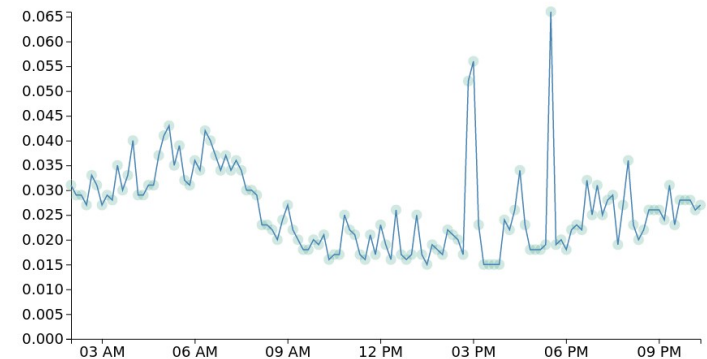
Heatmap dragonlab, gap from 2022-04-05 for 24 hours for down_ppm
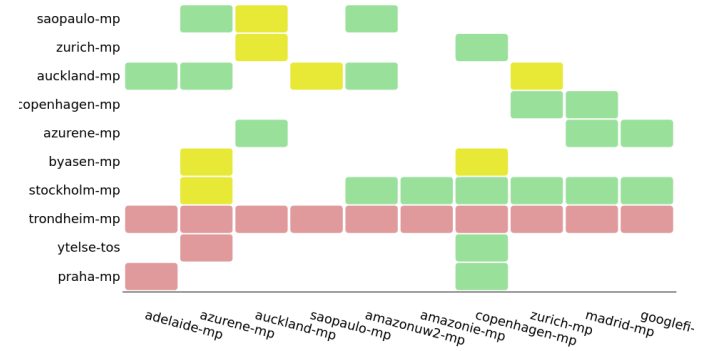
Gaps / packetloss events

- 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
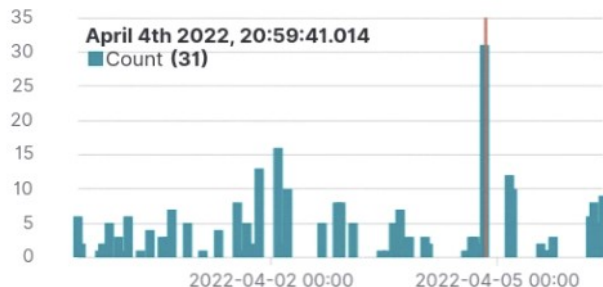

sum loss dragonlab

■ Sum down(min)

2022-04-02 00:00   2022-04-05 00:00
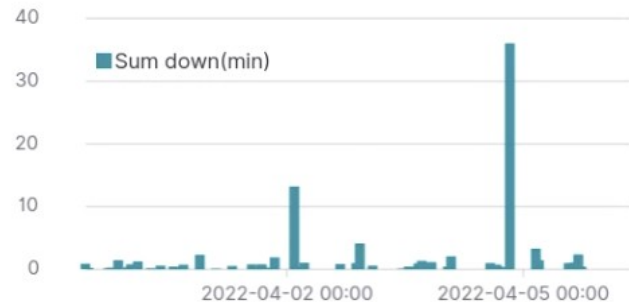
dragonlab count tot

| 261 Count | 6,672,609 sum ms | 25,565.552 Average tloss |

count dragonlab

April 4th 2022, 20:59:41.014
■ Count (31)

2022-04-02 00:00   2022-04-05 00:00

Sikt

Queues / Jitter events

- Jitter definition from RTCP (rfc???) applied

  – ... 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

Sikt

#1 Queue(ms)   #2 Jitter(ms)

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

#1 Queue(ms)   #2 Jitter(ms)

From amazonuw2-mp to adelaide-mp on 2022-04-04 for h_ddelay
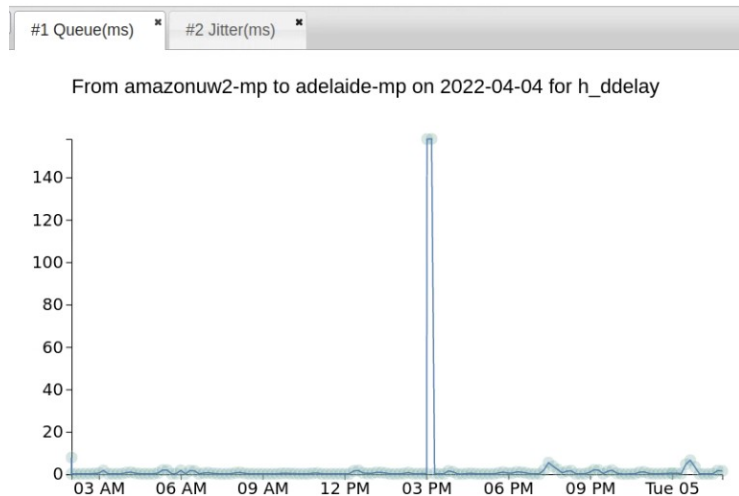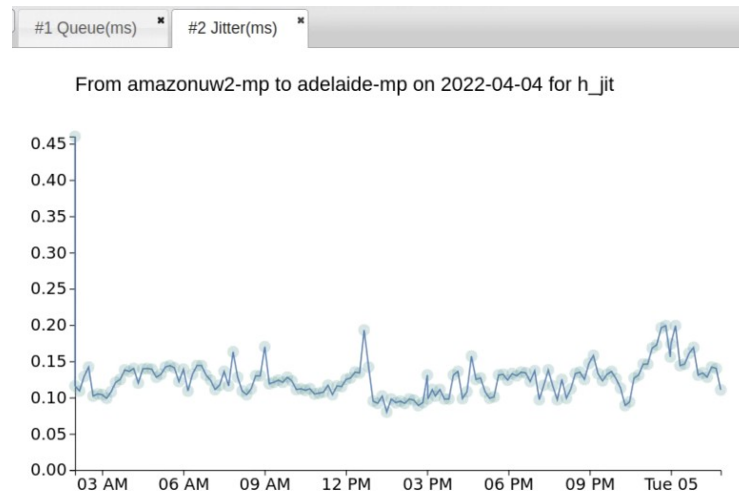
Route failure events

- Route failure = «never ending» traceroute

- Detect periodes with route failures

  – Find «* * * * * *» at max-hops

- Report ICMP errors

  – Network unreachable (N!)

  – ...

Route change events

- Route change = **significant** new route

- Detect **change in distribution of seen ip** addresses for each traceroute hop

  - Differential cross entropy

- «Learns» which route changes are normal

Sikt

Quick demo...