RIPE NCC
RIPE NETWORK COORDINATION CENTER

Analysing the Baltic Sea Cable Breaks with RIPE Atlas

Gerardo Viviers | Netnod meeting | 18/03/2025

Baltic Sea cable breakages

Timeline

- 17 Nov 2024: BSC East-West broken
- 18 Nov 2024: C-LION1 broken
- 27 Nov 2024: BSC East-West restored
- 28 Nov 2024: C-LION1 restored
- 25 Dec 2024: C-LION1 broken
- 06 Jan 2025: C-LION1 restored
- 26 Jan 2025: LVRTC broken

Baltic Sea cable breakages

Media reaction

Two Baltic Sea cables disrupted – is this 'hybrid warfare'?

By **Annie Turner** - 19 November 2024

European governments point finger at Russia over Baltic cable cuts

Investigations are underway into two subsea cable breache and European governments are starting to suggest that Ru

Mary Lennighan
November 20, 2024

3 Min Read

Damaged cables appear to be accident, Finland says

3 December 2024

Share Save

George Wright
BBC News

Sweden opens inquiry into damaged undersea cable as Nato deploys ships

A vessel has been seized after suspected sabo optic line, probably due to external influence,

December 31, 2024

Christmas Day Cable Cuts in the Baltic Sea

Written by Alexander Lott

In less than 14 months, submarine telecommunications cables connecting Estonia, Finland, Germany, Lithuania, Russia, and Sweden have been cut altic Sea. In addition, an ur e been cut by a ship ancho cidents all involving a forei eafloor for over a hundred

r Bear incident occurred ir in November 2024, and th 024. As indicated on the m al offshore infrastructure lo e damaged in the NewN TLINK 1 electricity cable o Finland's decisive interve

o the critical offshore infras olar Bear and the Eagle S e only.

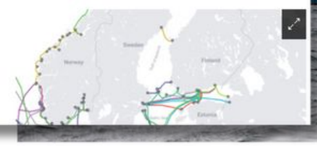
Baltic subsea cable damage was accidental, not sabotage - US and European officials

Refutes all claims of Russian sabotage

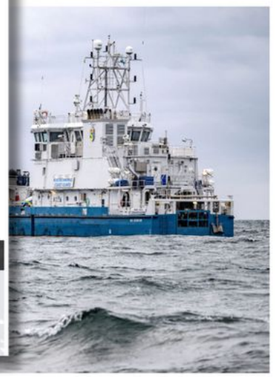
January 20, 2025 By: Niva Yadav Have your say

Subsea cable damage in the Baltic Sea in recent months was likely the result of maritime accidents, not Russian sabotage, according to several US and European intelligence officials.

As reported by The Washington Post, US and European officials have gathered evidence - including intercepted communications - which have concluded that anchors were dragged across the seabed accidentally because of inexperienced crews aboard poorly maintained



Share full article



Sweden Investigates New Cable Break Under Baltic Sea

The authorities are looking into possible damage to an undersea line east of Gotland island. NATO has stepped up its surveillance of the region.

A Swedish Coast Guard vessel in the Baltic Sea. Sweden also investigated the severing

Measuring incidents with RIPE Atlas

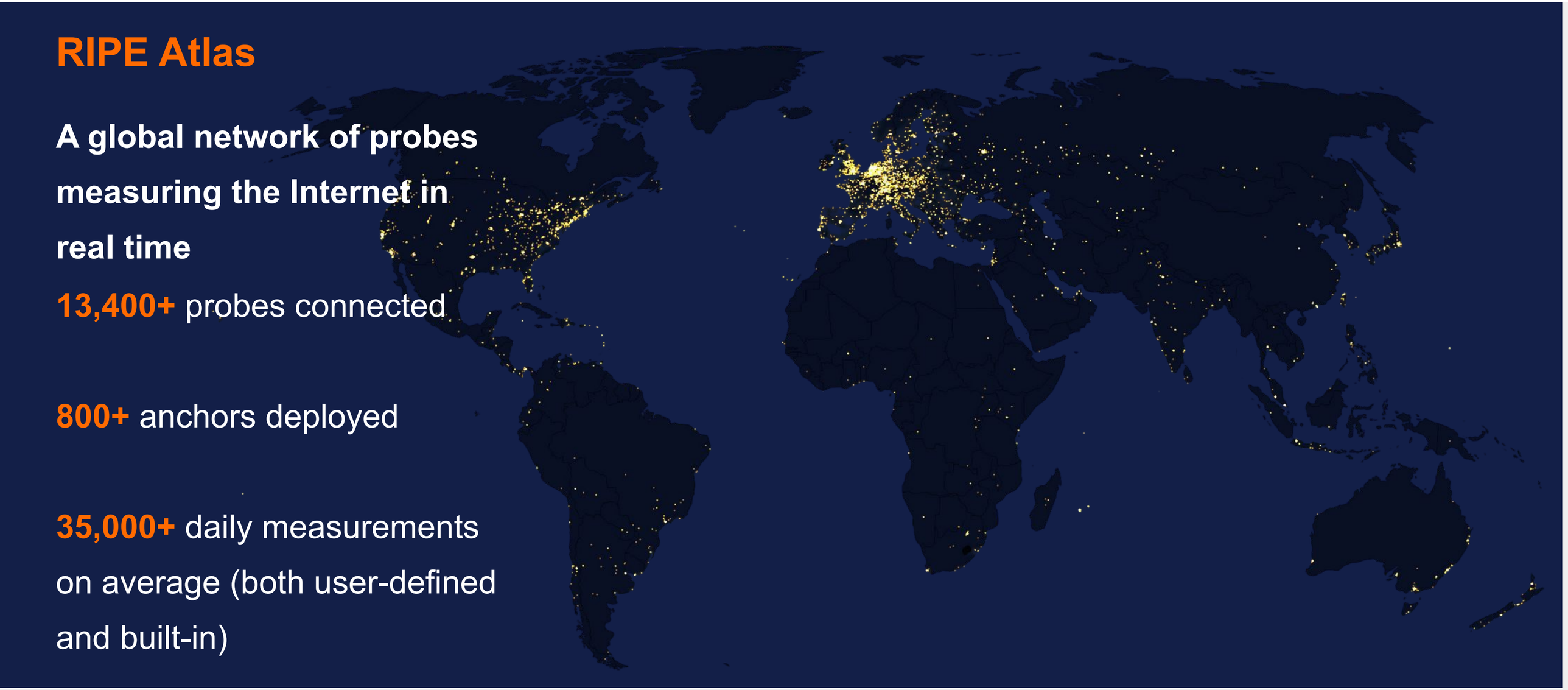
RIPE Atlas

A global network of probes measuring the Internet in real time

13,400+ probes connected

800+ anchors deployed

35,000+ daily measurements on average (both user-defined and built-in)



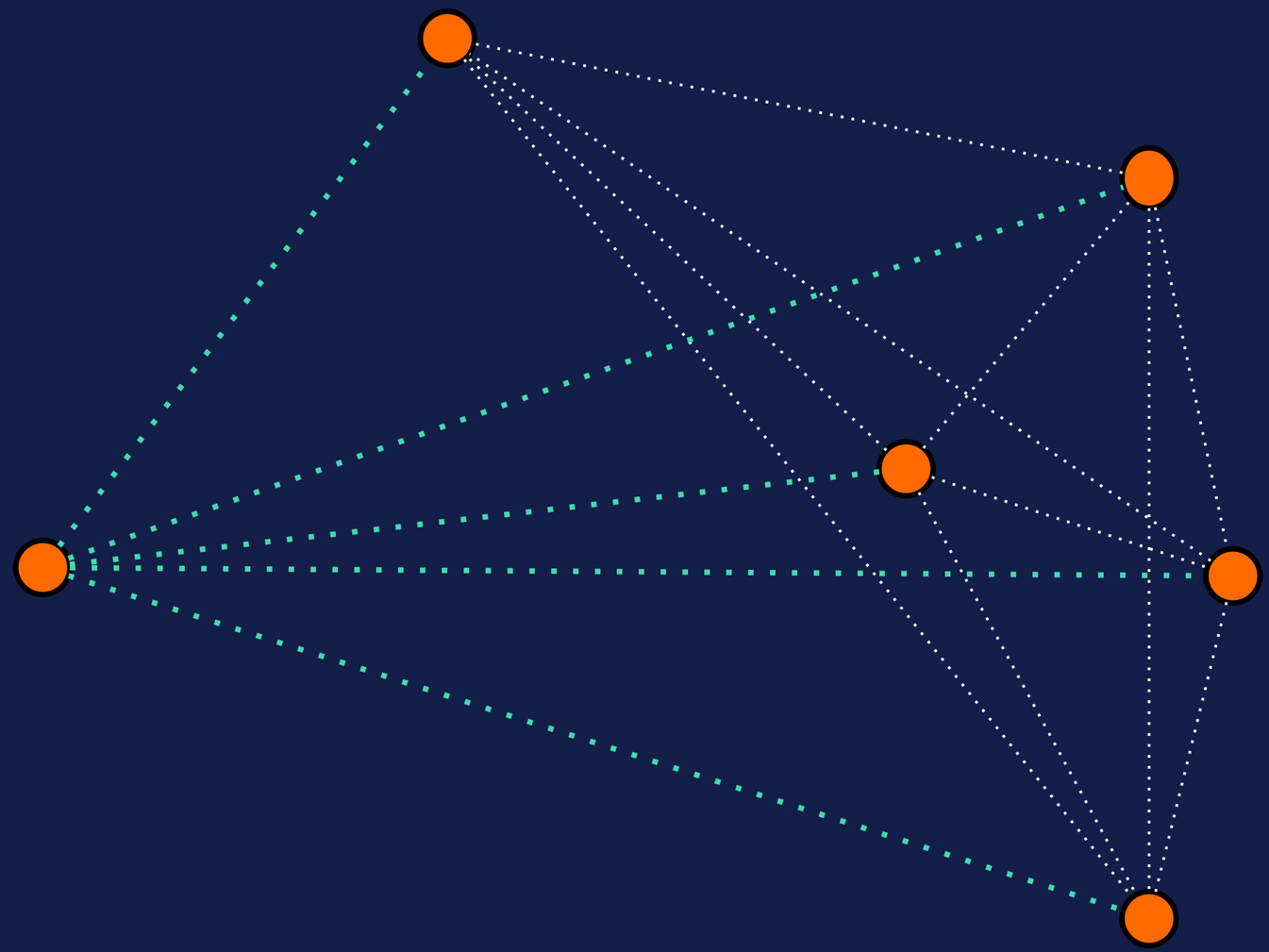
Measuring incidents with RIPE Atlas

Anchor mesh

RIPE Atlas anchors support ping, traceroute, DNS, HTTP/S measurements

Each anchor performs ongoing ping measurements to all other anchors at four-minute intervals

Resulting ‘mesh’ of measurements lets us observe latency changes and packet loss between anchors



First look

17/18 November

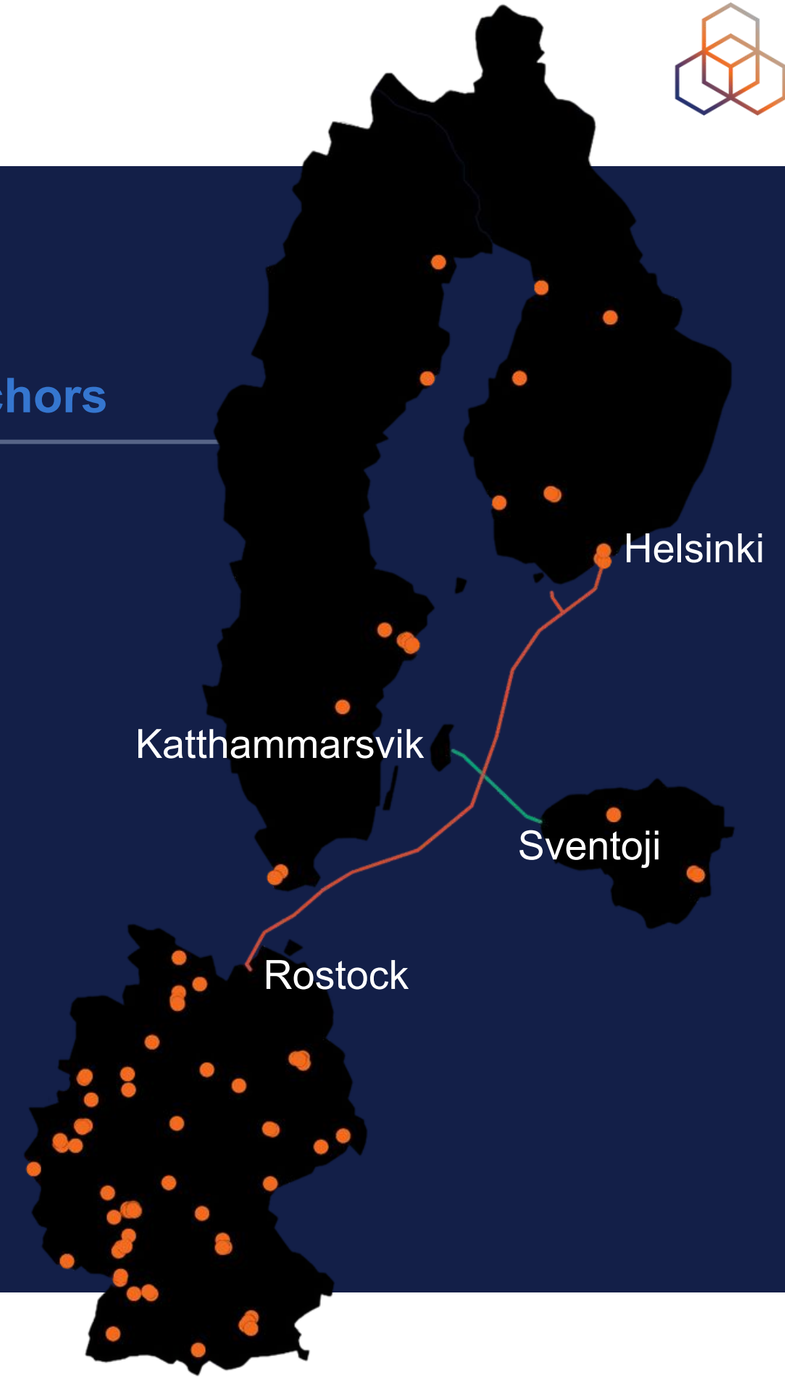
Damage reported:

BSC East-West (Sweden-Lithuania)

C-LION1 (Germany-Finland)

We looked at results in the RIPE Atlas anchor mesh between these countries around reported time of the event

Country	# anchors
Germany:	100
Sweden:	15
Finland:	12
Lithuania:	5



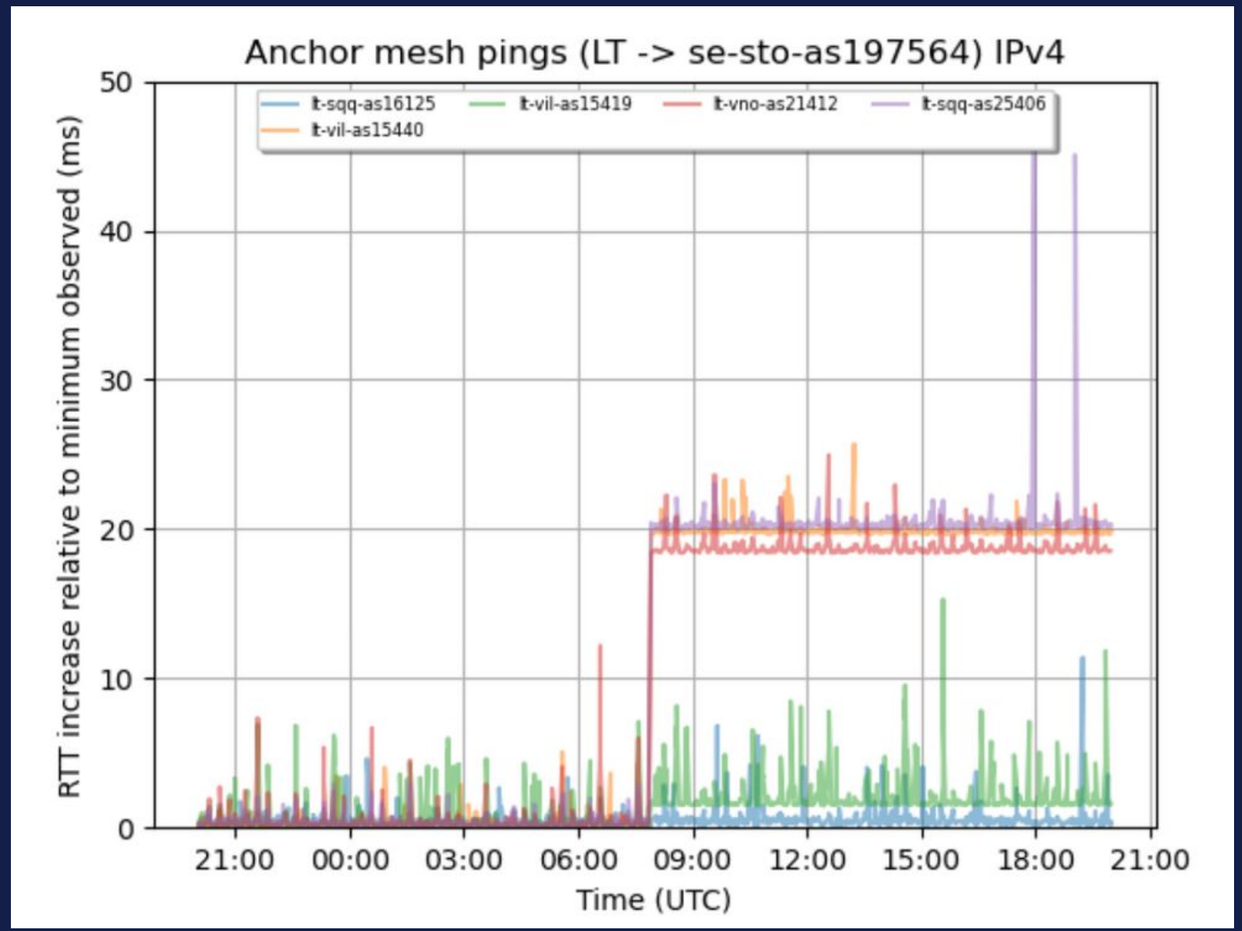
BSC East West

Latency shift

12 hours before/after time of event

Latency shifts a little after **08:00 UTC on 17 November**

We subtract the minimum latency for a path during our observation period to make the latency jumps comparable



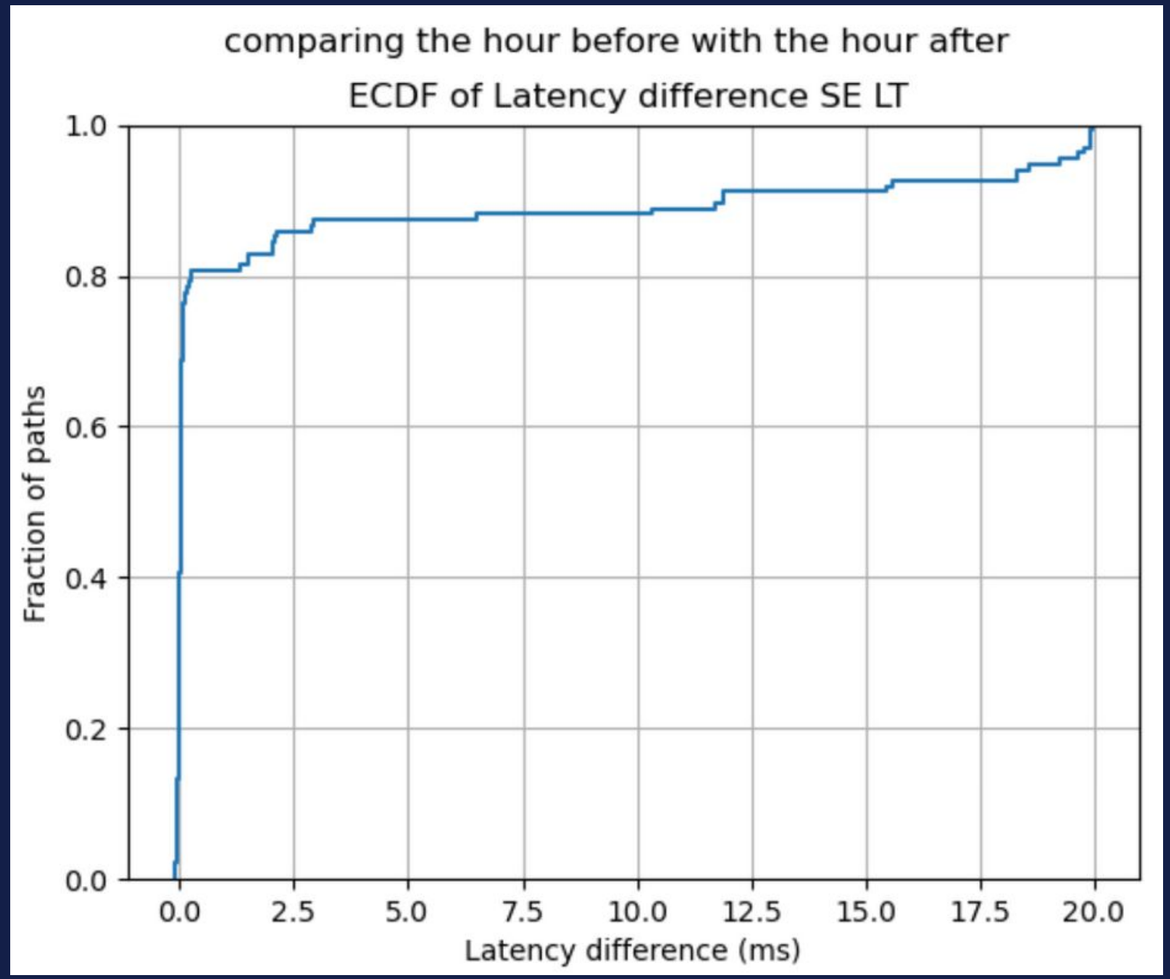
BSC East West

Distribution of latency shift

80% of paths: no significant difference

20% of paths: increased latency

10% of paths with the most latency difference see an increase of 10 - 20 ms.

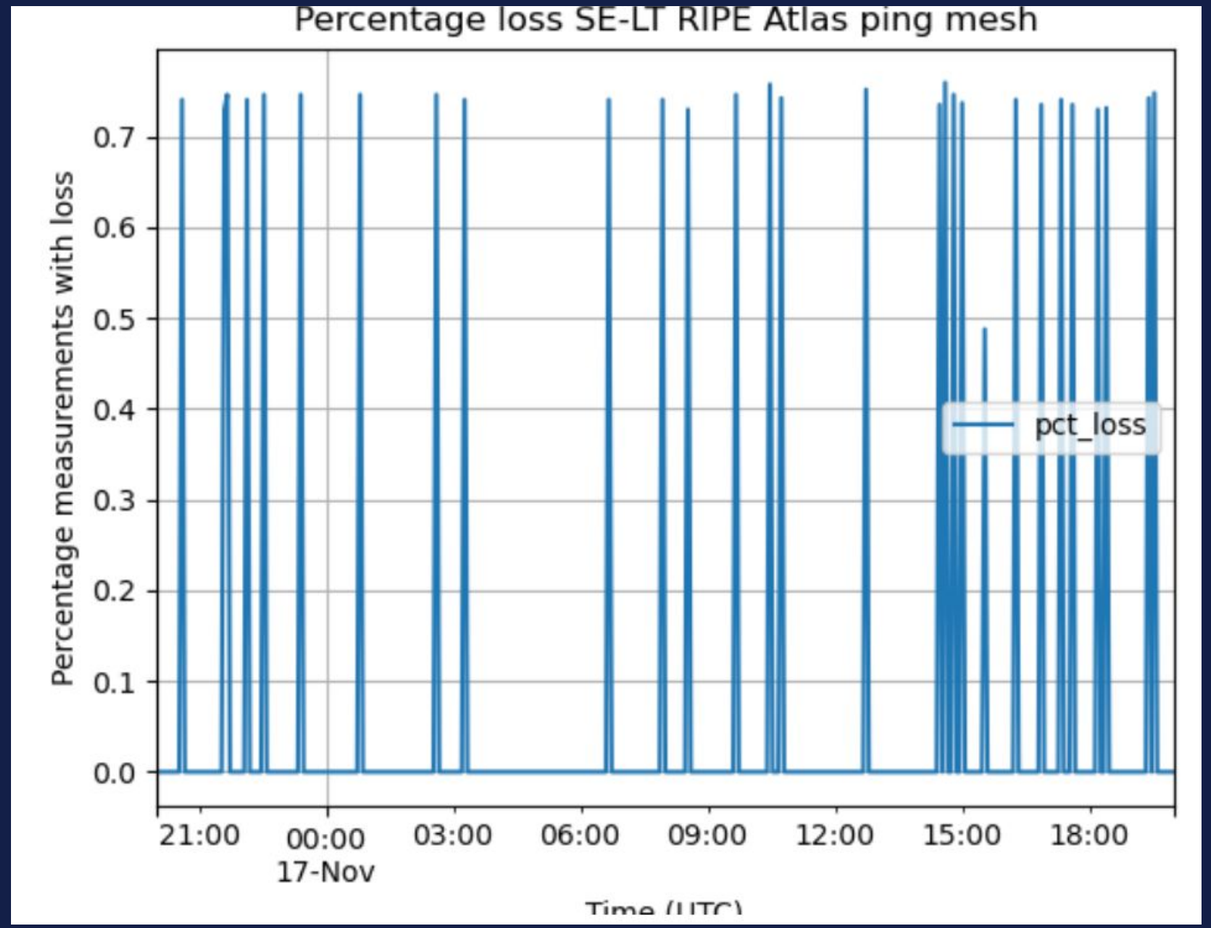


BSC East West

Packet loss

Baseline of 0% packet loss with occasional spikes

No significant increase in packet loss at time of the cable break (shortly before 08:00 UTC)



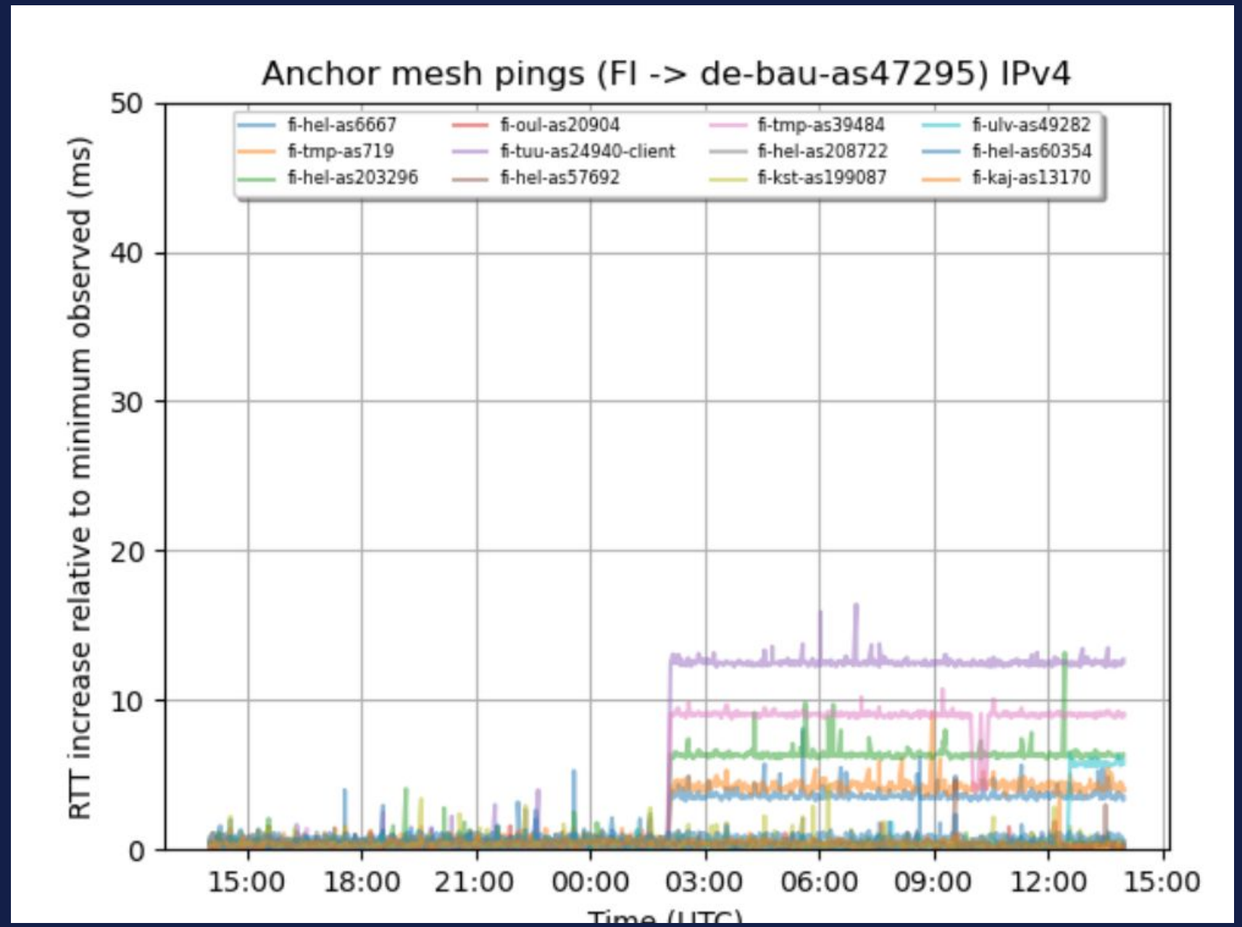
C-LION1

Latency shift

12 hours before/after time of event

Notable shift in latency for multiple paths a little after **02:00 UTC on 18 November**

We subtract the minimum latency for a path during our observation period to make the latency jumps comparable



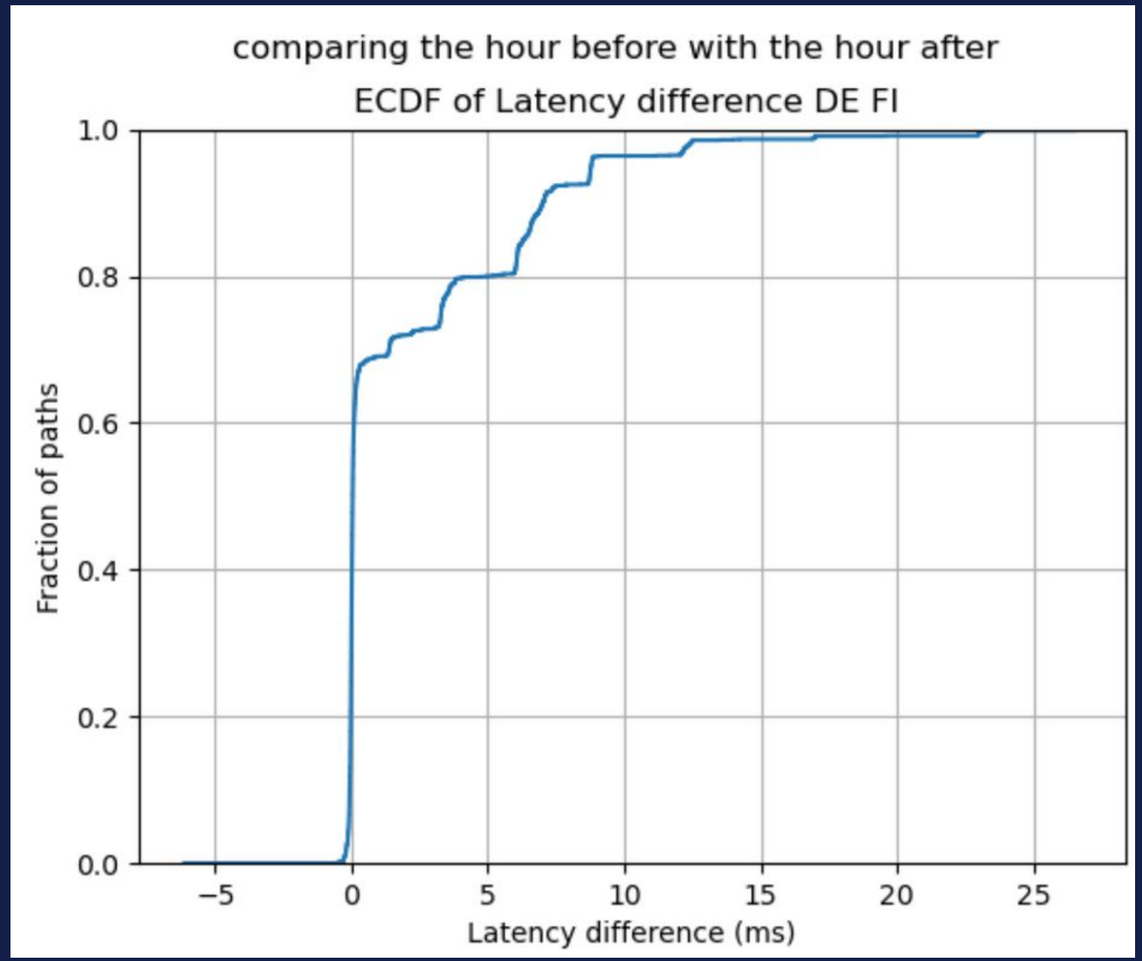
Distribution of latency shift

One hour before/after time of event:

70% of paths: no difference

30% paths: increased latency

20% paths: latency increases of 5ms or more



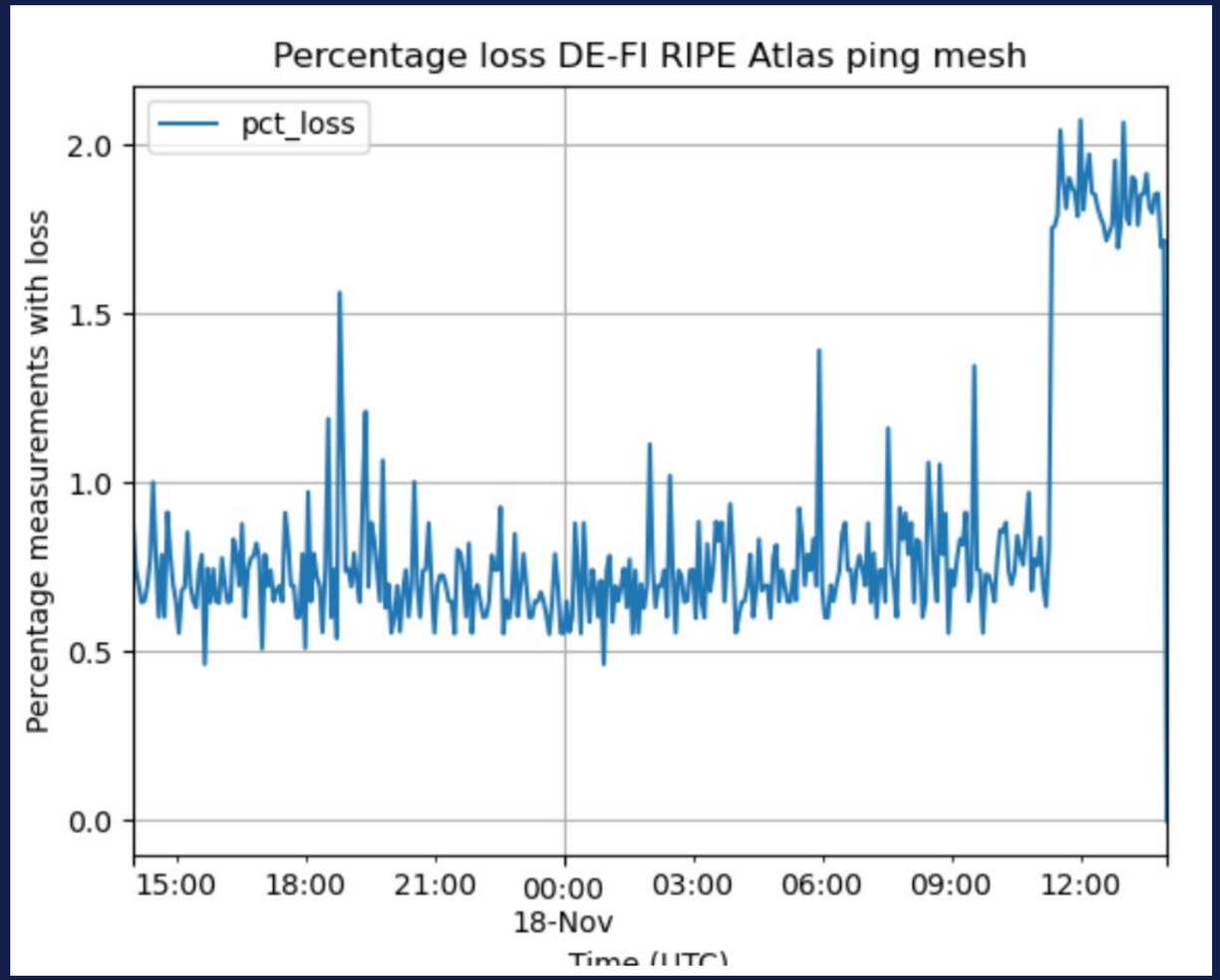
C-LION1

Packet loss

Baseline of between 0.5% and 1.0% packet loss during most of this time.

Again, no significant increase in packet loss at time of the cable break (02:00 UTC)

Note: increased packet loss in the last 2 hours of this graph - unclear what caused jump, but unlikely that this is an immediate effect of the earlier break



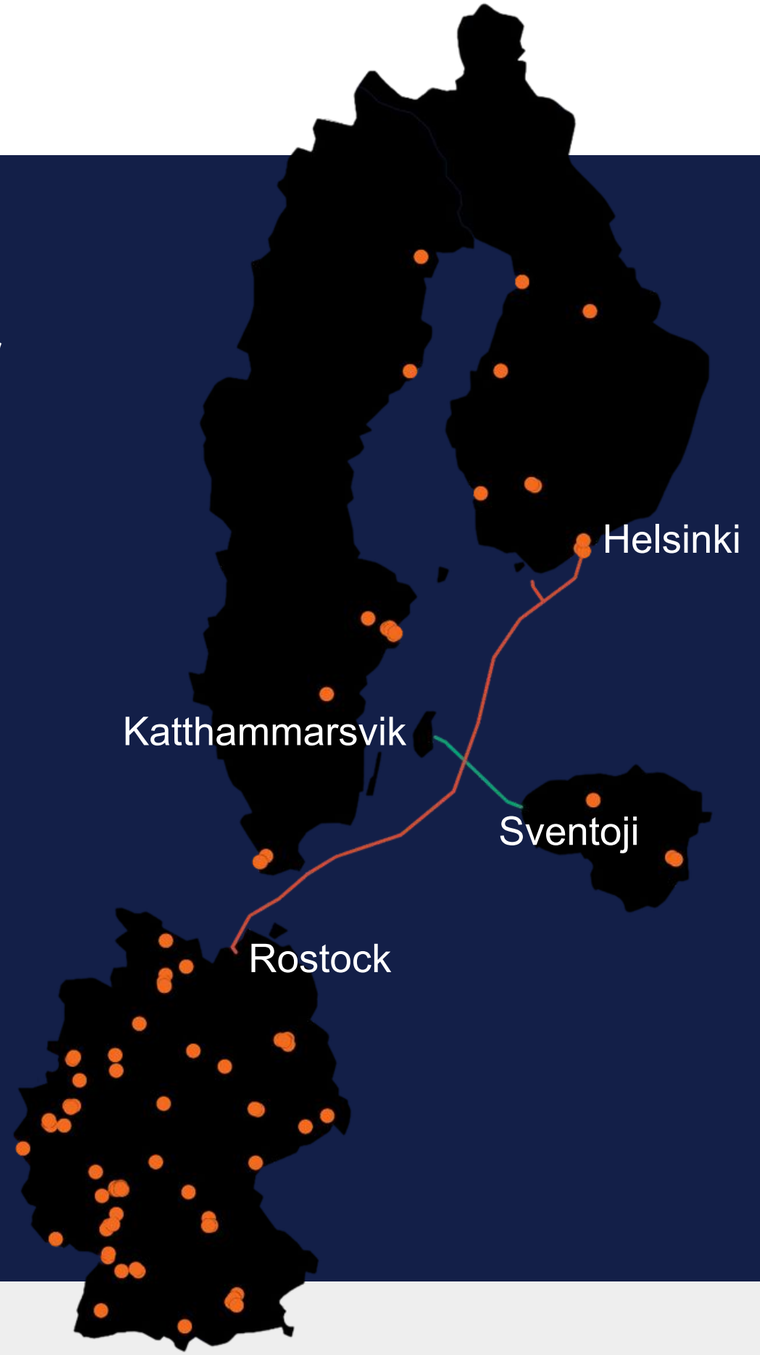
Summing up

There was a relatively minor but visible shift in latency for around 20-30% of paths between observed anchors

This shift allows us to pinpoint the precise time at which damage occurred

But there was no concurrent increase in packet loss

The Internet routed around damage!

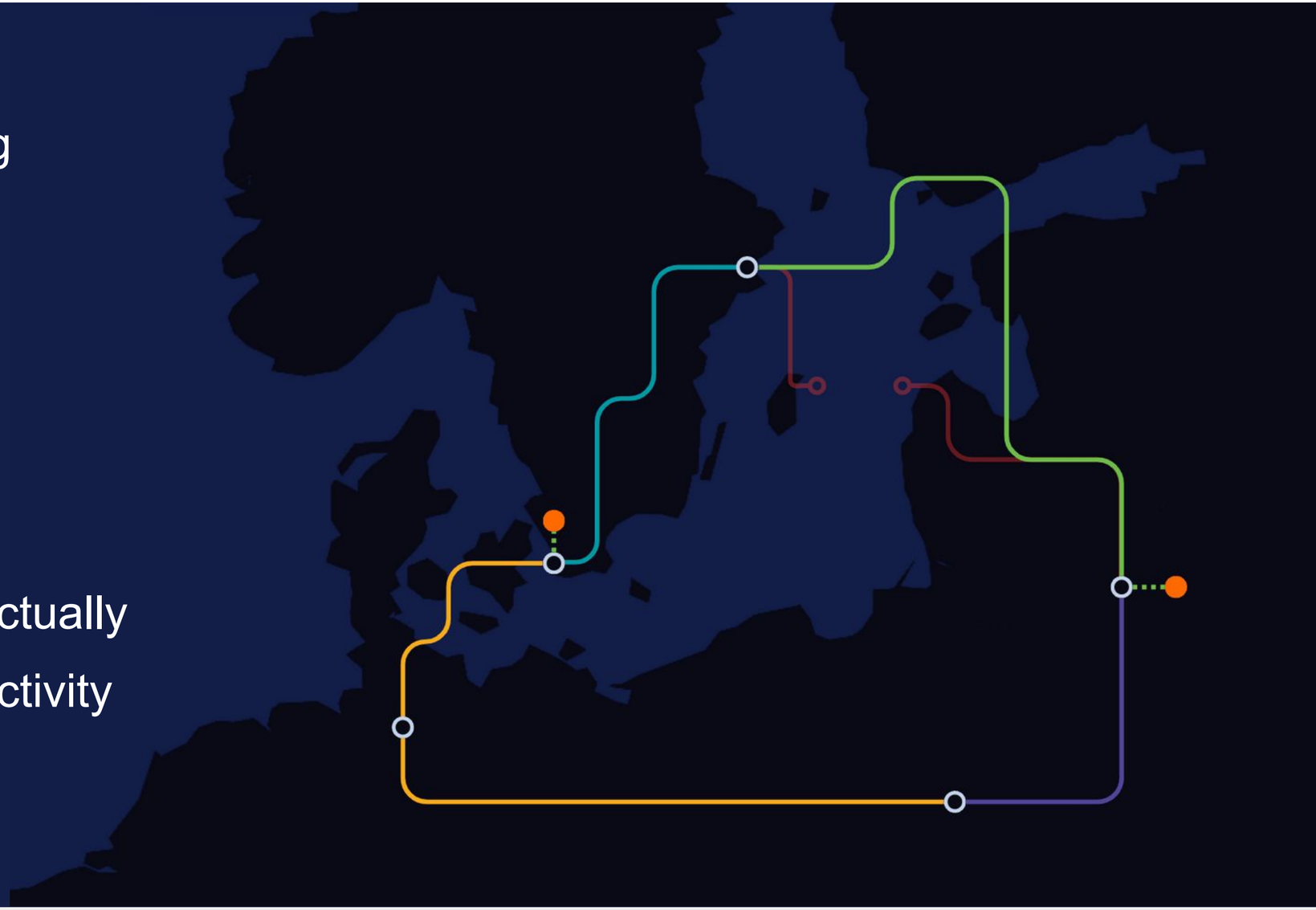


Deeper dive

Initial analysis was based on ping (end-to-end latency) data

We followed this up with in depth analysis using traceroute data

Aim: to examine how the paths actually changed while end-to-end connectivity was maintained



Levels of resilience

Inter-domain rerouting:

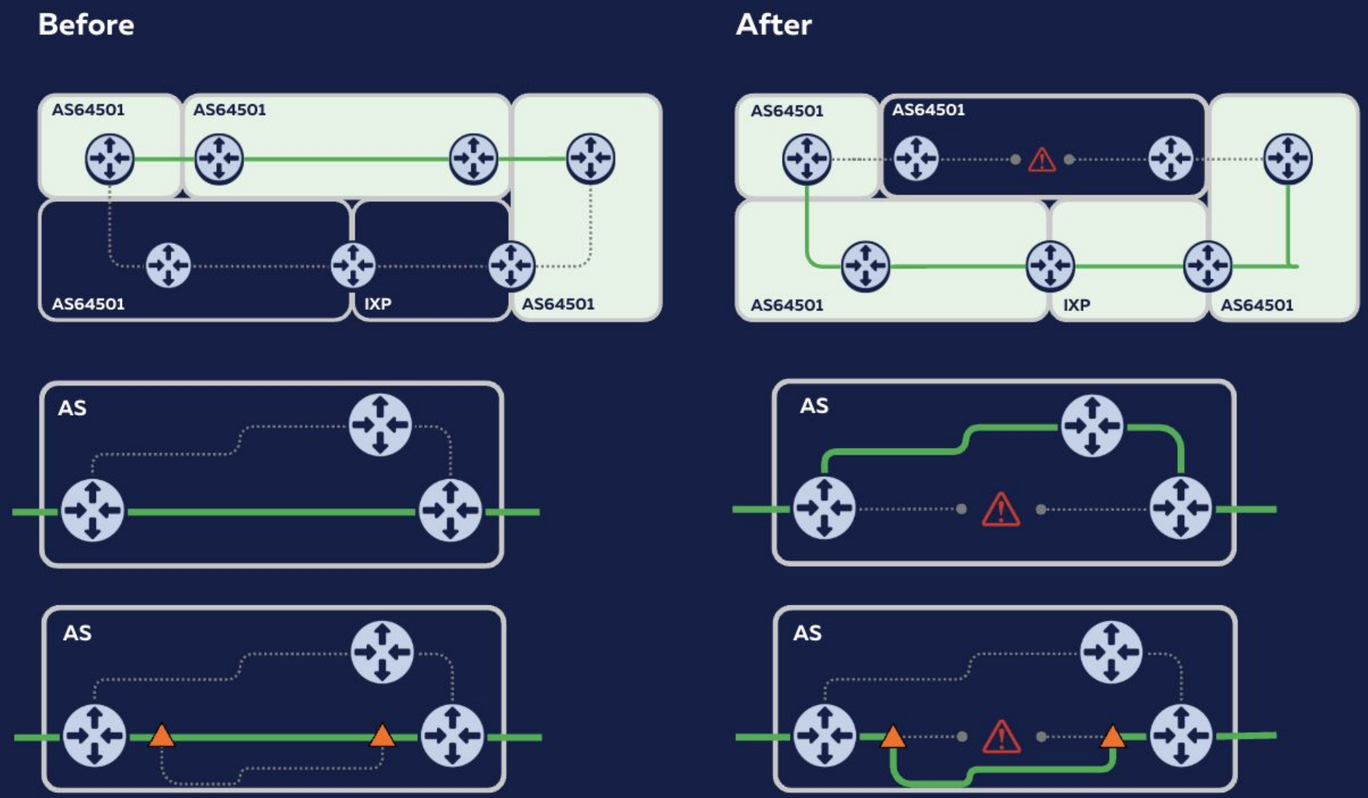
Traffic rerouted through alternative ASes/IXPs (eBGP routing protocol)

Intra-domain rerouting:

Rerouting *within* networks along alternative paths (IGP - e.g., OSPF, IS-IS)

Circuit-level rerouting:

Rerouting along alternative circuit-level connections between routers (same IP address)



Levels of resilience

Of the 2,141 bidirectional paths between anchors in Germany and Finland used for this analysis:

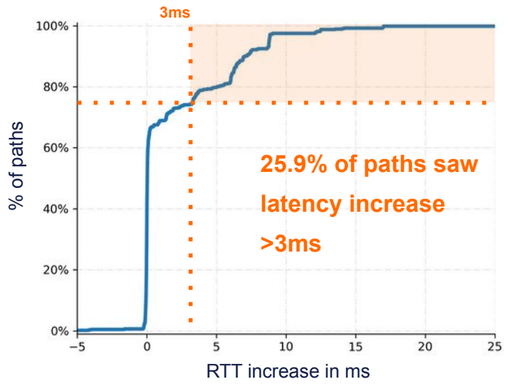
Inter-domain changes: 637 (29.8%)

Intra-domain changes: 1,044 (48.8%)

No inter-domain or intra-domain changes: 460 (21.5%)

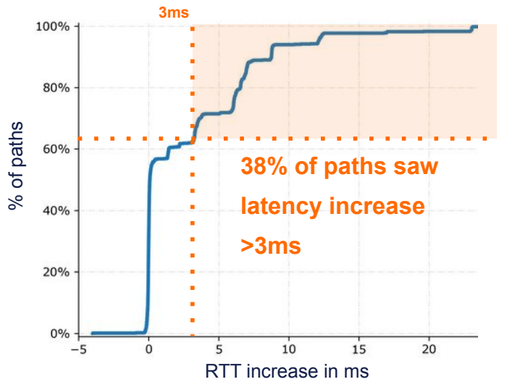
Inter-domain rerouting

RTT profile for paths where inter-domain routing changed.



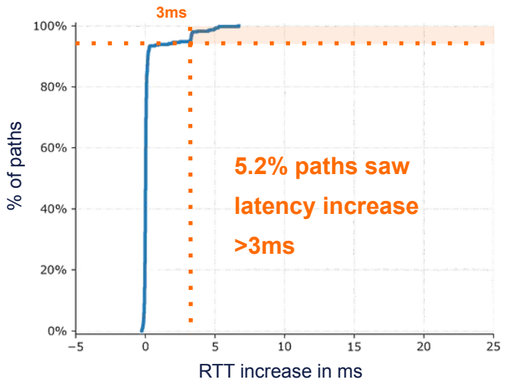
Intra-domain rerouting

RTT profile for paths with IP-level changes, but no inter-domain changes.



Circuit-level rerouting

RTT profile for paths without IP-level changes.



Conclusions

What can we learn from this?

Internet resilience depends on multiple levels of redundancy - redundancy mechanisms provided a defence against damage in the seconds following the Baltic Sea cable breaks

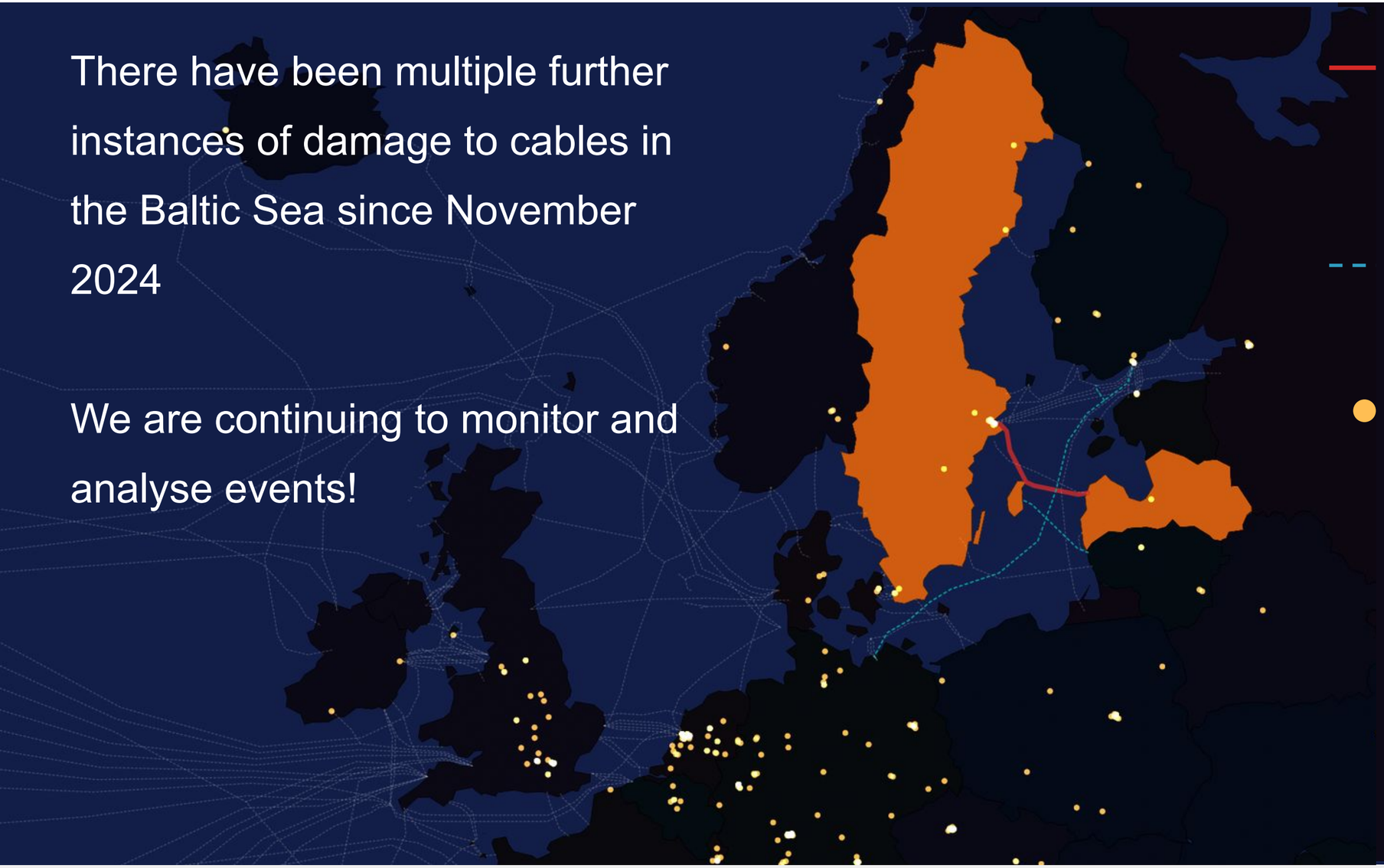
Building redundancy into the networks means holding on to a mindest that opts for:

- Decentralised connectivity
- Inter-provider transit diversity
- Interconnection at geographically diverse IXPs

Ongoing incidents

There have been multiple further instances of damage to cables in the Baltic Sea since November 2024

We are continuing to monitor and analyse events!



— Sweden-Latvia Internet cable belonging to Latvia State Radio and Television Center (LVRTC) was reportedly broken on 26 Jan 2025.

– – This is another in a series of breaks on submarine cables in the region in recent months.

● Packet delays between selected RIPE Atlas anchors increased by 5-20ms at around 00:45 UTC – *but absence of packet loss indicates that the Internet successfully routed around the damage.*

Read further analyses of cable breaks and Internet outages on RIPE Labs:

https://labs.ripe.net/search/tag/outages/

Beyond the Baltic Sea

Analysing other cable breaks

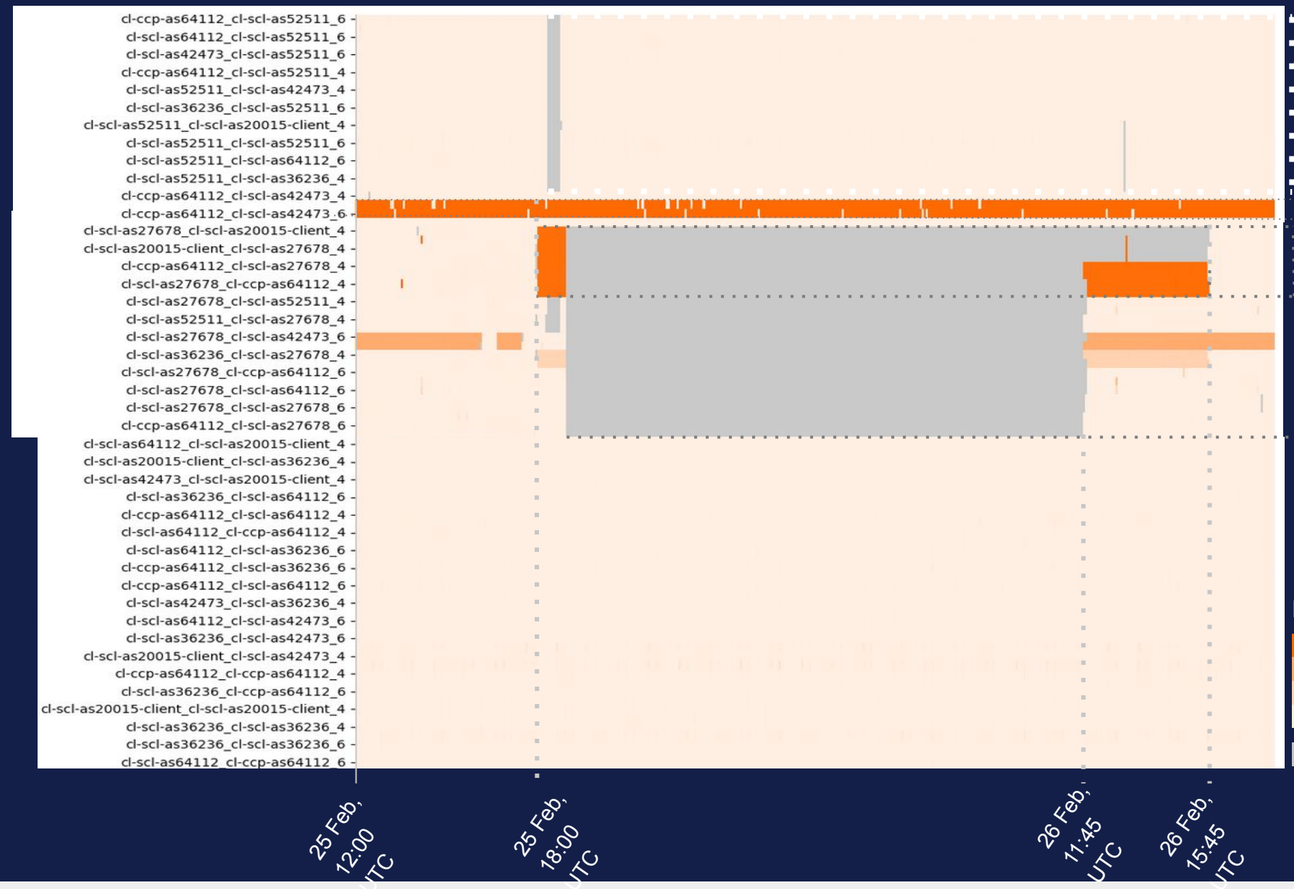
We have a relatively high number of RIPE Atlas anchors in **some** countries around the Baltic Sea

Damage to cables is not so easy to analyse: e.g., much less visibility into recent damage to Taiwan cables

We are actively seeking hosts who can help us get RIPE Atlas probes and anchors set up in locations where they can shed light on the state of the Internet.

Chile Power Outage

On 25 February, at around 18:00 UTC, a nationwide power outage affected Chile. The RIPE Atlas anchors (Internet measurement devices) in Chile give us a glimpse of how the Internet infrastructure coped with the power outage. Here's a breakdown of the effects we saw on the paths between the anchors.



Paths that encounter relatively short period of disconnect from around 18:15 to 18:45 UTC

Higher latencies along certain paths don't seem to correlate with outage

On 25 Feb At 18:00 UTC, some paths start to encounter high latency that was not resolved until 15:45 UTC the next day

The grey area across these paths indicates a period over which there is no latency data, which implies power loss

The rest of the paths saw neither latency increases, nor signal loss. This is an indication that part of the core Internet infrastructure in Chile was functional during the outage

Legend

- High latency increase (>100ms extra)
- No latency increase
- No data

Data source: atlas.ripe.net

Questions & Comments

gviviers@ripe.net

RIPE NCC
RIPE NETWORK COORDINATION CENTER

THANK YOU!