Middle Eastern Cable Cuts And Network Outages

Mark Dranse
RIPE NCC
markd@ripe.net

Research

- Carried out by RIPE NCC Science Group

Robert Kisteleki

Antony Antony

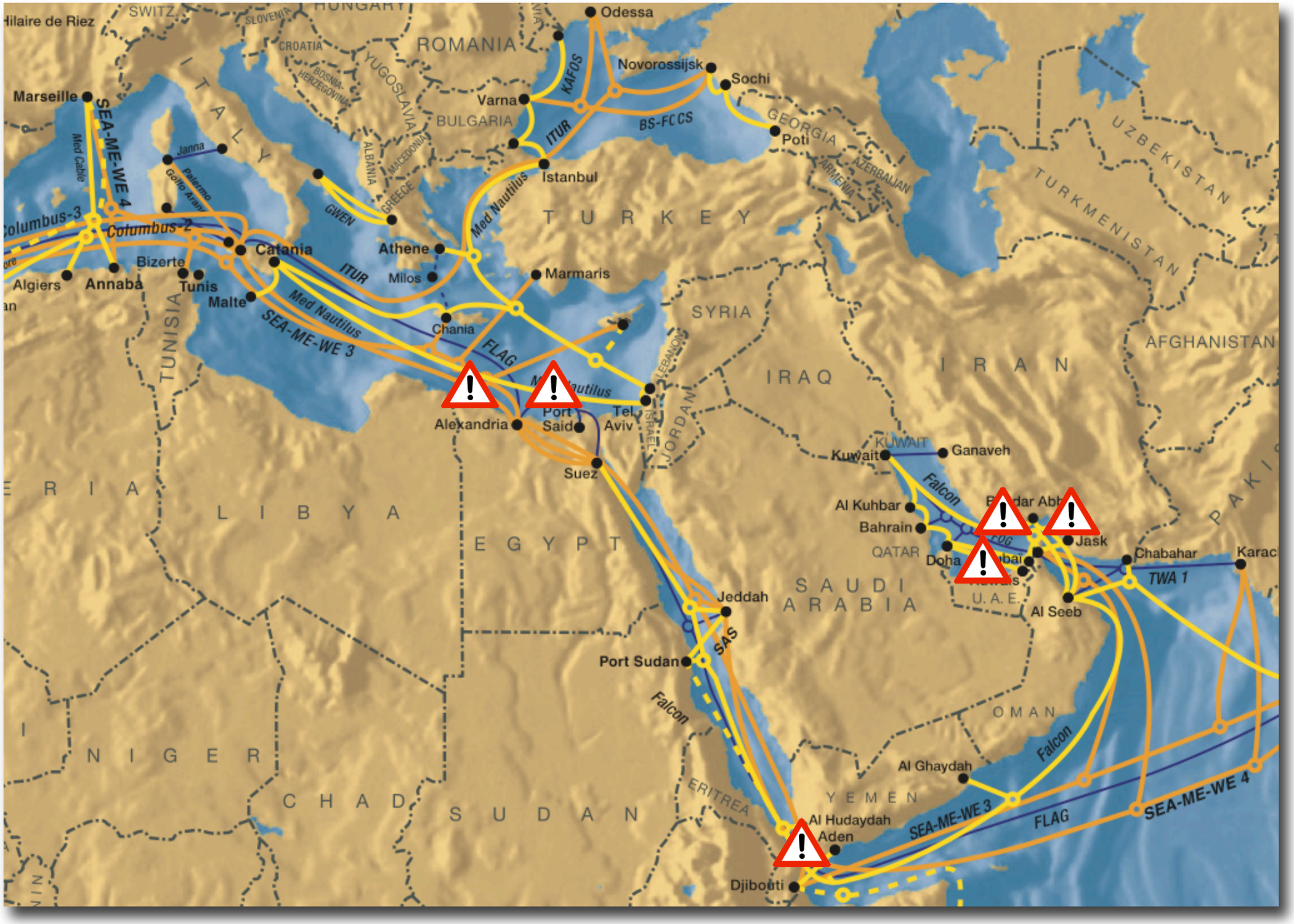
Tiziana Refice

Rene Wilhelm

http://ripe.net/projects/reports/2008cable-cut

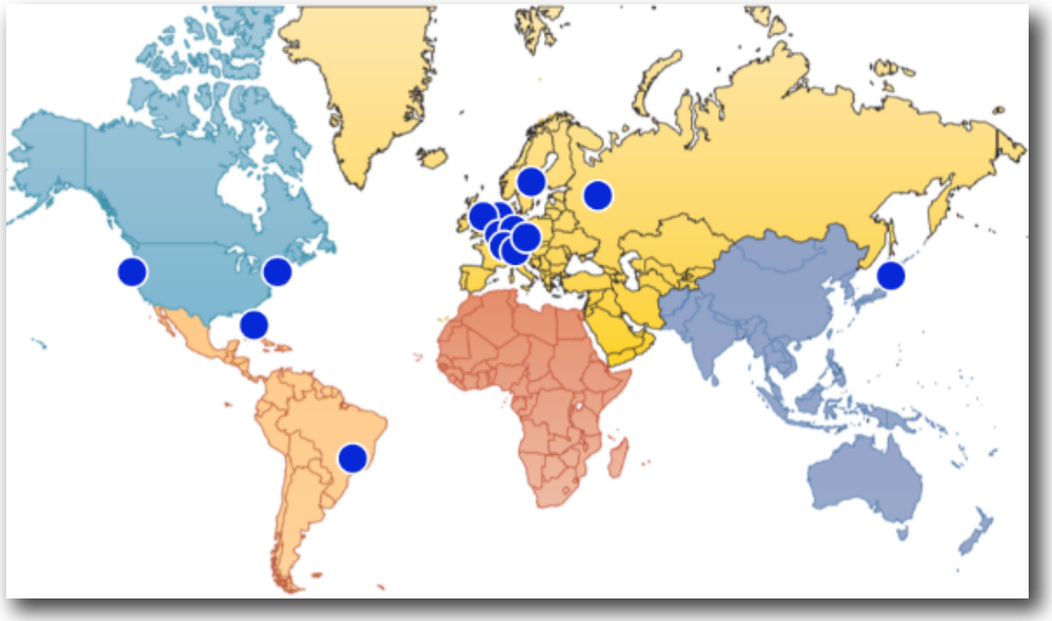
Submarine cables

Just three cables connect Europe with Egypt and beyond

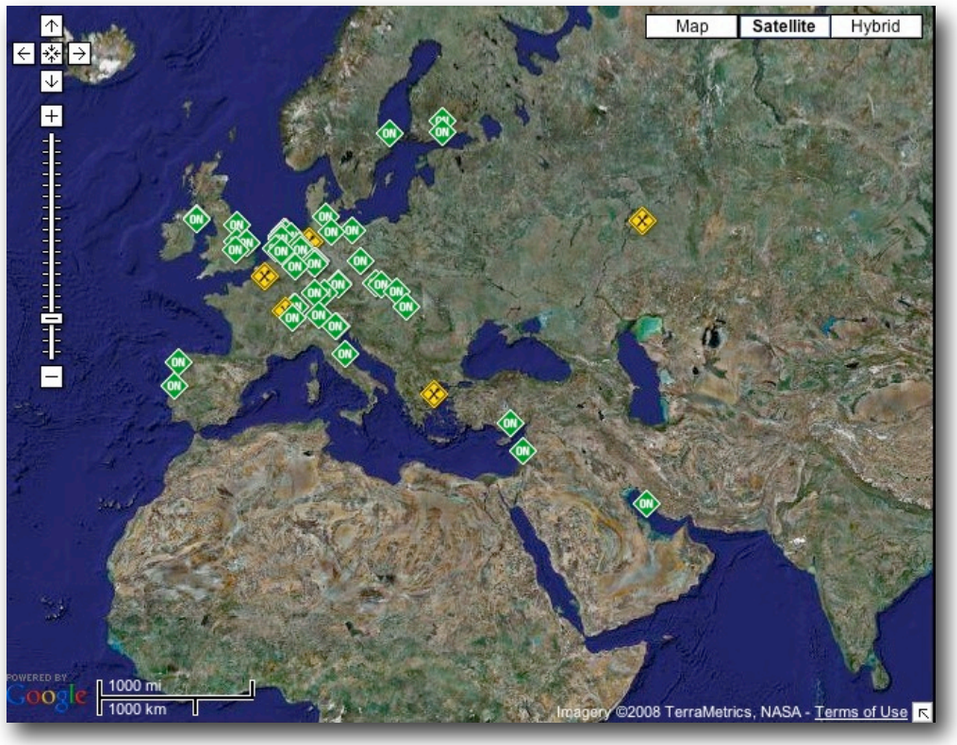


RIPE NCC Analysis

- Routing Information Service (RIS)
  - Collects BGP data
  - 600 peers
  - 16 Internet Exchange Points
  - http://www.ripe.net/ris

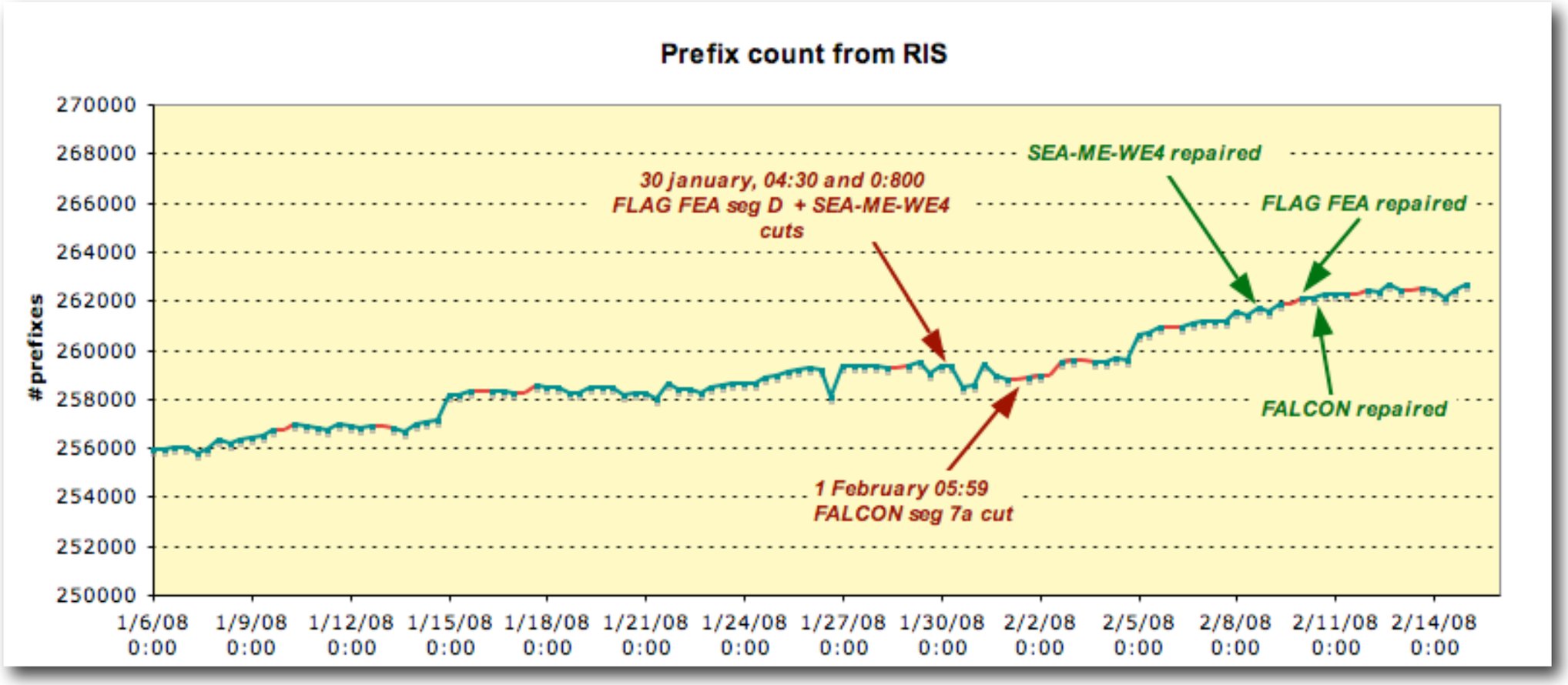


- Test Traffic Measurements (TTM)
  - Measures delay and loss
  - Stores traceroute data
  - Full mesh ~80 nodes
  - http://www.ripe.net/ttm



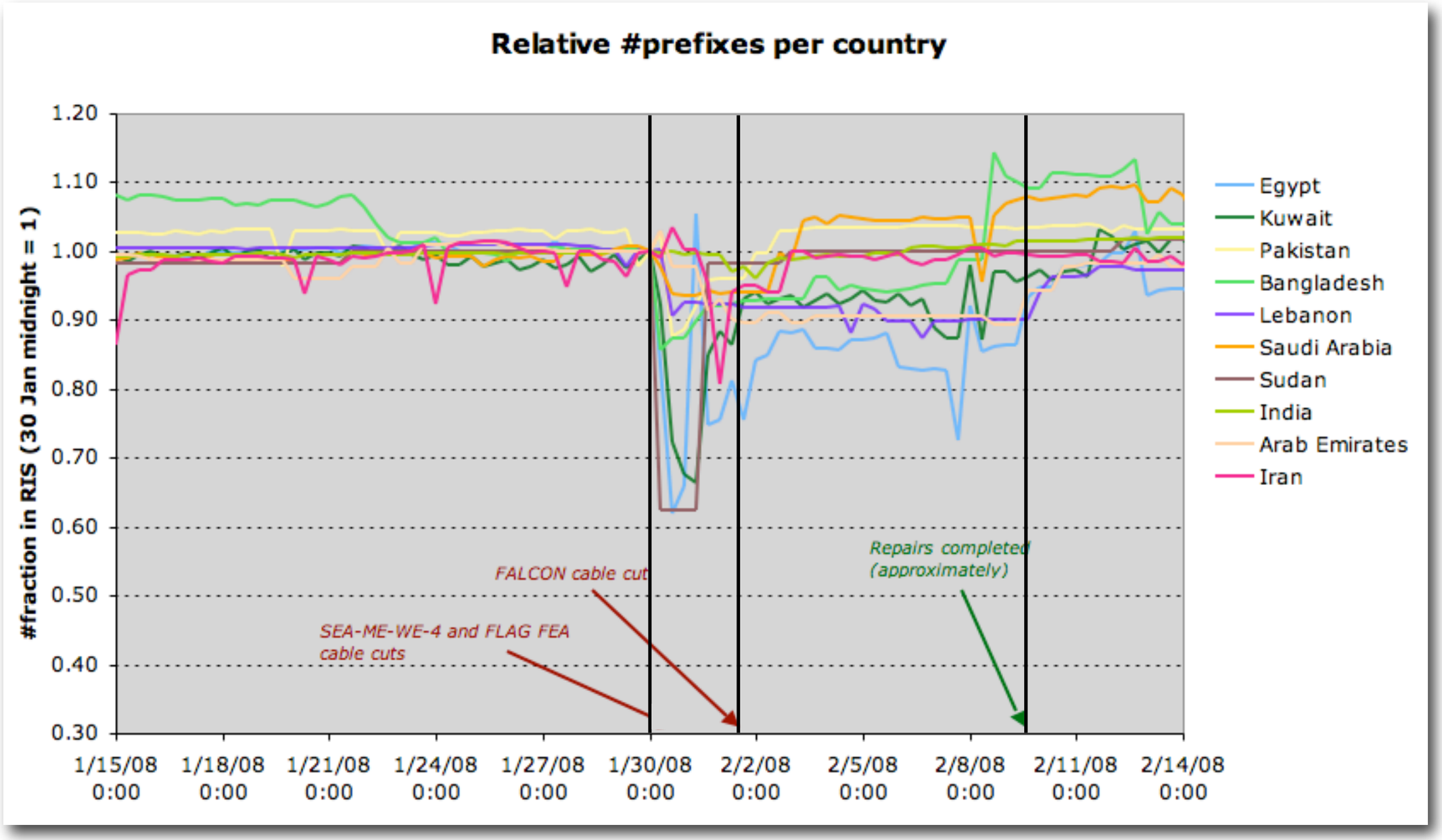
- DNSMON - http://dnsmon.ripe.net - Monitors 200 DNS servers

Prefix view - Global



- Total RIS prefixes indicate global reachability
- Cable cut/fix times show no significant changes
  - Globally, only a small percentage of ASs affected

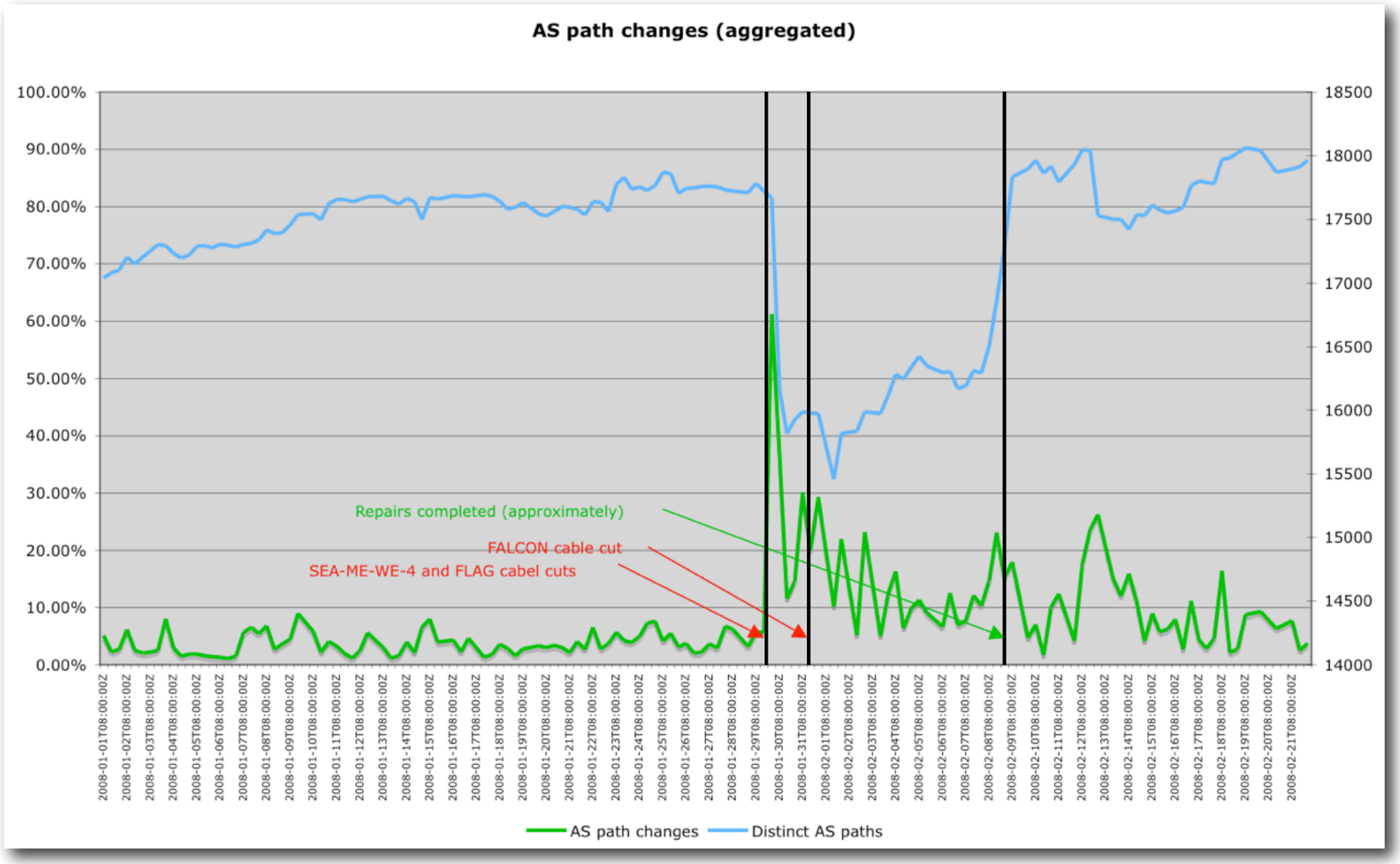
Prefix view - Local country view



- Egypt, Sudan and Kuwait see up to 40% visibility drop

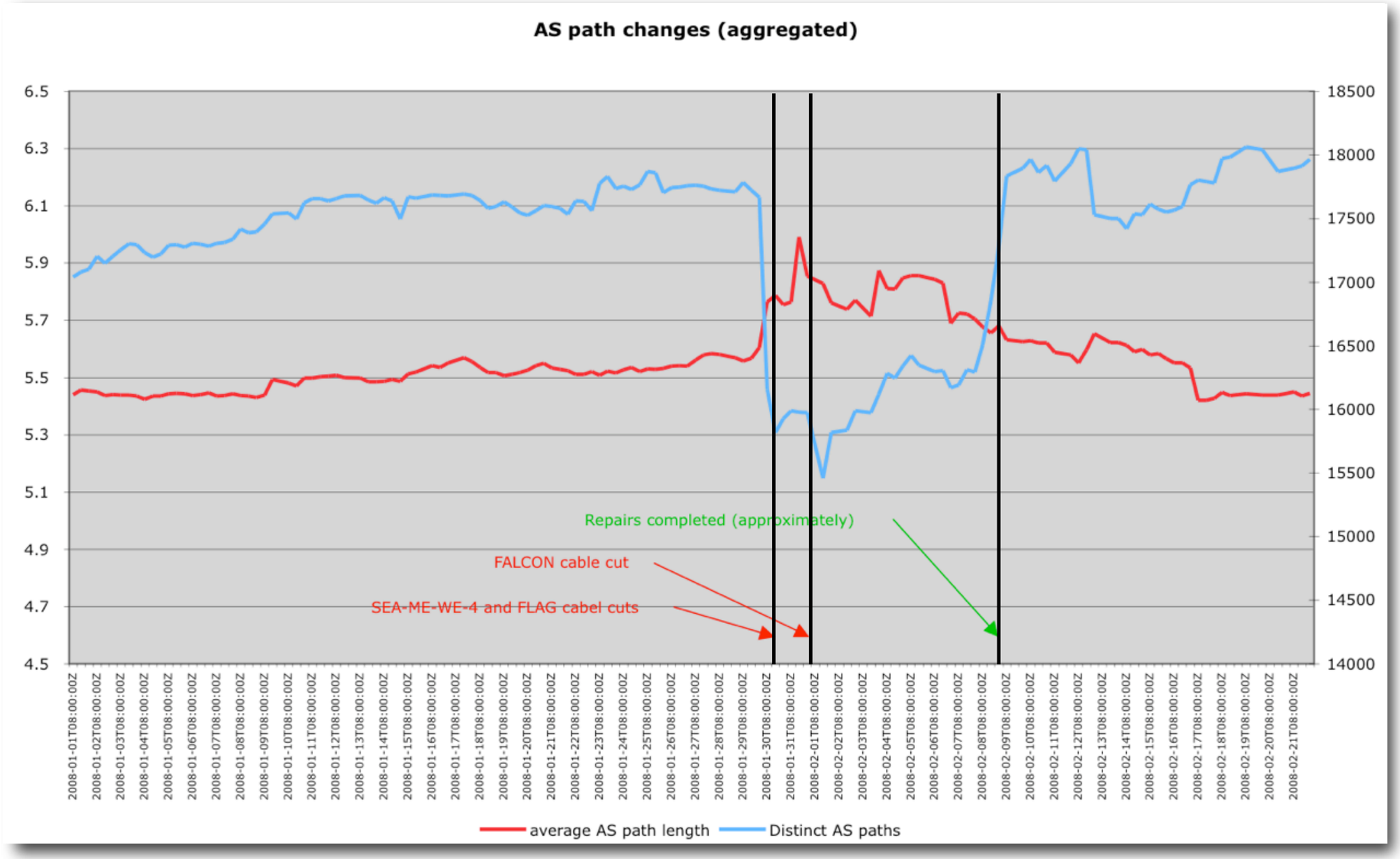
AS path changes

- Local networks disappear from routing tables
  - Distinct AS paths drop 14% from 18k to 15.5k



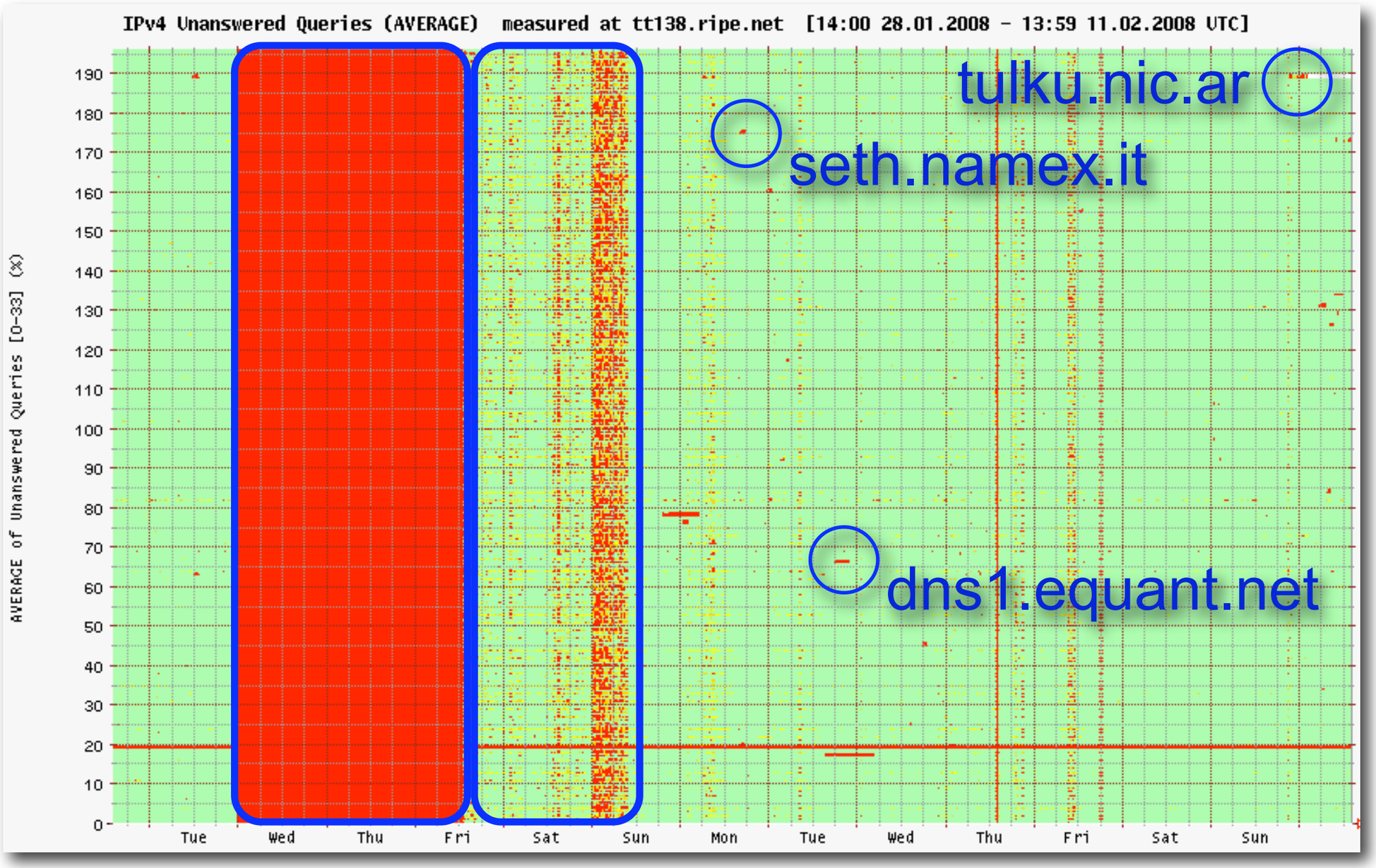
AS path changes

- Average AS path length changes
  - Increases by 9% (~0.5)



1. DNSMON Observations

Observations from DNSMON

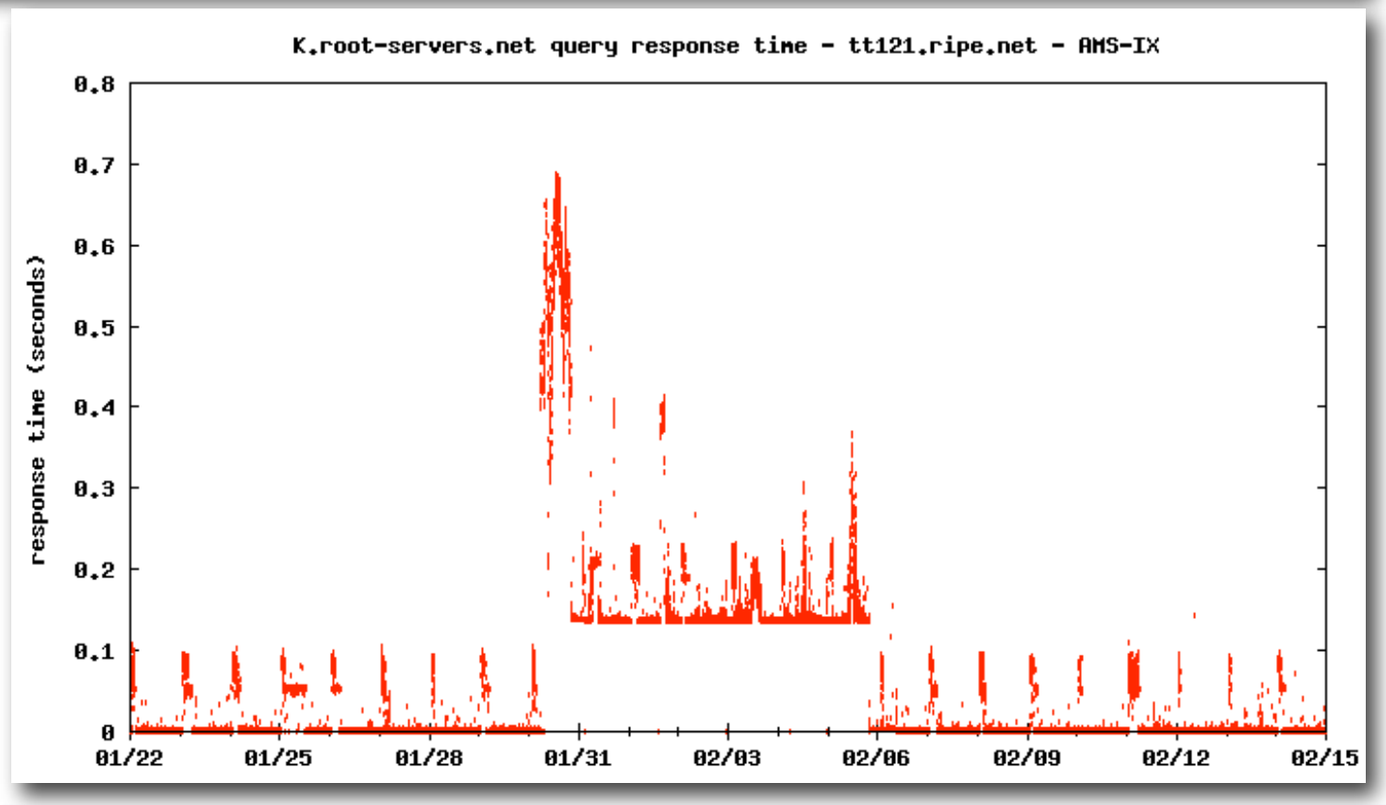


- Individual DNS server outages quite normal
- ALL queries dropped indicates testbox issue

DNSMON - K-root anycasting

- K-Root local node instances: Qtel (Doha) and EMIX (UAE)
  - Local nodes, routes should not be propagated
- DNSMON stores instance data (id.server)

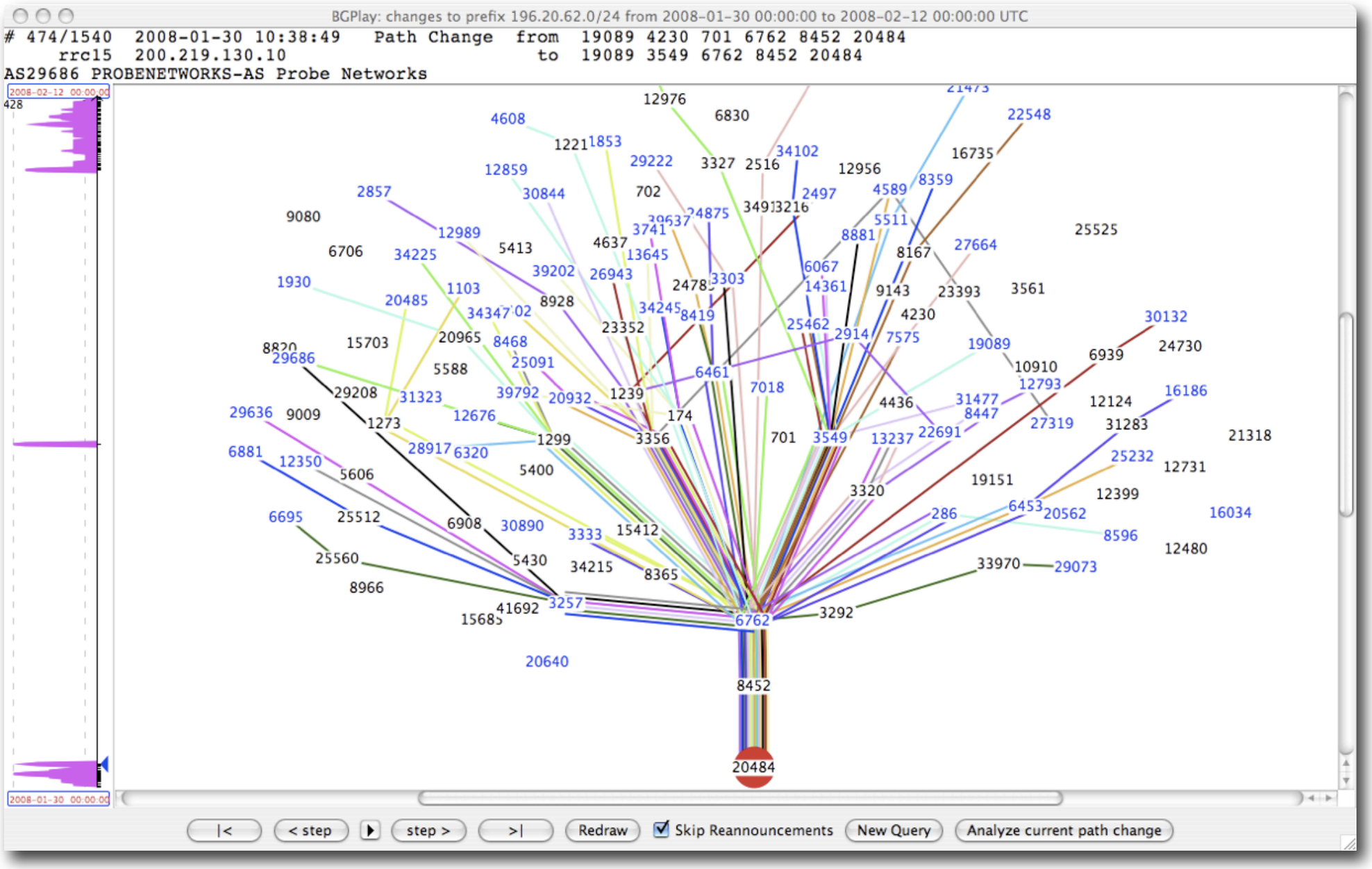
DNSMON



- AMS-IX probe chose EMIX (UAE) K node for DNS
- Proves EMIX was visible
- Slower response times suggest congested backup links
- Caused by unintentional leak - preferred due to prepending

2. Unreachable Prefixes

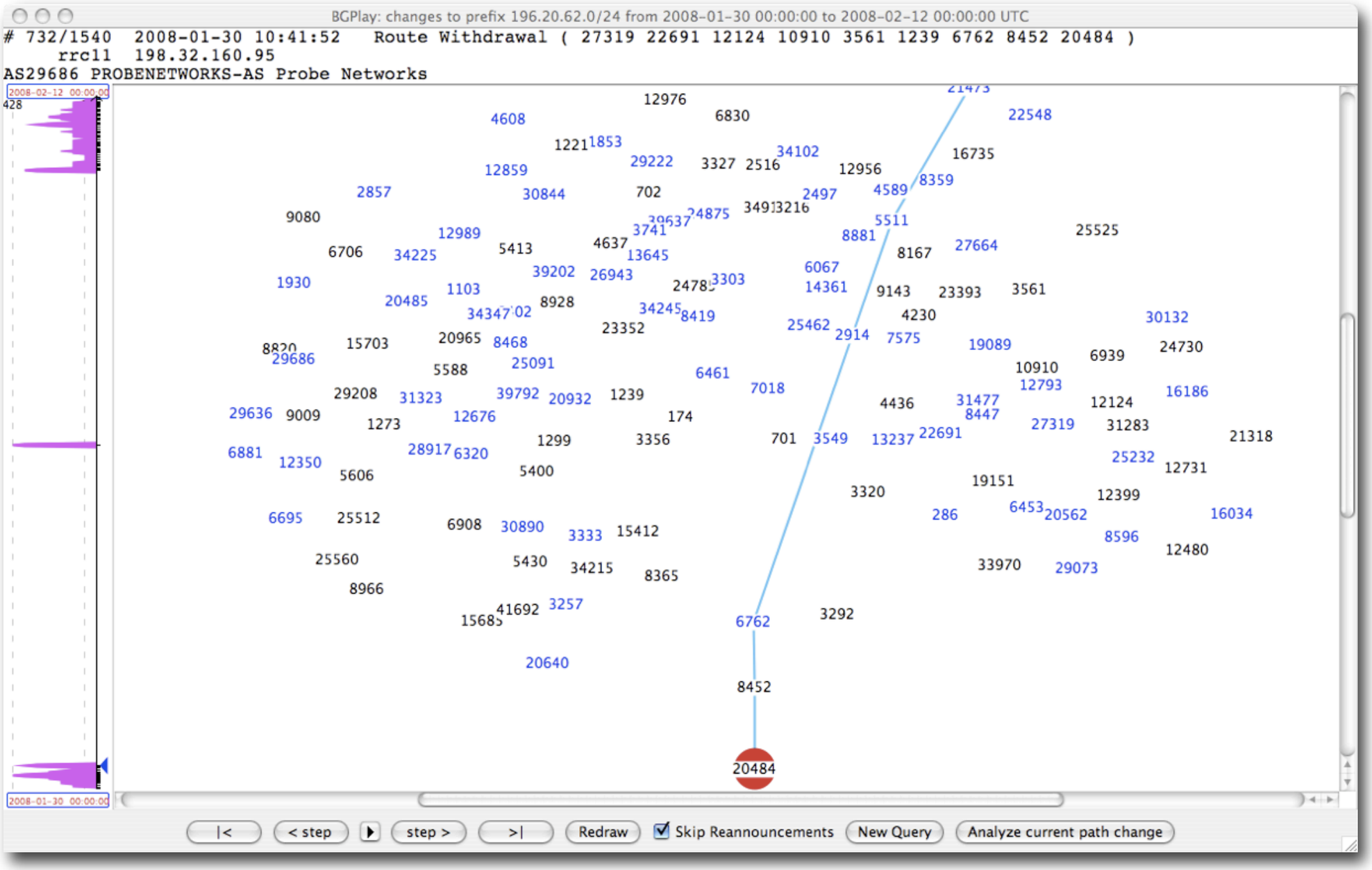
Unreachable prefixes



30/1 @ 10:38 >

- Some hours after the cut, this /24 in Egypt is still reachable

Unreachable prefixes



30/1 @ 10:41 >
30/1 @ 10:38 >

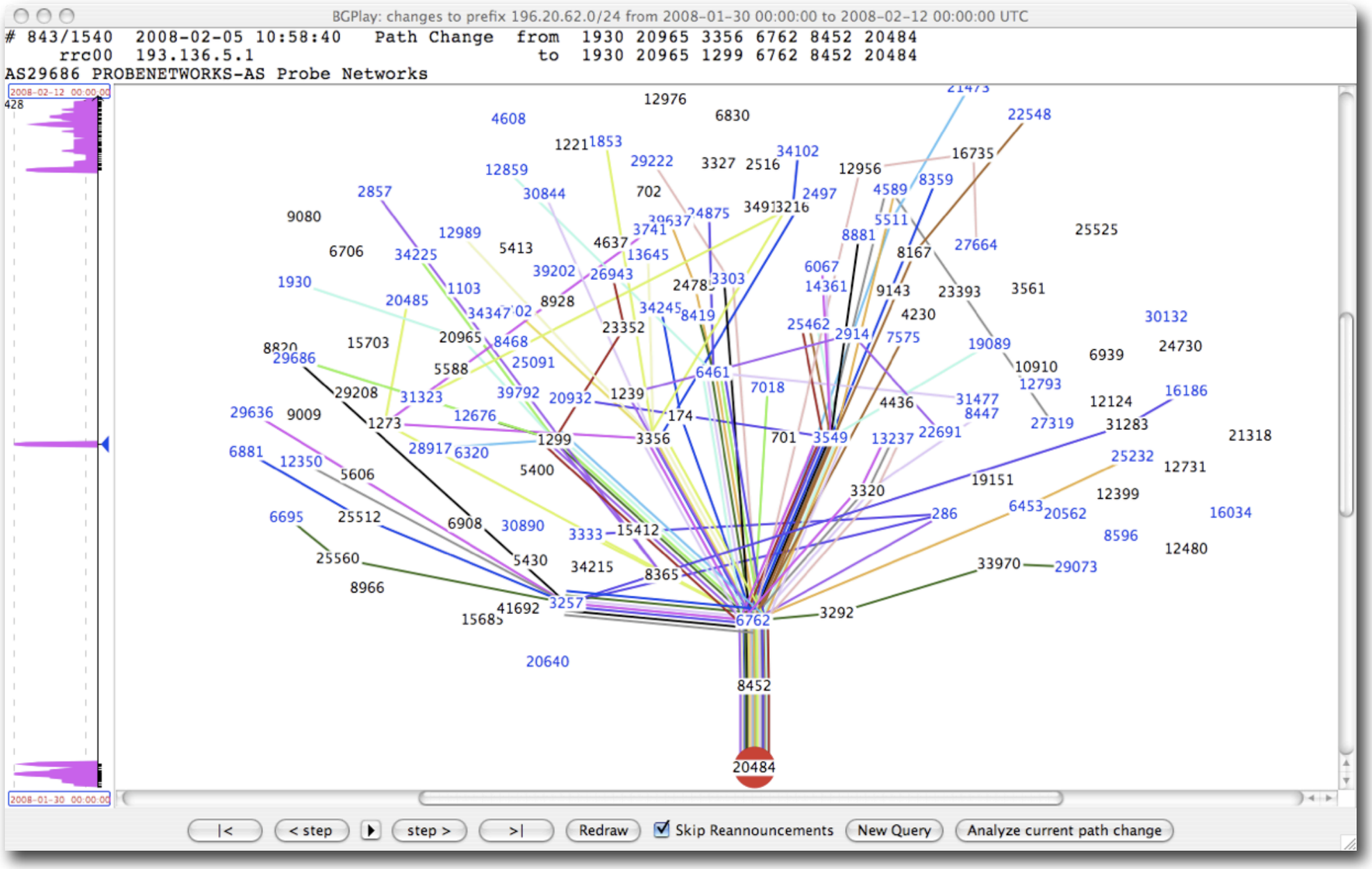
- A few minutes later, the prefix disappears

Unreachable prefixes

5/2 @ 10:58 >

30/1 @ 10:41 >

30/1 @ 10:38 >



- The prefix reappears momentarily
  - Manual configuration changes?

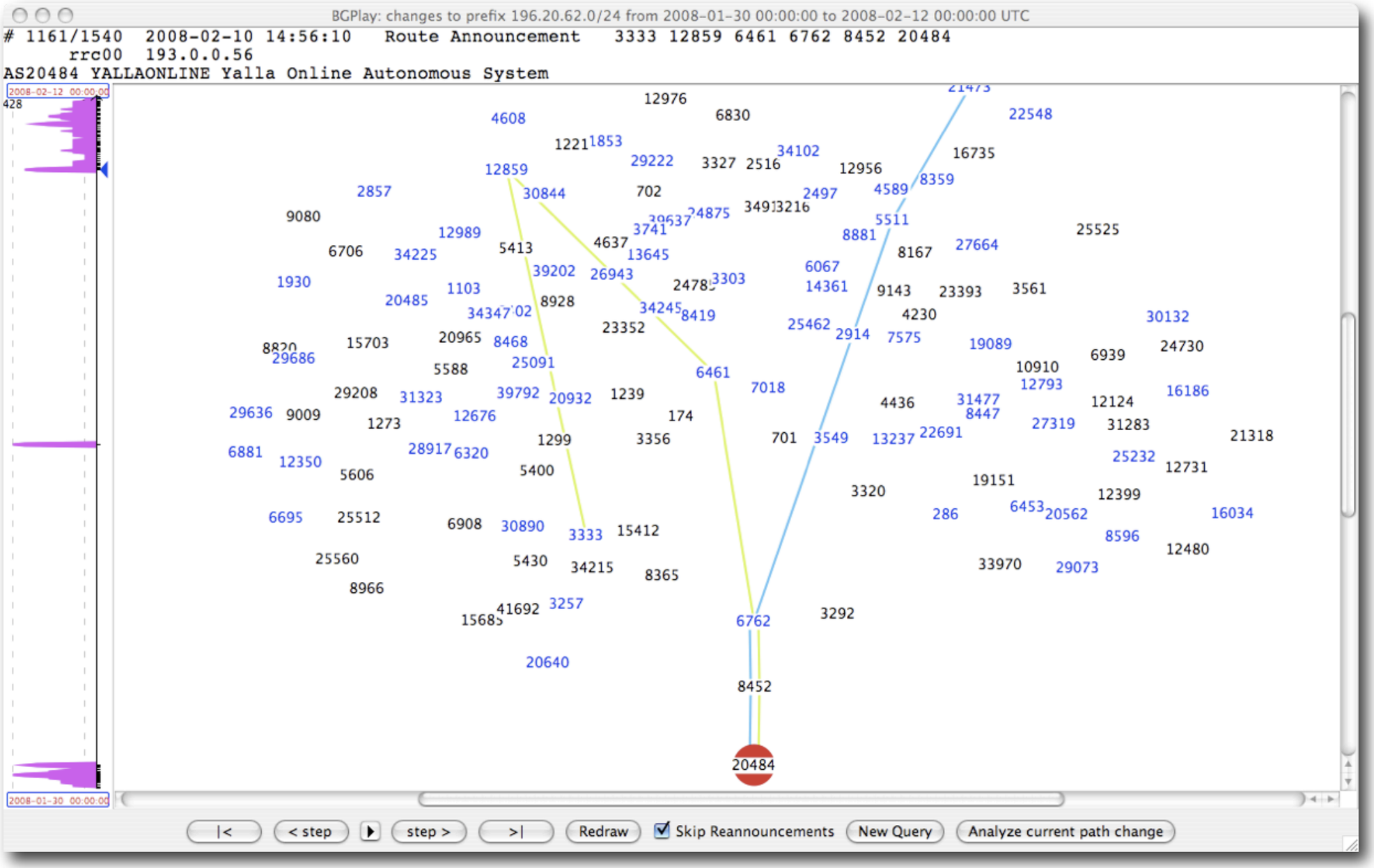
Unreachable prefixes

10/2 @ 14:56 >

5/2 @ 10:58 >

30/1 @ 10:41 >

30/1 @ 10:38 >



- First signs of full recovery
  - route announcements begin to arrive at RIS peers

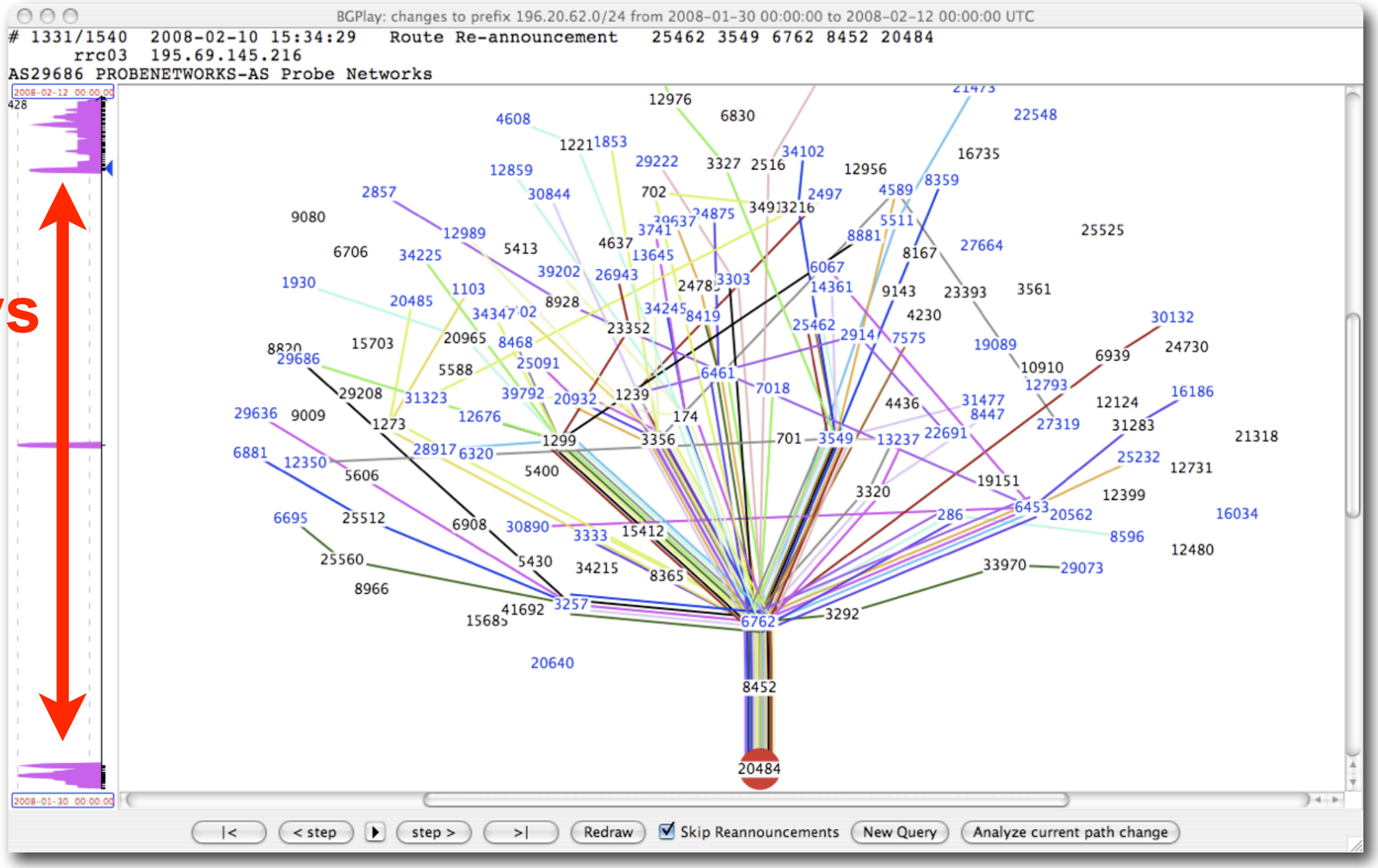
Unreachable prefixes

10/2 @ 15:34 >
10/2 @ 14:56 >

11 days

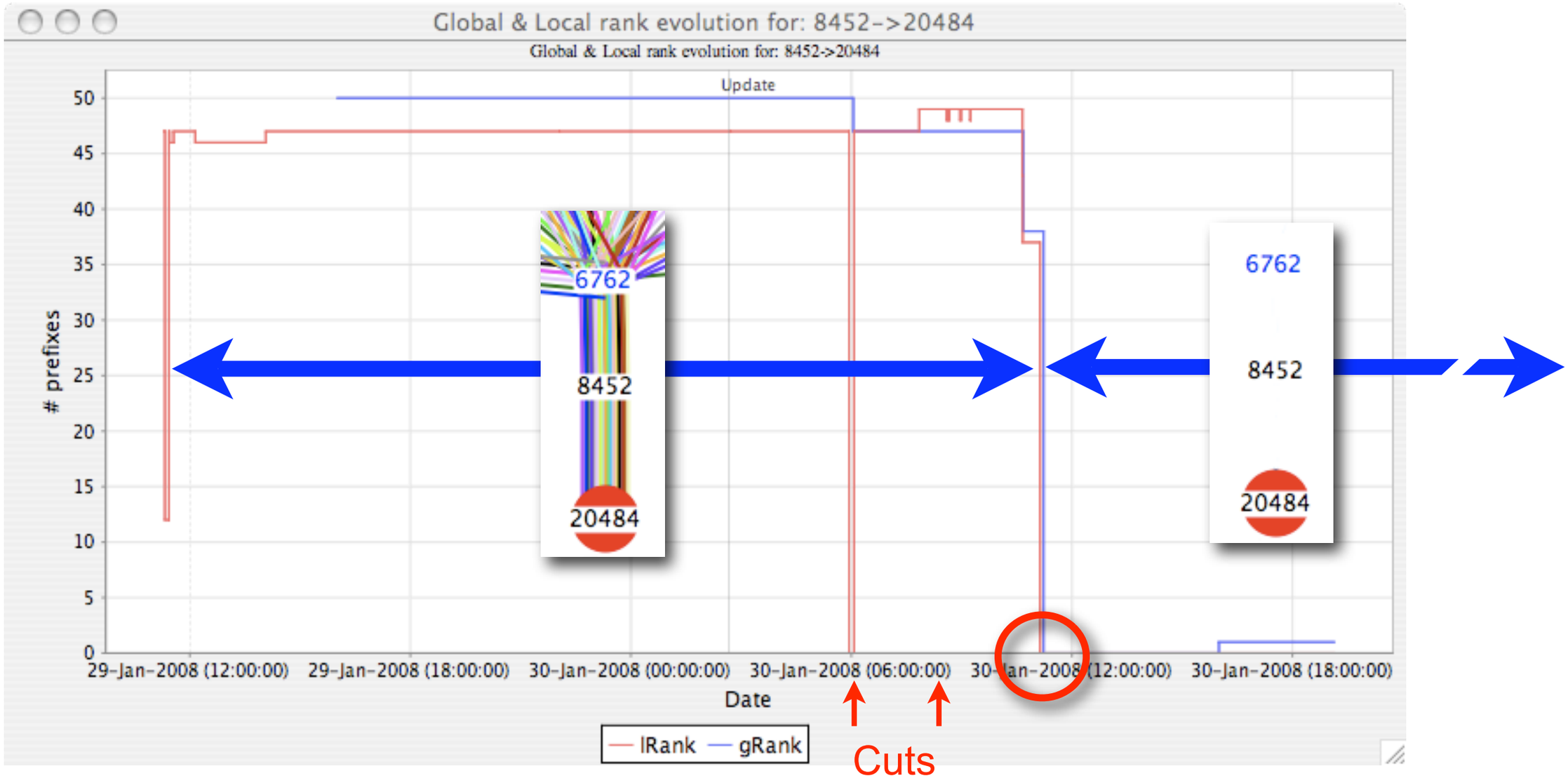
5/2 @ 10:58 >

30/1 @ 10:41 >
30/1 @ 10:38 >



- Prefix is now visible to all RIS peers again
  - But was gone for 11 days

Unreachable prefixes



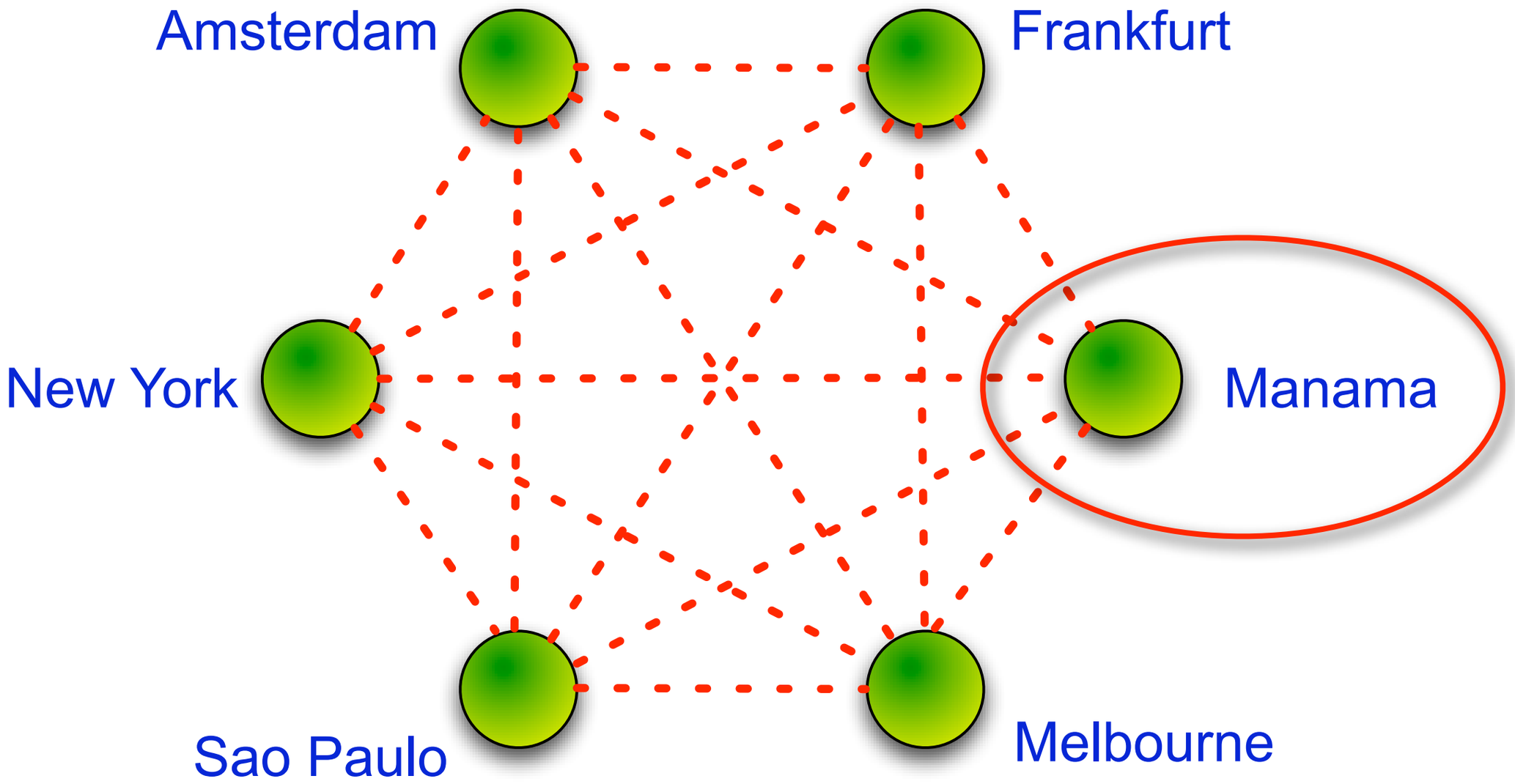
- Conclusion:
  - All 50 prefixes changed path, or lost connectivity
  - Change not aligned with cuts - probably manual intervention

3. Route visible, no traffic

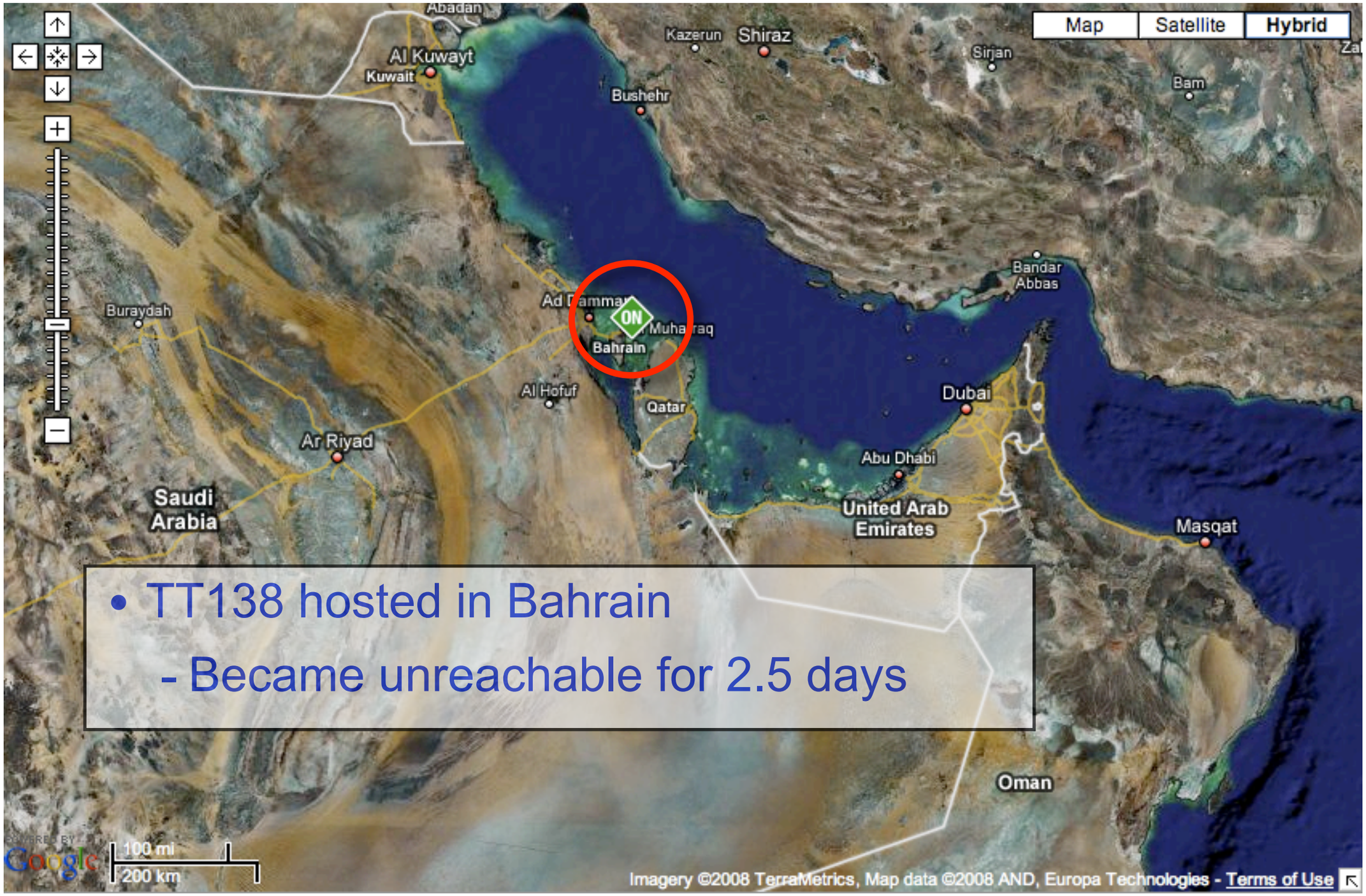
TTM

Bidirectional measurements of:

- Delay
- Loss
- Jitter
- Traceroute



TTM



- TT138 hosted in Bahrain
  - Became unreachable for 2.5 days

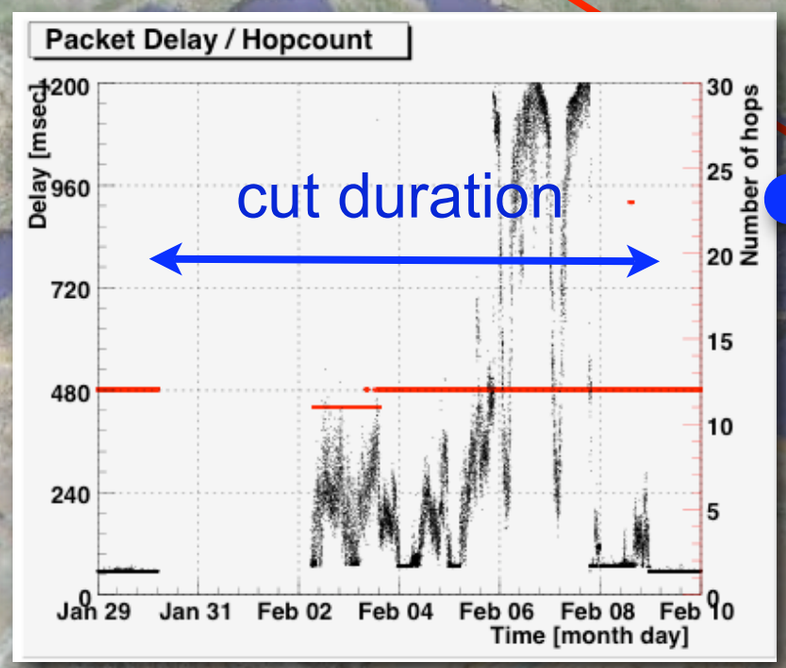
BGPlay: changes to prefix 196.20.62.0/24 from 2008-01-30 00:00:00 to 2008-02-12 00:00:00 UTC

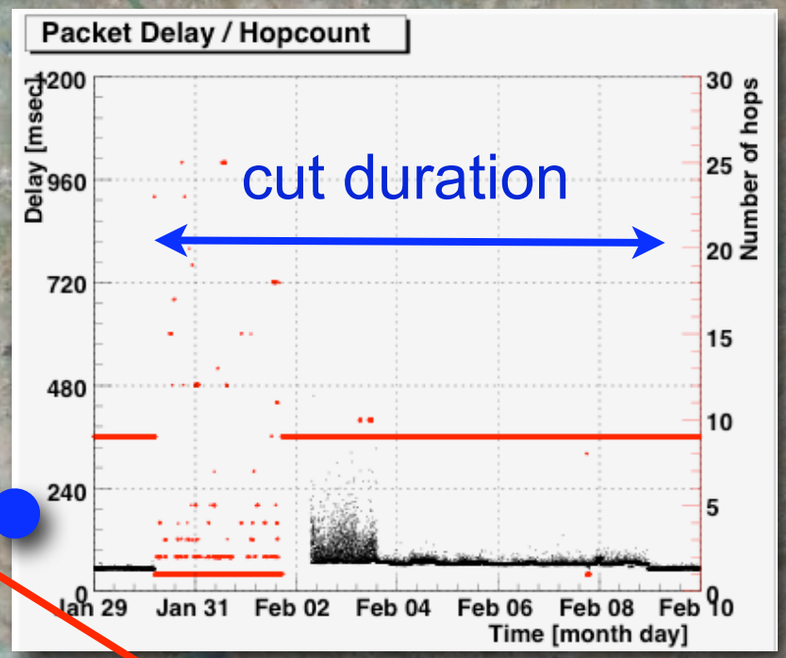
732/1540 2008-01-30 10:41:52 Route Withdrawal (27319 22691 12124 10910 3561 1239 6762 8452 20484)
rrc11 198.32.160.95
AS29686 PROBENETWORKS-AS Probe Networks

|< | < step | step > | >| | Redraw | Skip Reannouncements | New Query | Analyze current path change

TT01
NCC
Amsterdam

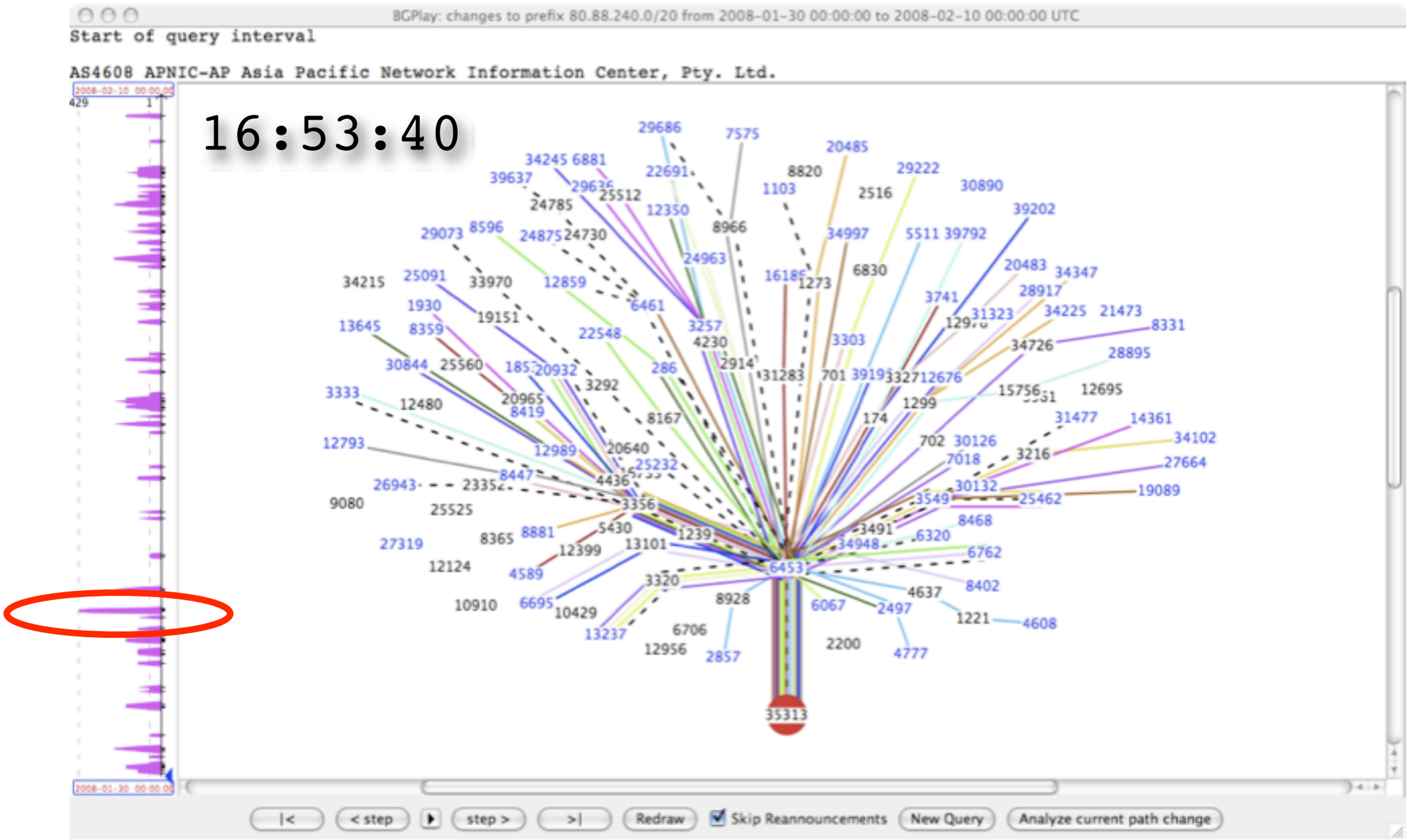
TT138
Manama
Bahrain





Google
500 mi
500 km
Imagery ©2008 TerraMetrics, NASA - Terms of Use

Visibility - 1 Feb 2008



- Prefix was constantly announced from 30 Jan to 10 Feb

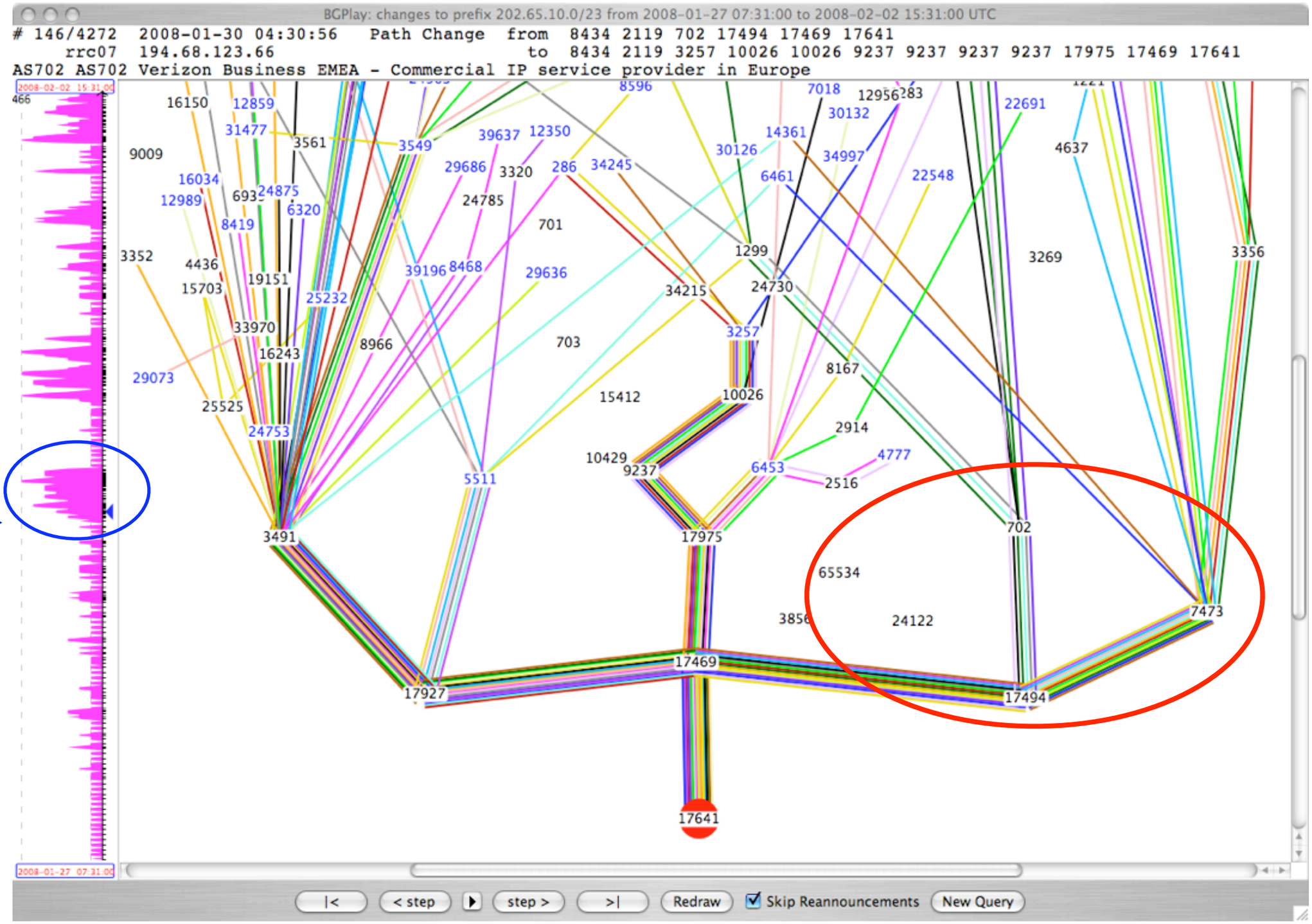
Conclusion

- Traceroutes reached Teleglobe
  - Prefix probably originated from their router in London
    - irrespective of link to Bahrain
  - Cable cut didn't trigger a withdrawal
  - Presence of a route does not imply reachability

4. AS path re-routes

BGP Rerouting - Bangladesh

- A /23 originated from Bangladesh



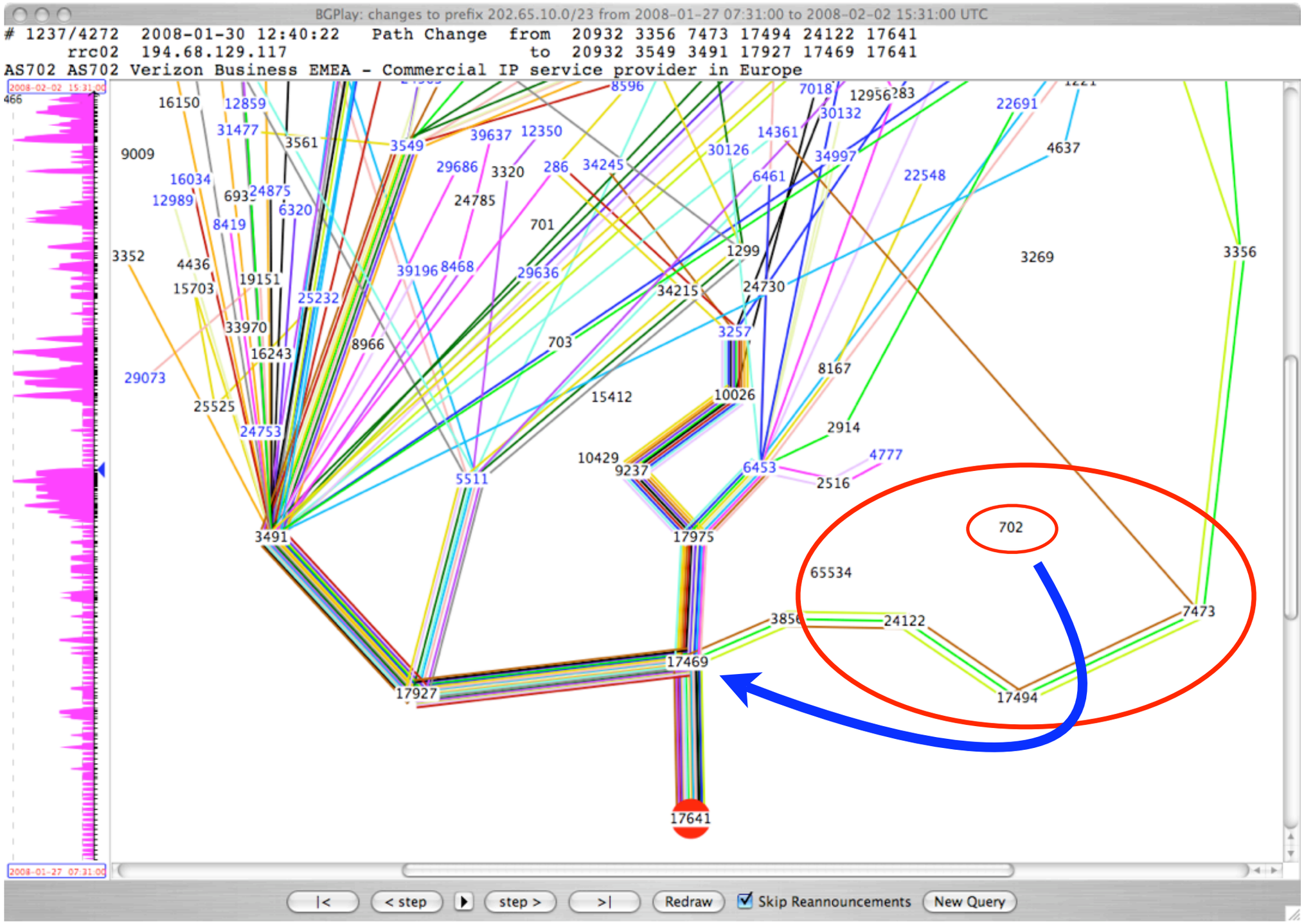
30/1 @ 04:30 >

BGP Rerouting - Bangladesh

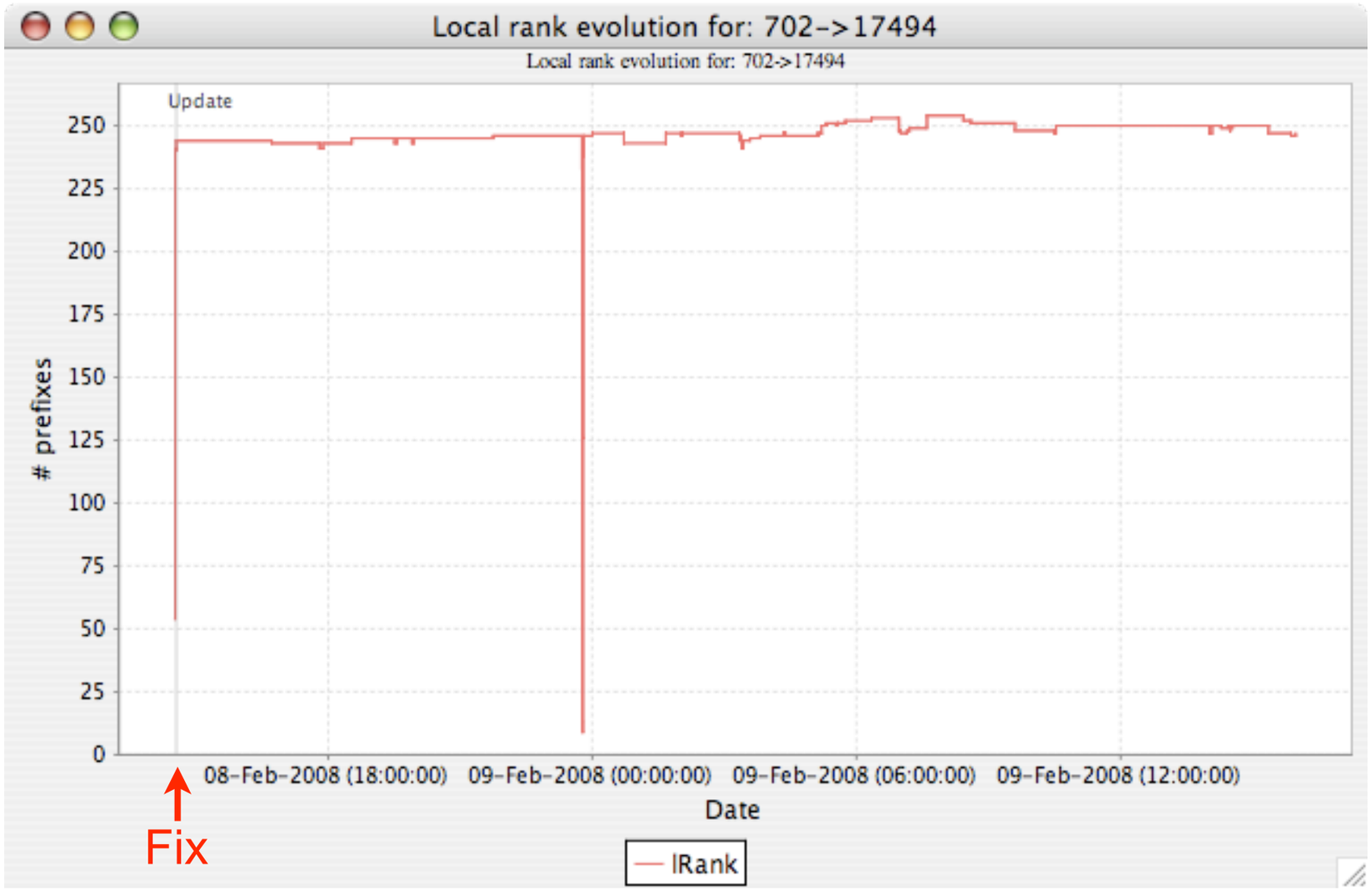
- Most routes now going via Singapore and Hong Kong

30/1 @ 12:40 >

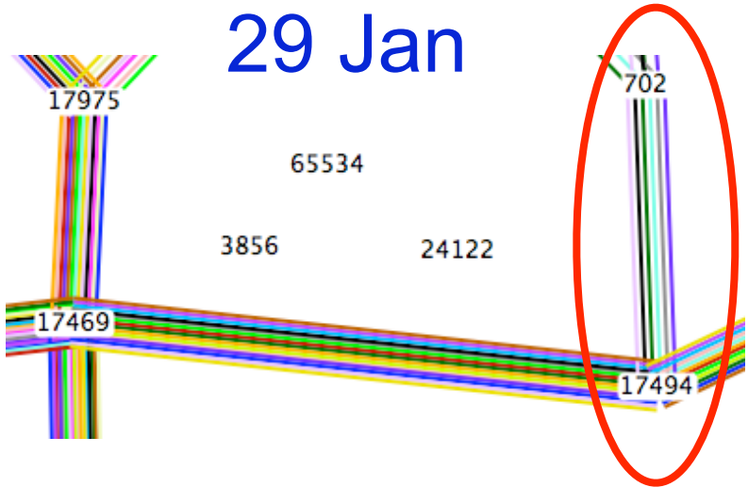
30/1 @ 04:30 >



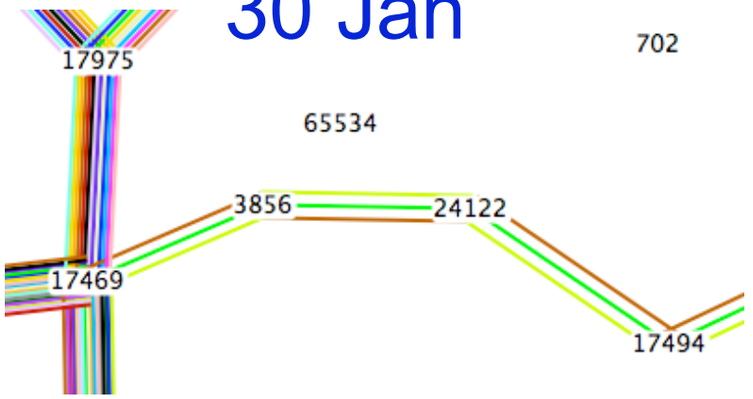
BGP Rerouting - Bangladesh



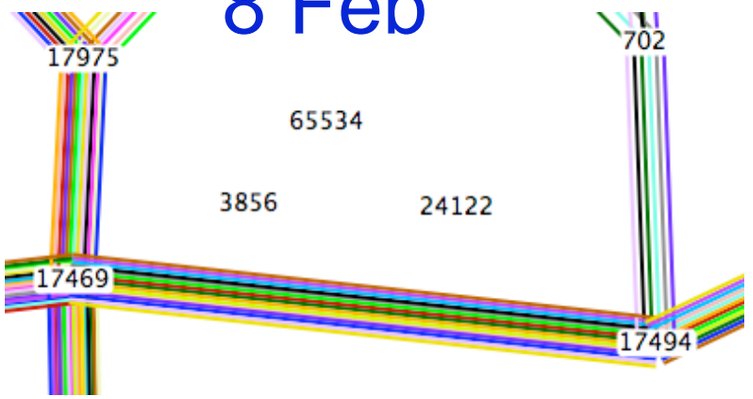
29 Jan



30 Jan



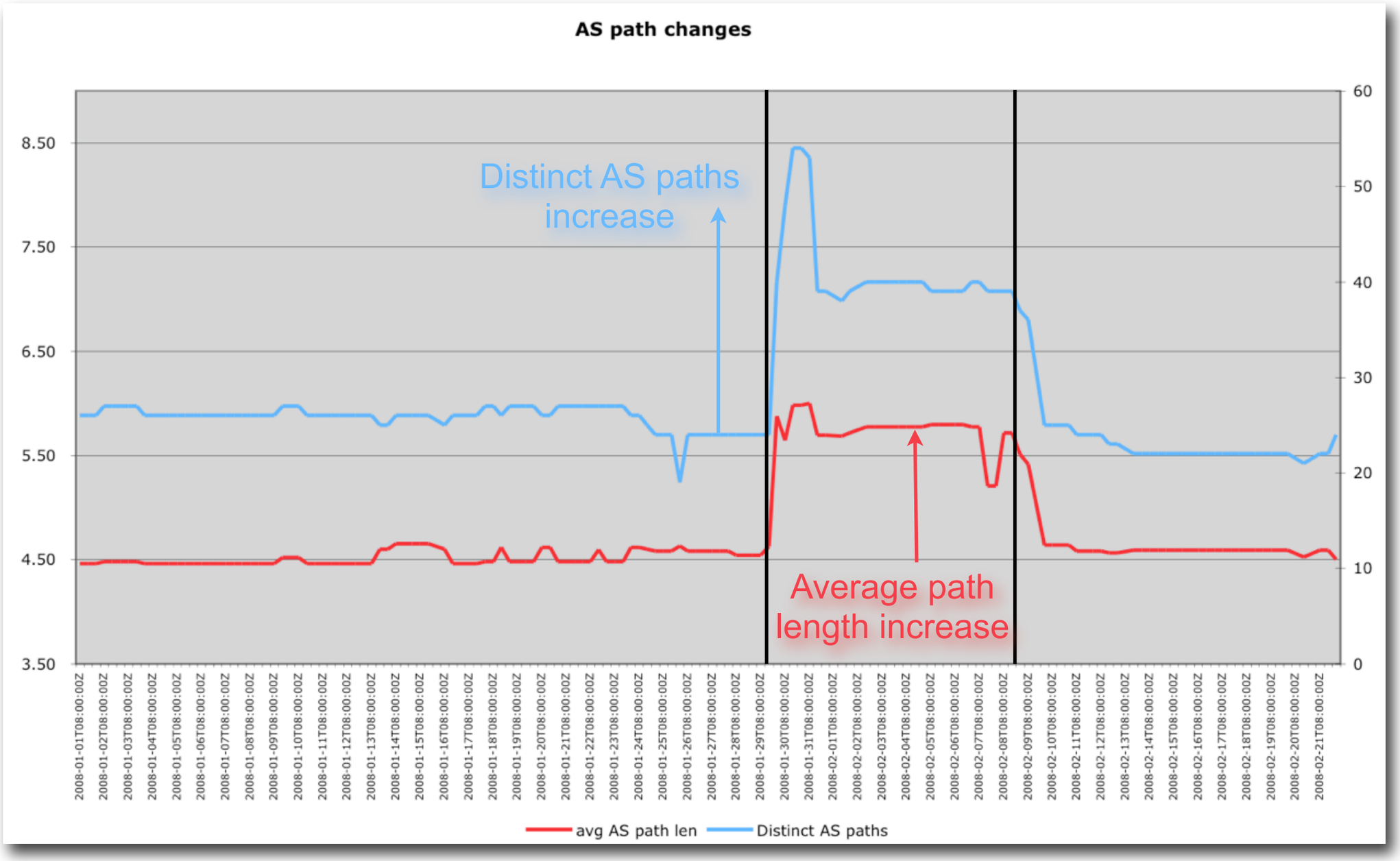
8 Feb



- Path outage at 0430, prior to FEA cut
- We assume this link uses SEA-ME-WE4

5. BGP Churn

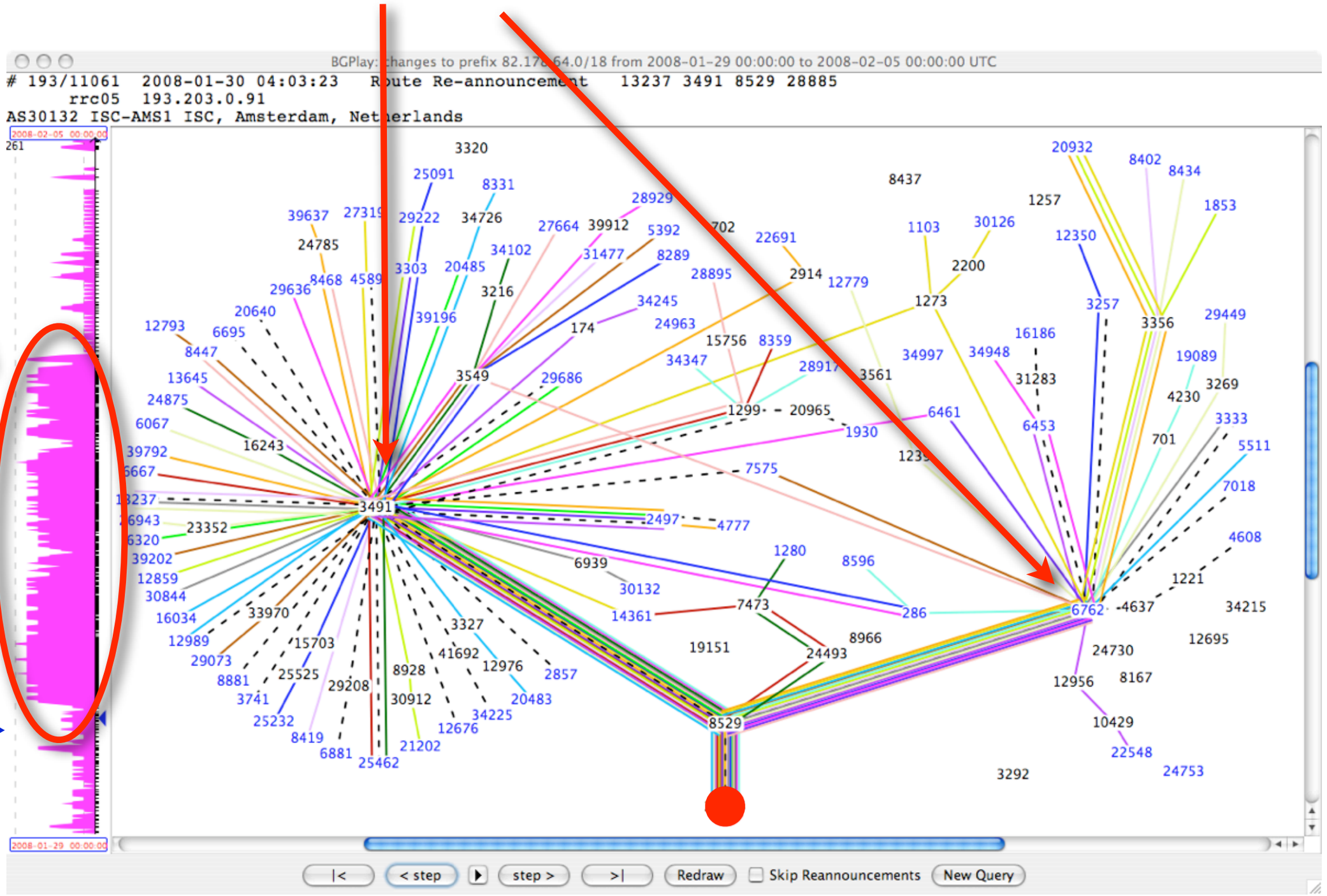
BGP churn



- Prefixes usually announced in batches
- Multiple different announcements seen per prefix set

BGP churn

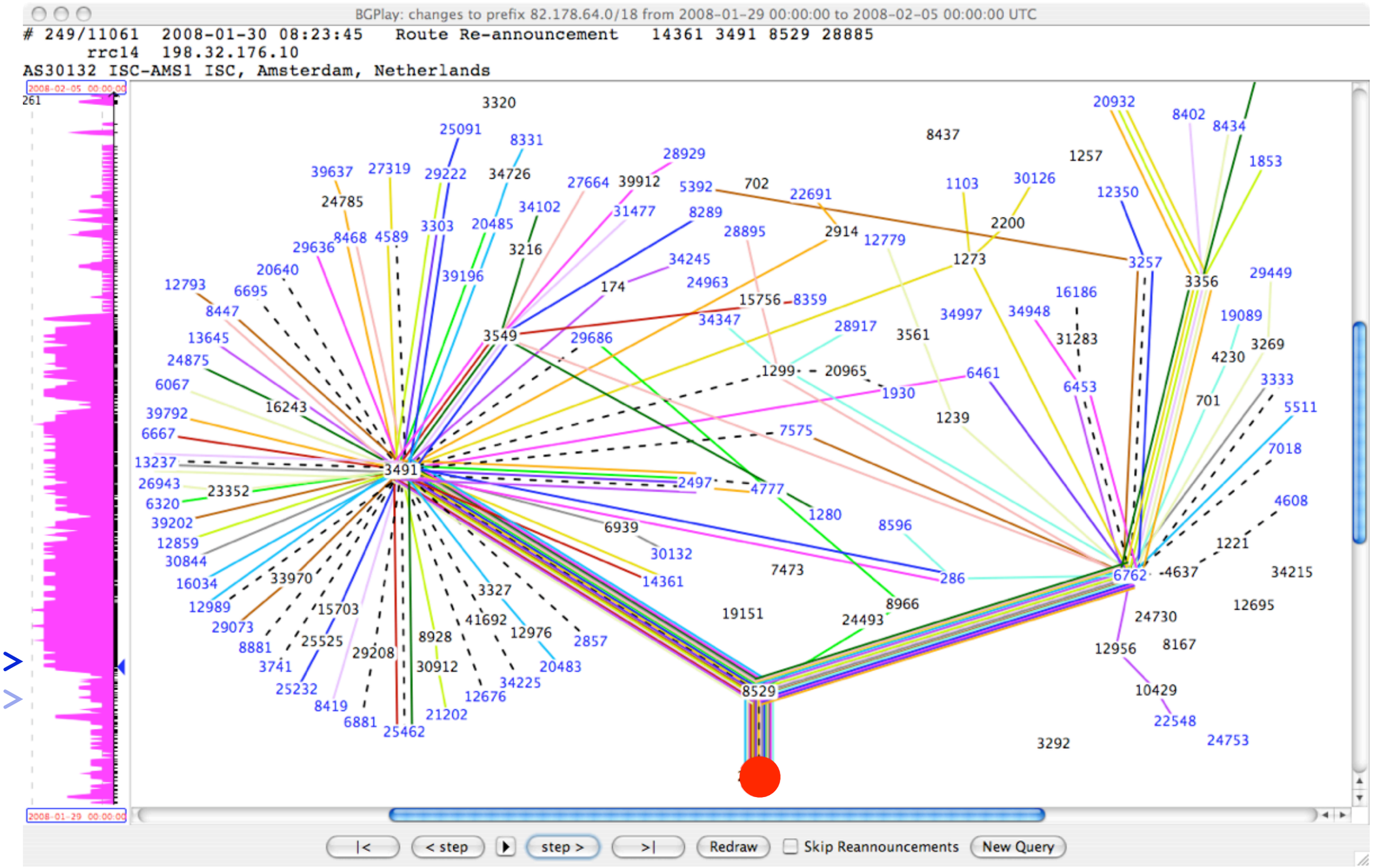
- Before outages: Two primary transits
- Many updates



30/1 @ 04:03 >

BGP churn

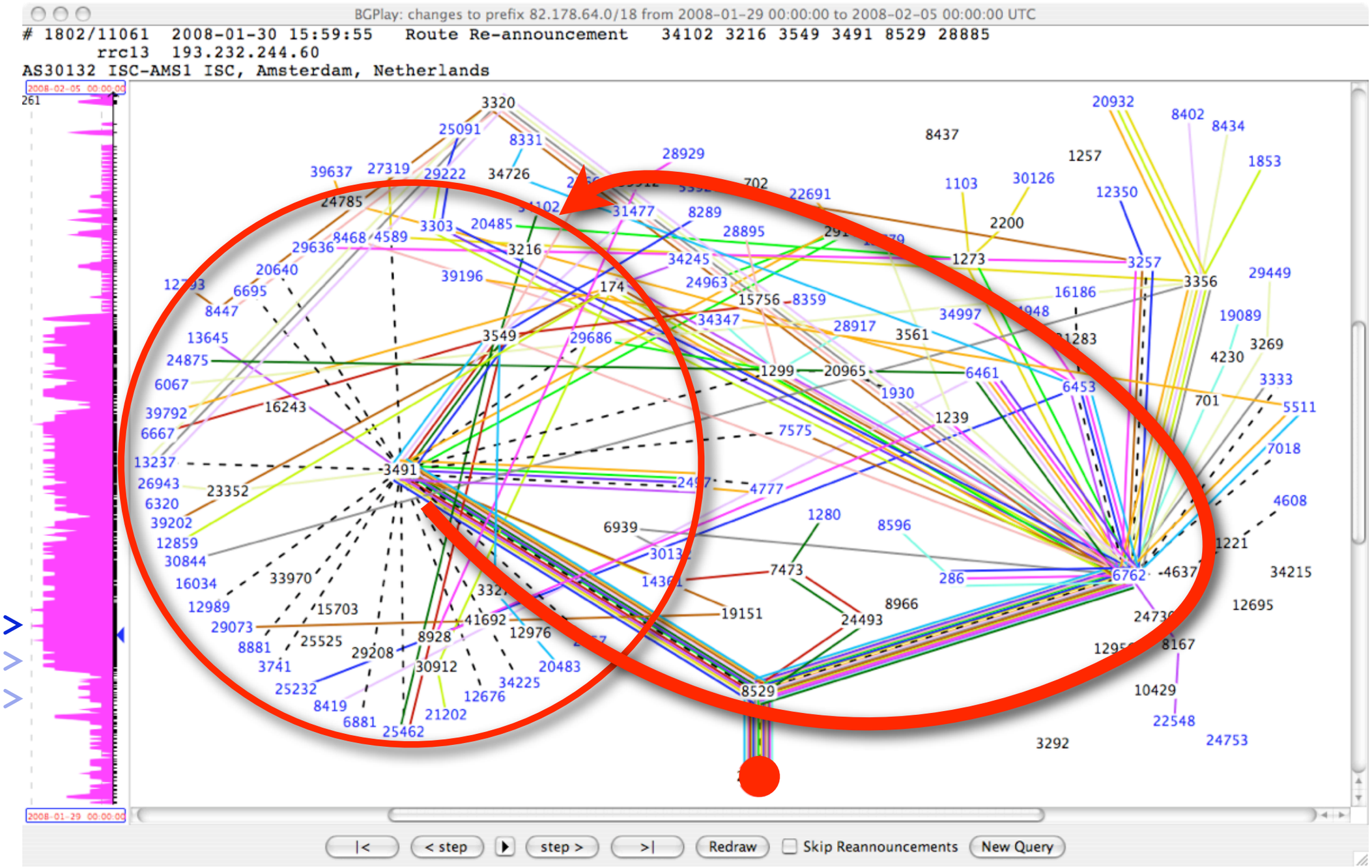
- First signs of rerouting
- Total of 10k messages recorded in 90 hours



30/1 @ 08:23 >
30/1 @ 04:03 >

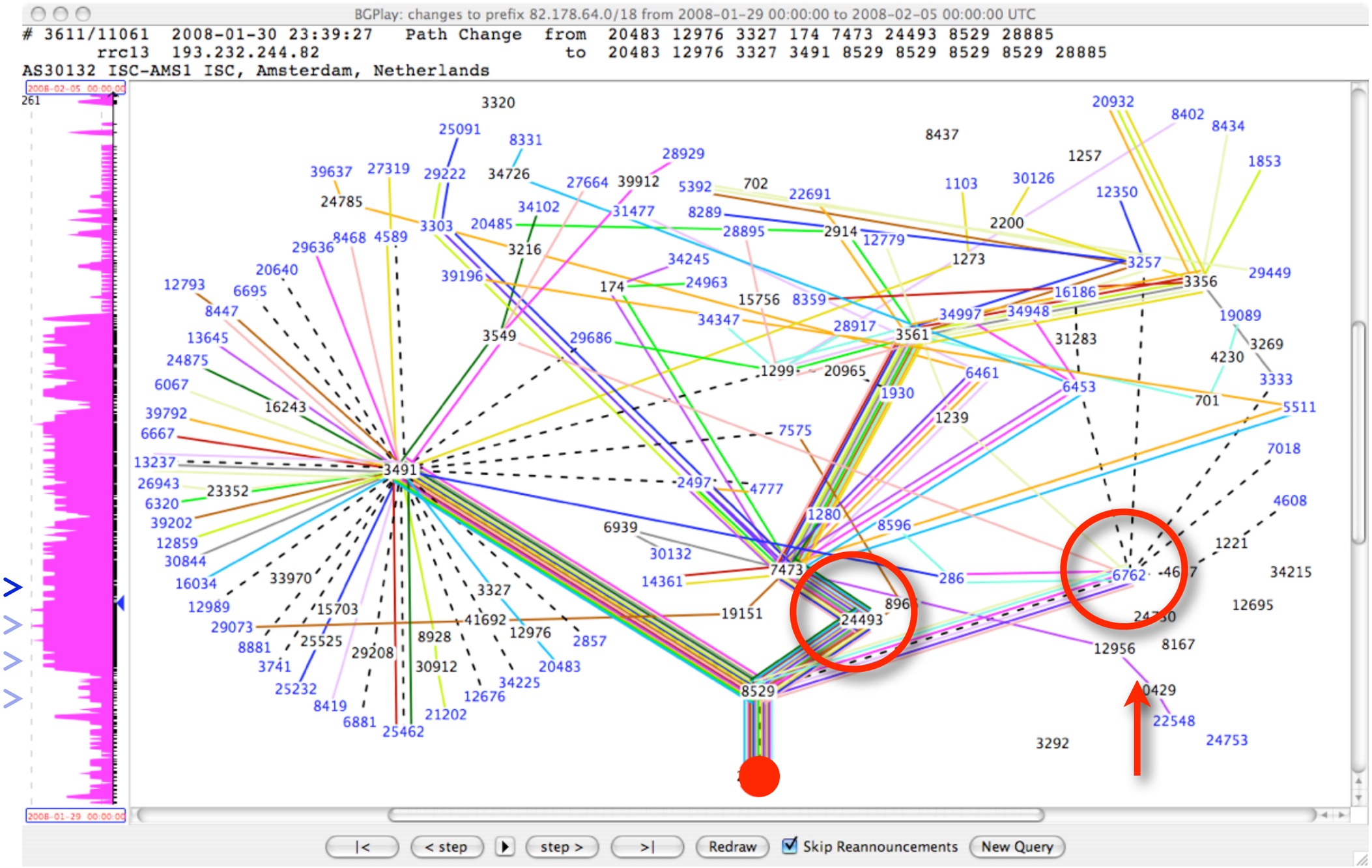
BGP churn

- Many peers switched from one transit to the other
- AS paths become longer - average path length increases



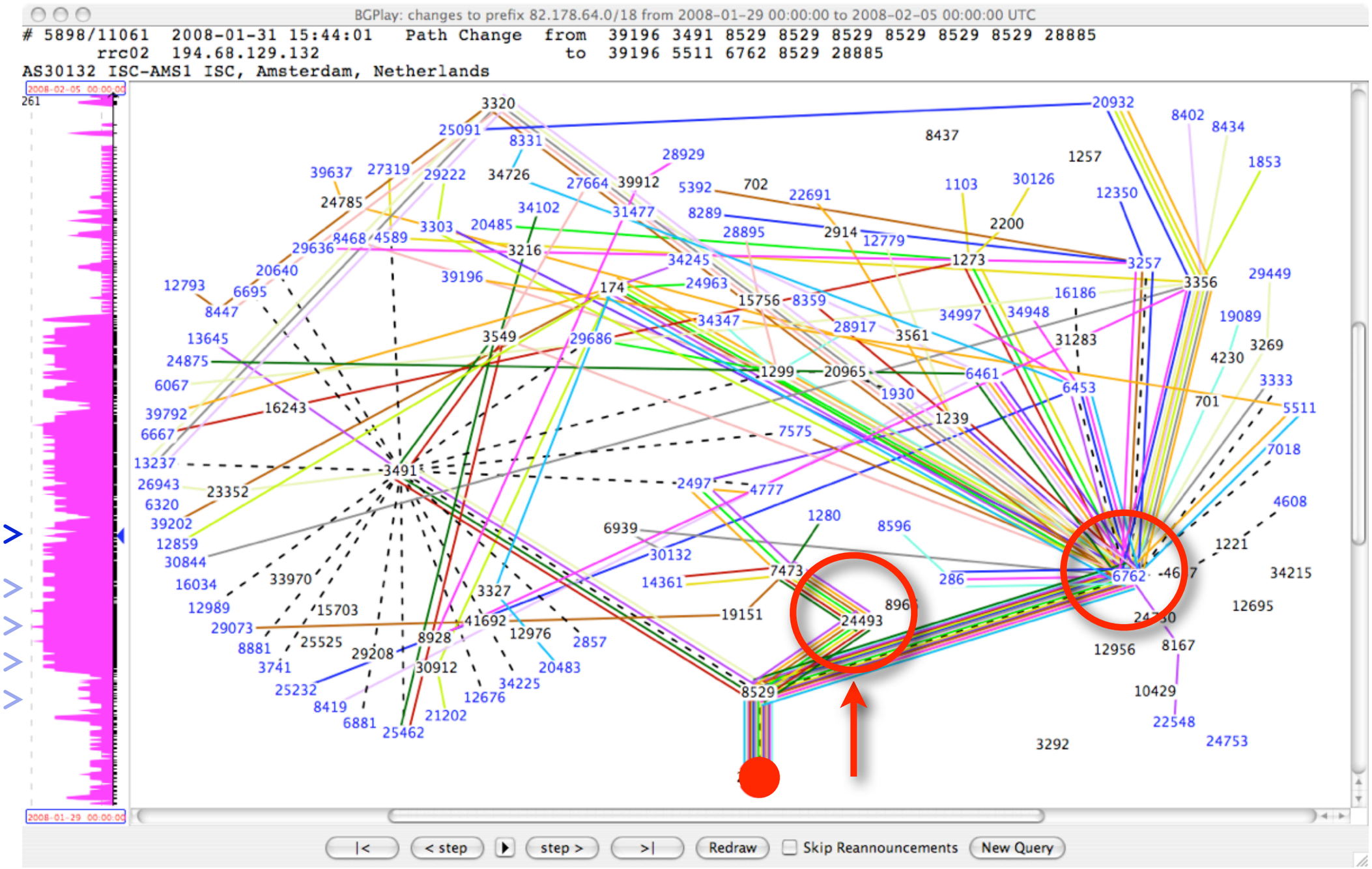
BGP churn

- Seven hours pass, another different path

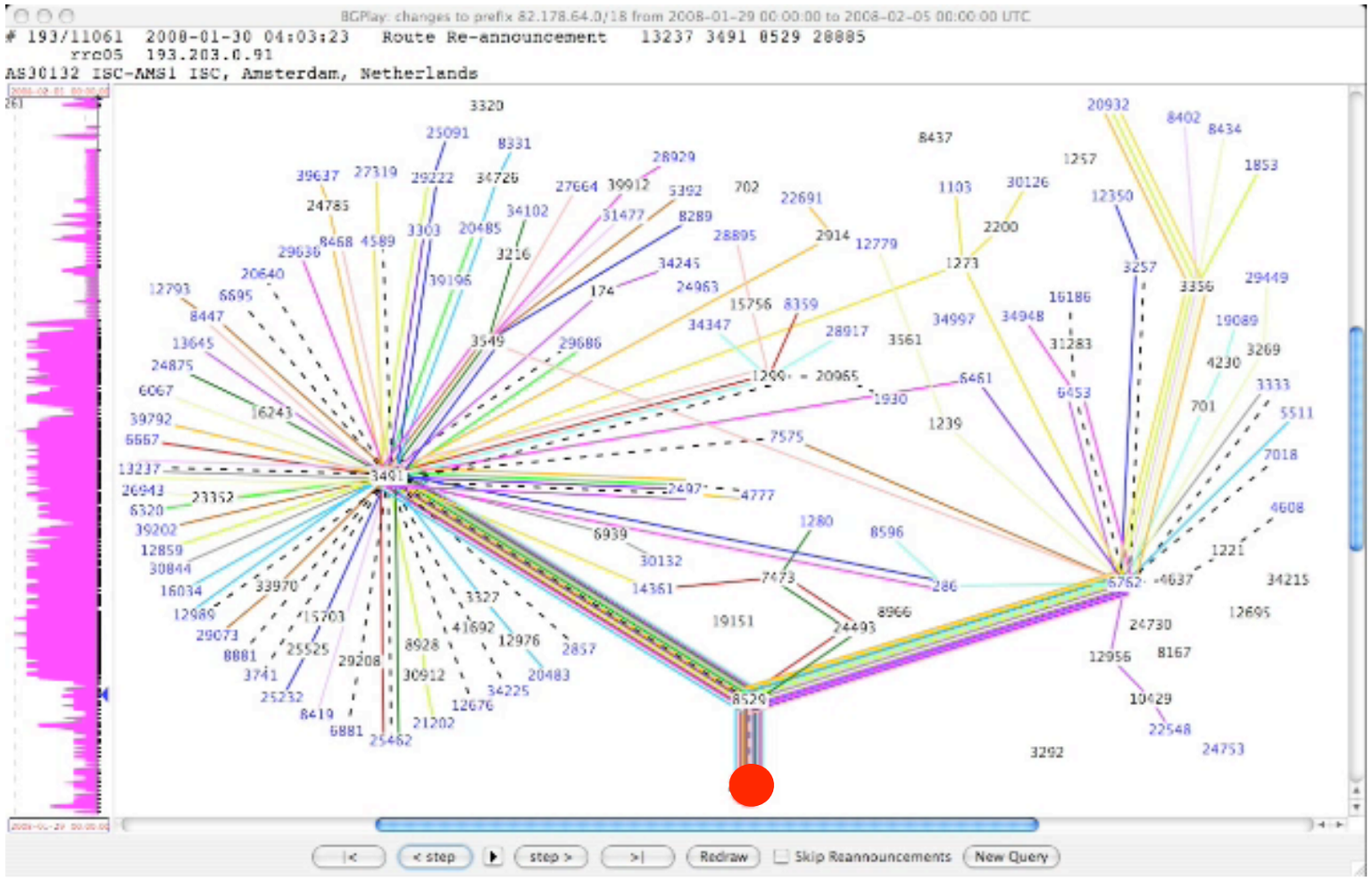


BGP churn

- Another day, another routing state



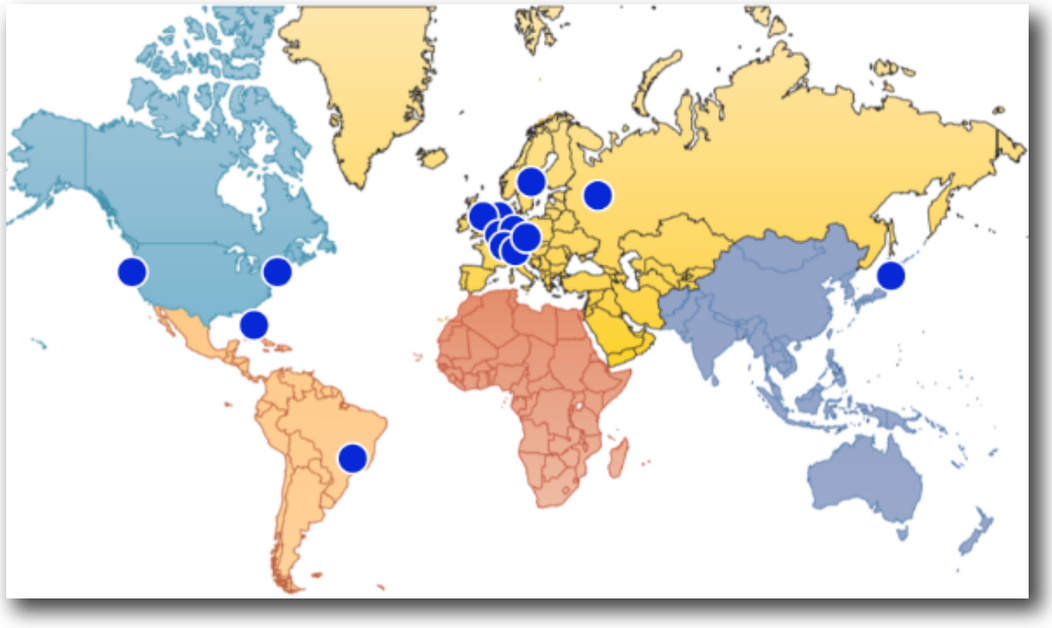
BGP churn



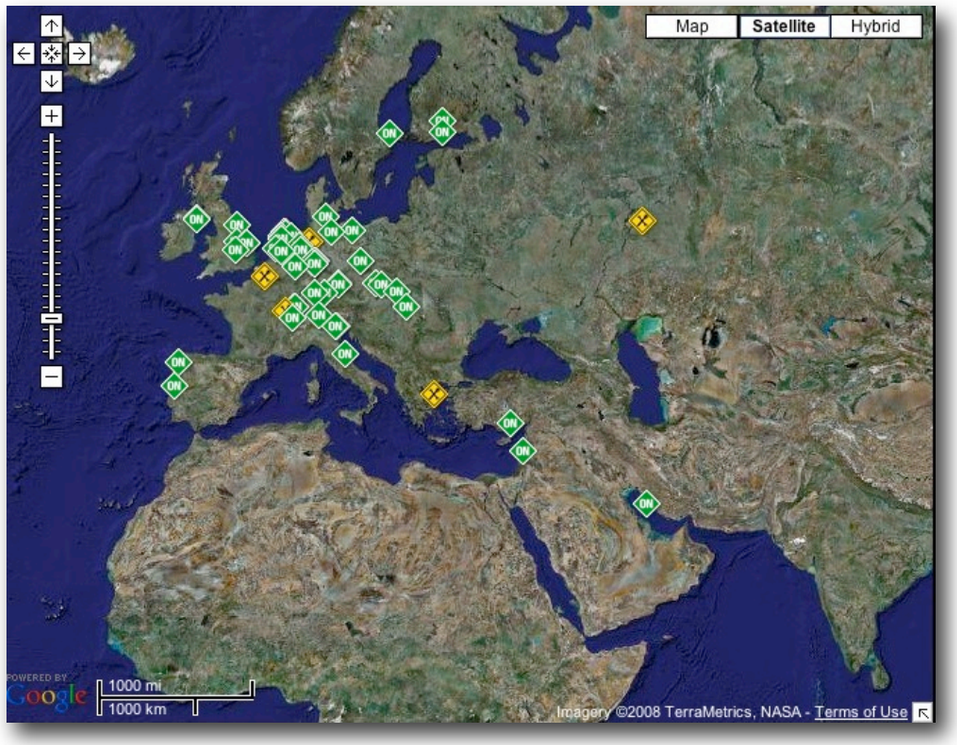
- Explosion in BGP activity
- Distinct AS paths double
  - Average AS path length increased by 20%
- Constant high rate of changes
  - Uncertain if BGP ever converged or if the routes were usable?

Credits

- Routing Information Service (RIS)
  - http://www.ripe.net/ris
- Test Traffic Measurements (TTM)
  - http://www.ripe.net/ttm
- DNSMON
  - http://dnsmon.ripe.net



- RIPE NCC Information Services
  - http://is-portal.ripe.net



- Full NCC Science Group analysis
  - http://ripe.net/projects/reports/2008cable-cut

Questions?