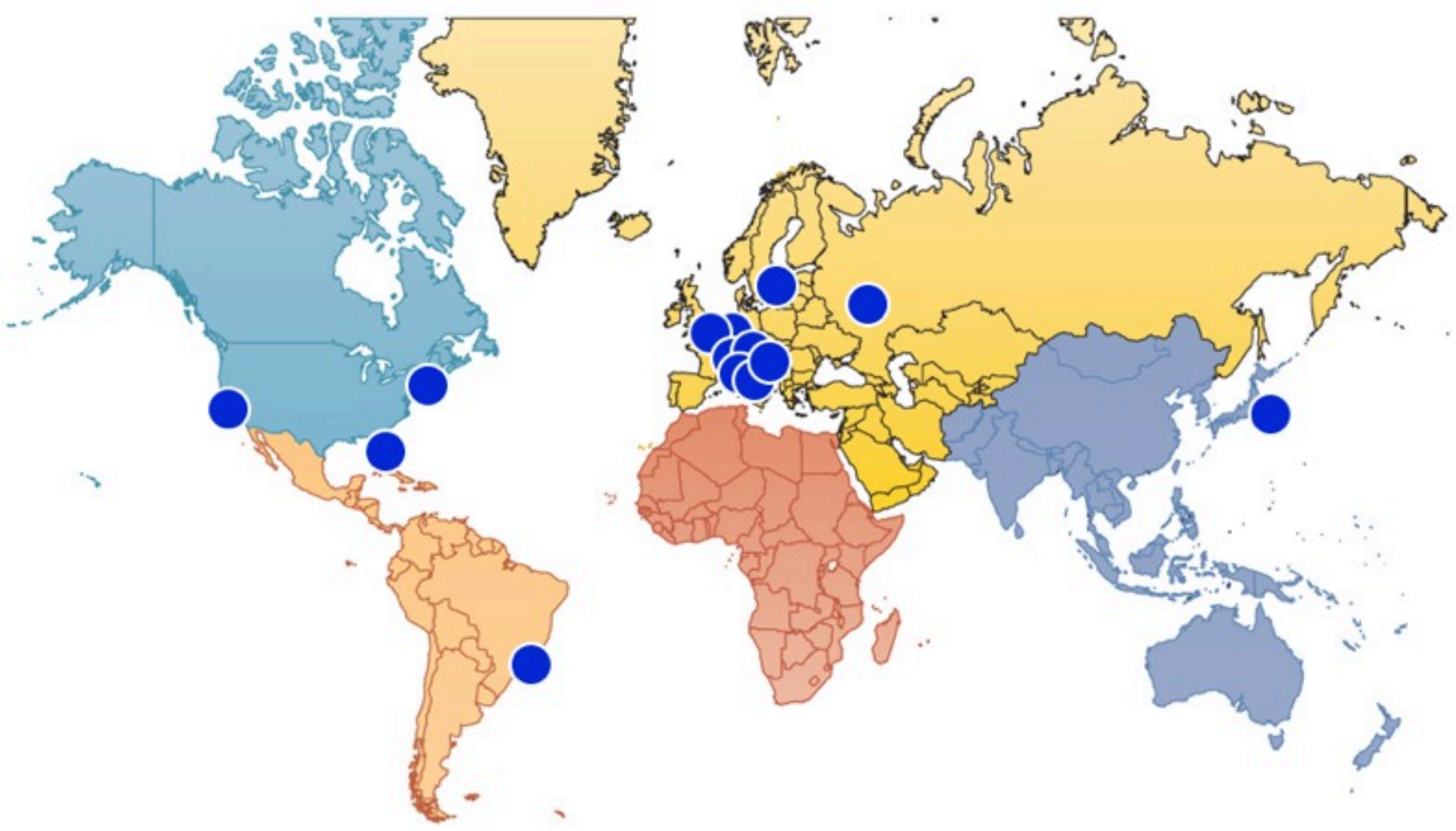
Incident analysis with RIPE NCC tools

Analysing the RIS/Duke BGP incident

Erik Romijn <eromijn@ripe.net>
Senior Software Engineer

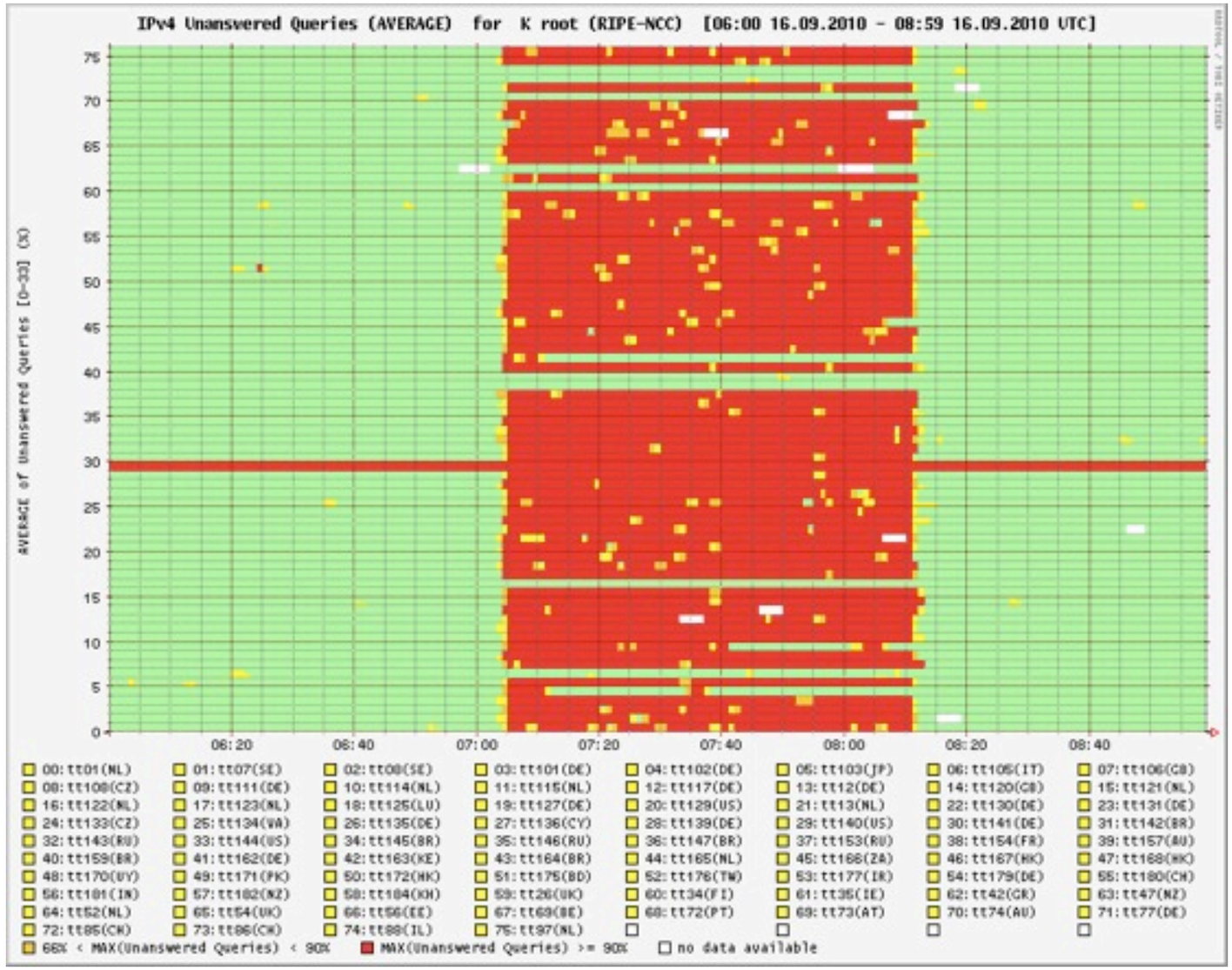
RIPE NCC information collection

- Routing Information Service (RIS)
  - Listens to and stores all BGP updates
  - Receiving data form 600 peers



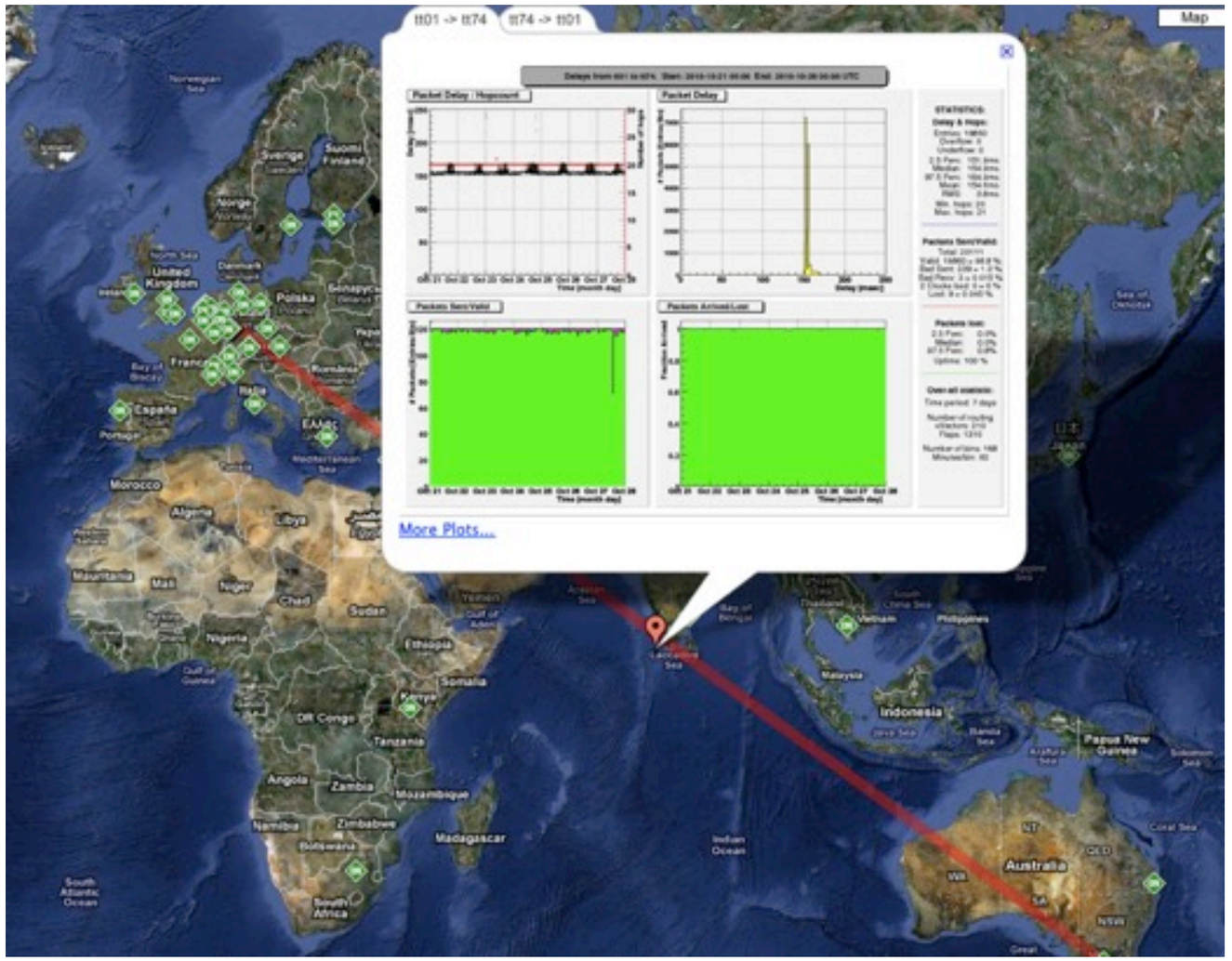
RIPE NCC information collection

- DNS monitoring service (DNSMON)
  - Monitors critical DNS infrastructure
  - About 100 vantage points worldwide



RIPE NCC information collection

- Test Traffic Measurements (TTM)
  - One-way latency/jitter/loss & traceroutes
  - About 100 nodes in full mesh



Case study:

RIPE NCC / Duke University BGP experiment

RIS experiments & announcements

- RIS has a long tradition of supporting research

- Second AS in the world to announce 4-byte AS numbers

- Beacon prefixes from RIS available since 2002
  - Also a vital part of debogonizing

Case study: RIPE NCC BGP experiment

- RIPE NCC conducted an experiment on 27-08-2010
  - An optional BGP attribute was announced
  - This was a optional transitive attribute of 3000 bytes
  - The announcement was valid according to RFC4271

- Some routers corrupted the route and sent it
  - Peers who saw this dropped the session

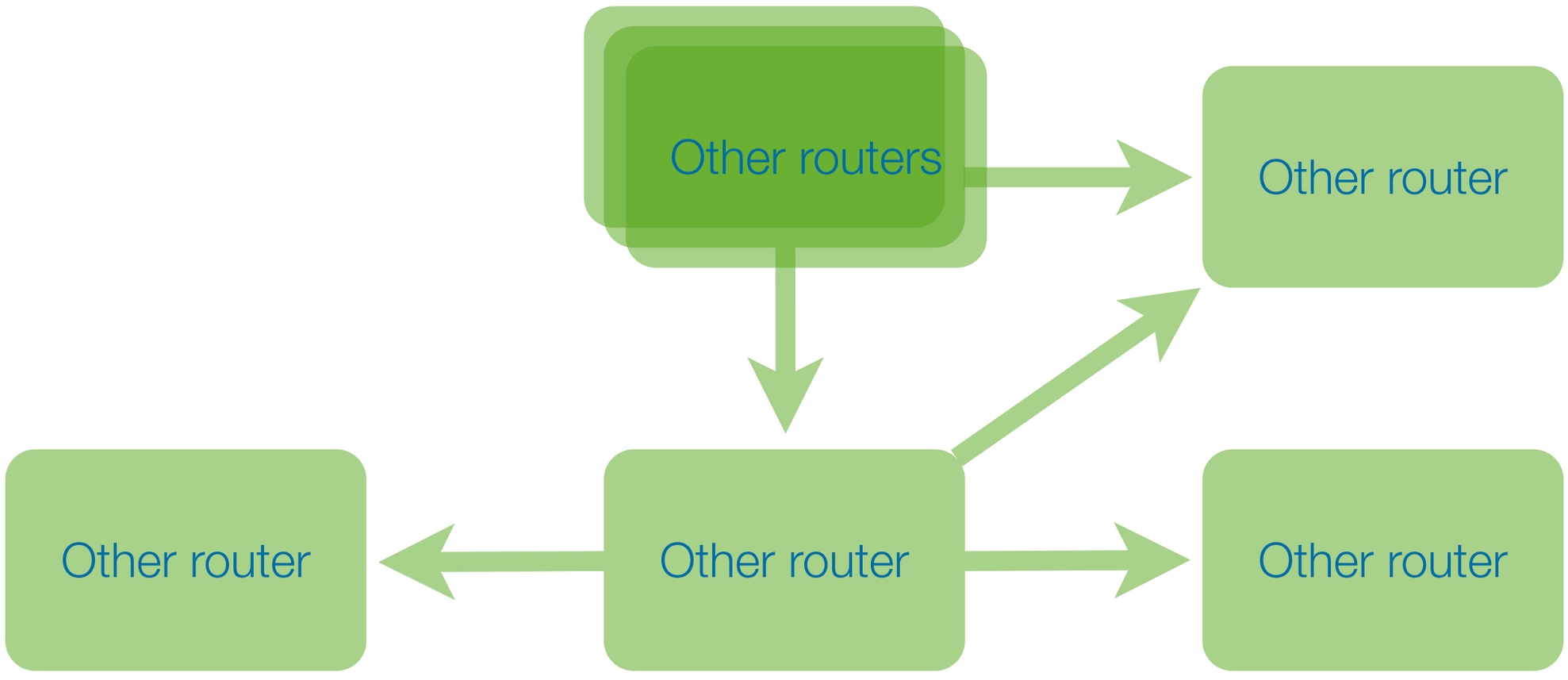
- This caused disruption to some internet traffic

Case study: 27 August 2010

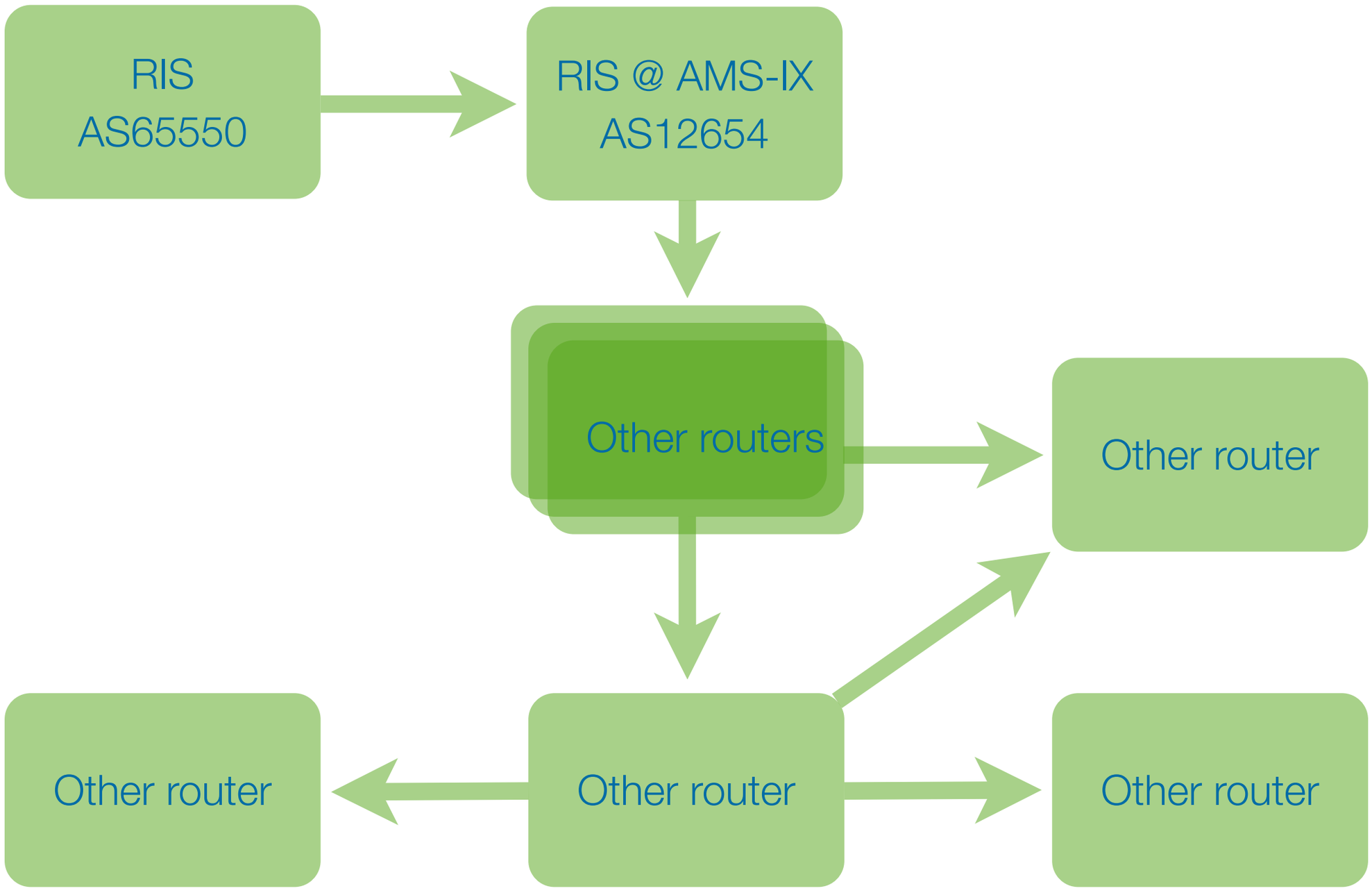
- Announcement active from 08:41 to 09:08 UTC, using 93.175.144.0/24
- We later observed some negative impact

- Immediately started an extensive investigation
  - This pointed towards a Cisco IOS XR bug
  - Sent out a very detailed private announcement
  - Also provided Cisco with all details
- Cisco released cisco-sa-20100827-bgp

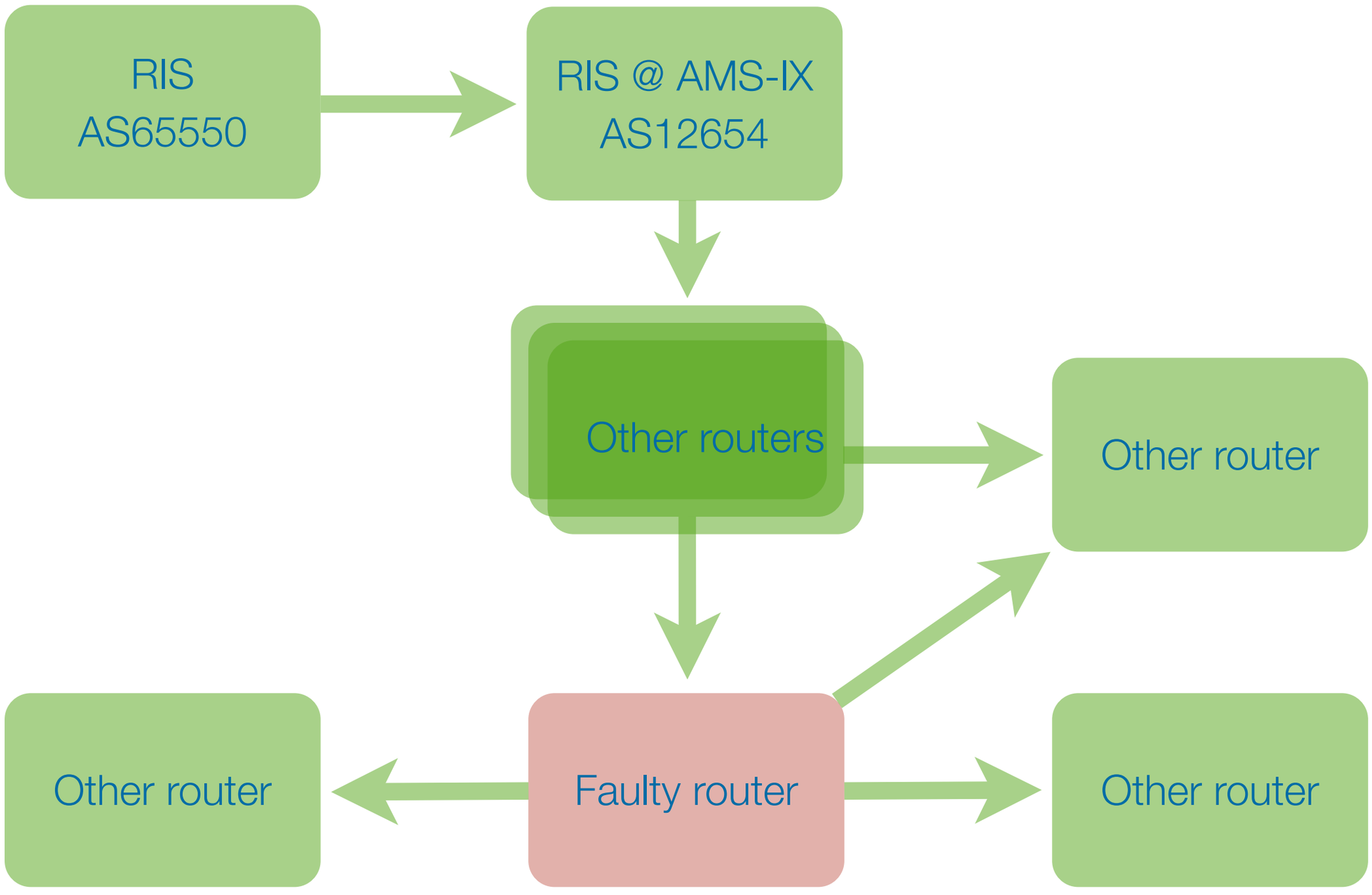
Propagation of the announcement



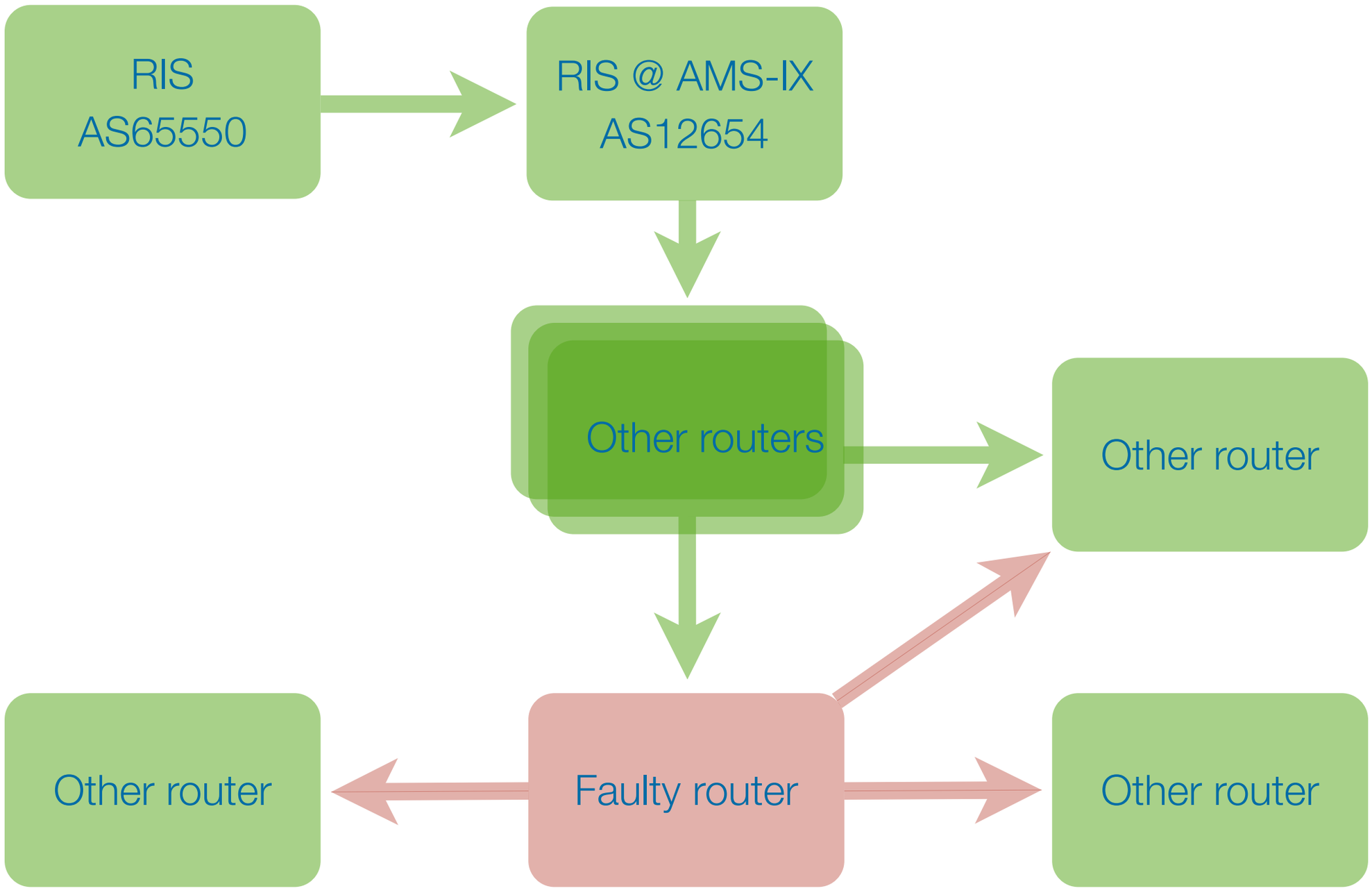
Propagation of the announcement



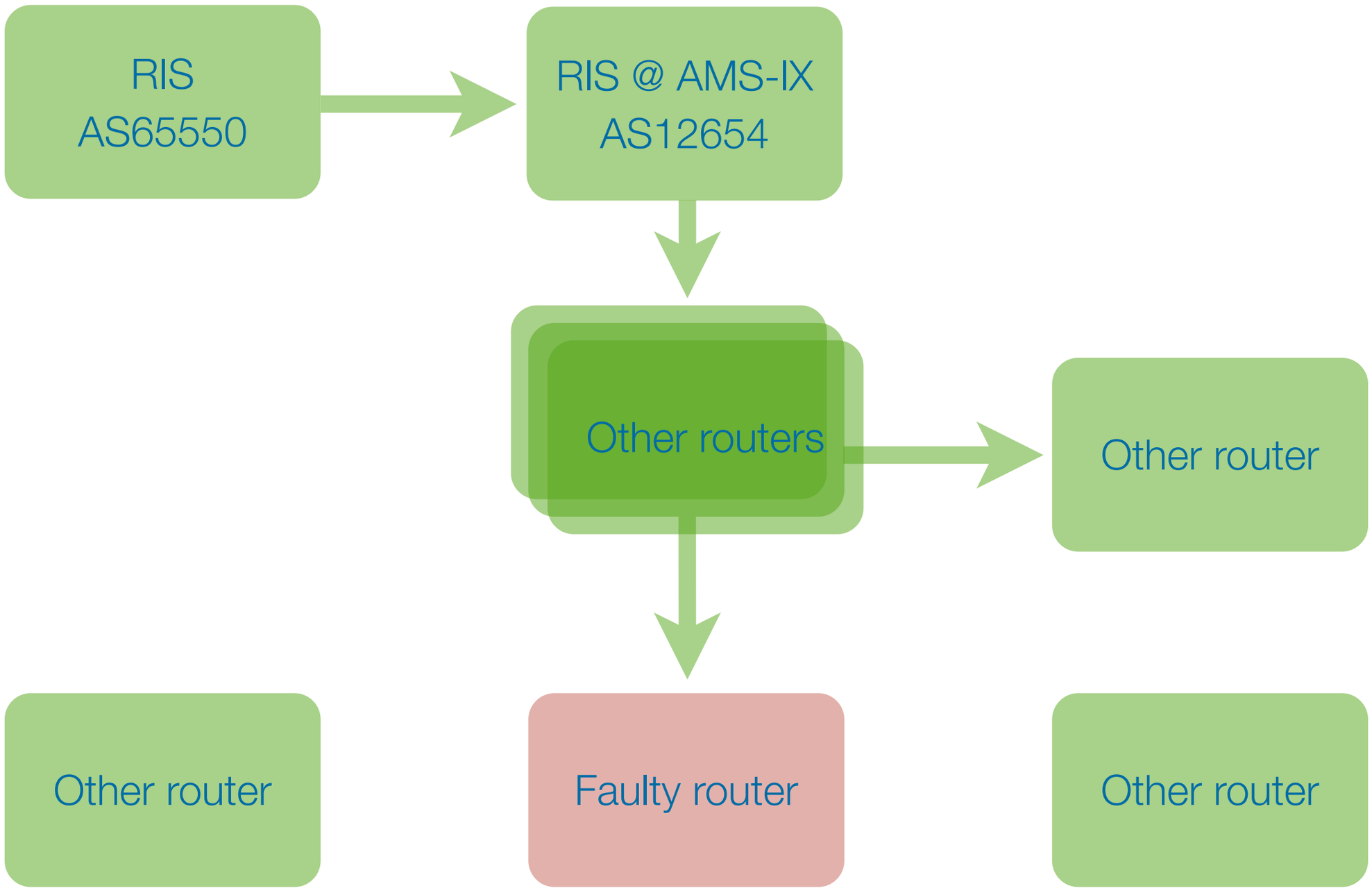
Propagation of the announcement



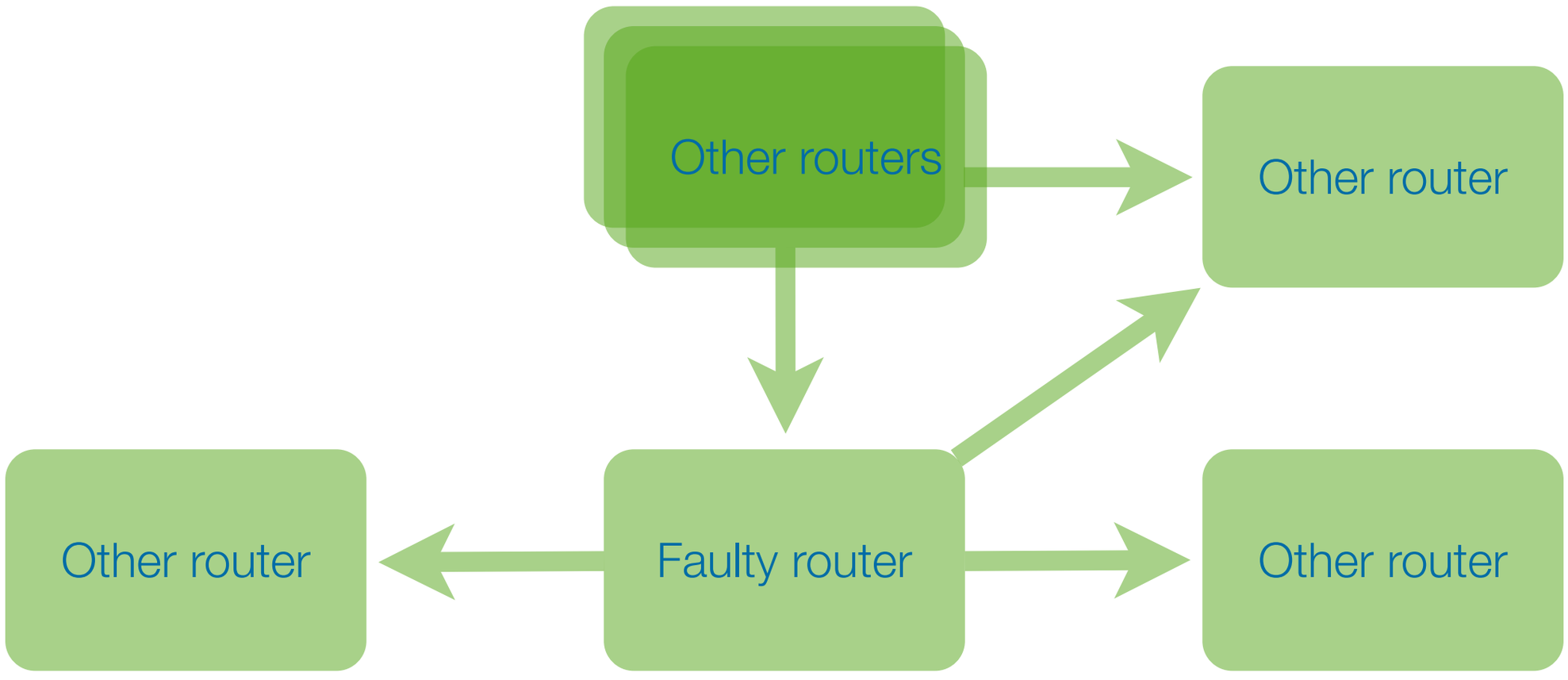
Propagation of the announcement



Propagation of the announcement



Propagation of the announcement



Goal of the experiment

- Research group from Duke University
  approached RIPE NCC to help

- Their goal was to measure support for long
  optional transitive attributes
  - Intended to be used for certificates for secure routing

- They did not have an AS number or addresses
- Provided RIPE NCC with a patched Quagga

Expected results

A. The route propagates with the attribute intact

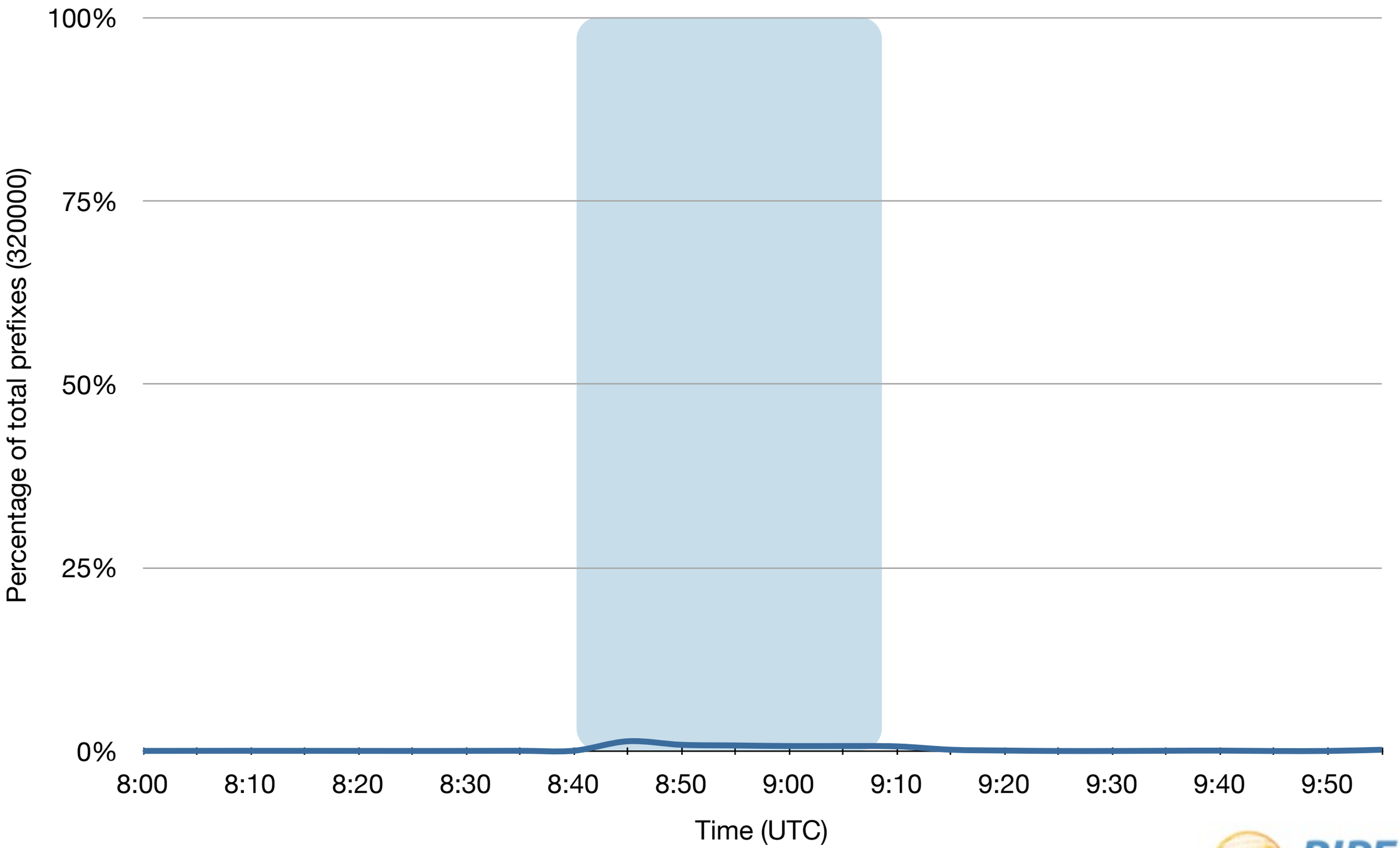
B. The route propagates, with some AS in the path removing the attribute

C. The route propagates, but takes a different path because some ASes drop the route

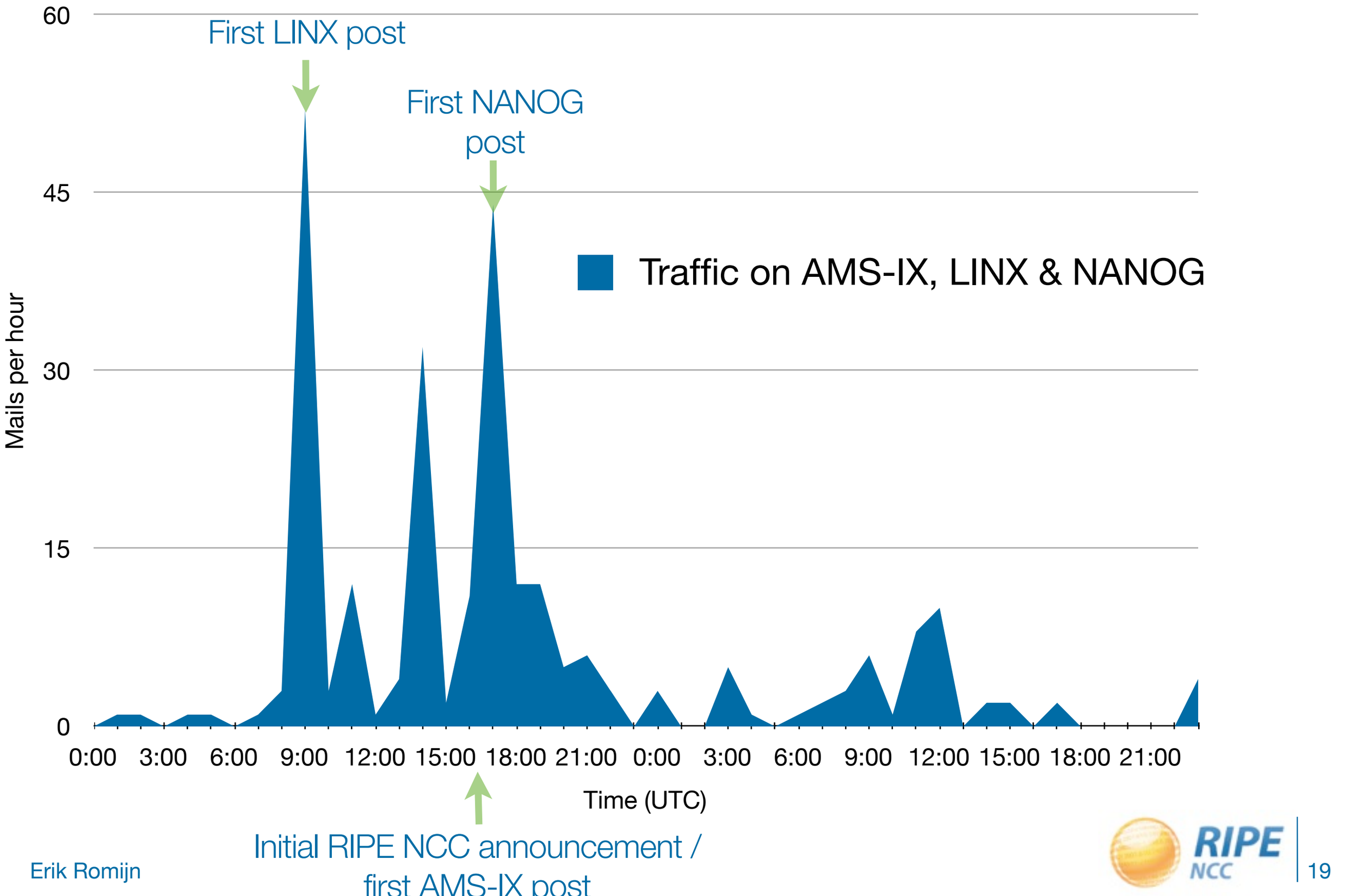
A and B were seen in 4-byte AS number tests.

Impact of the experiment on the Internet

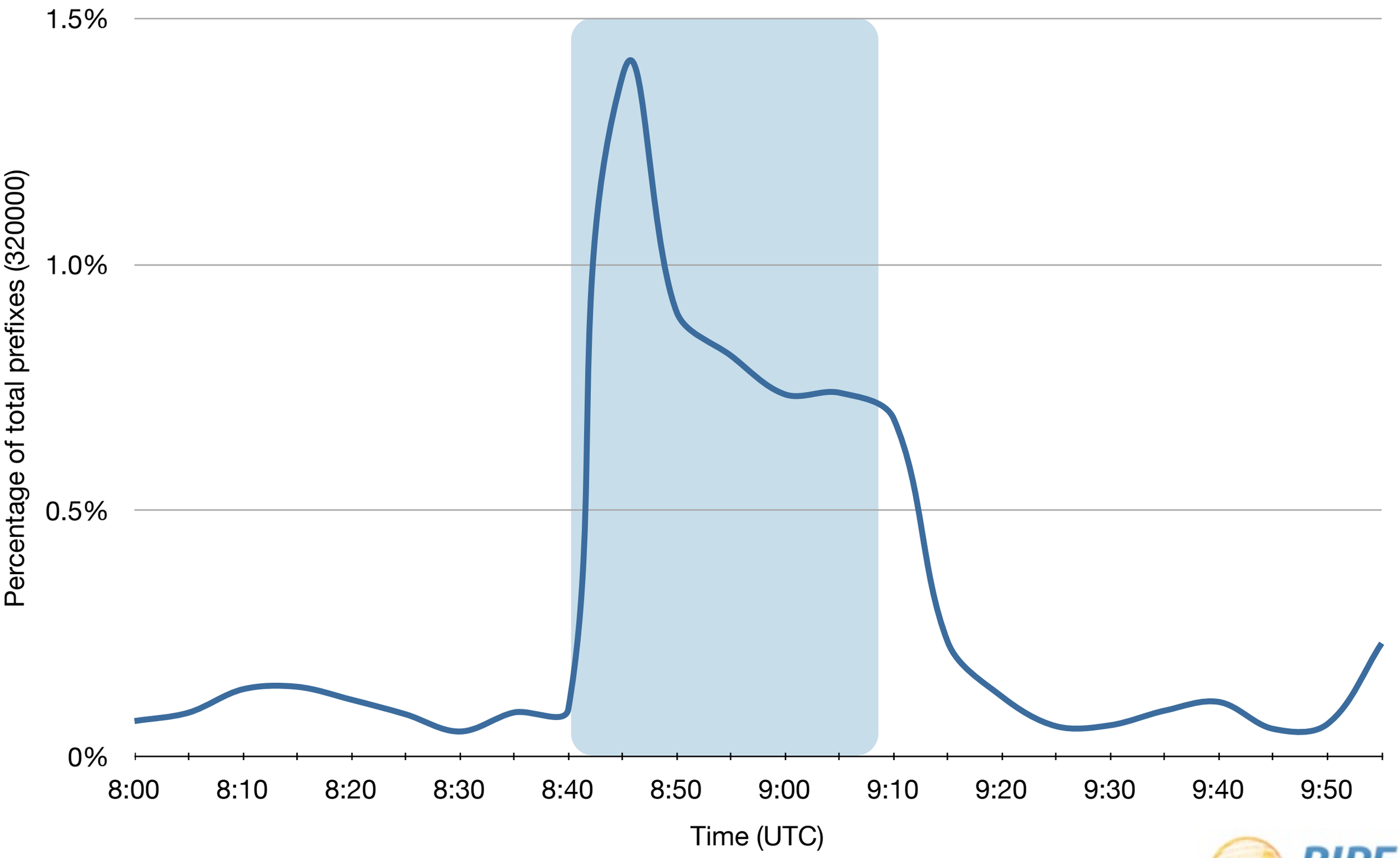
Unstable prefixes



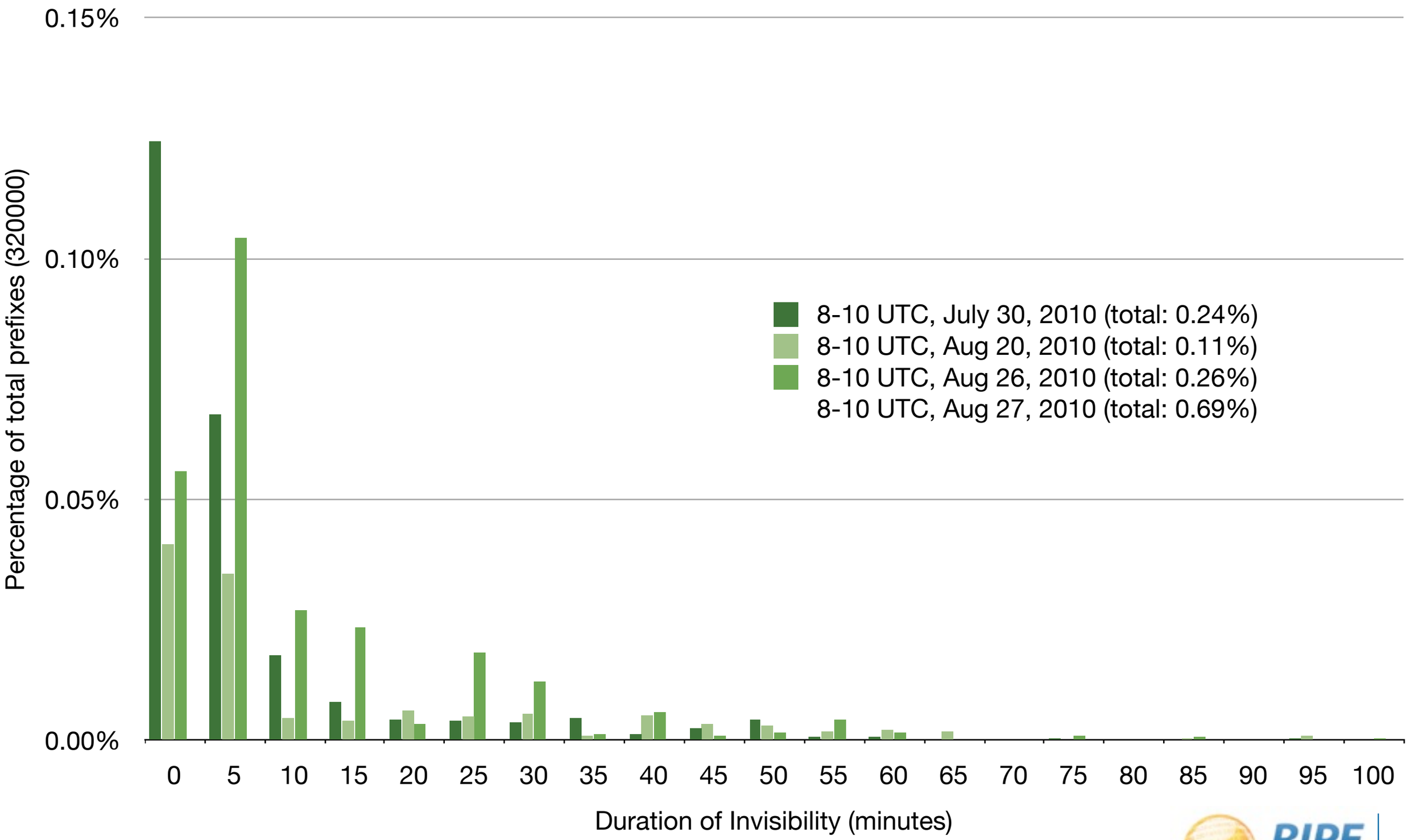
E-mails per hour - 28-29 August



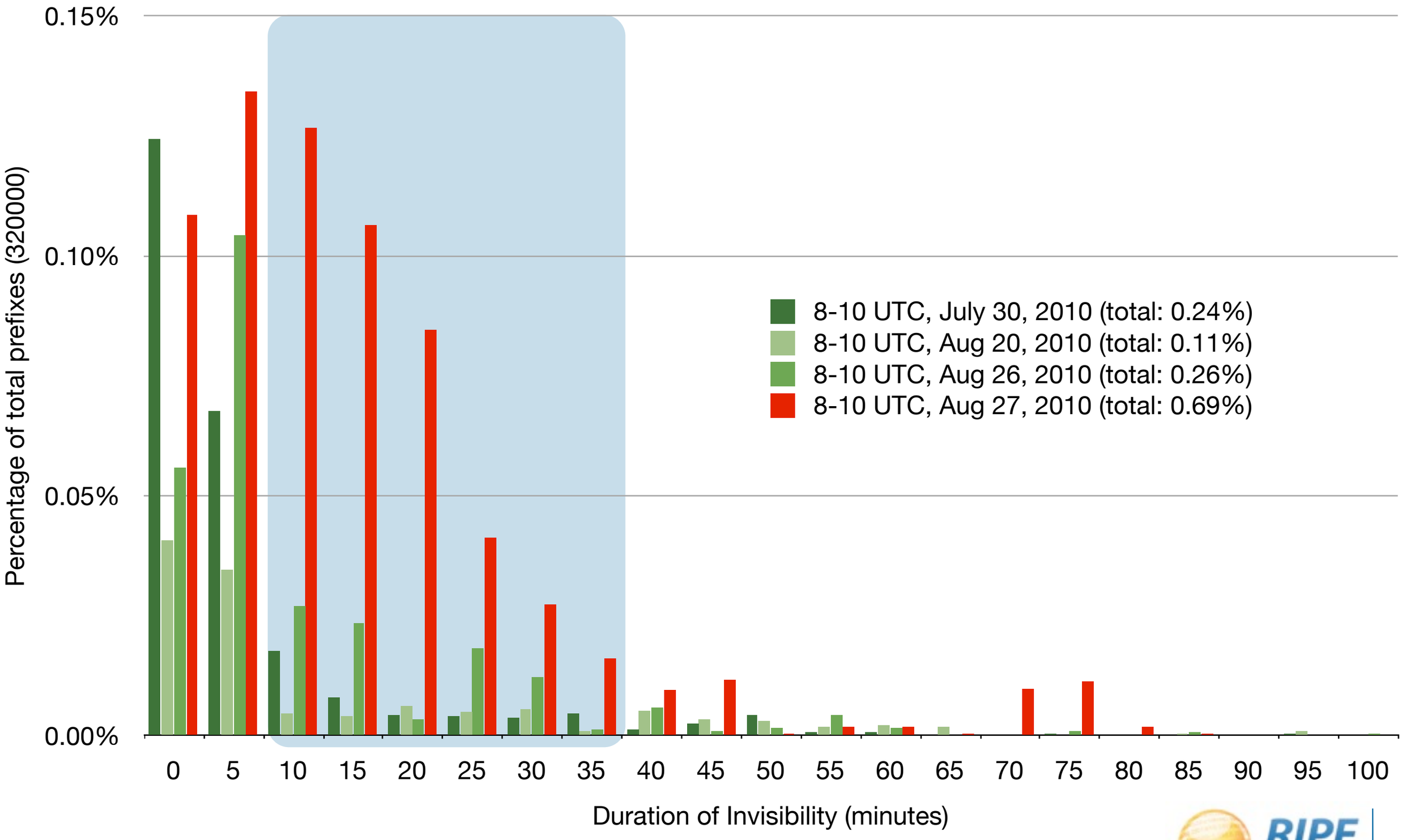
Unstable prefixes



Length of invisibilities



Length of invisibilities



Critical DNS infrastructure (from DNSMON)

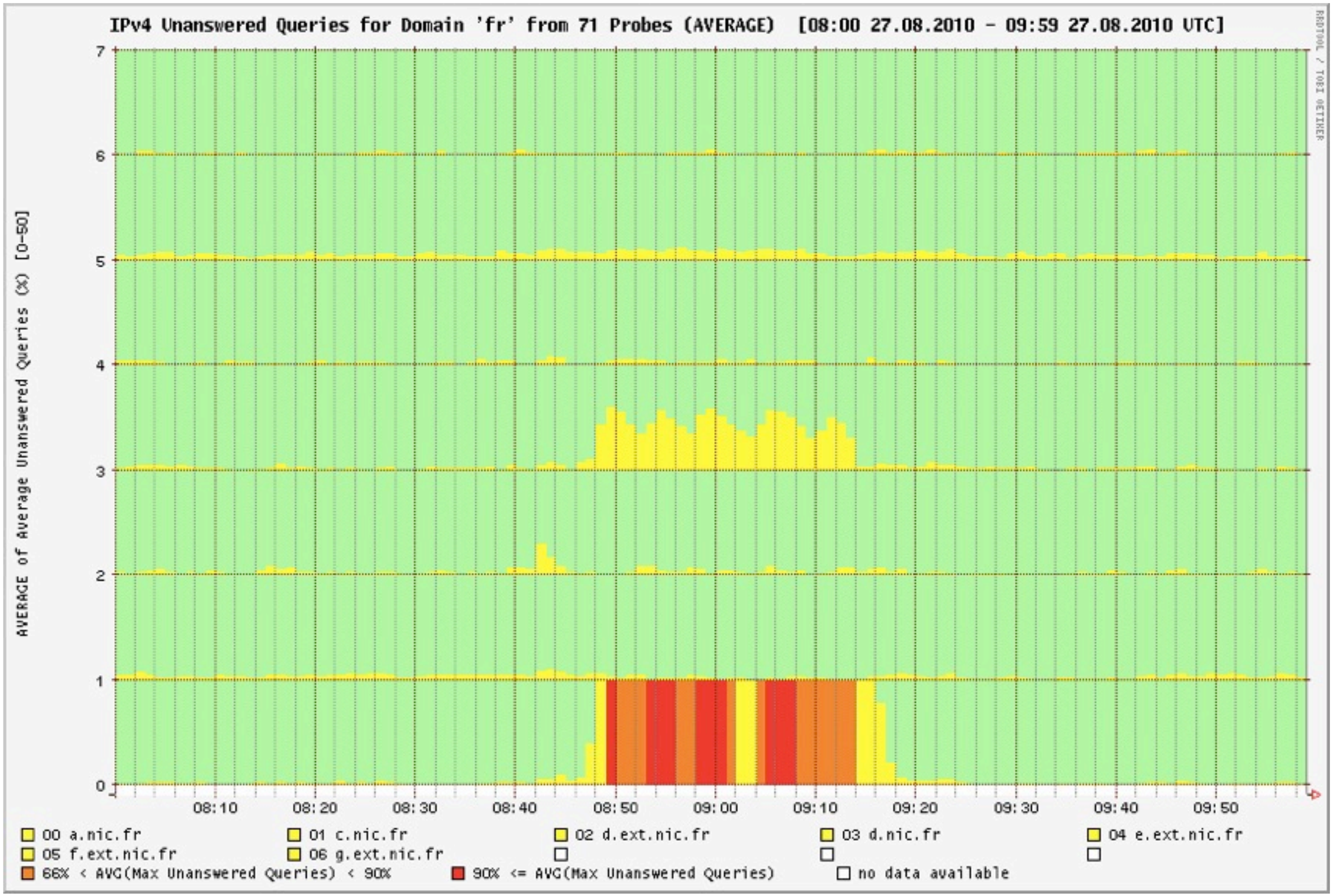
- Root servers unaffected

- 57% of TLDs unaffected

- Minor effects for 38% of the TLDs
  - Some dropped queries for one or two servers

- More significant effects on 5% of the TLDs

Critical DNS infrastructure



Visualization parameters

Prefix 192.93.0.0 / 24

Start date 27/08/2010 Time 10 : 47

End date 27/08/2010 Time 10 : 50

View Cancel

BGPviz Graph View Help

Last updates seen in the graph: Clear

update 1/4 (27/08/2010 10:48 | ANNOUNCEMENT): **AS9002** (193.232.244.187 - MSK-IX) changing path from 9002 3561 1273 2200 2485 2485 to 9002 3356 3561 1273 2200

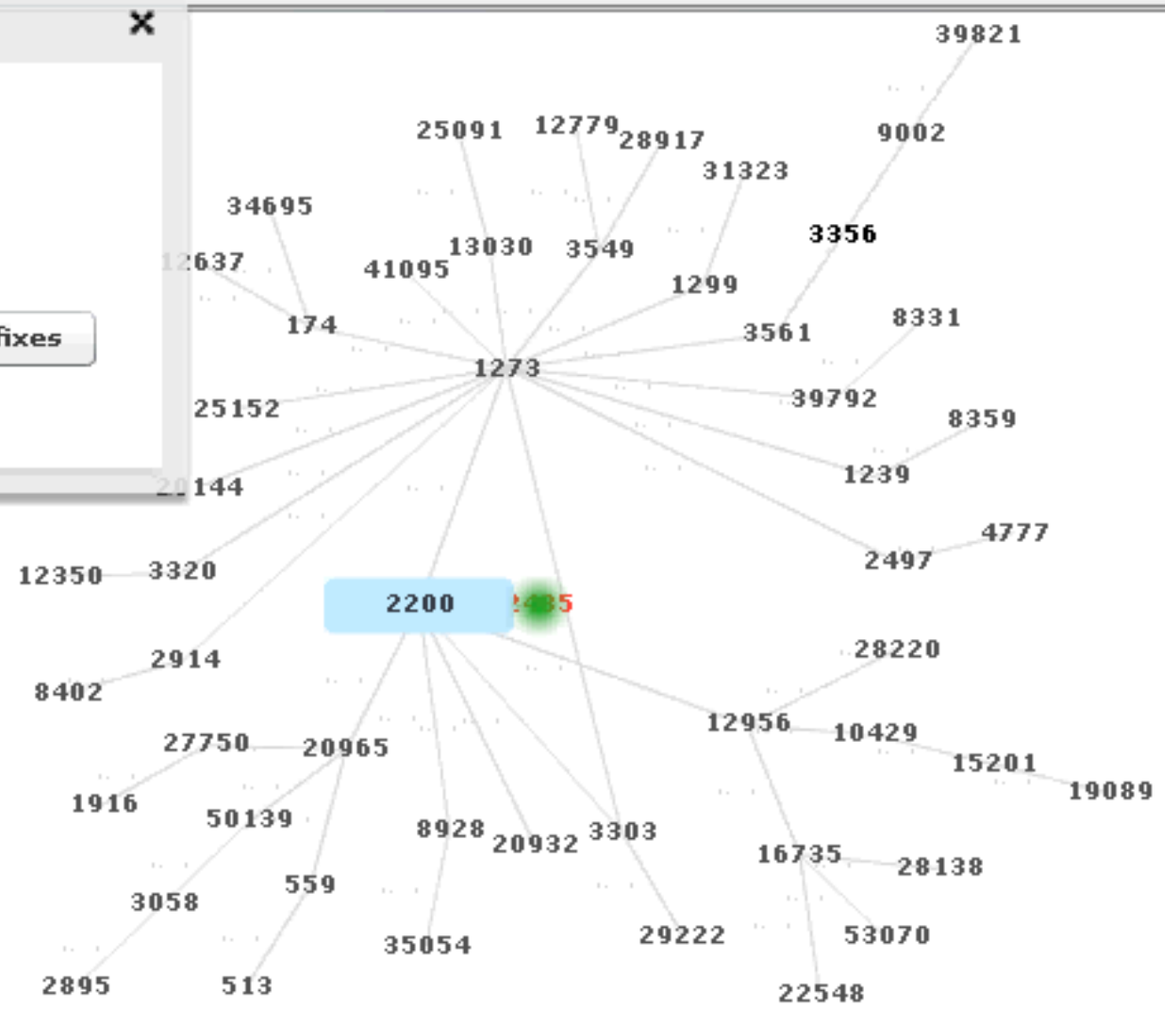
AS Details

AS 2200

IP: not available

location: not available

WHOIS info | Announced Prefixes



27/08/2010 10:47 | 192.93.0.0/24 | 27/08/2010 10:50

4 updates

Animate reannouncements

BGPviz Graph View Help

Whois

Whois info for the **AS 2200**

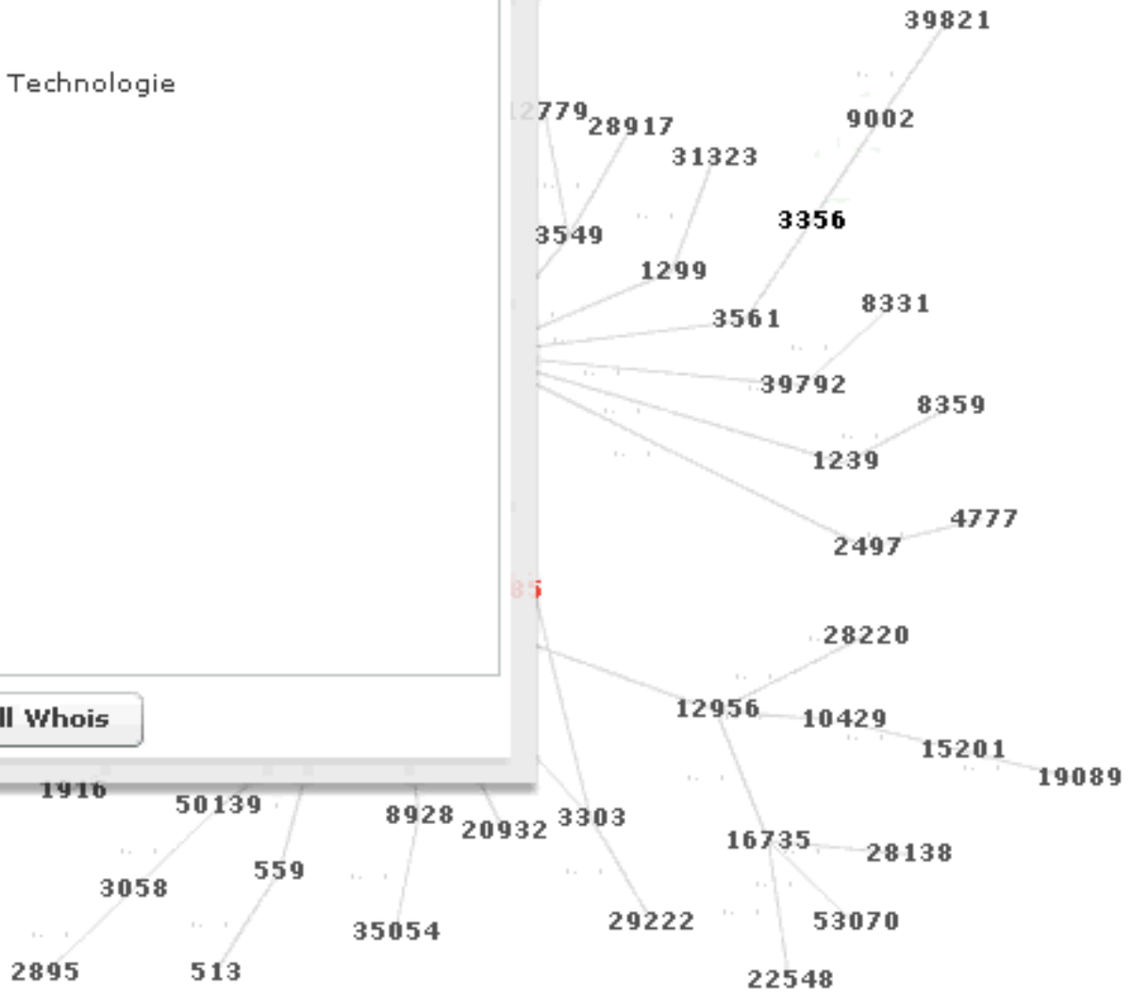
```
aut-num:
AS2200
FR-RENATER
Reseau National de telecommunications pour la Technologie
l'Enseignement et la Recherche
FR

role:
GIP RENATER
GIP RENATER
23-25 Rue Daviel
75013 PARIS
FRANCE
+33 1 53 94 20 30
RenSVP@Renater.fr
```

AS number: Call Whois

Clear

changing path from 9002 3561 1273 2200 2485 2485 to 9002 3356 3561 1273 2200



27/08/2010 10:47 — 192.93.0.0/24 — 27/08/2010 10:50

4 updates

Animate reannouncements

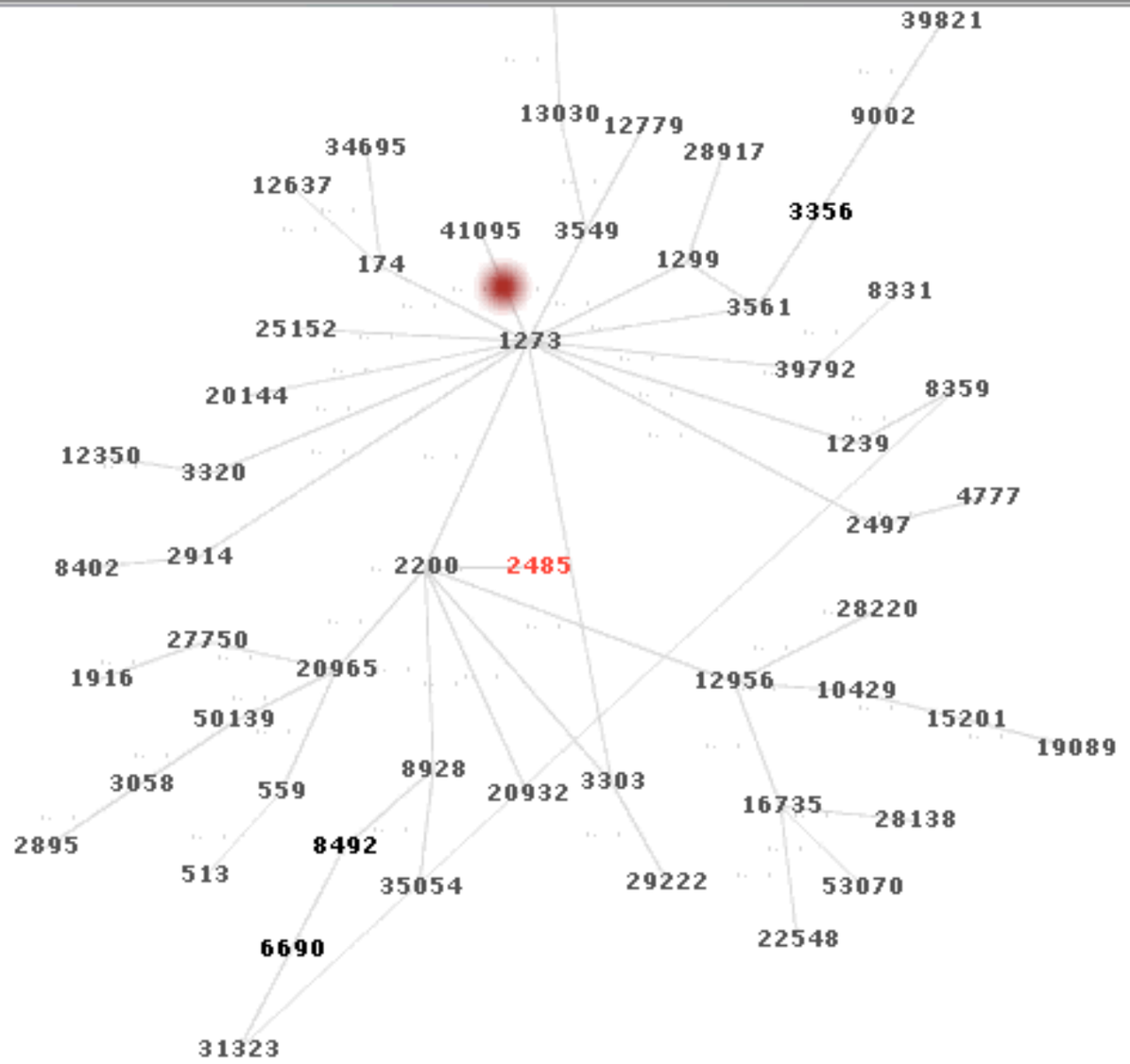
BGPviz Graph View Help

Last updates seen in the graph: Clear

update 2/2 (27/08/2010 10:48 | ANNOUNCEMENT): **AS31323** (193.232.244.172 - MSK-IX) changing path from 31323 6690 8492 8928 2200 2485 2485 to 31323 8359 1239 1

update 1/2 (27/08/2010 10:48 | ANNOUNCEMENT): **AS39821** (193.232.244.15 - MSK-IX) changing path from 39821 9002 3561 1273 2200 2485 2485 to 39821 9002 3356 35

update 2/2 (27/08/2010 10:48 | ANNOUNCEMENT): **AS41095** (193.232.245.4 - MSK-IX) changing path from 41095 1273 2200 2485 2485 to 41095 3356 3561 1273 2200 248



27/08/2010 10:47 | 192.93.0.0/24 | 27/08/2010 10:50

4 - 27/08/2010 10:47 27/08/2010 10:47 27/08/2010 10:47 27/08/2010 10:48 27/08/2010 10:48 27/08/2010 10:48 27/08/2010 10:48 27/08/2010 10:49 27/08/2010 10:49 27/08/2010 10:49 - 4

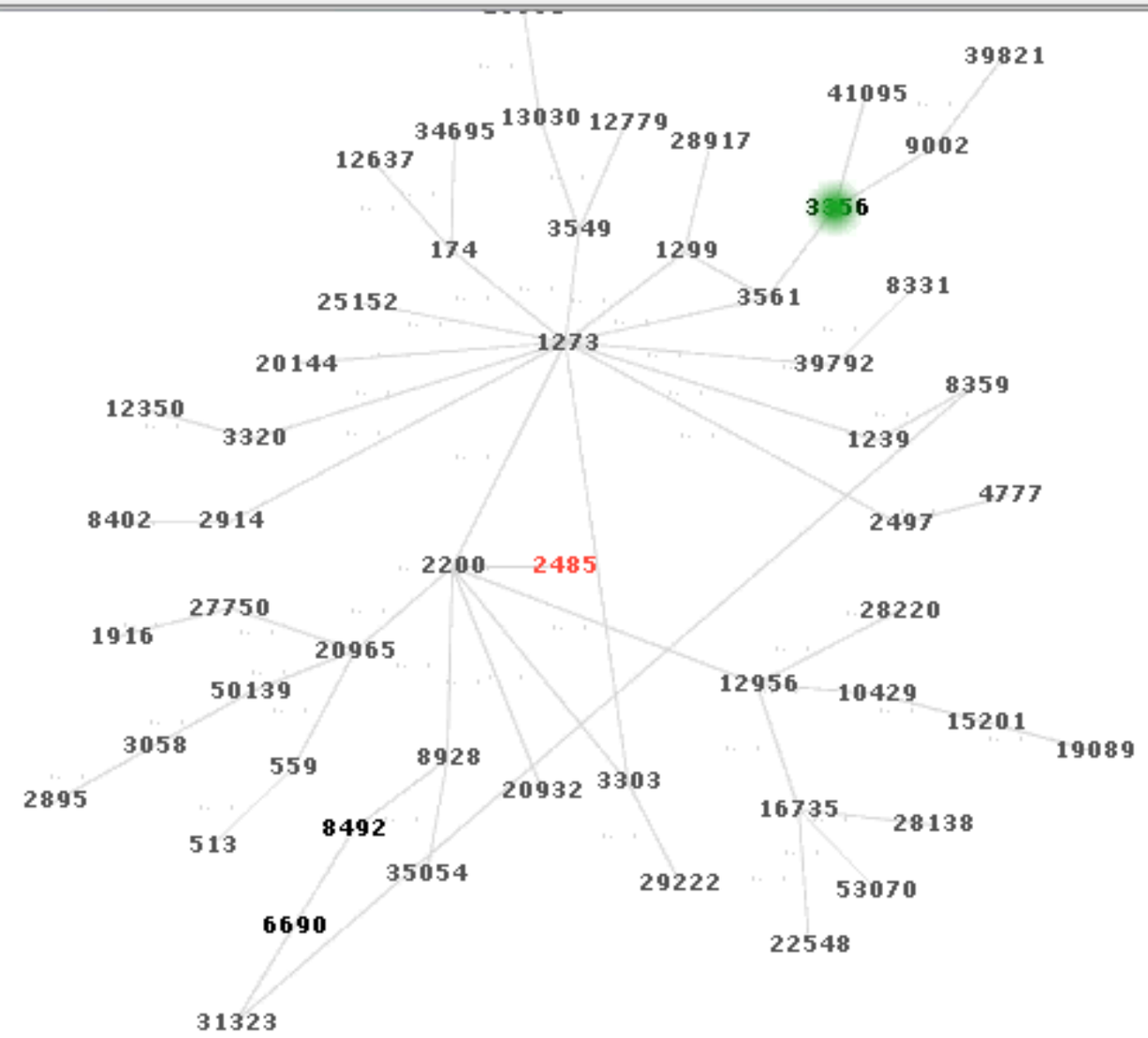
2 updates

Animate reannouncements

BGPviz Graph View Help

Last updates seen in the graph: Clear

update 2/2 (27/08/2010 10:48 | ANNOUNCEMENT): **AS31323** (193.232.244.172 - MSK-IX) changing path from 31323 6690 8492 8928 2200 2485 2485 to 31323 8359 1239 1
update 1/2 (27/08/2010 10:48 | ANNOUNCEMENT): **AS39821** (193.232.244.15 - MSK-IX) changing path from 39821 9002 3561 1273 2200 2485 2485 to 39821 9002 3356 35
update 2/2 (27/08/2010 10:48 | ANNOUNCEMENT): **AS41095** (193.232.245.4 - MSK-IX) changing path from 41095 1273 2200 2485 2485 to 41095 3356 3561 1273 2200 248



27/08/2010 10:47 | 192.93.0.0/24 | 27/08/2010 10:50

4 - 27/08/2010 10:47 27/08/2010 10:47 27/08/2010 10:47 27/08/2010 10:48 27/08/2010 10:48 27/08/2010 10:48 27/08/2010 10:48 27/08/2010 10:49 27/08/2010 10:49 27/08/2010 10:49 - 4

2 updates

Animate reannouncements

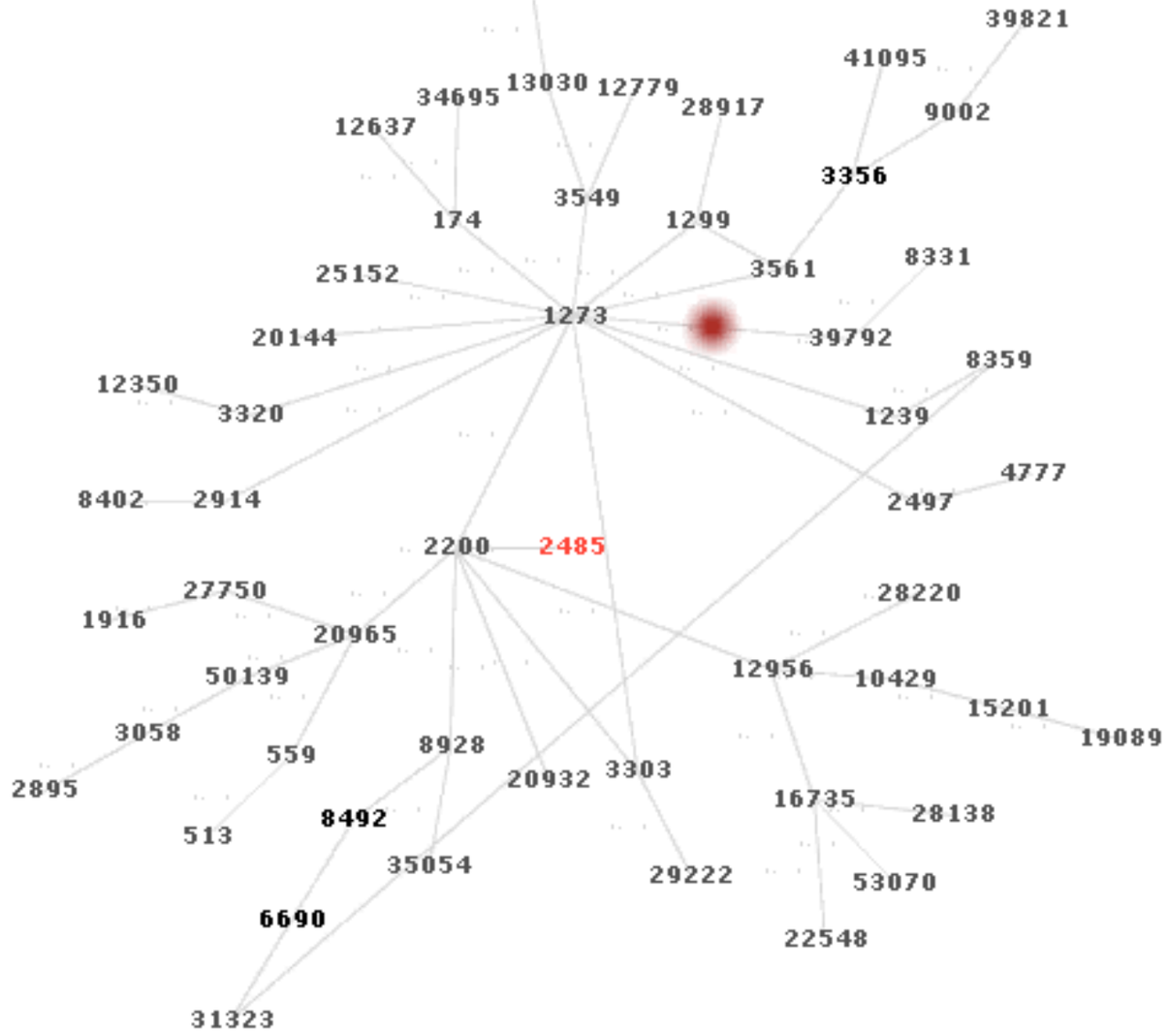
BGPviz Graph View Help

Last updates seen in the graph: Clear

update 1/2 (27/08/2010 10:48 | ANNOUNCEMENT): **AS39821** (193.232.244.15 - MSK-IX) changing path from 39821 9002 3561 1273 2200 2485 2485 to 39821 9002 3356 35

update 2/2 (27/08/2010 10:48 | ANNOUNCEMENT): **AS41095** (193.232.245.4 - MSK-IX) changing path from 41095 1273 2200 2485 2485 to 41095 3356 3561 1273 2200 248

update 1/1 (27/08/2010 10:48 | ANNOUNCEMENT): **AS39792** (193.232.244.136 - MSK-IX) changing path from 39792 1273 2200 2485 2485 to 39792 3549 1273 2200 2485 2



27/08/2010 10:47 | 192.93.0.0/24 | 27/08/2010 10:50

4 - 27/08/2010 10:47 27/08/2010 10:47 27/08/2010 10:47 27/08/2010 10:48 27/08/2010 10:48 27/08/2010 10:48 27/08/2010 10:48 27/08/2010 10:49 27/08/2010 10:49 27/08/2010 10:49 - 4

1 update

Animate reannouncements

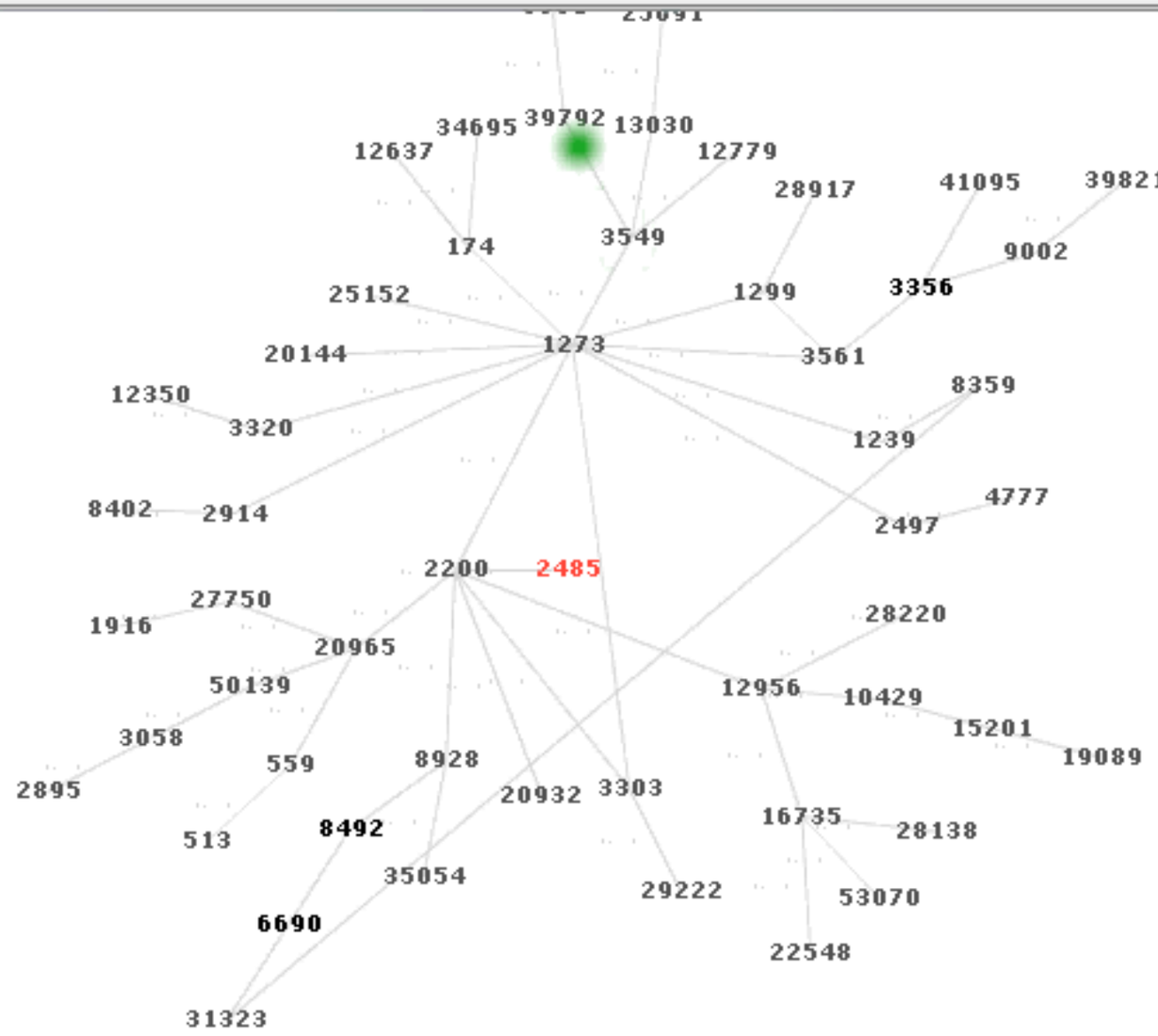
BGPviz Graph View Help

Last updates seen in the graph: Clear

update 1/2 (27/08/2010 10:48 | ANNOUNCEMENT): **AS39821** (193.232.244.15 - MSK-IX) changing path from 39821 9002 3561 1273 2200 2485 2485 to 39821 9002 3356 35

update 2/2 (27/08/2010 10:48 | ANNOUNCEMENT): **AS41095** (193.232.245.4 - MSK-IX) changing path from 41095 1273 2200 2485 2485 to 41095 3356 3561 1273 2200 248

update 1/1 (27/08/2010 10:48 | ANNOUNCEMENT): **AS39792** (193.232.244.136 - MSK-IX) changing path from 39792 1273 2200 2485 2485 to 39792 3549 1273 2200 2485 2



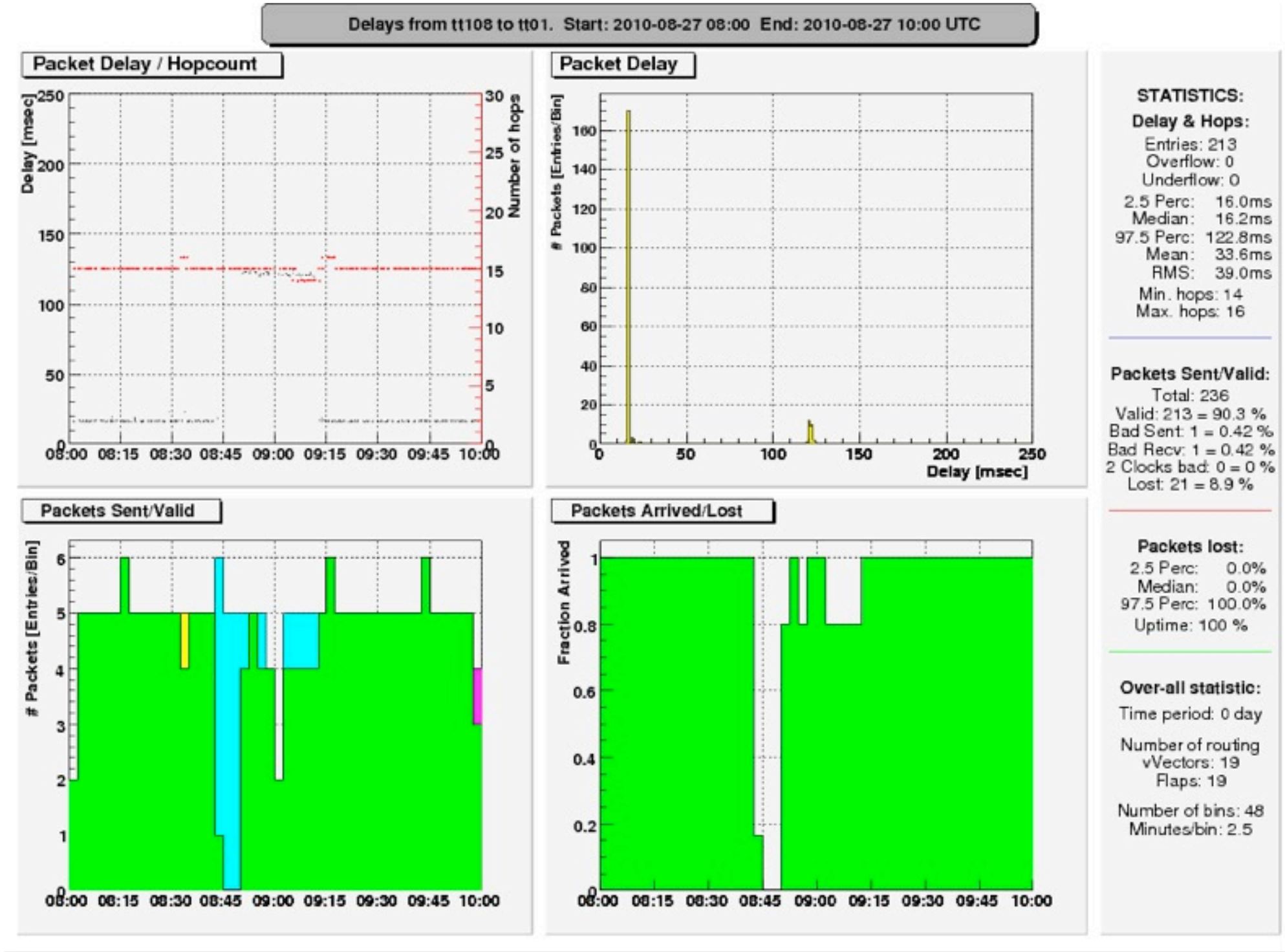
27/08/2010 10:47 | 192.93.0.0/24 | 27/08/2010 10:50

4 - 27/08/2010 10:47 27/08/2010 10:47 27/08/2010 10:47 27/08/2010 10:48 27/08/2010 10:48 27/08/2010 10:48 27/08/2010 10:48 27/08/2010 10:49 27/08/2010 10:49 27/08/2010 10:49 - 4

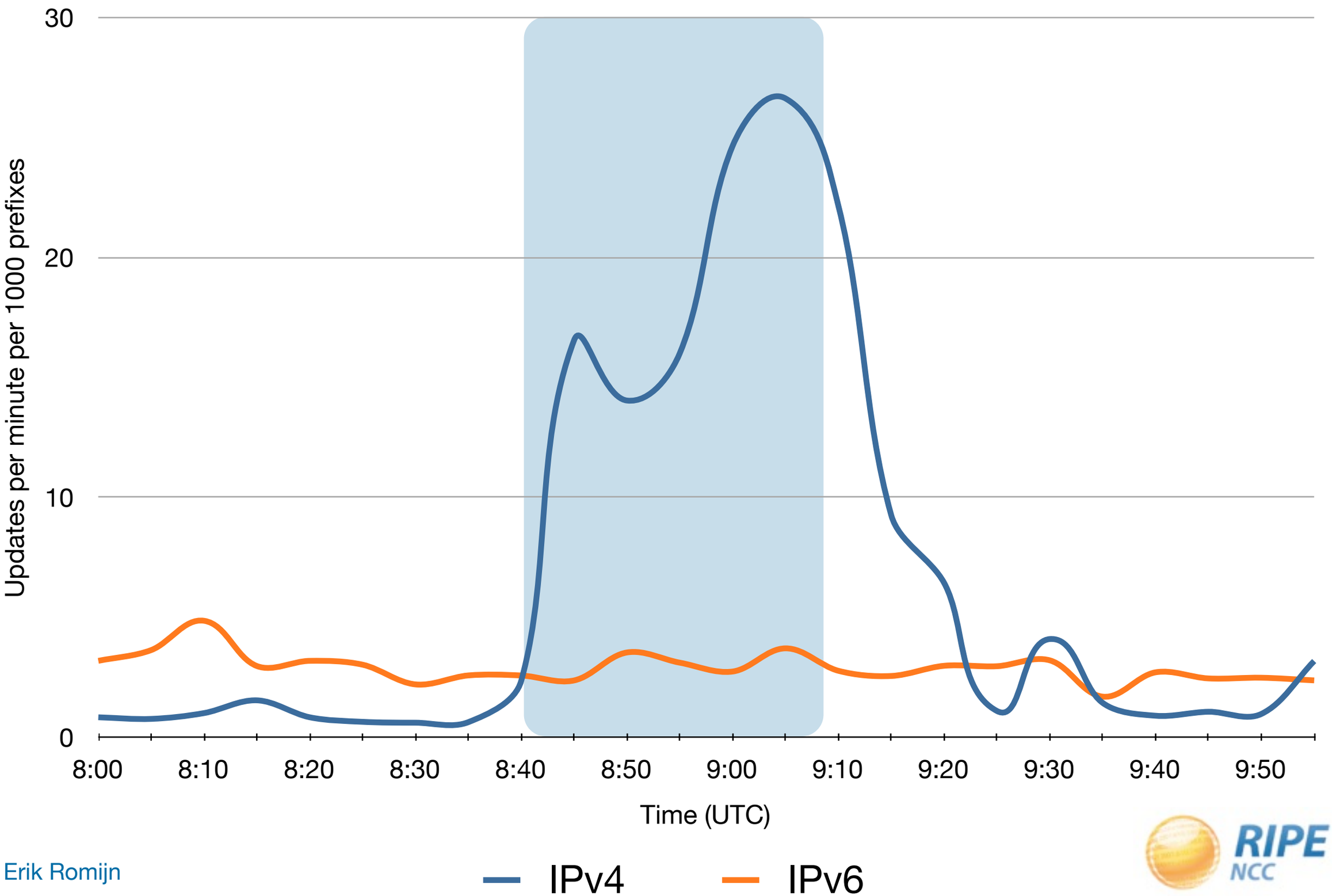
1 update

Animate reannouncements

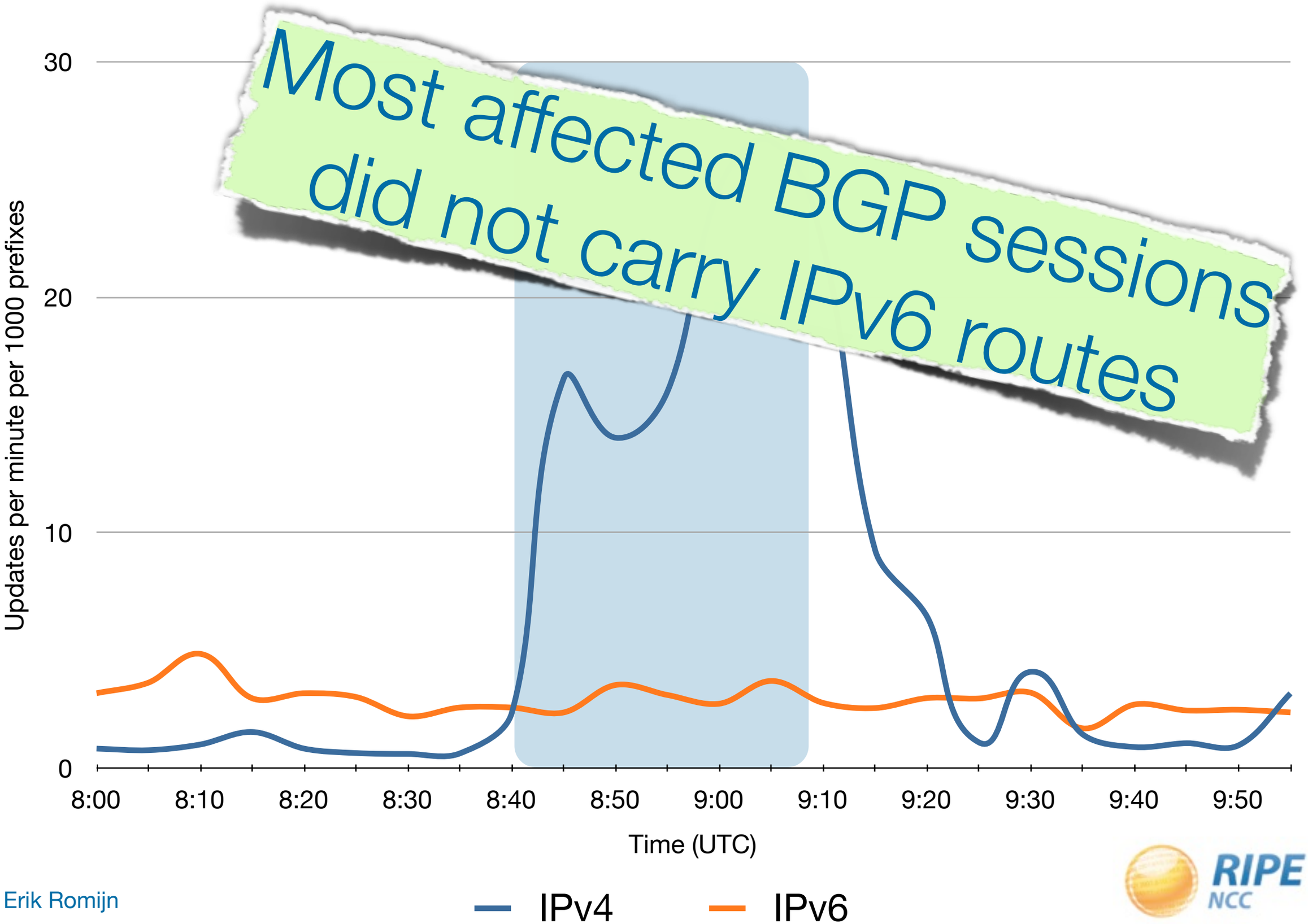
View from a TTM probe in Prague, CZ



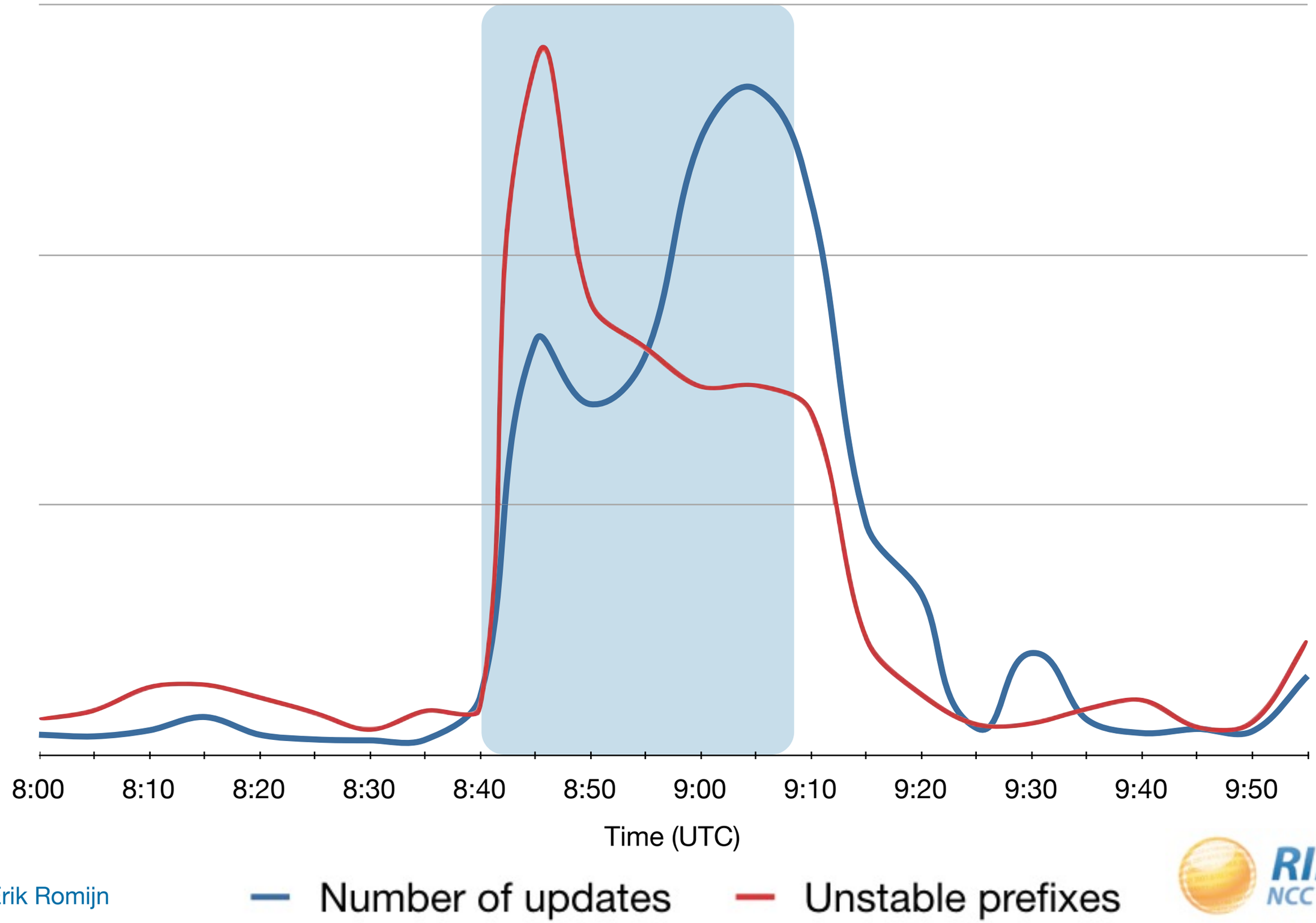
Updates for IPv4 vs IPv6



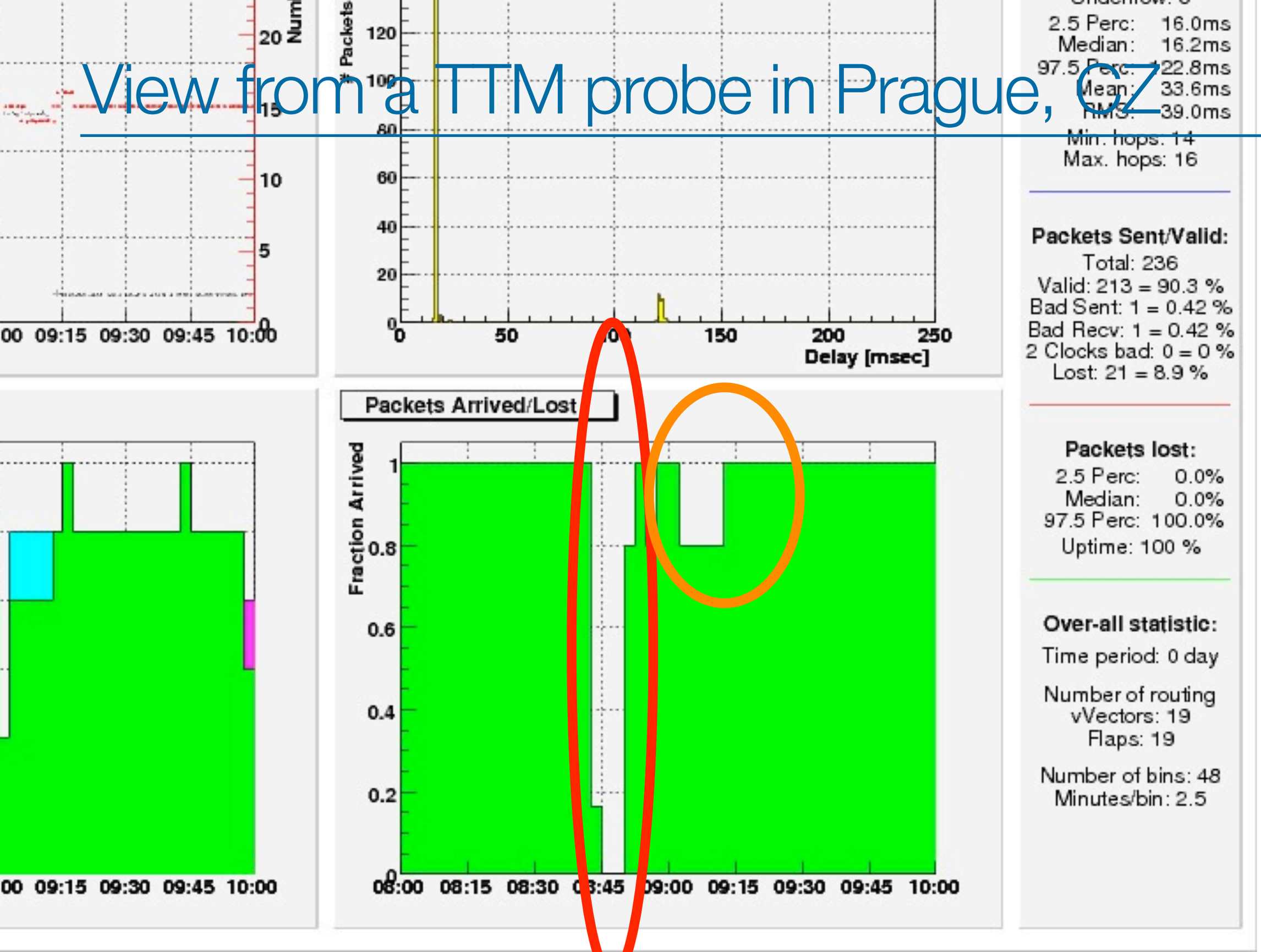
Updates for IPv4 vs IPv6



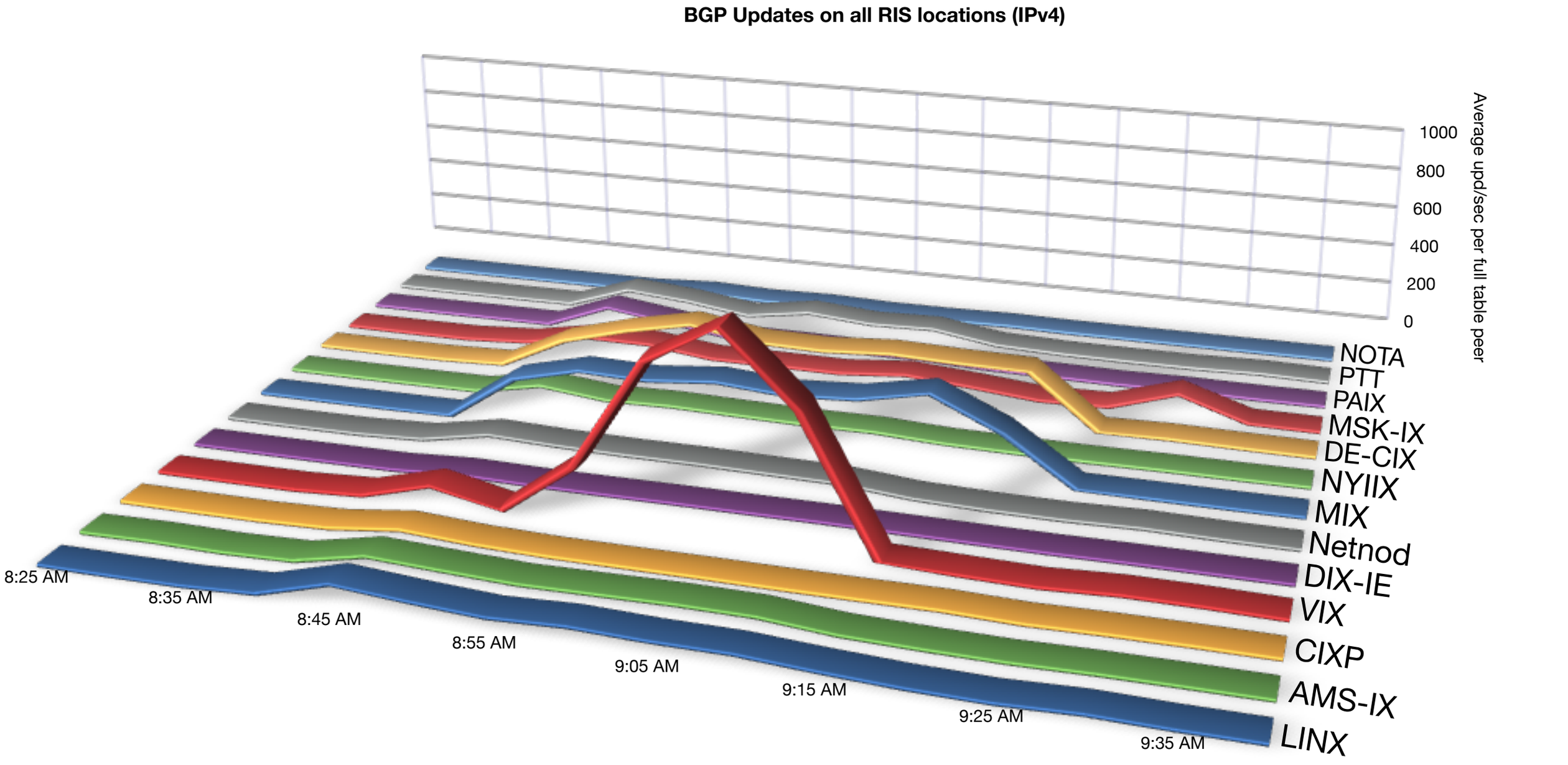
Unstable prefixes vs number of updates



View from a TTM probe in Prague, CZ

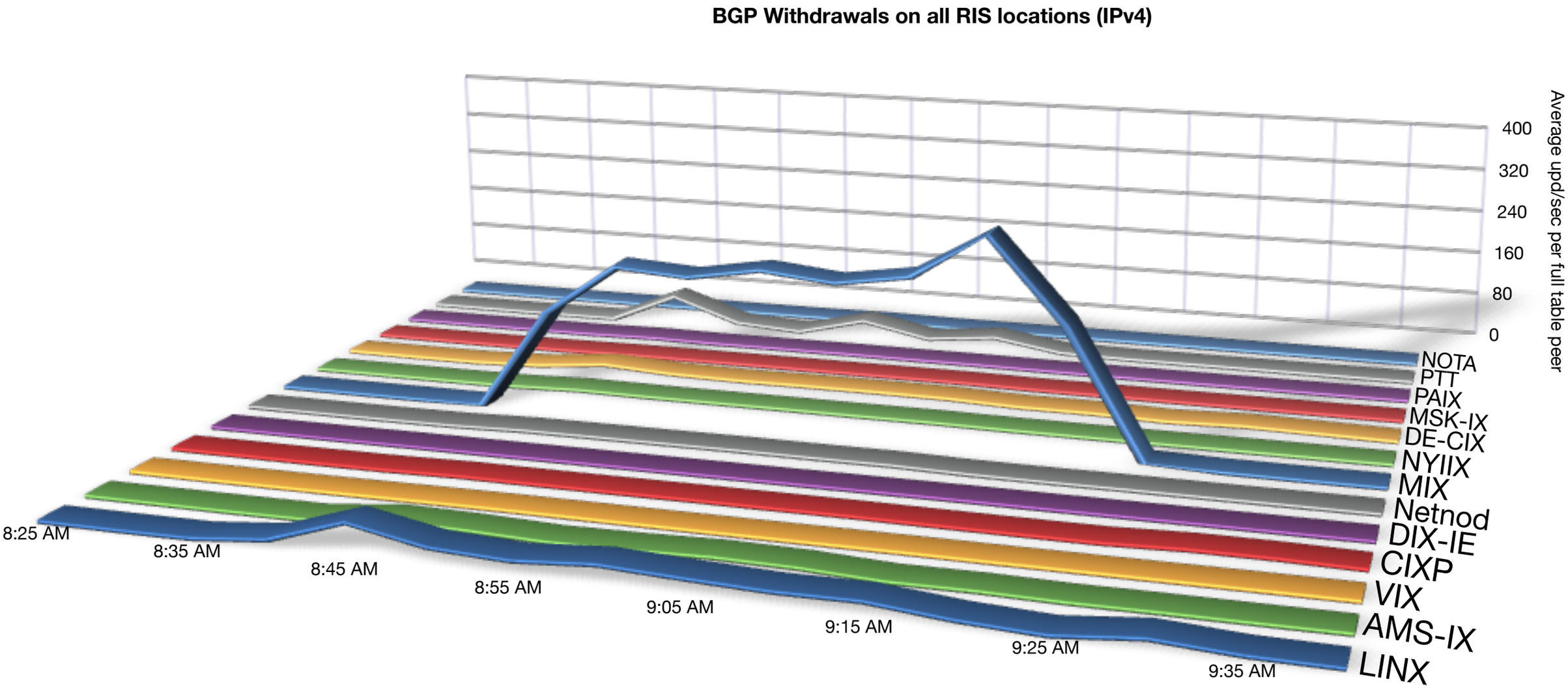


Locality of effects - updates



- LINX, London
- CIXP, Geneva
- DIX-IE, Tokyo
- MIX, Milan
- DE-CIX, Frankfurt
- PAIX, Palo Alto
- NOTA, Miami
- AMS-IX/NL-IX/GN-IX, Amsterdam
- VIX, Vienna
- Netnod, Stockholm
- NYIIX, New York
- MSK-IX, Moscow
- PTT, Sao Paulo

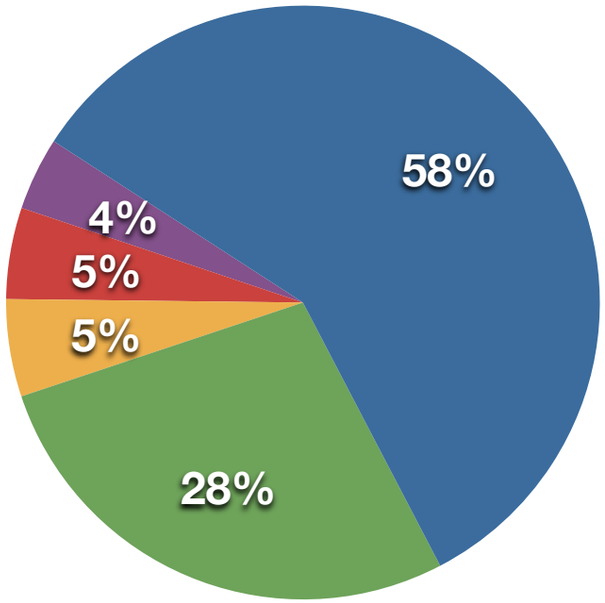
Locality of effects - withdrawals



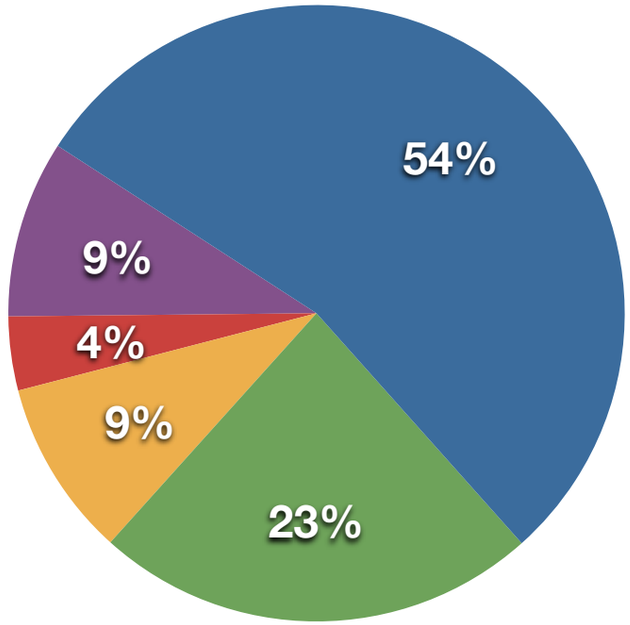
- LINX, London
- CIXP, Geneva
- DIX-IE, Tokyo
- MIX, Milan
- DE-CIX, Frankfurt
- PAIX, Palo Alto
- NOTA, Miami
- AMS-IX/NL-IX/GN-IX, Amsterdam
- VIX, Vienna
- Netnod, Stockholm
- NYIIX, New York
- MSK-IX, Moscow
- PTT, Sao Paulo

Locality of effects - vendors per IX

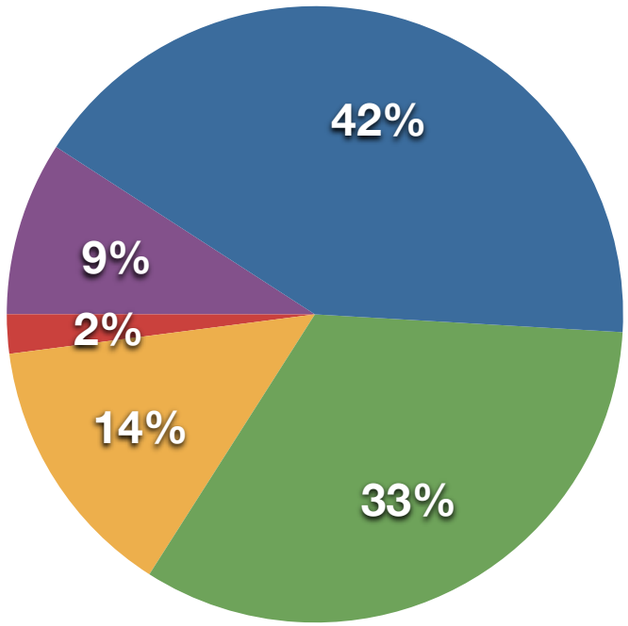
LINX



NYIIX

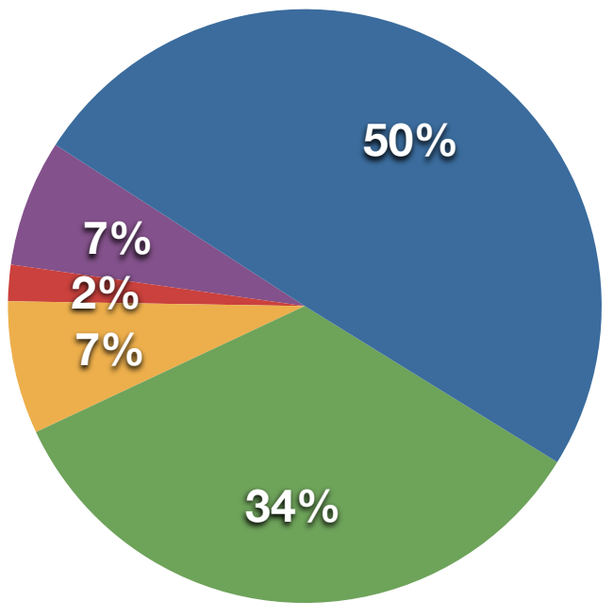


AMS-IX

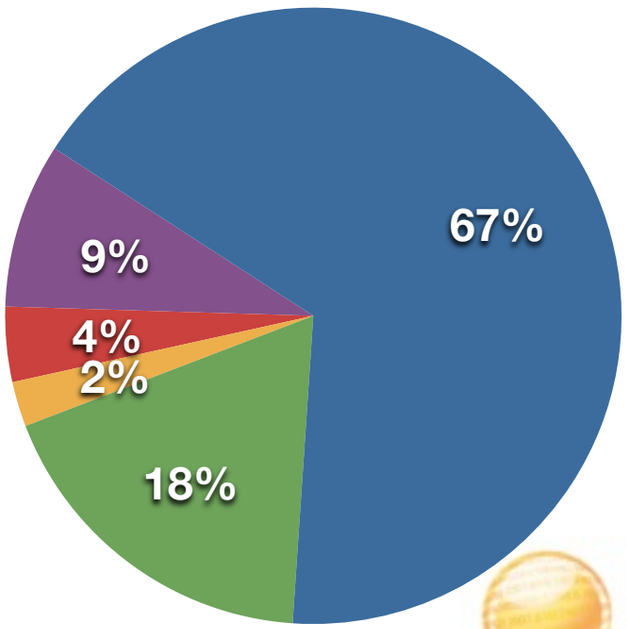


- Cisco
- Juniper
- Brocade
- Intel
- Other

DE-CIX



VIX



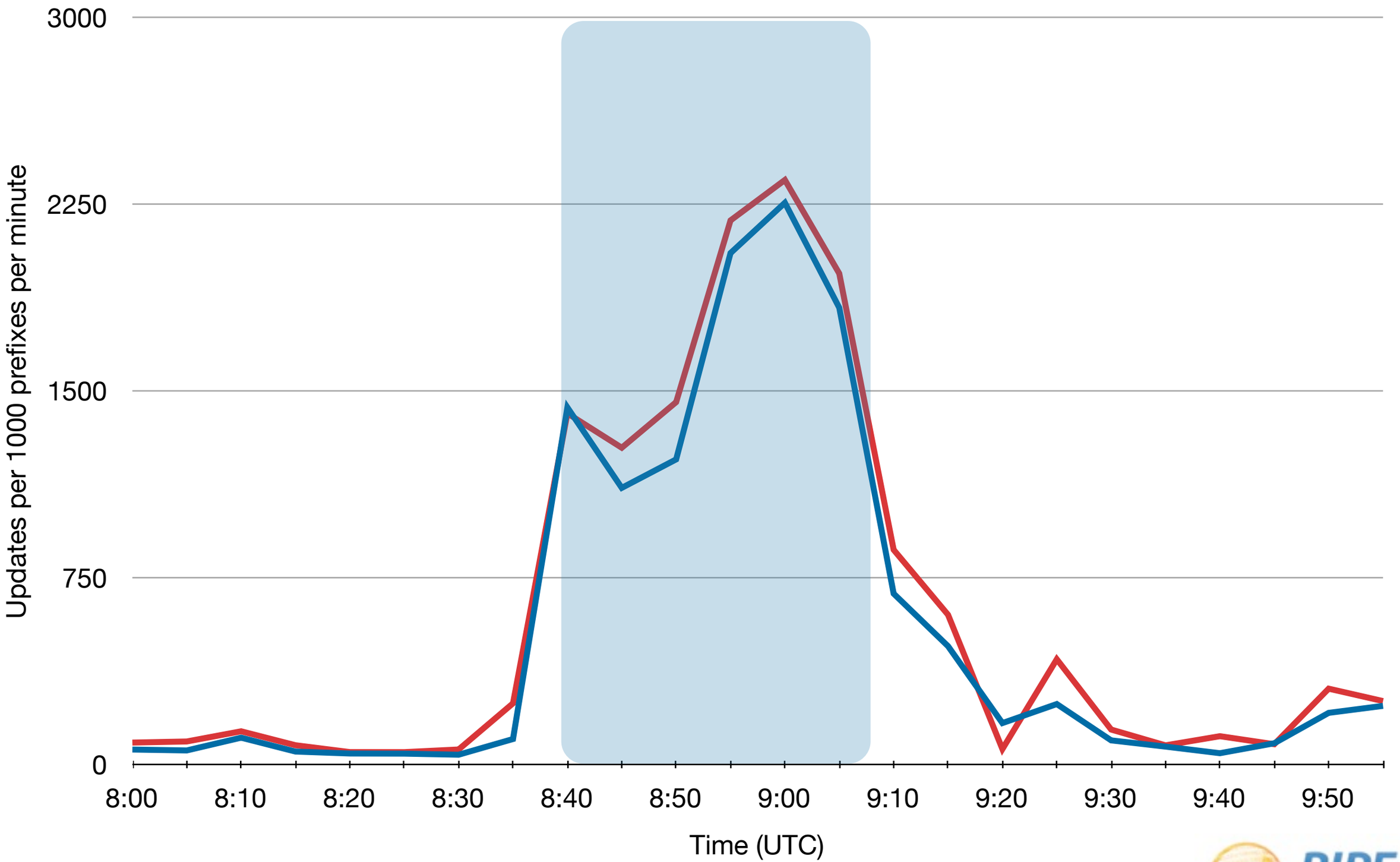
Lessons learned

- Future experiments should be pre-announced with sufficient lead time
- Detected vulnerabilities should be handled with more care
- More comprehensive impact assessments are needed
- Your input is welcome: <ris@ripe.net>

Questions?

Erik Romijn <eromijn@ripe.net>

Updates per prefix range



AS path length