

FCC Workshop on Network Resiliency 2013

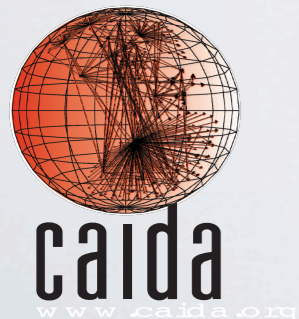
6 February, 2013 - Brooklyn, New York, USA

Lessons learned by "measuring" the Internet during/after the Sandy storm

Emile Aben*, Alistair King, Karyn Benson, Young Hyun,
Alberto Dainotti, KC Claffy

alberto@caida.org

Cooperative Association for Internet Data Analysis



*RIPE NCC

ANALYSIS OF INTERNET OUTAGES

By combining different measurement sources

- BGP
 - BGP updates from route collectors of **RIPE-NCC RIS** and **RouteViews**
- Active Traceroute Probing
 - Archipelago Measurement Infrastructure (**ARK**)
 - **RIPE-NCC Atlas**
- Internet Background Radiation (IBR)
 - Traffic reaching the **UCSD Network Telescope**
- *more data sources to come...*



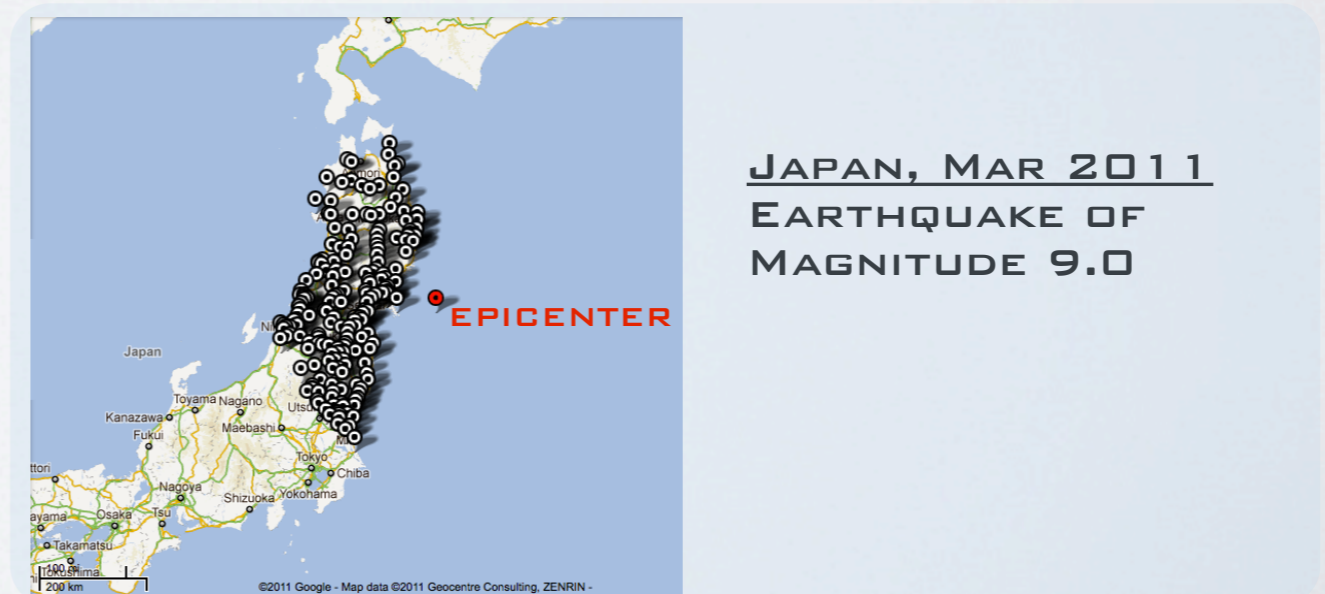
CASE STUDIES

Different for causes/tech implications/impact

- Country-level Internet Blackouts
(*BGP withdrawals, packet-filtering, satellite-signal jamming, ...*)



- Natural disasters affecting the infrastructure/population



SANDY: IS IT DIFFERENT?

(compared to our previous case studies)

- Movement over a large area
 - with no fixed epicenter like an earthquake has
- High level of Internet penetration in the affected region, including major hubs for international Internet connectivity
- Disruption was limited to only a subset of networks/hubs in the affected region, making it harder to identify geographic areas of massive impact
- For the 1st time we tried to measure in realtime

ACTIVE MEASUREMENTS

ARK + ATLAS

- CAIDA ARCHIPELAGO (ARK)
 - Coordinate traceroute-based topology measurement probing the full routed IPv4 address space

<http://www.caida.org/projects/ark/>



- RIPE ATLAS
 - traceroutes/pings to fixed destinations
 - user-defined measurements (a community-oriented tool)

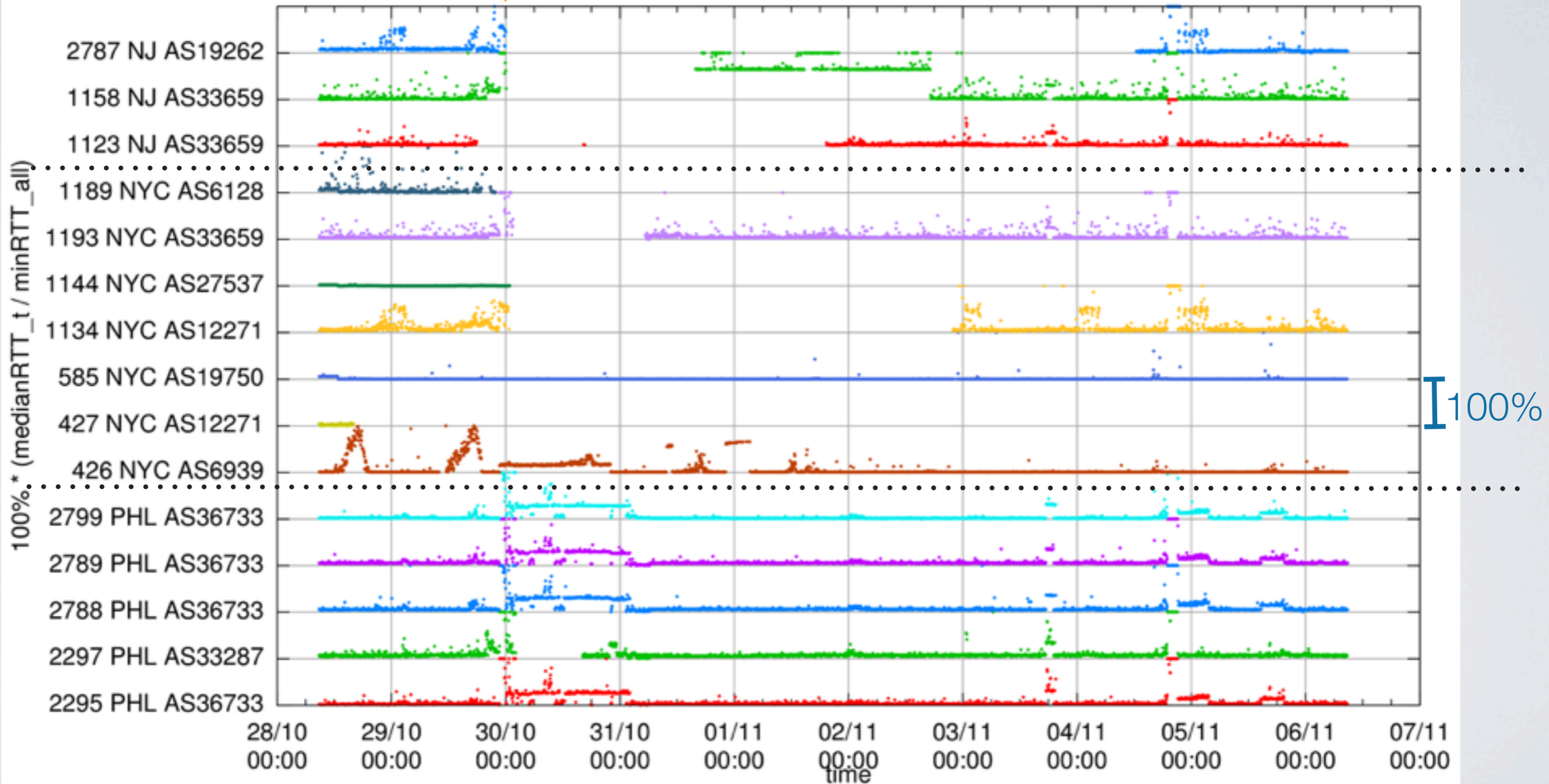
<https://atlas.ripe.net/>



ATLAS: RTT

Sandy Landfall

Probes to dst 1017, relative rtt trends



ATLAS: PATH CHANGES

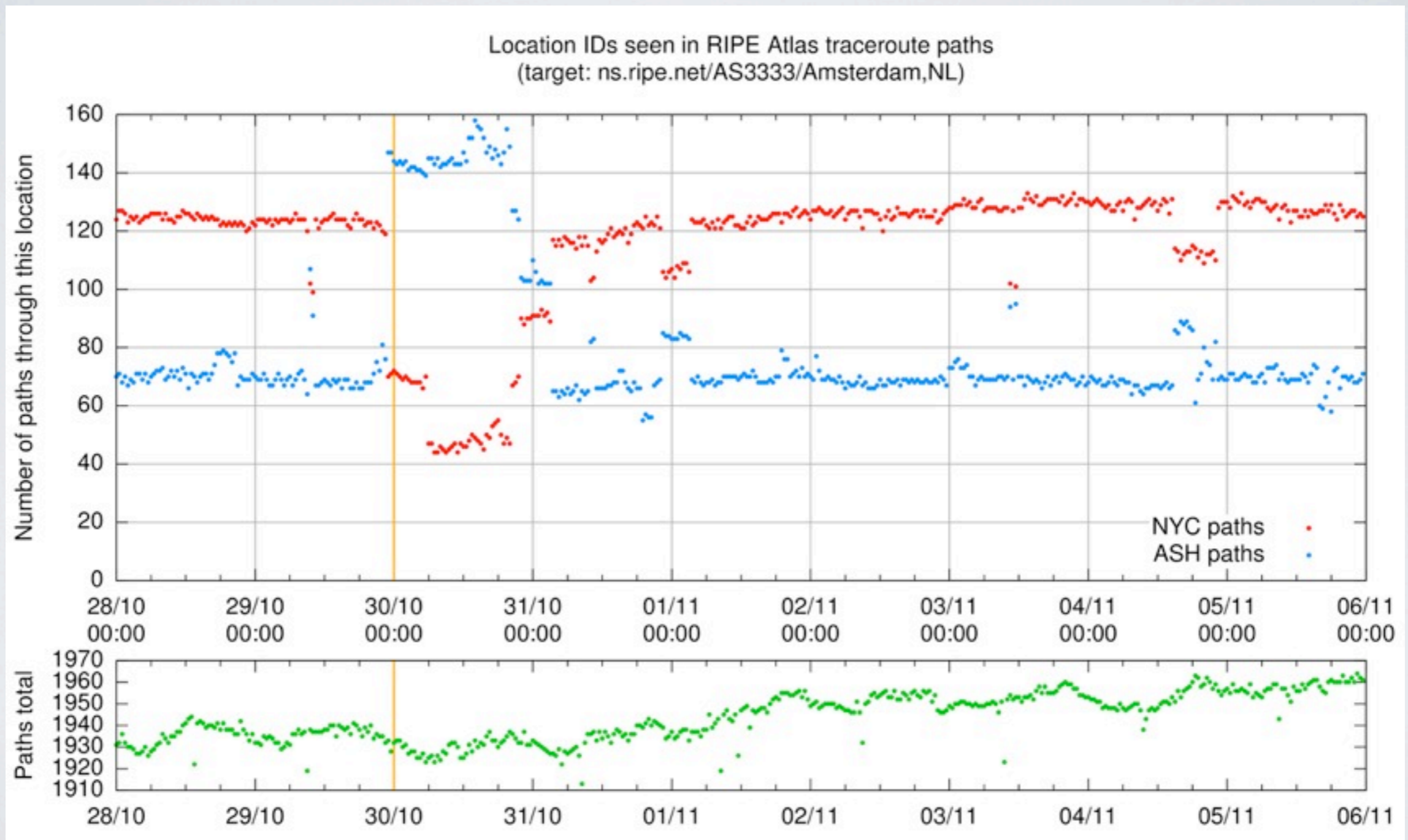
Looking at two major hubs

- New York City (NYC) is a major Internet connectivity hub
- Ashburn/Washington DC (ASH) is the other for US-Europe traffic



ATLAS: PATH CHANGES

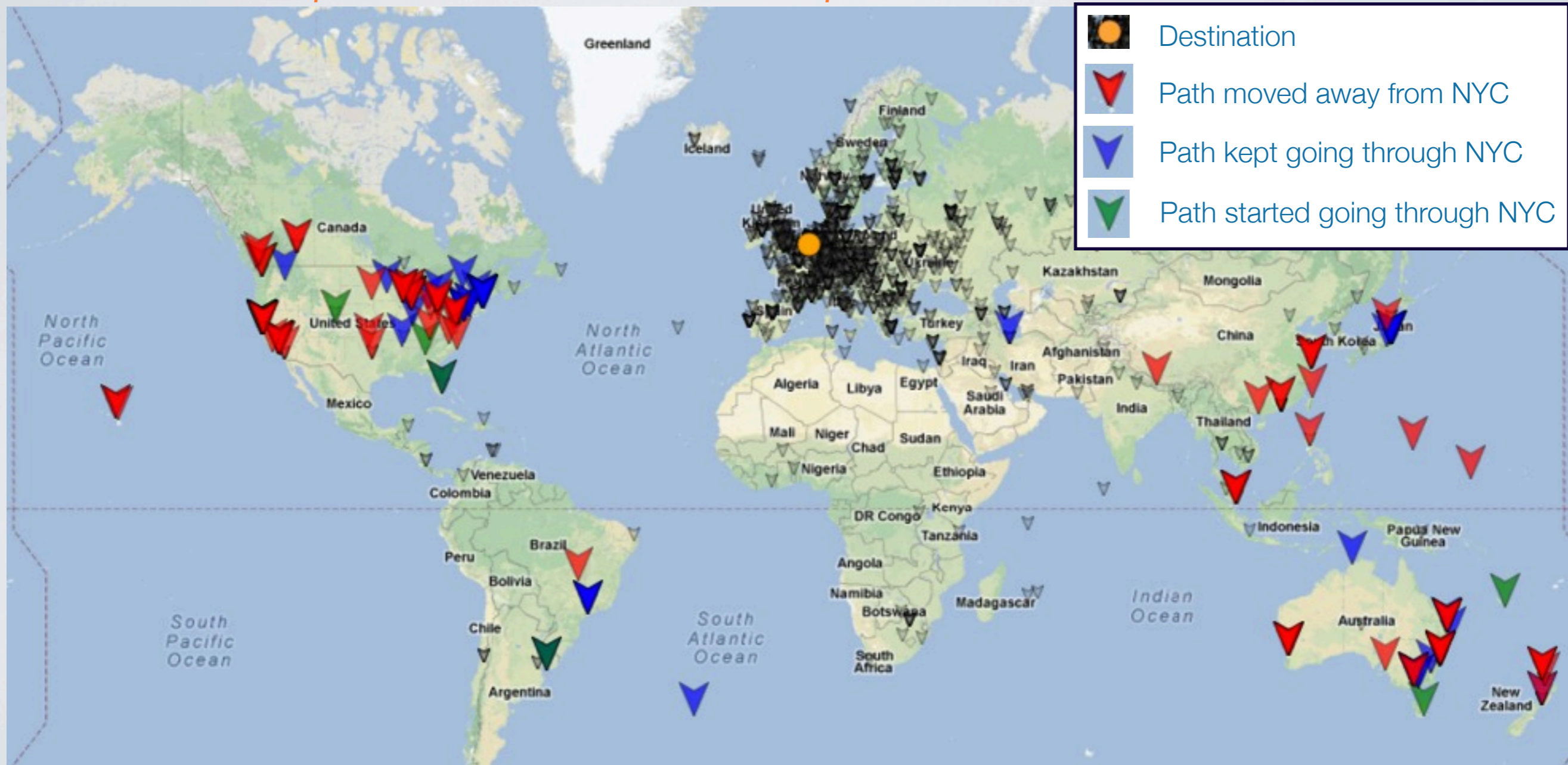
dst: ns.ripe.net / AS3333 / NL



ATLAS: NYC PATH CHANGES

dst: ns.ripe.net / AS3333 / NL

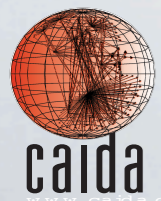
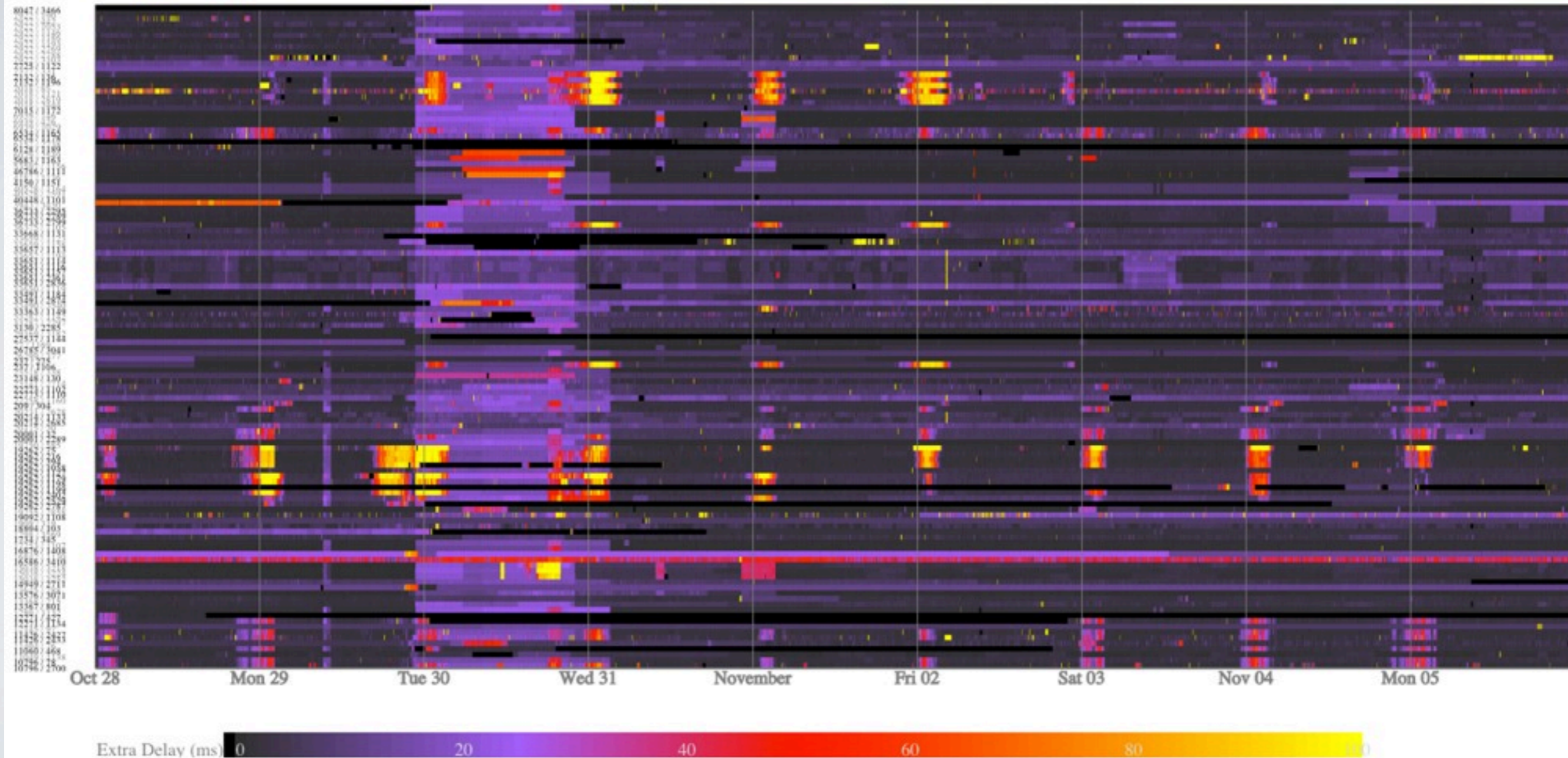
pre: 22:00 UTC vs. post: 09:00 UTC



ATLAS: LATENCY

RTT US -> AS3333/NL (+20 ms)

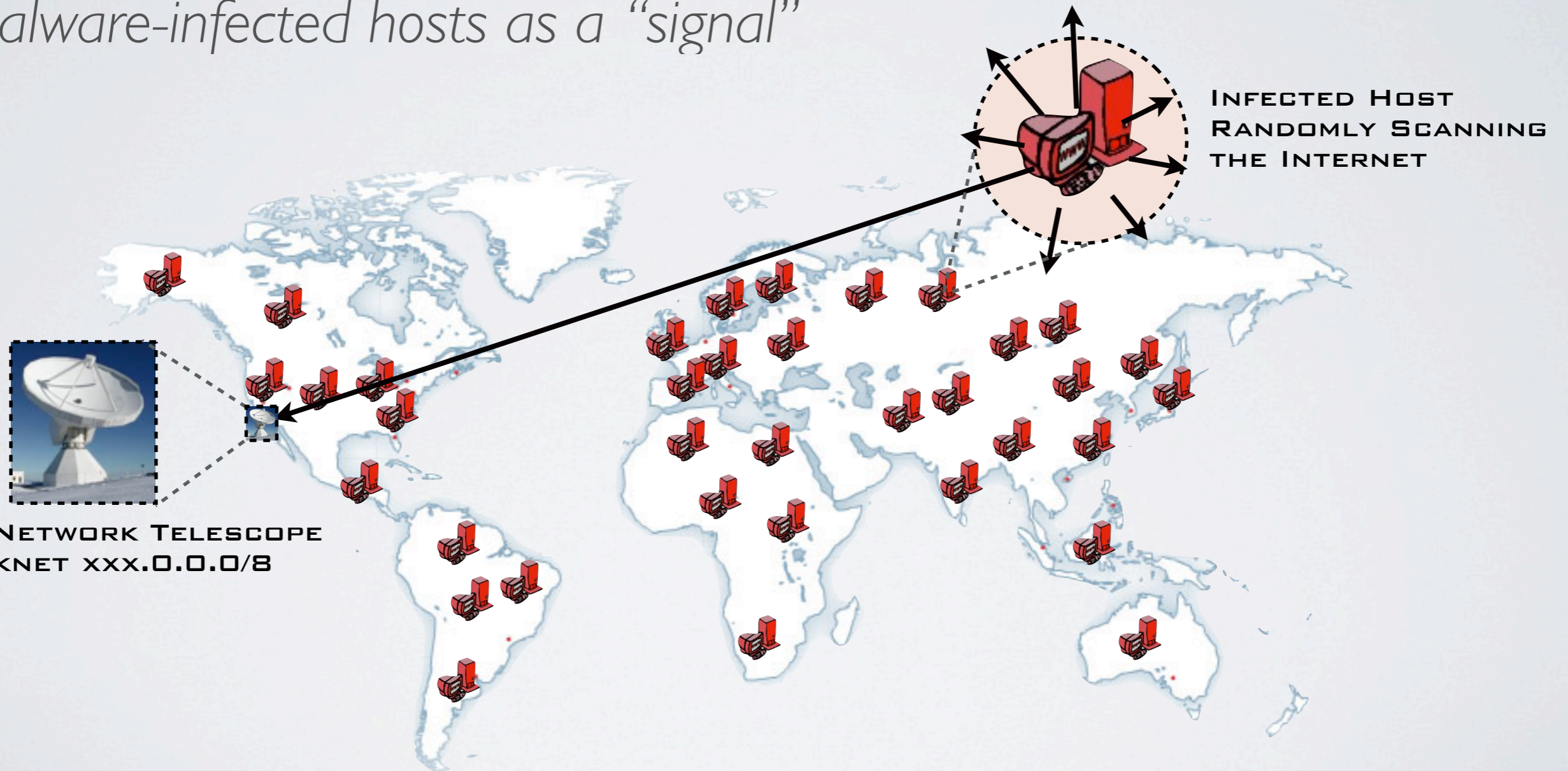
RTT increase (relative to the minimum RTT seen) Source: US Dst: 1003



IBR

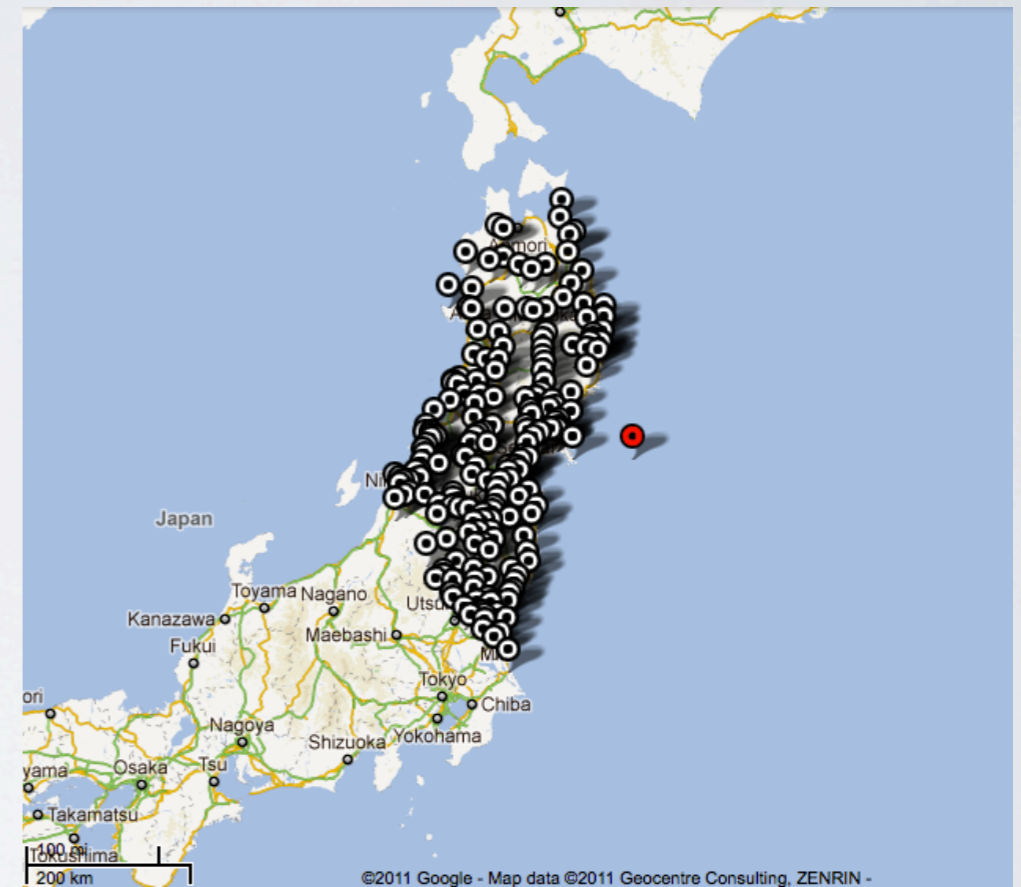
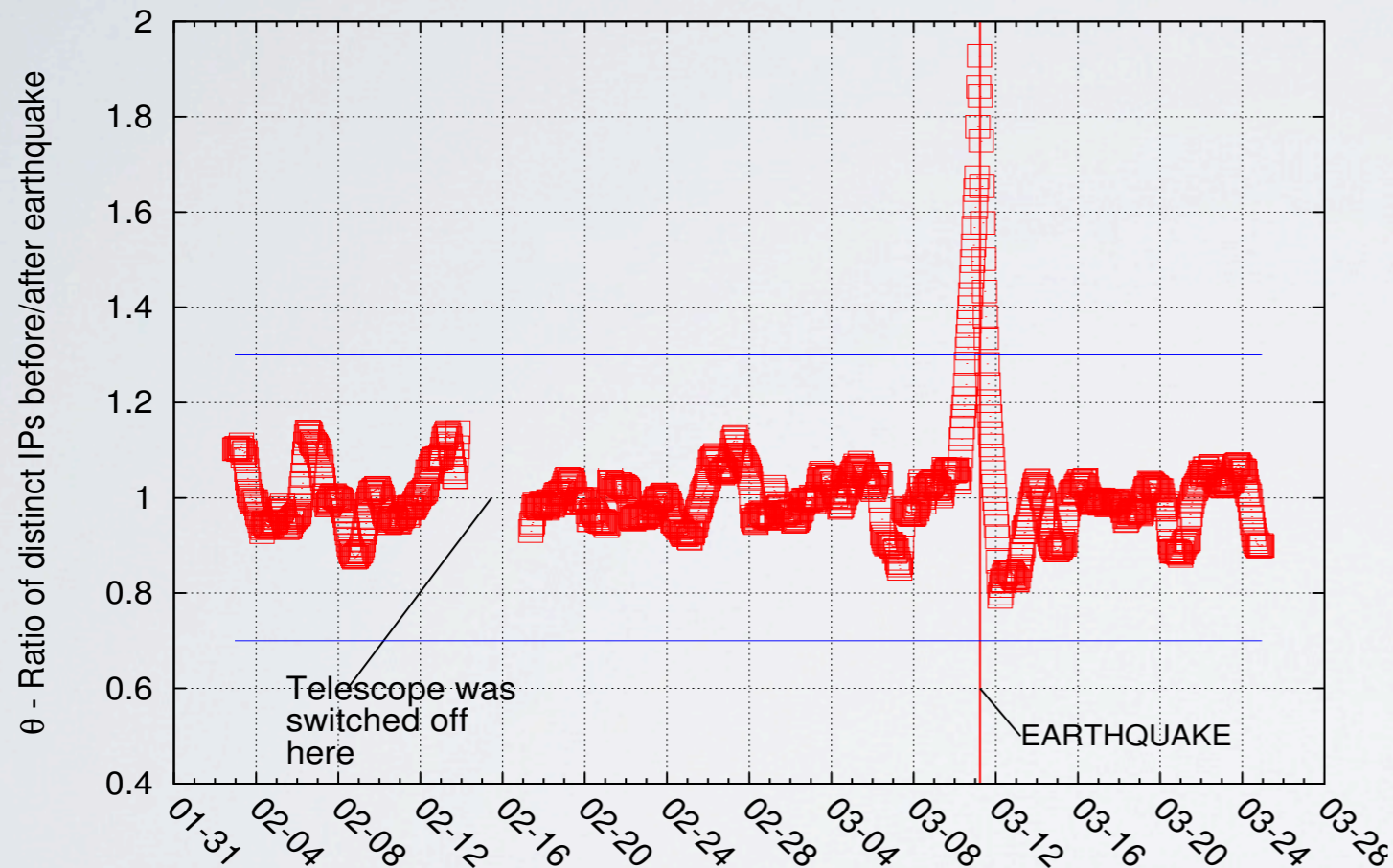
“Extracting benefit from harm..”

- Use *Internet Background Radiation (IBR)* generated by *malware-infected hosts* as a “signal”



IBR: TOHOKU'S EARTHQUAKE

the effect of the 2011 earthquake/tsunami in Japan



Extracting Benefit from Harm: Using Malware Pollution to Analyze the Impact of Political and Geophysical Events on the Internet

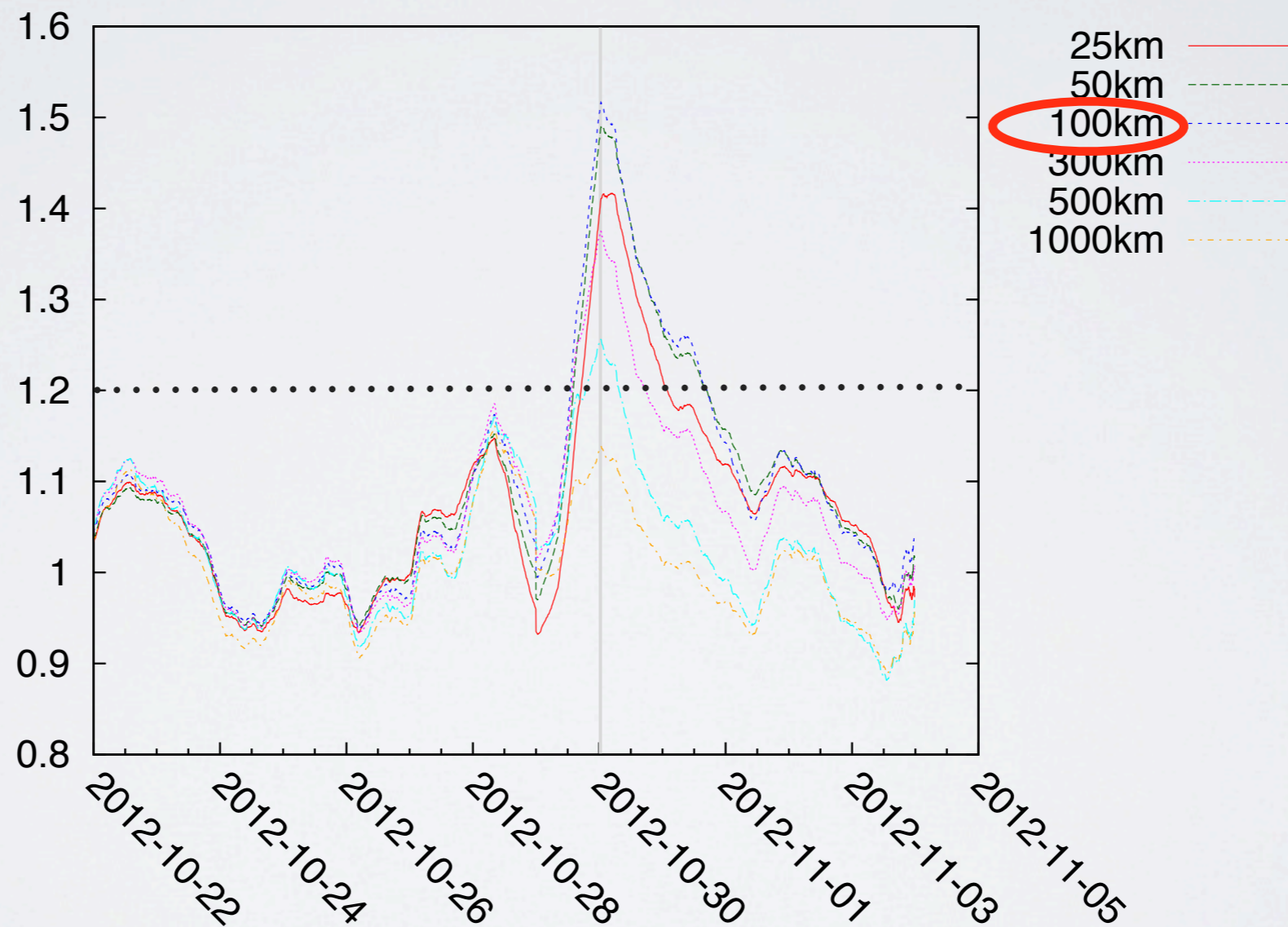
A. Dainotti, R. Amman, E. Aben, K. C. Claffy

ACM SIGCOMM Computer Communication Review, January 2012

Cooperative Association for Internet Data Analysis
University of California San Diego

IBR: SANDY IN NYC

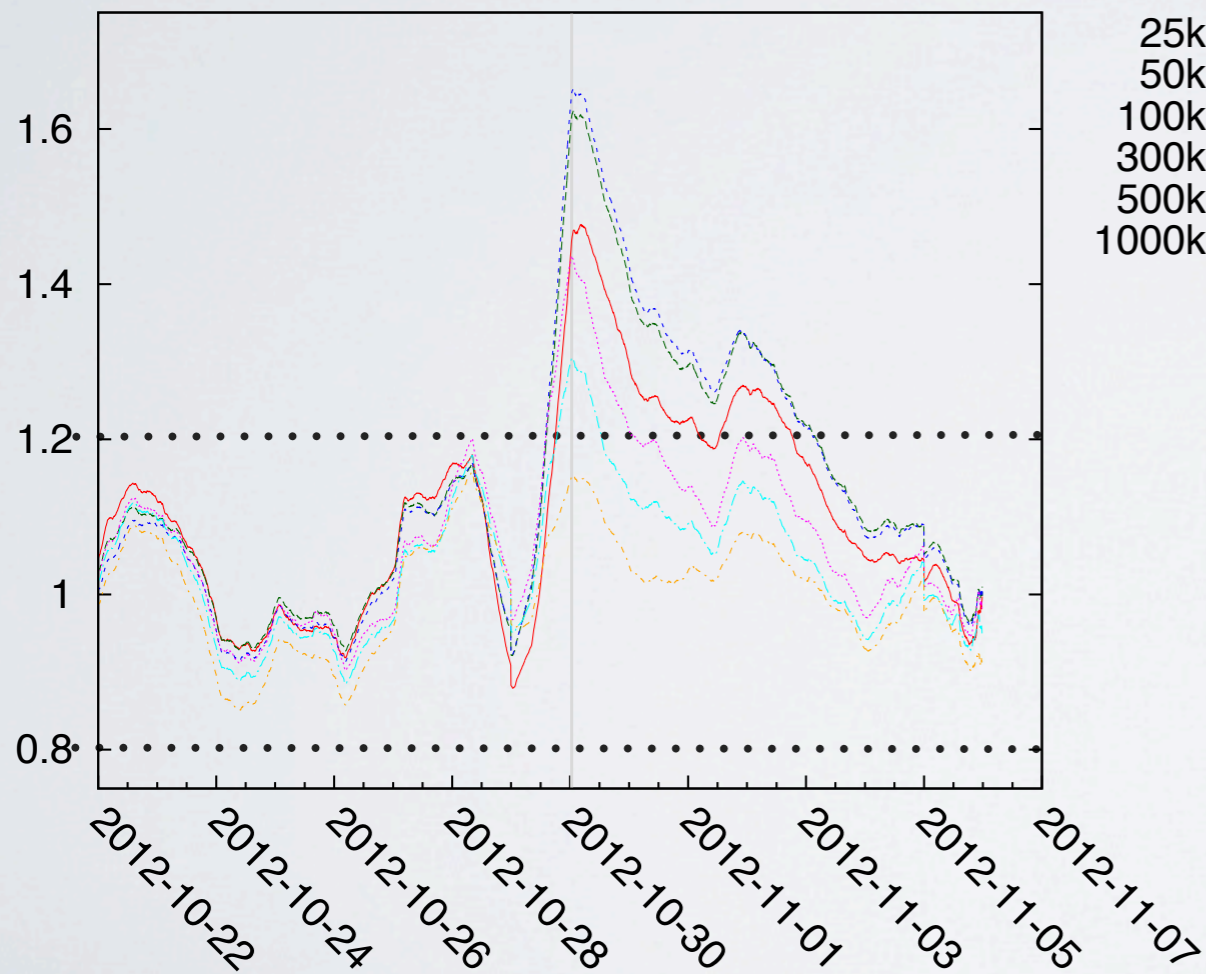
*Reusing the same metric based on
ratio of distinct source IPs*



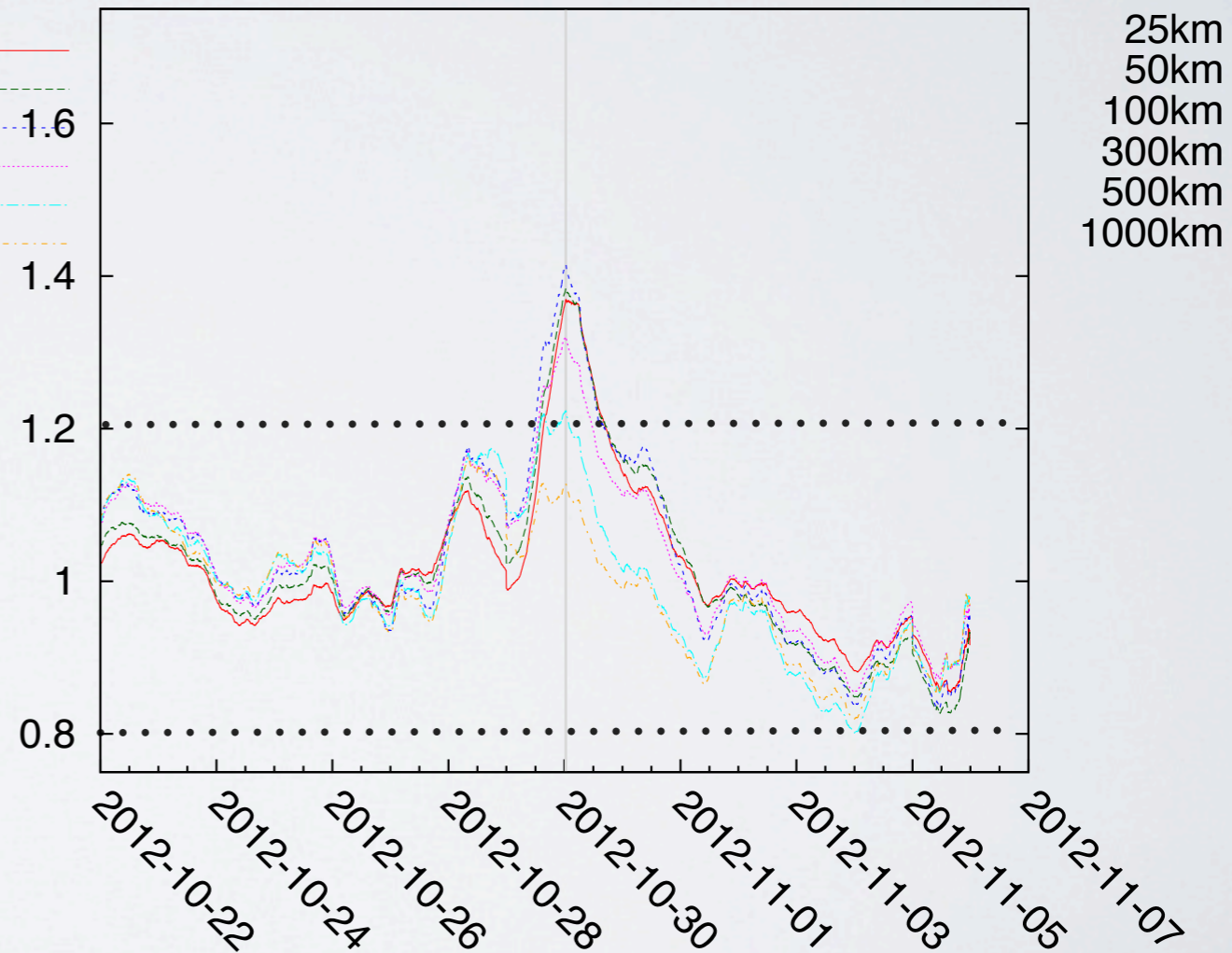
IBR: NY, HOME vs BUSINESS

*Different impact on home vs business users**

Home



Business



*** according to NetAcuity**
www.digitalelement.com/NetAcuity

WISHLIST / CURRENT WORK

(partial list)

- ARK

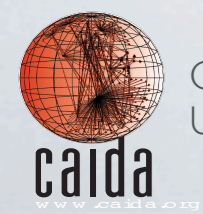
- Increase (time + space) granularity
- *wish*: IP Census data, to be used to improve on-demand probing
- Geo-Ark on demand, for realtime measurements

- Improve tools for geography-based analysis of Internet data

- which helps also with *realtime analysis* and *combining* different measurements

- Geolocation of BGP-advertised prefixes
- Fast/interactively-visual selection of network blocks/prefixes
- Implement different cartography/geo-analysis techniques (e.g., for IBR)
- Realtime/Interactive geographical visualization

THANKS



Cooperative Association for Internet Data Analysis
University of California San Diego

