Combining Active and Passive Monitoring

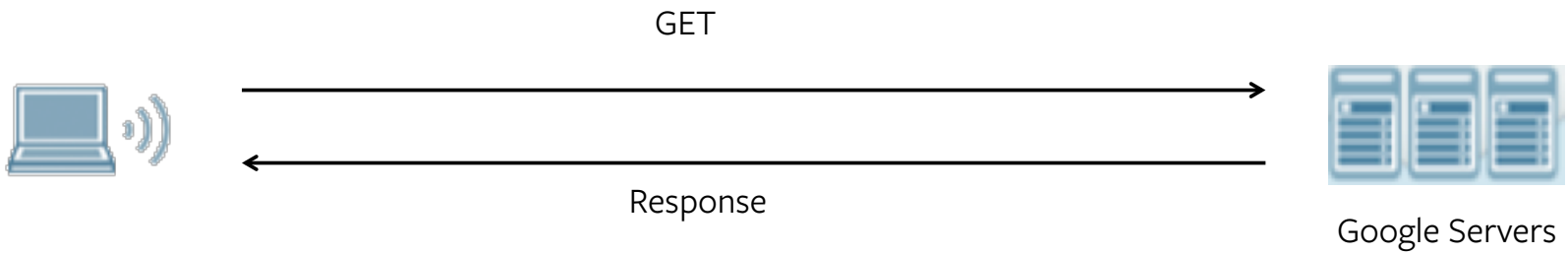
Mohit Lad
CEO, ThousandEyes
mohit@thousandeyes.com

Basics

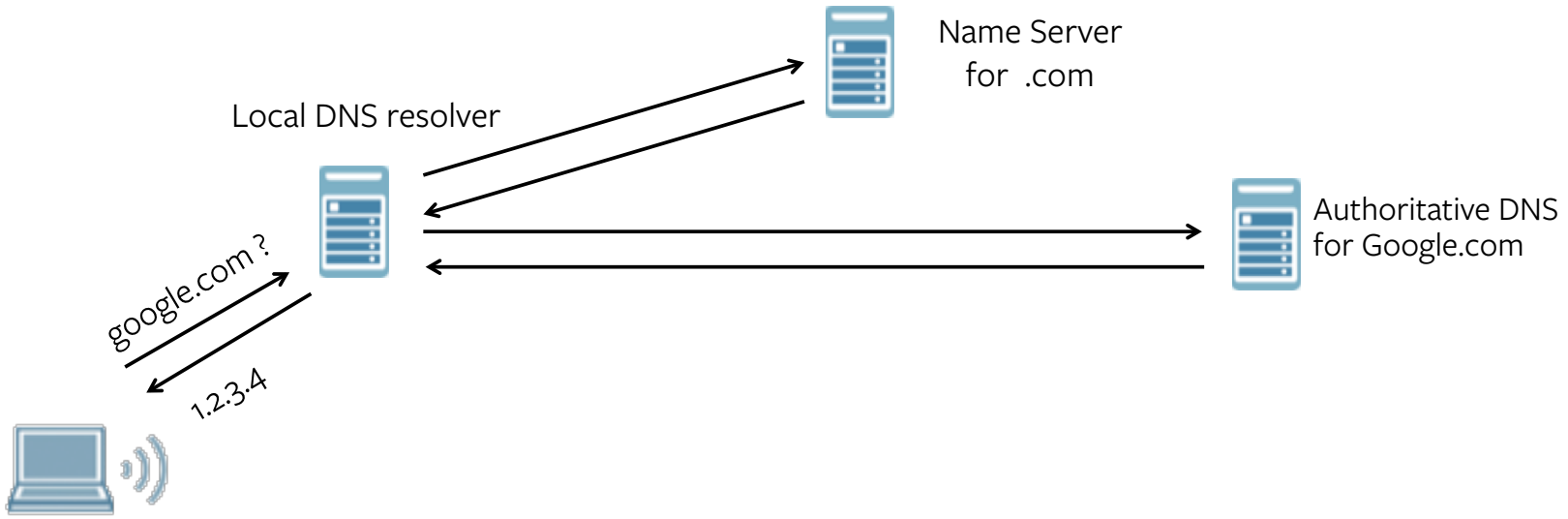
- Passive Monitoring
  - Capture traffic from the network by generating a copy of the traffic usually via a span port, mirror port or network tap
  - Typical Use: Discover what is going on

- Active Probing
  - Generating a synthetic probe that will discover information and report back
  - Examples: ping, traceroute
  - Typical Use: Find the root cause

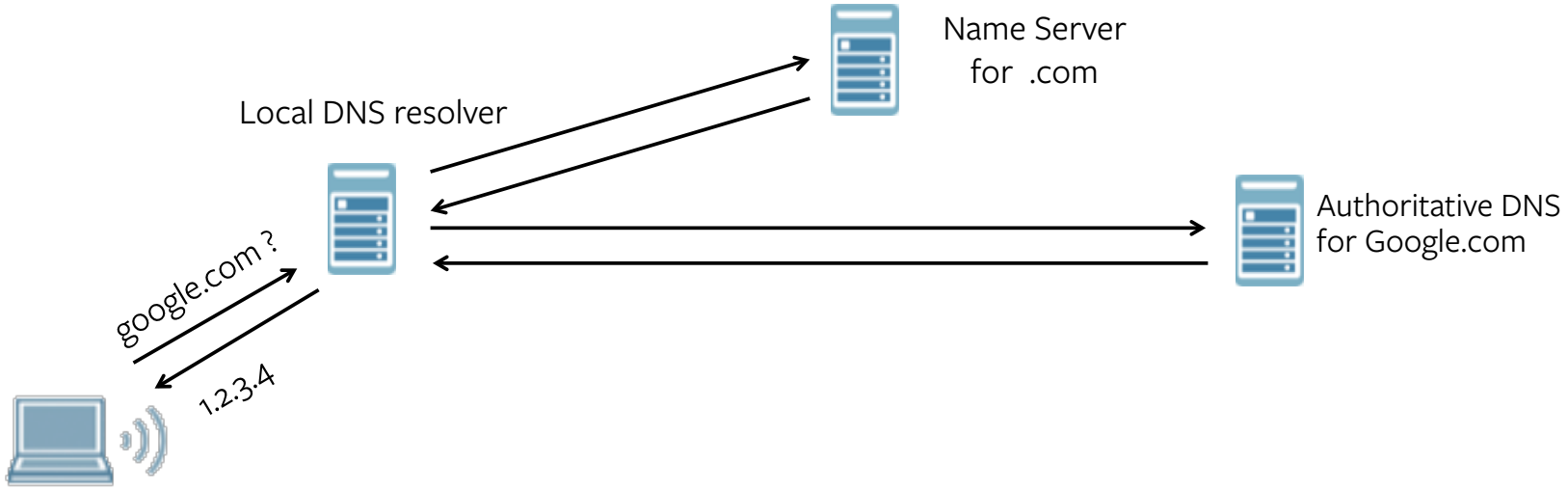
Example: Google does not load



Example: Google does not load: Step 1 DNS resolution

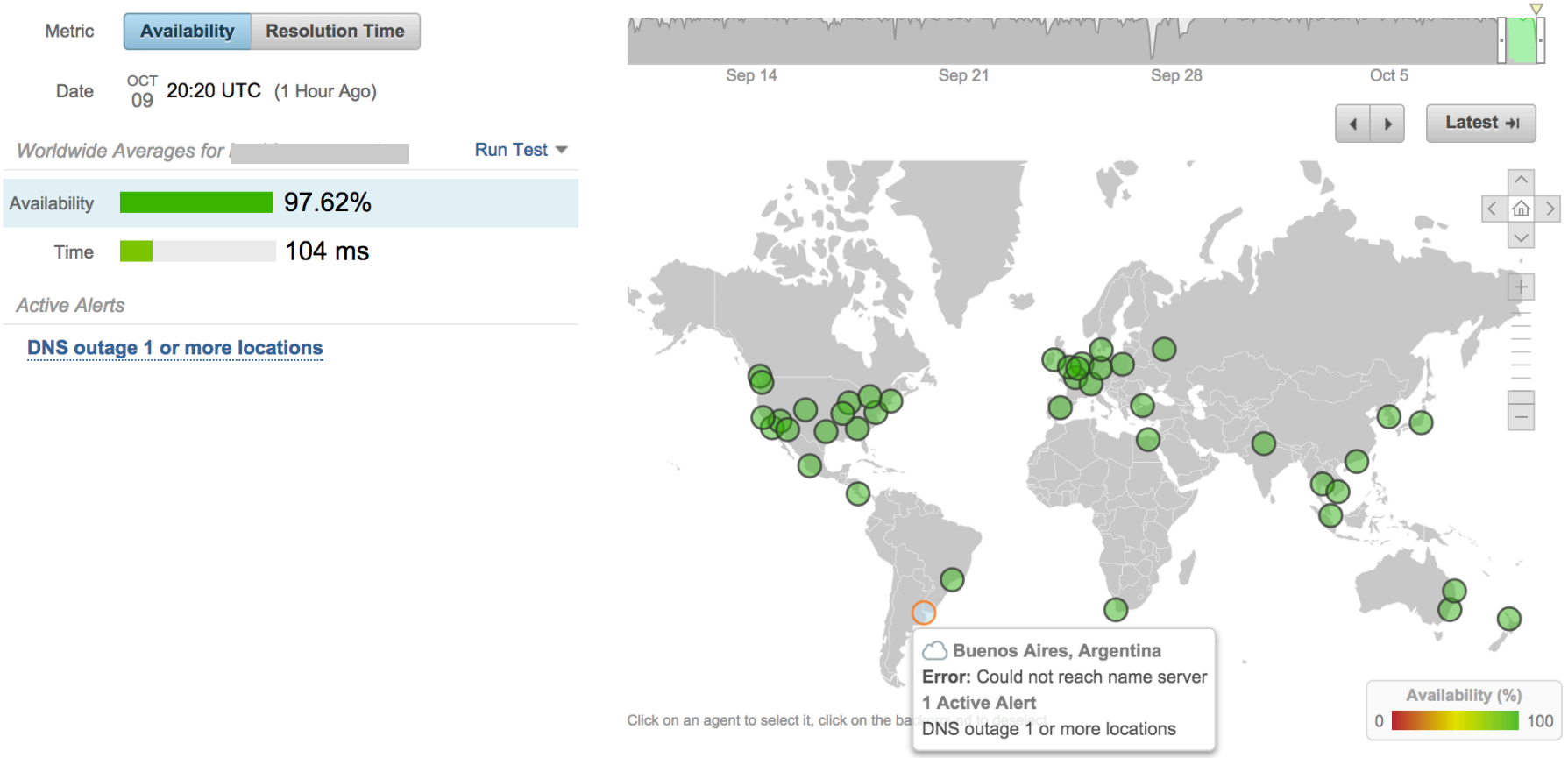


Probing for DNS issues



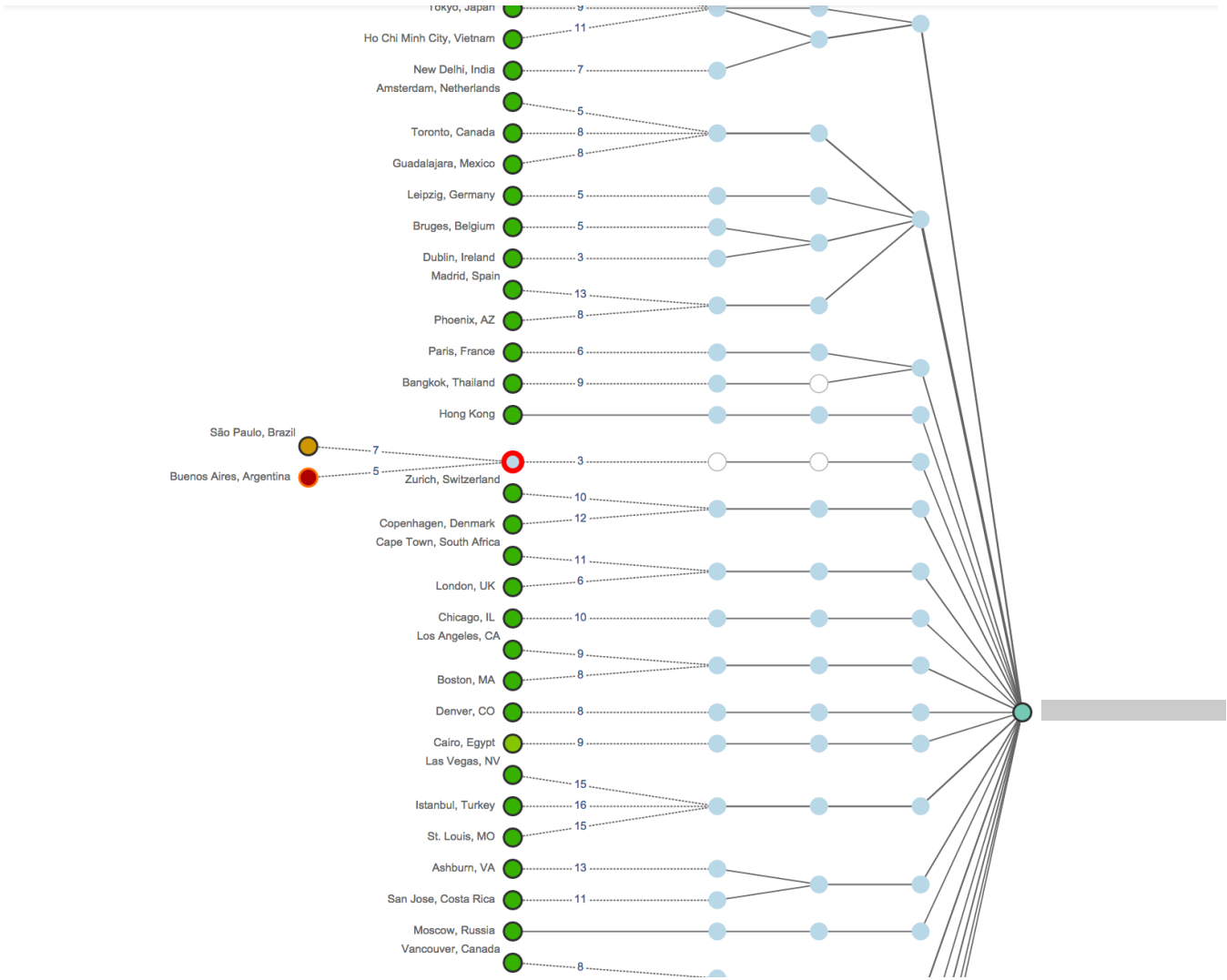
- Tcpdump on client -> tells us if we get a DNS reply or not
- What if we don't get a reply?
  - Check for resolver, returns replies to other domains
  - Troubleshoot DNS from resolver to Google
- If we get a reply, is DNS working?

Buenos Aires cannot resolve DNS

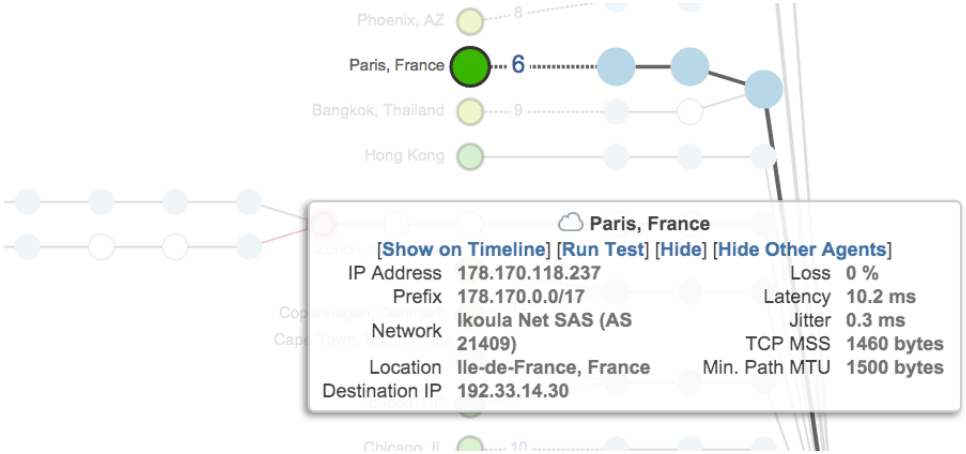


Agent	Date	Mappings	Error Details ↓	Resolution Time (ms)
Buenos Aires, Argentina	2014-10-09 20:21:56		Could not reach name server	

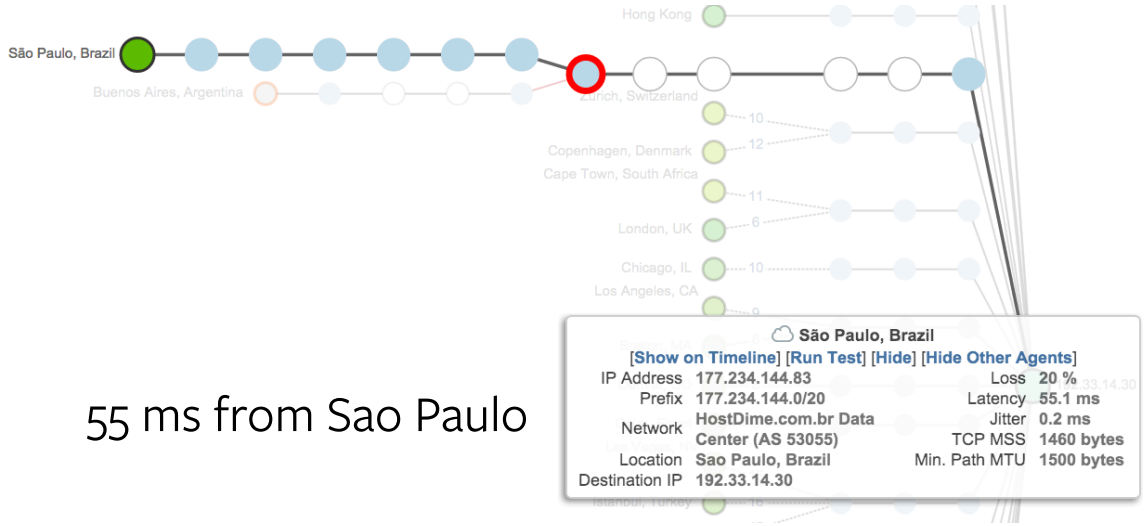
Domain in question is anycasted



How do we know it's anycast?

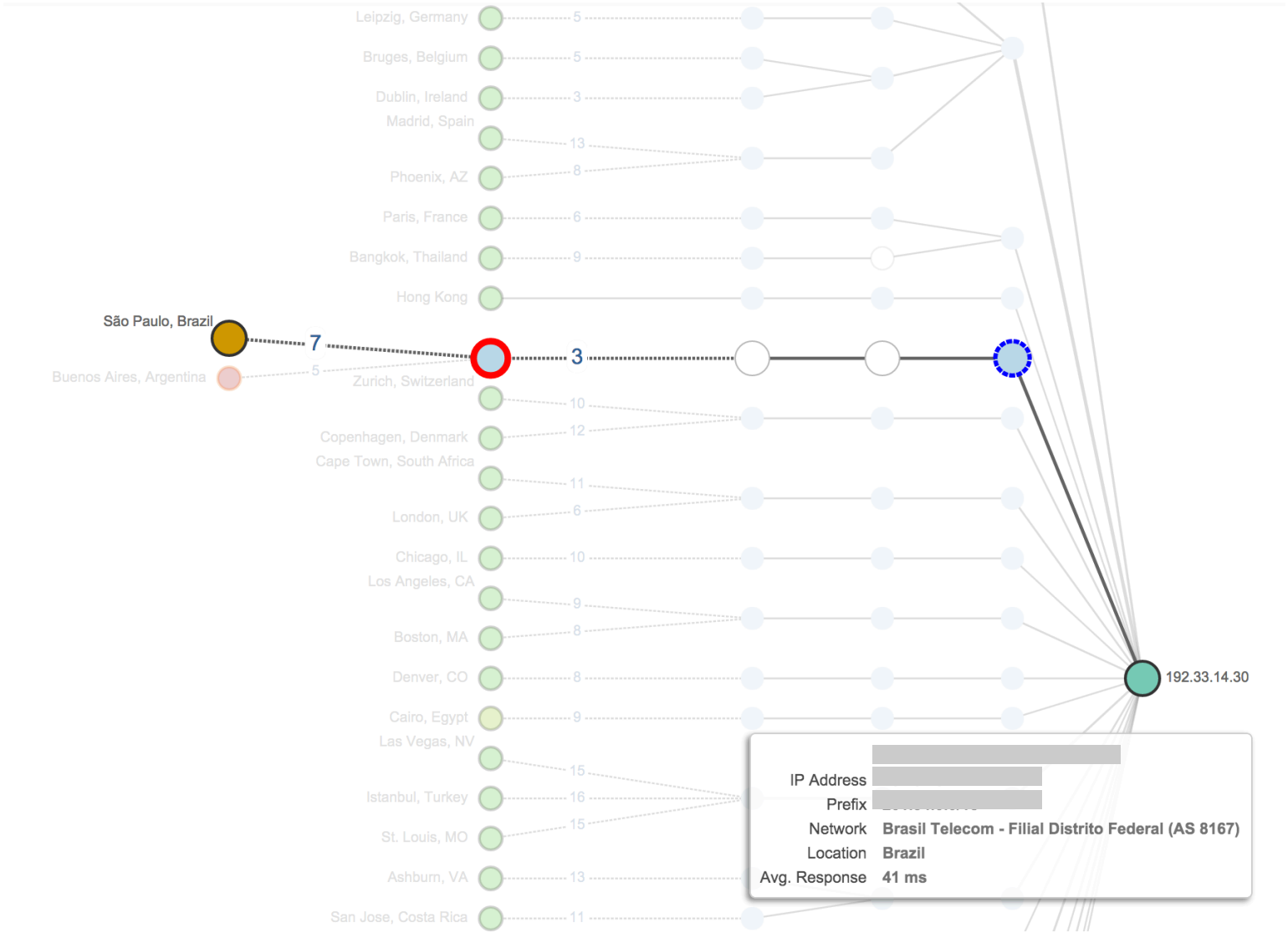


10 ms from Paris

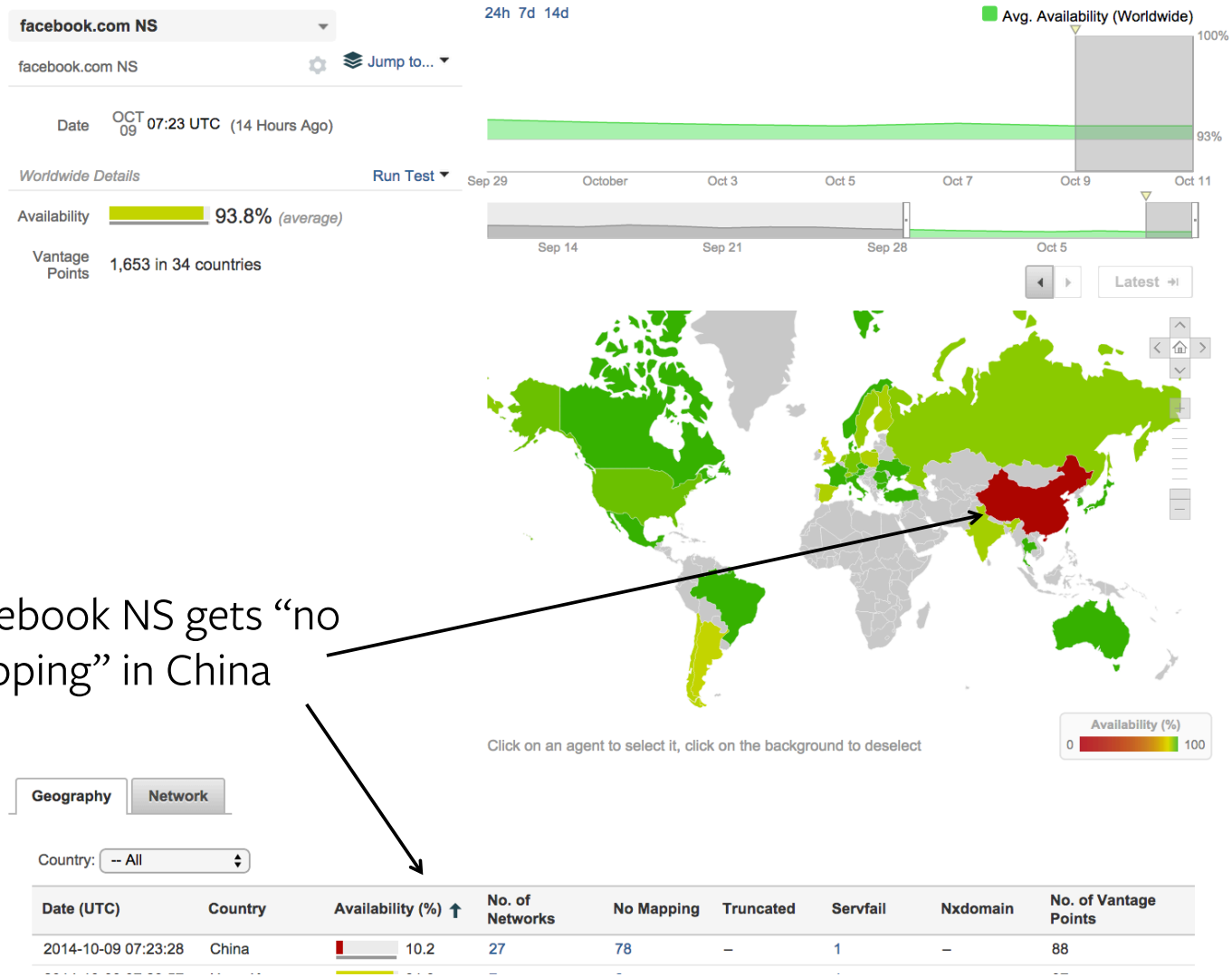


55 ms from Sao Paulo

Identifying the problematic Anycast instance

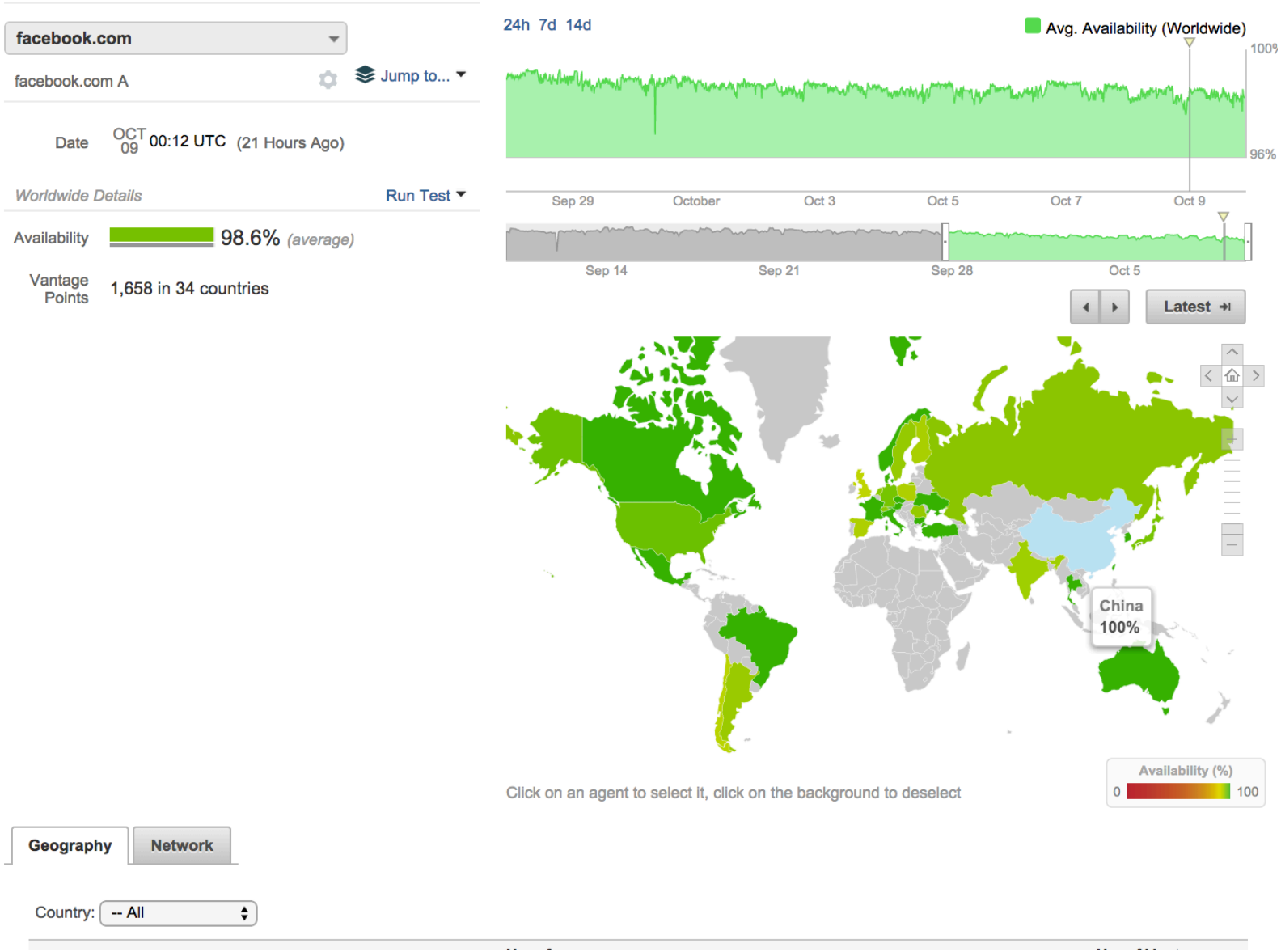


So is everything ok if we get a DNS reply? Lets look at Facebook NS

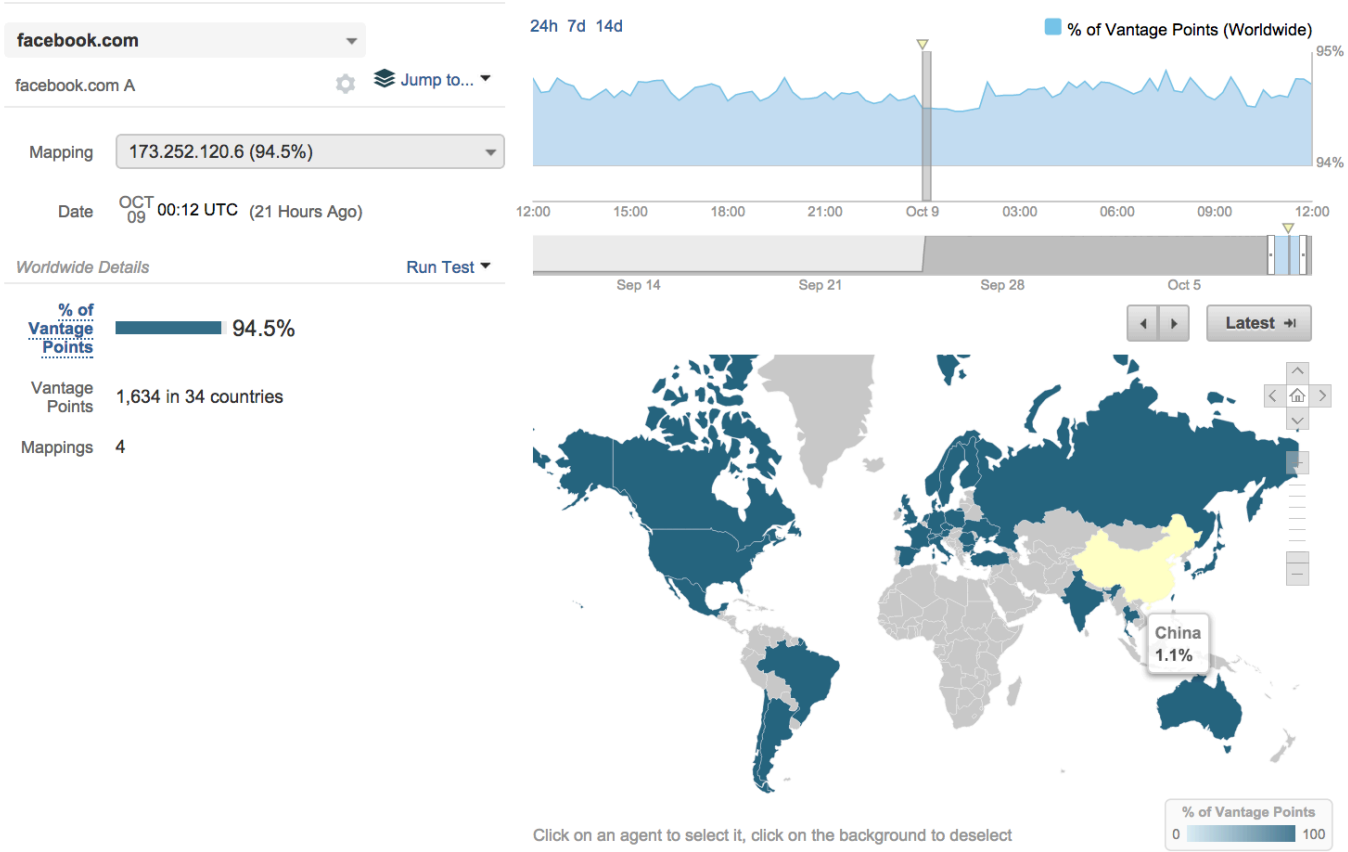


Facebook NS gets “no mapping” in China

Facebook.com A record is 100% available in China



Most of the world maps facebook.com to 173.252.120.6



Geography | Network

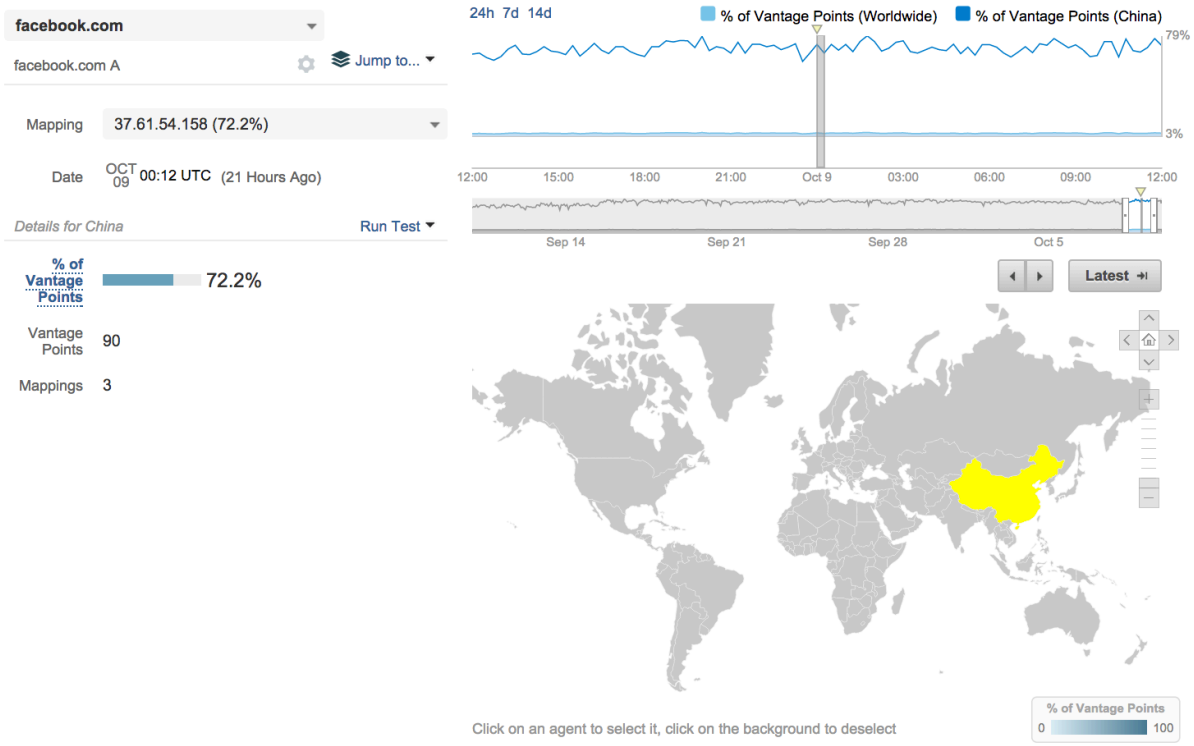
Country: -- All

Date (UTC)	Country	% of Vantage Points ↓	No. of Networks
2014-10-09 00:12:05	Argentina	100	12
2014-10-09 00:12:09	Poland	100	14
2014-10-09 00:12:06	Ukraine	100	21
2014-10-09 00:12:05	Bulgaria	100	24

Who owns 173.252.120.6

```
NetRange:       173.252.64.0 - 173.252.127.255
CIDR:           173.252.64.0/18
OriginAS:       AS32934
NetName:        FACEBOOK-INC
NetHandle:      NET-173-252-64-0-1
Parent:         NET-173-0-0-0-0
NetType:        Direct Assignment
RegDate:        2011-02-28
Updated:        2012-02-24
Ref:            http://whois.arin.net/rest/net/NET-173-252-64-0-1
```

72% of China sees a different IP 37.61.54.158

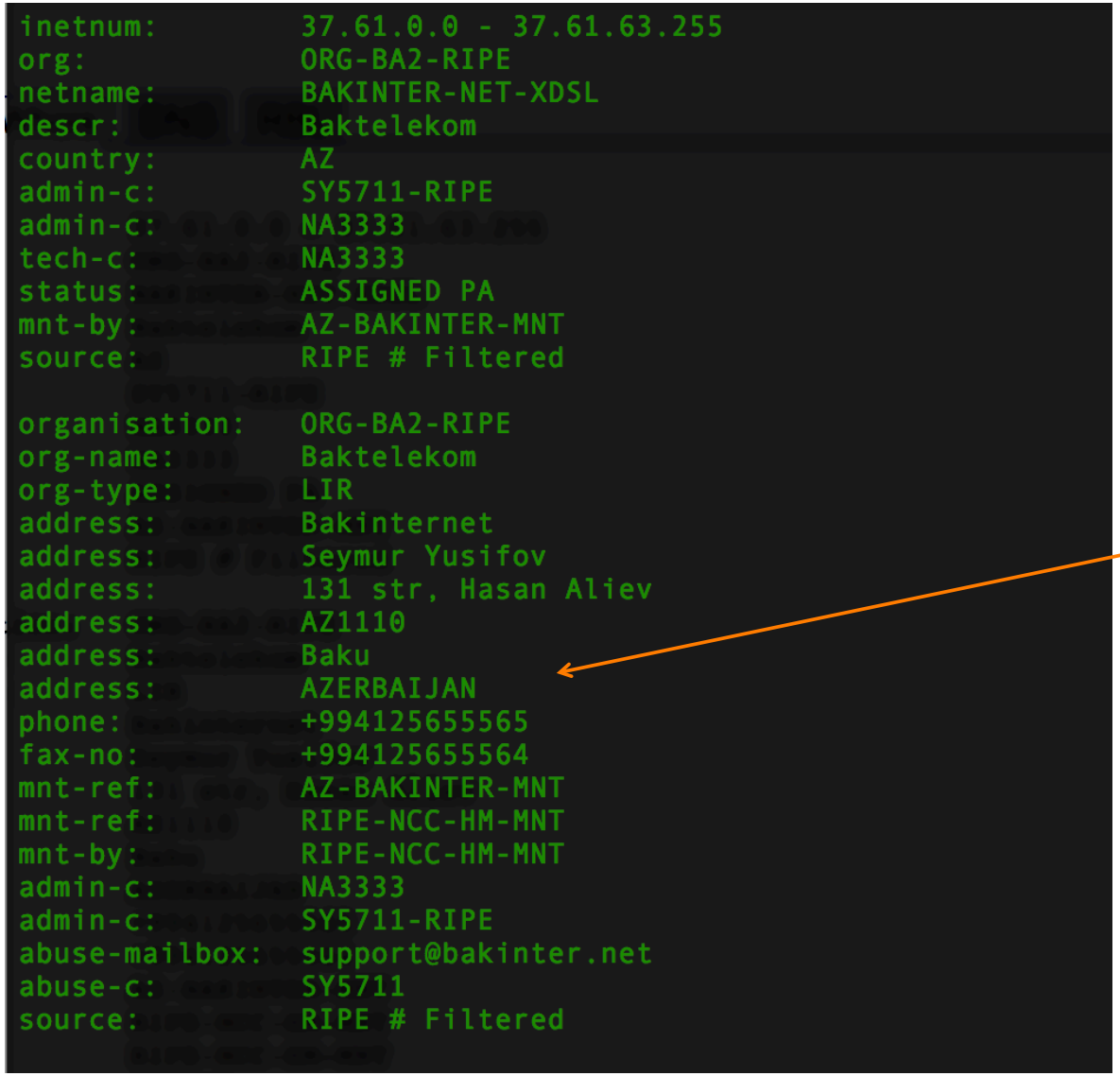


Geography | Network

View all countries → Country: **China**

Date (UTC)	Network	% of Vantage Points ↓	No. of Vantage Points
2014-10-09 00:12:05	China Unicom Shenzen network (AS 17623)	100	1
2014-10-09 00:12:05	IDC, China Telecommunications Corporation (AS 23724)	100	1
2014-10-09 00:12:05	Daqing zhongji petroleum telecommunication construction limited cpmpany (AS 17968)	100	2
2014-10-09 00:12:05	ASN for TIANJIN Provincial Net of CT (AS 17638)	100	1

Who owns 37.61.54.158?

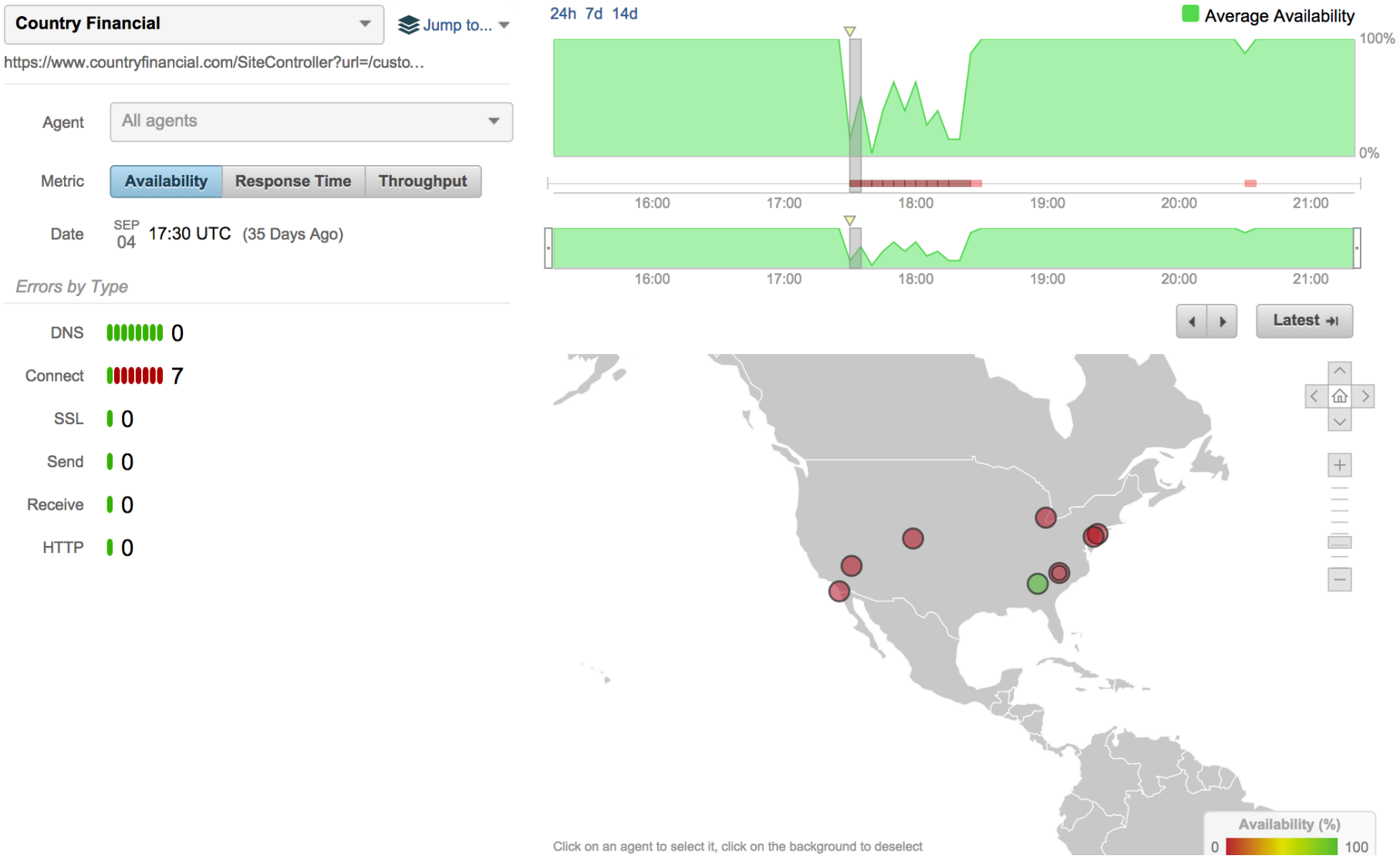


Azerbaijan

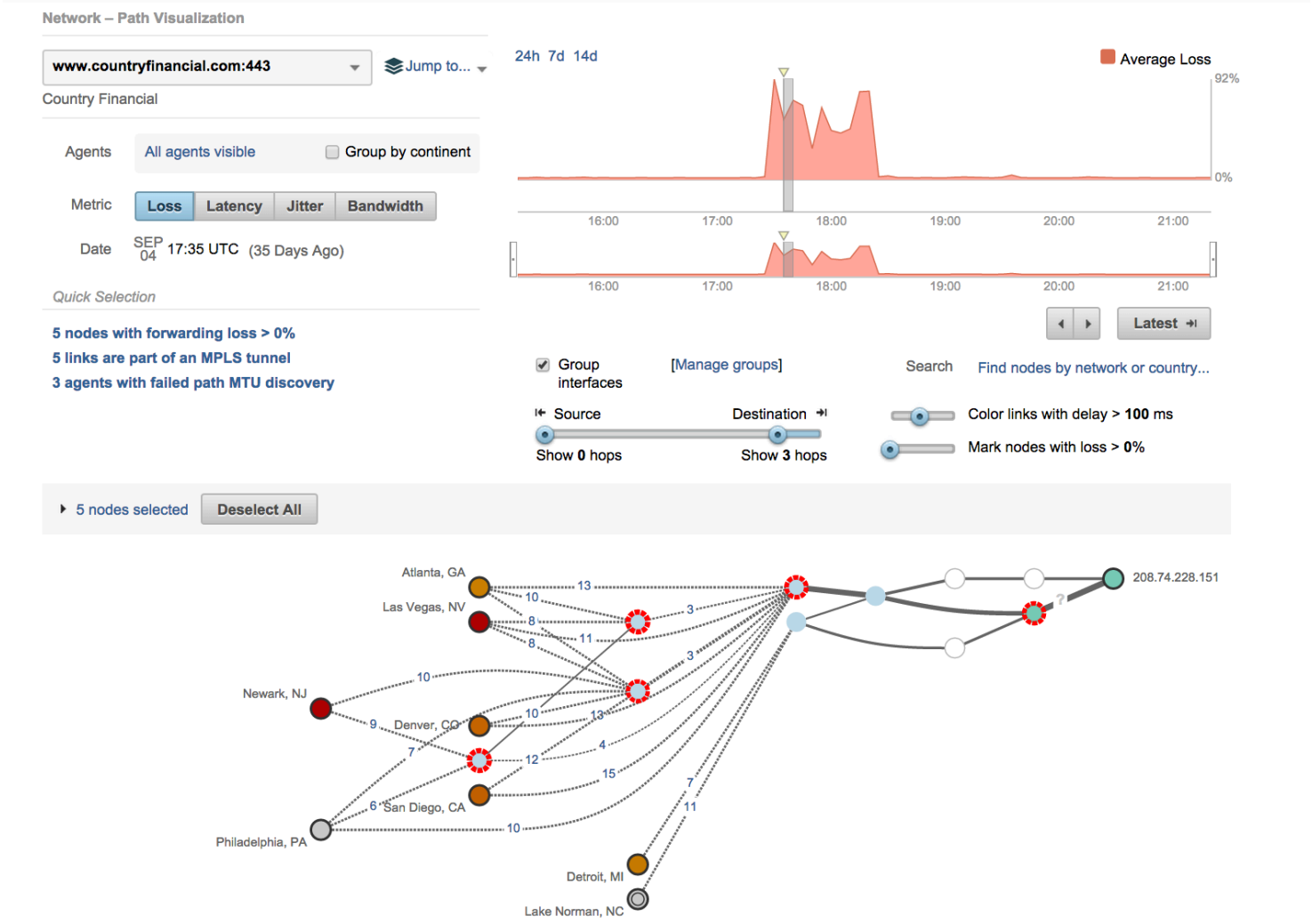
Traceroute

- Protocol used can make a big difference, TCP, UDP or ICMP
- Load balancing can distort discovered routes
- Hard to distinguish between muted interfaces and real loss
- Multiple routes exist, need several probes
- MPLS can distort delays

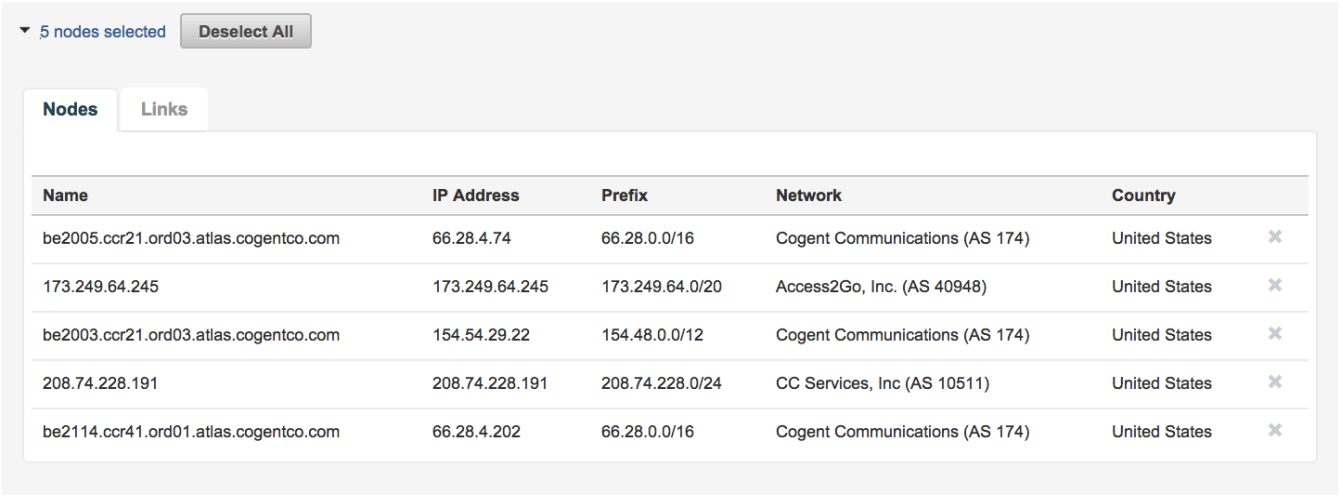
Country Financial Outage



Looking at the network

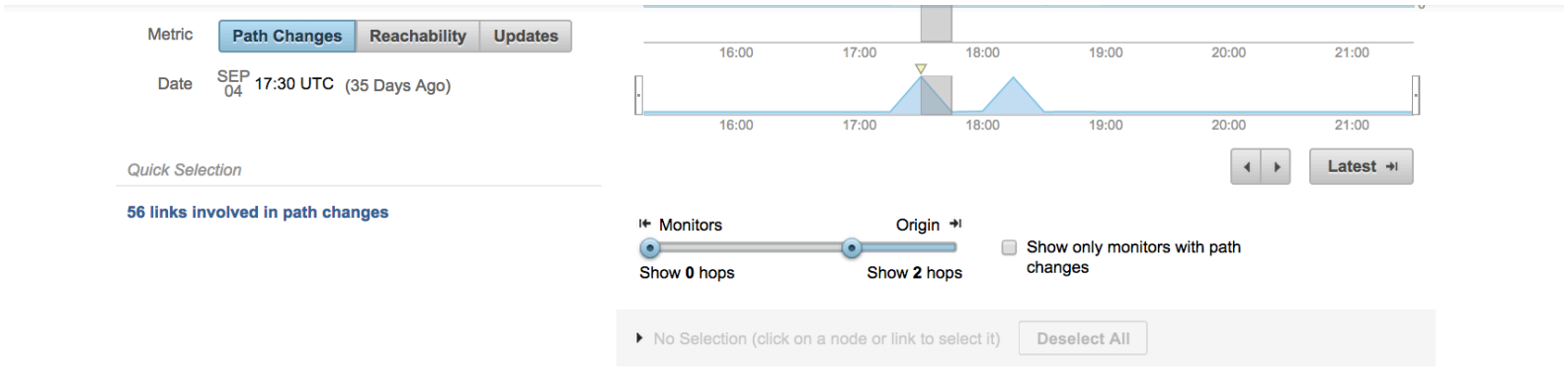


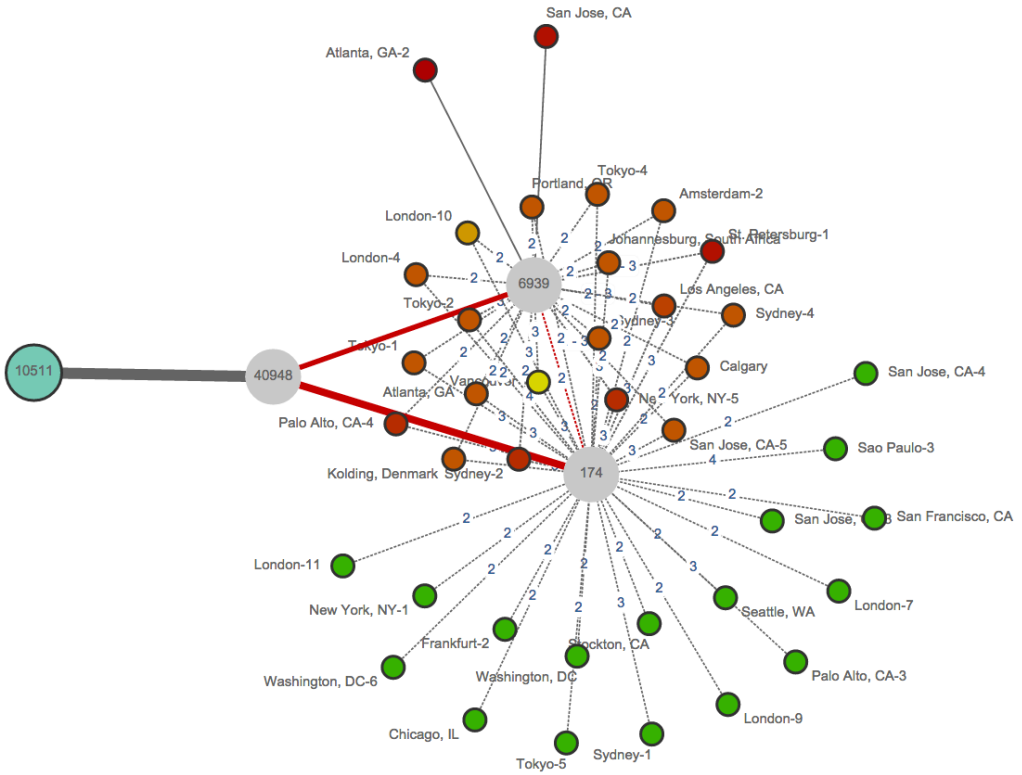
Looking at the network



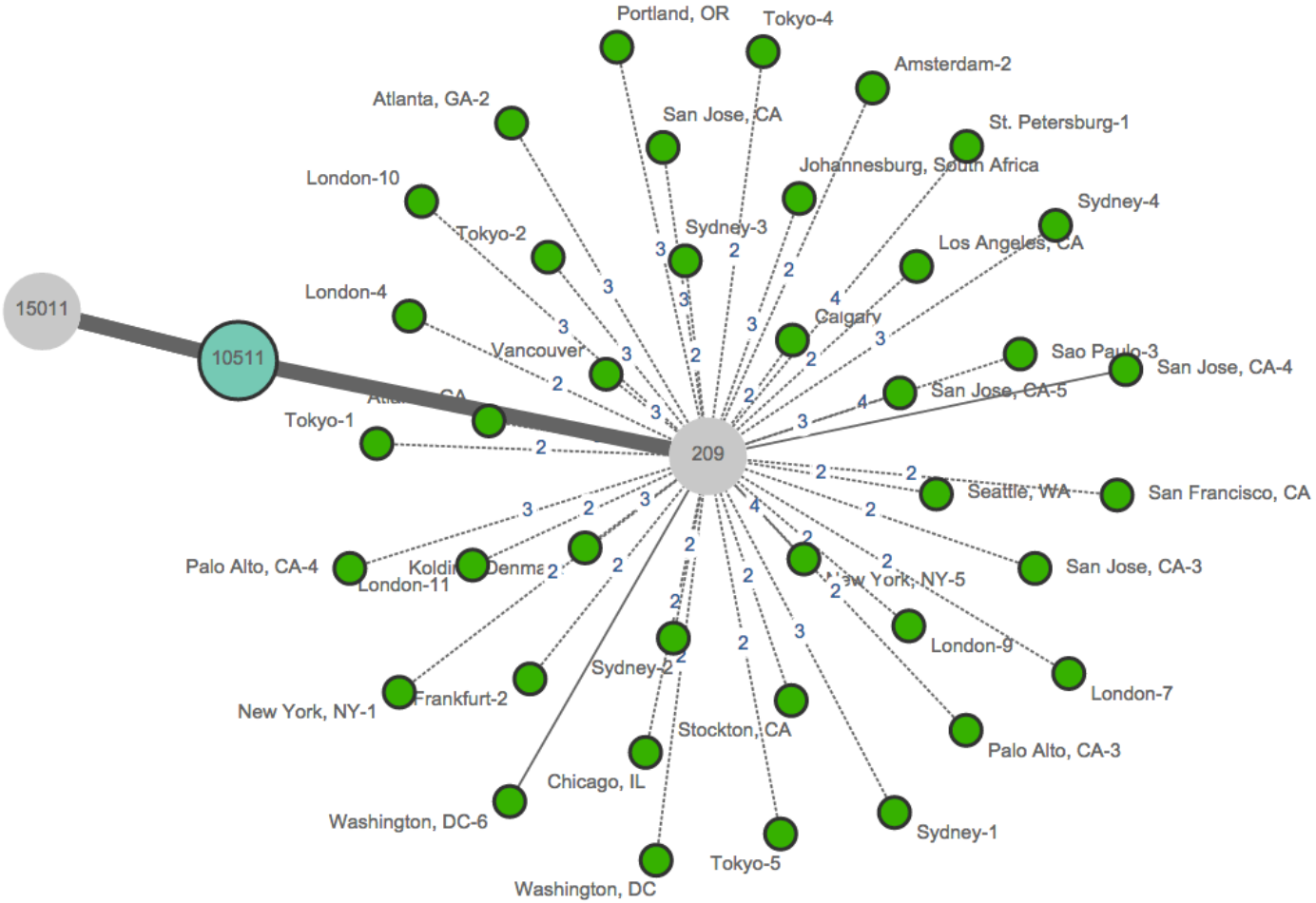
Name	IP Address	Prefix	Network	Country
be2005.ccr21.ord03.atlas.cogentco.com	66.28.4.74	66.28.0.0/16	Cogent Communications (AS 174)	United States
173.249.64.245	173.249.64.245	173.249.64.0/20	Access2Go, Inc. (AS 40948)	United States
be2003.ccr21.ord03.atlas.cogentco.com	154.54.29.22	154.48.0.0/12	Cogent Communications (AS 174)	United States
208.74.228.191	208.74.228.191	208.74.228.0/24	CC Services, Inc (AS 10511)	United States
be2114.ccr41.ord01.atlas.cogentco.com	66.28.4.202	66.28.0.0/16	Cogent Communications (AS 174)	United States

Diving deeper into BGP





After things are stable



Lets look at a DDoS attack

Web – HTTP Server

HSBC DDoS

Jump to...

http://www.us.hsbc.com

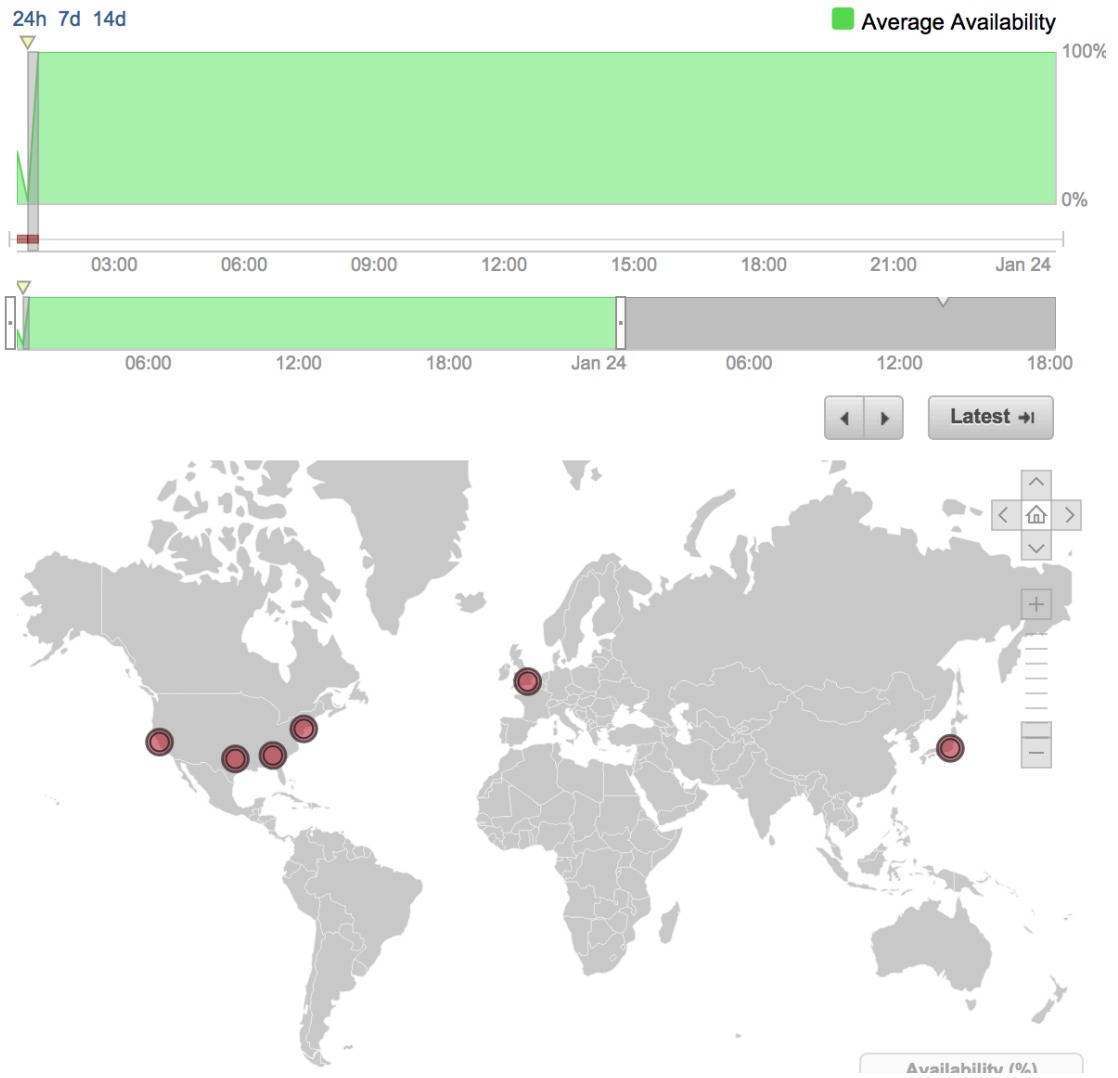
Agent: All agents

Metric: Availability | Response Time | Throughput

Date: JAN 23 01:00 UTC (259 Days Ago)

Errors by Type

DNS	0
Connect	2
SSL	0
Send	0
Receive	4
HTTP	0



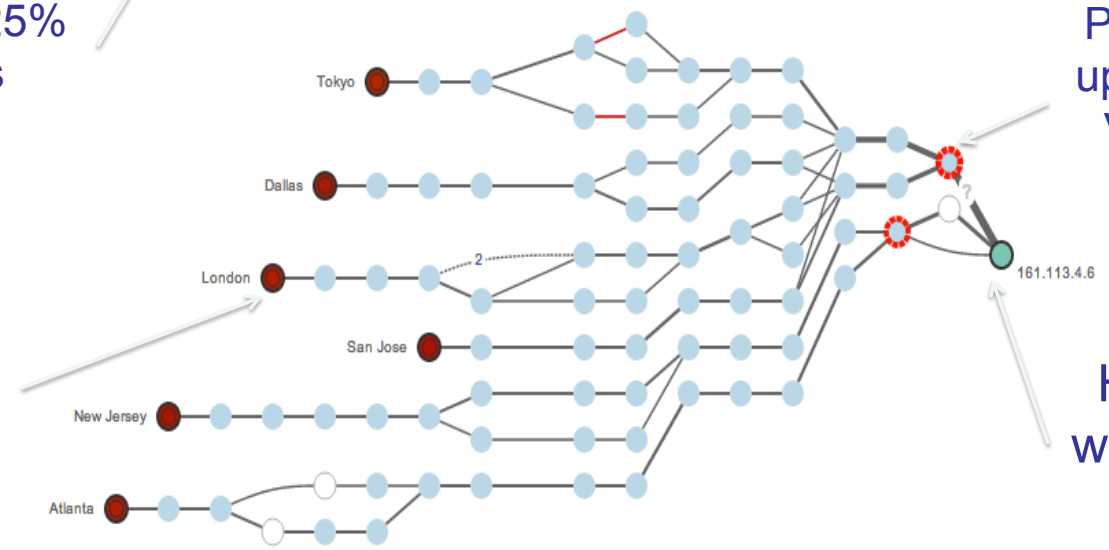
Network View shows congested Nodes in Upstream ISPs

2 nodes selected | Deselect All

Nodes | Links

Name	IP Address	Prefix	Network	Country
us-hsbc-gw.customer.alter.net	157.130.18.202	157.130.0.0/16	Verizon Business/UUnet (AS 701)	United States
12.88.0.70	12.88.0.70	12.0.0.0/9	AT&T Services, Inc. (AS 7018)	United States

Nodes with >25% packet loss

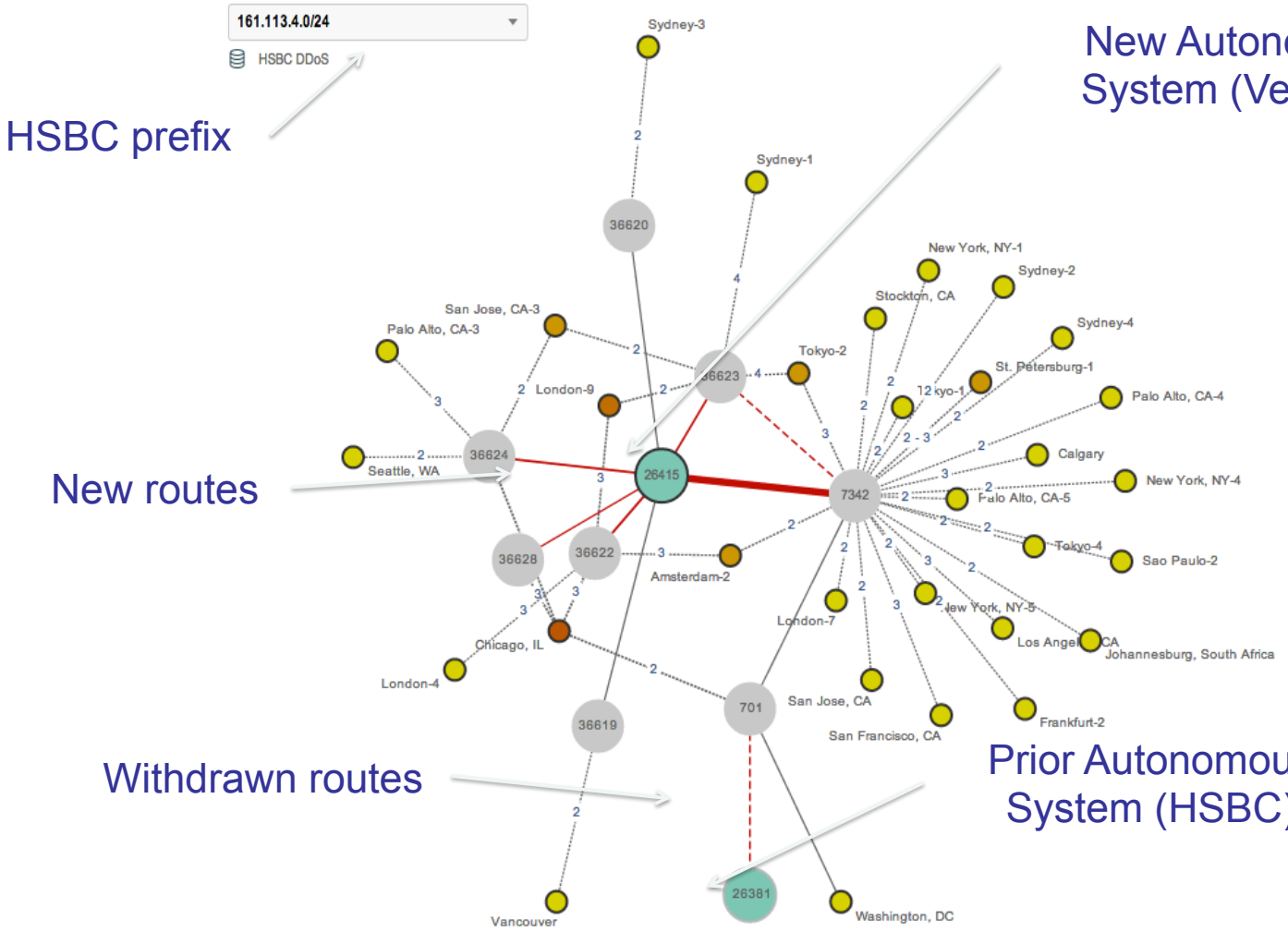


Packet loss in upstream ISPs Verizon and AT&T

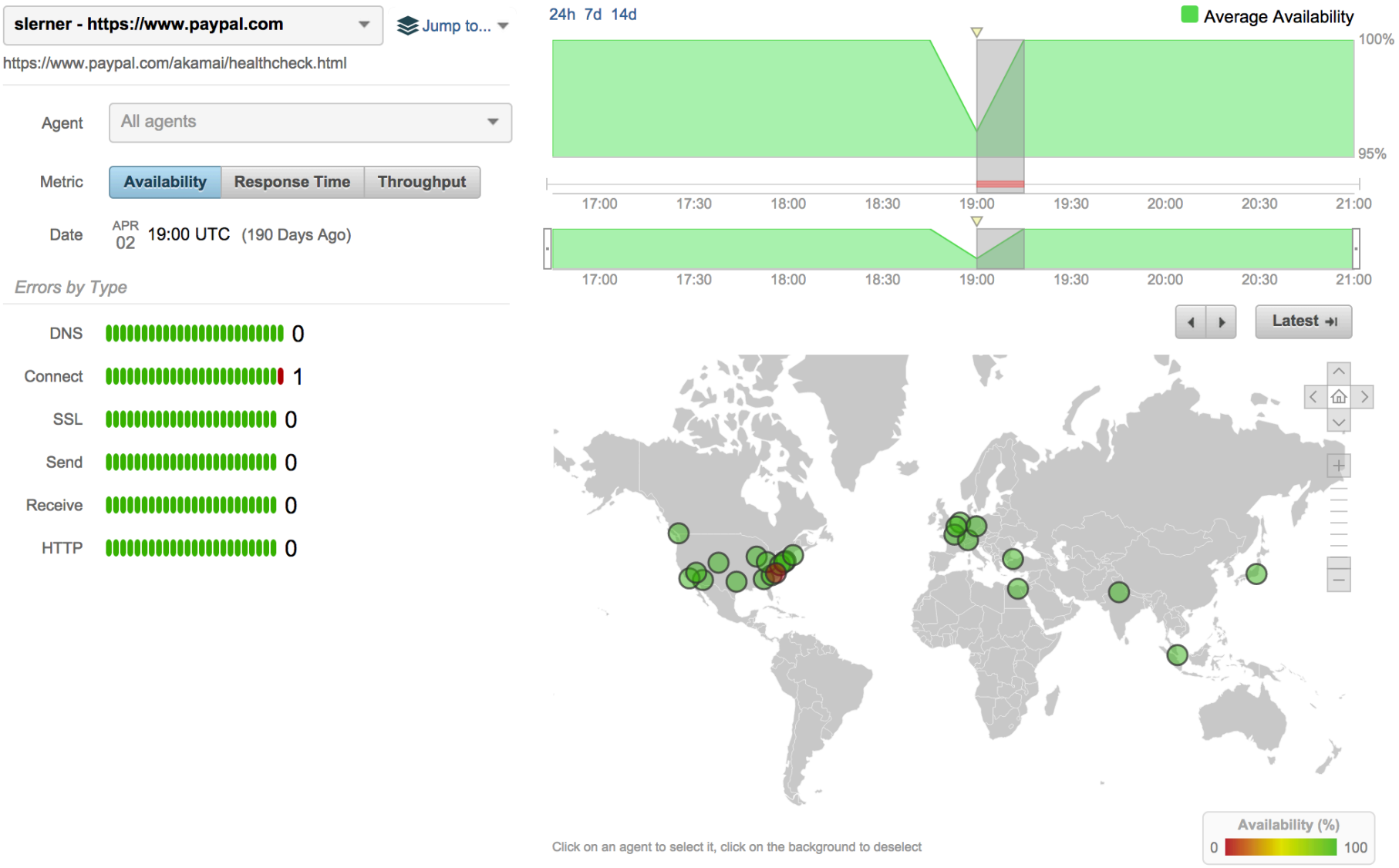
High packet loss from all testing points

HSBC bank website under attack

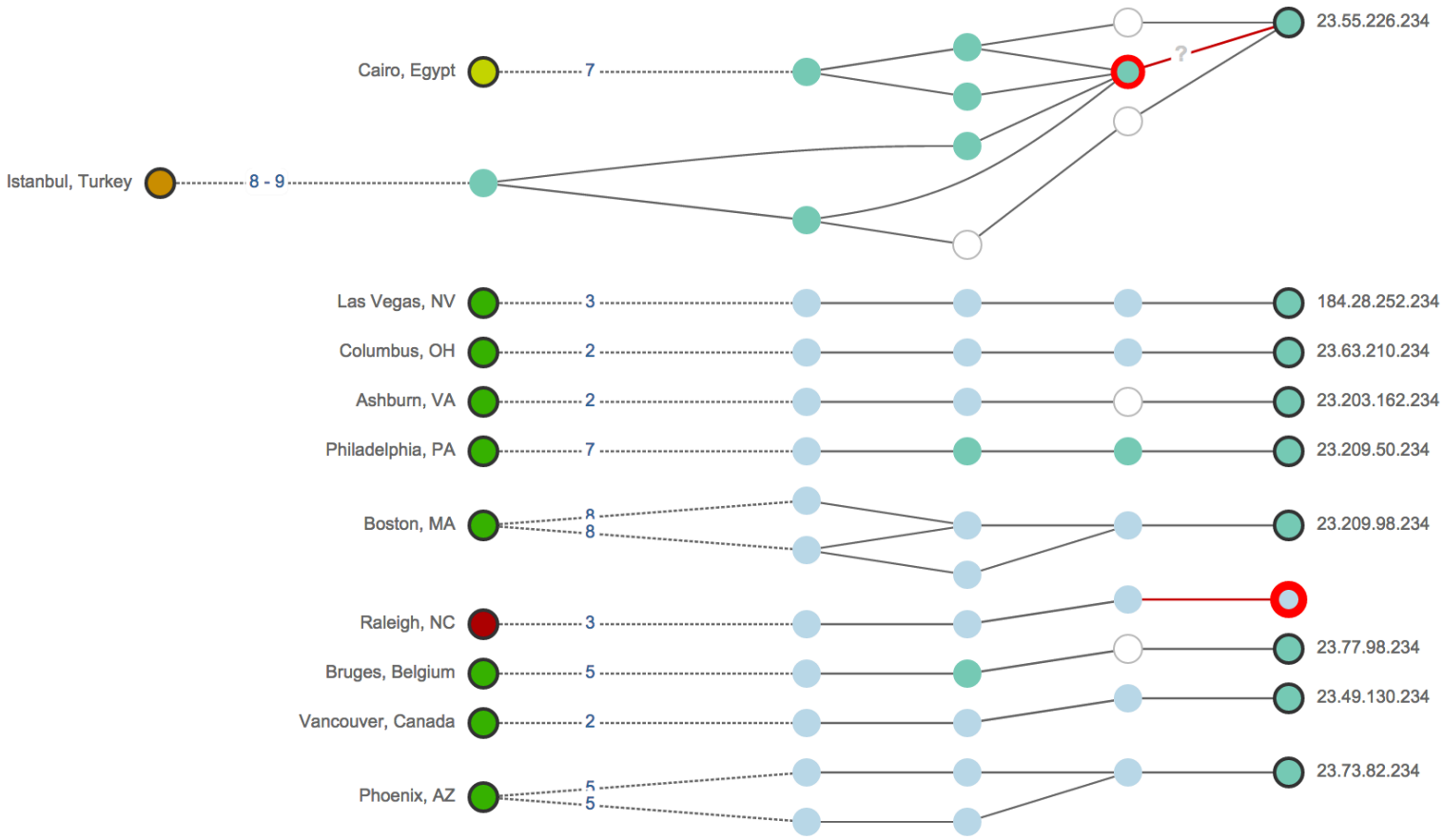
DDoS Attack: Mitigation Handoff Using BGP



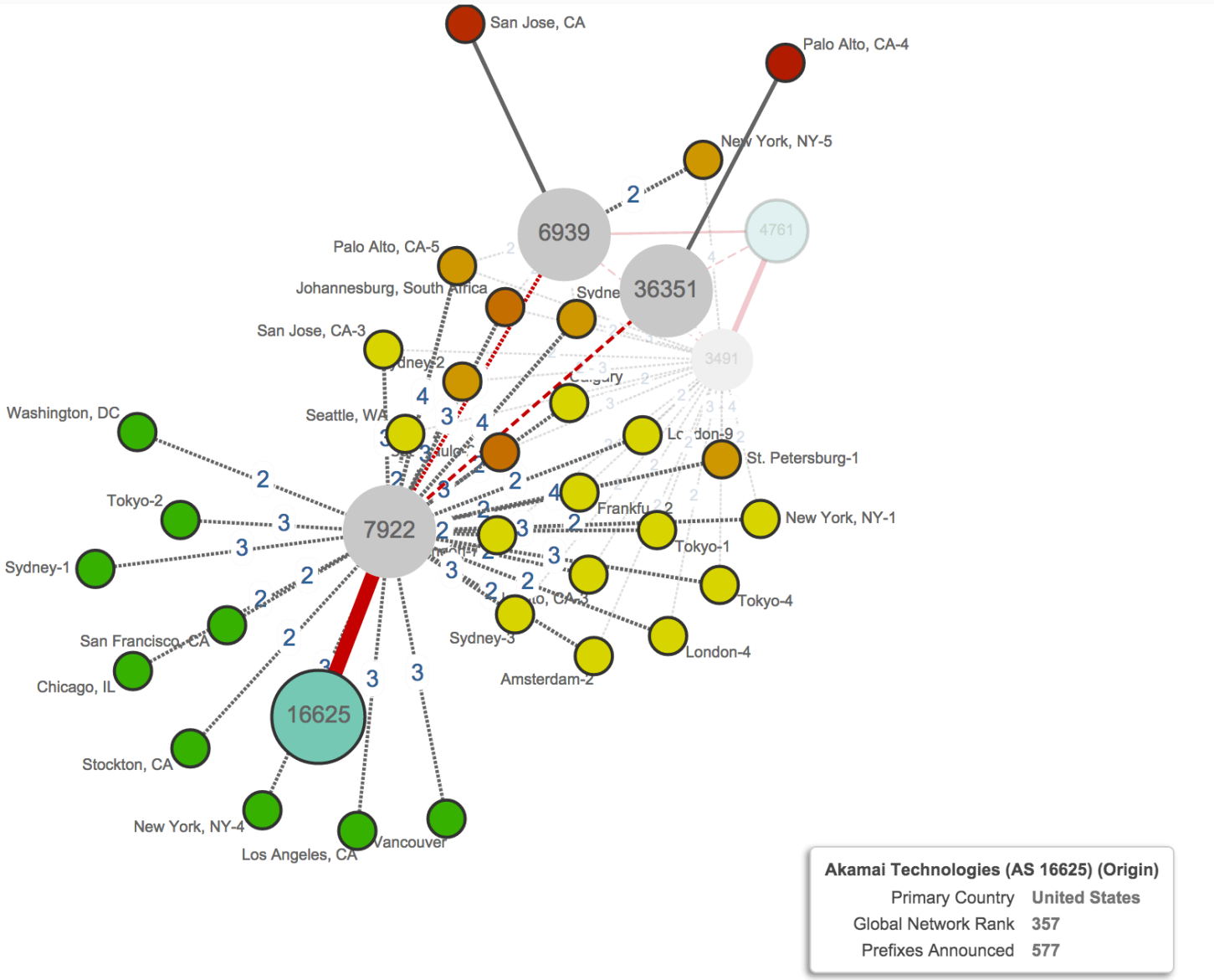
Paypal Issues



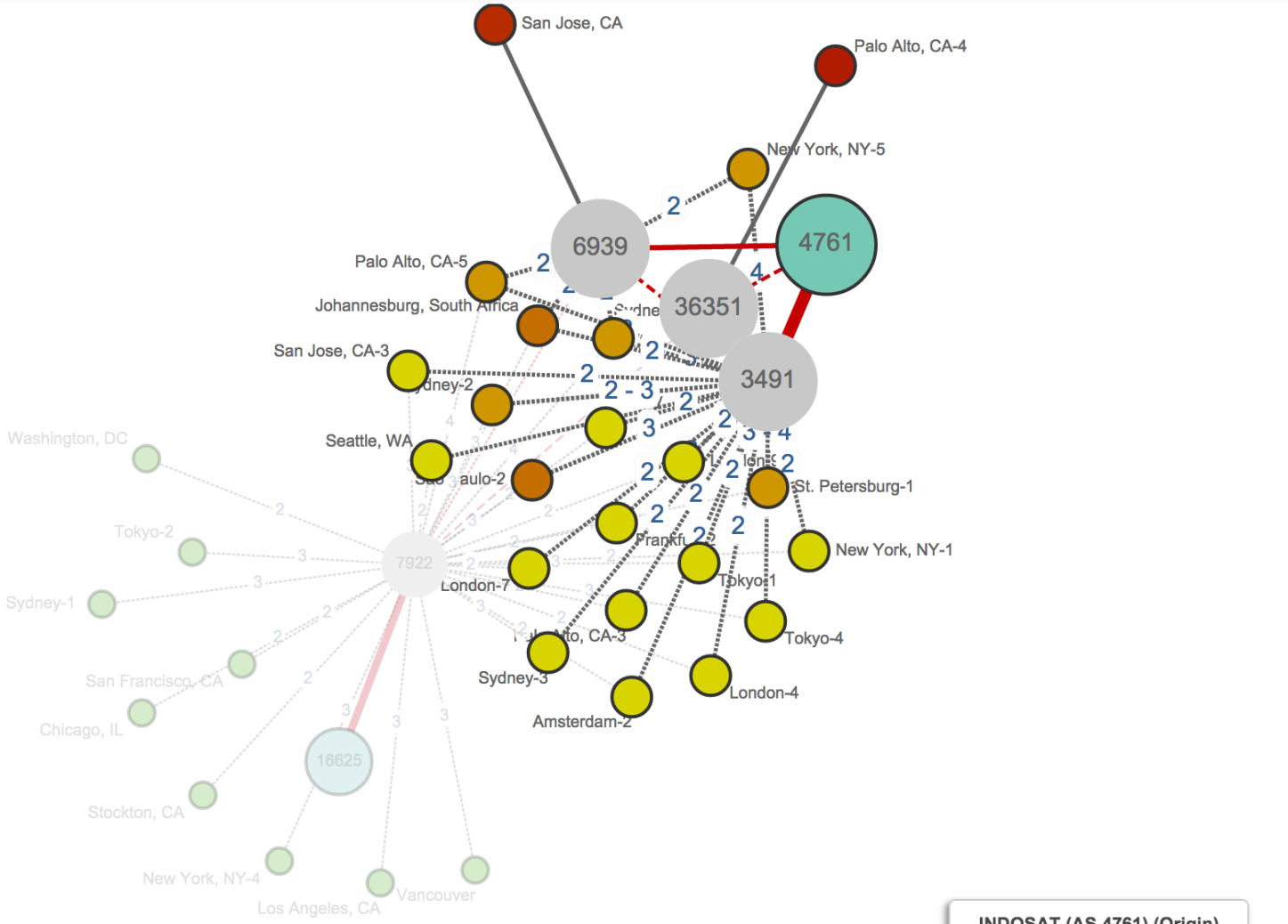
Lets look at the network



Akamai advertising address block



Indosat advertising the same prefix block



Thanks !

mohit@thousandeyes.com