

# Combining Active and Passive Monitoring

---

Mohit Lad  
CEO, ThousandEyes  
[mohit@thousandeyes.com](mailto:mohit@thousandeyes.com)

## Basics

---

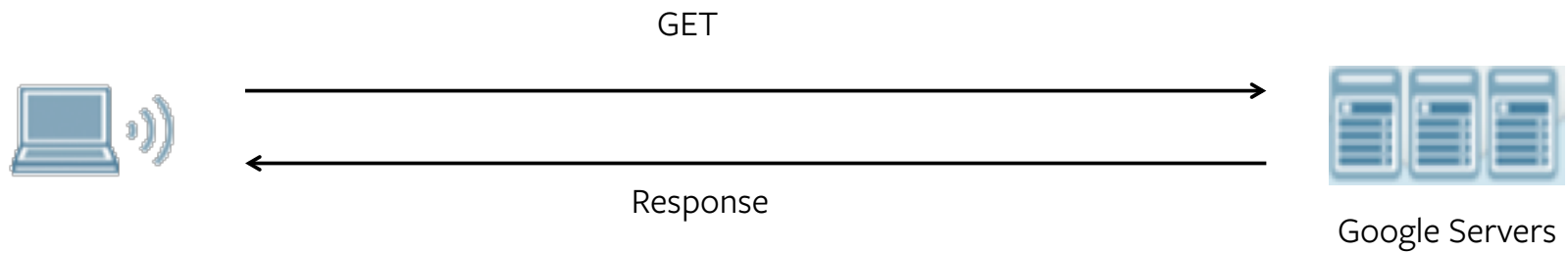
- » Passive Monitoring

- » 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

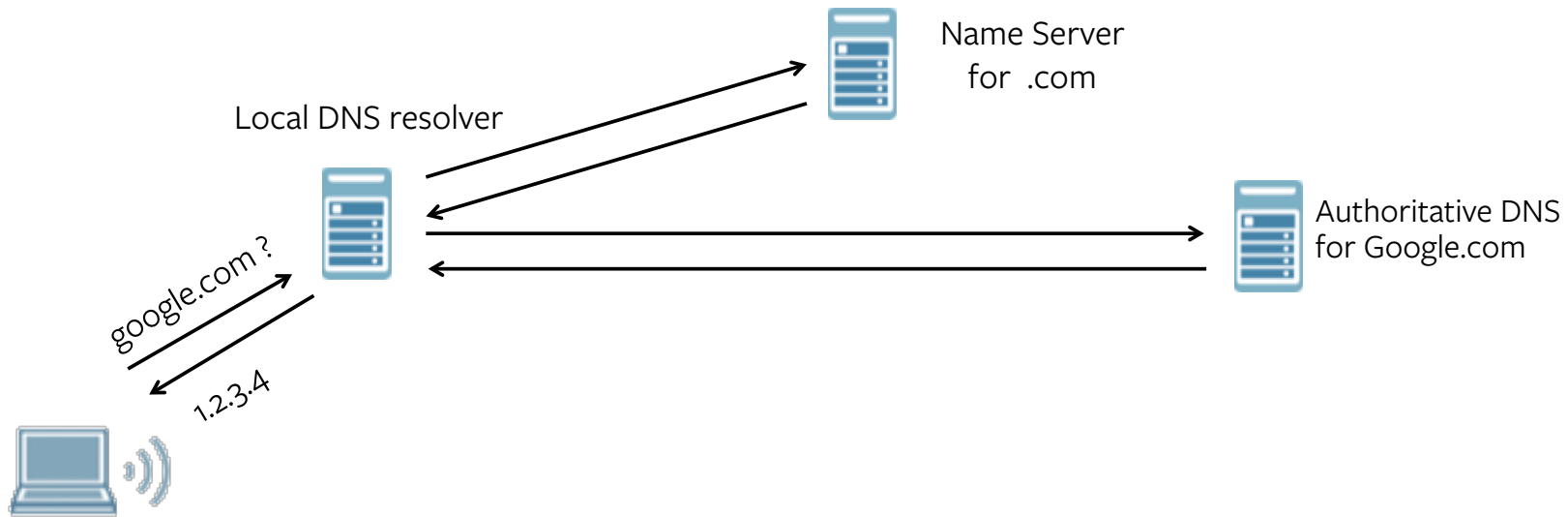
- » Active Probing

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

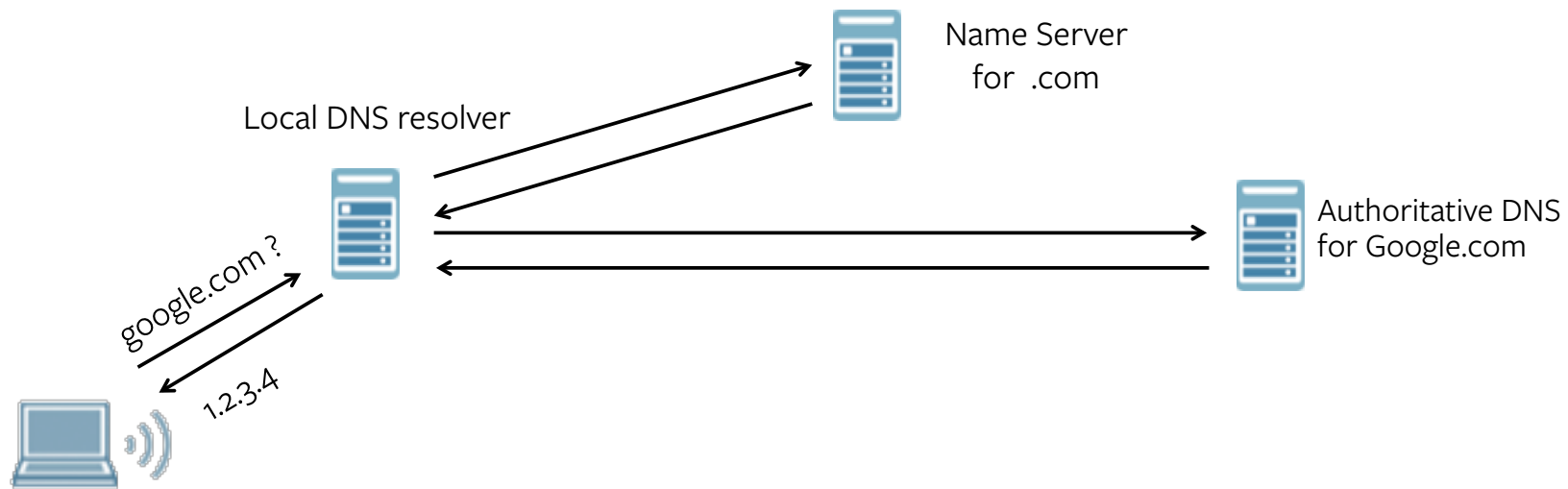
## Example: Google does not load



# 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

Metric **Availability** Resolution Time

Date **OCT 09 20:20 UTC** (1 Hour Ago)

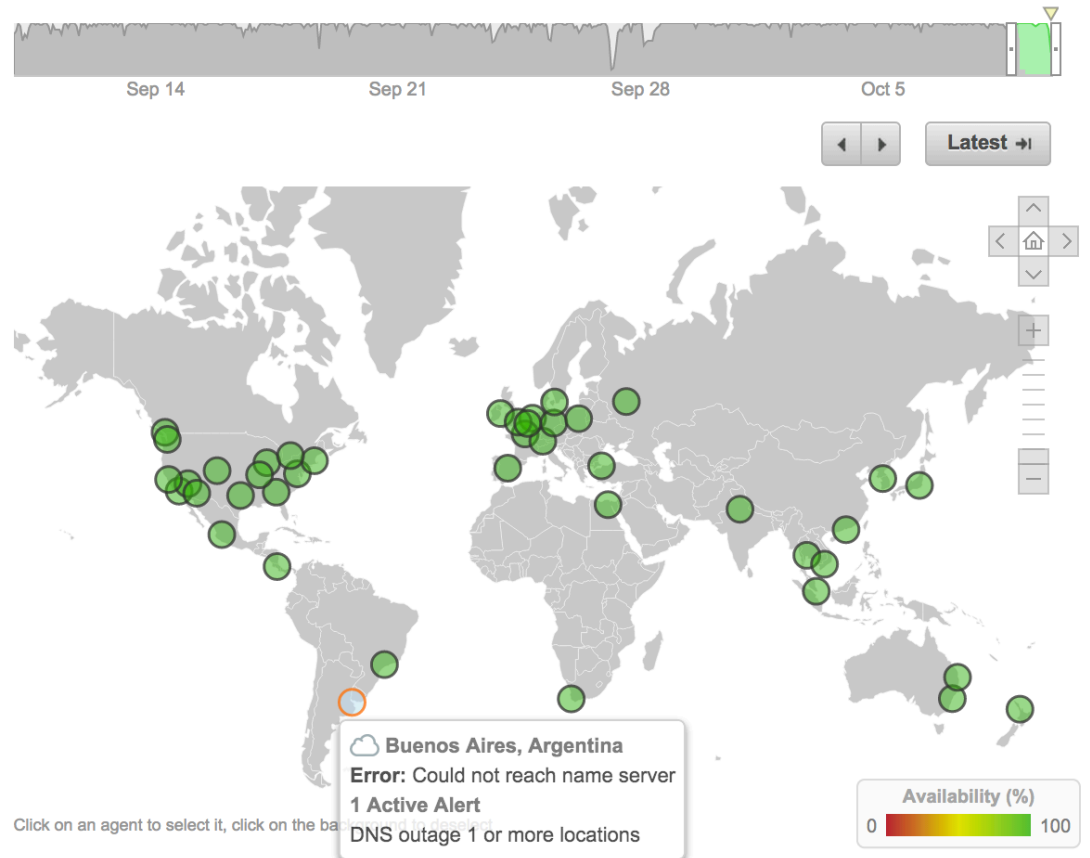
Worldwide Averages for  [Run Test](#)

Availability  **97.62%**

Time  **104 ms**

Active Alerts

**DNS outage 1 or more locations**

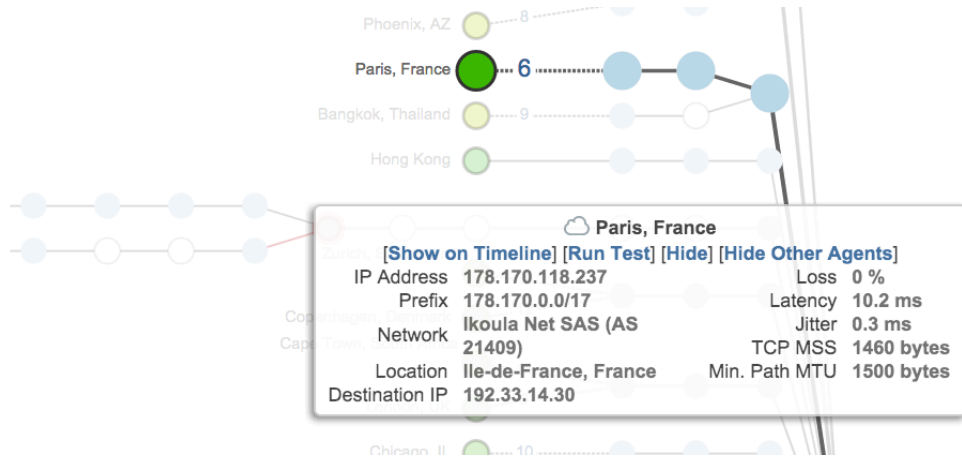


Agent	Date	Mappings	Error Details ↓	Resolution Time (ms)
Buenos Aires, Argentina	2014-10-09 20:21:56		Could not reach name server	

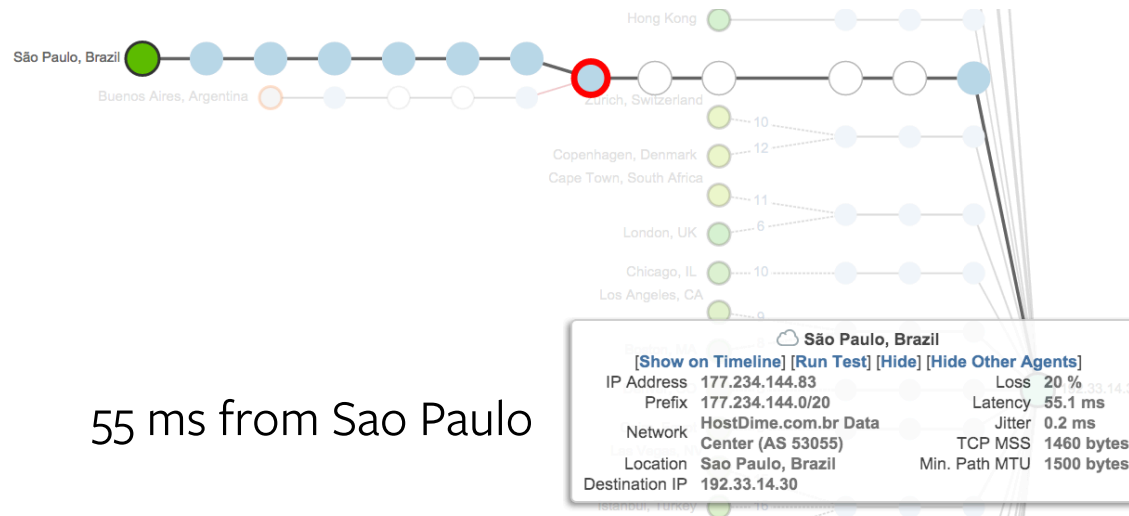
# Domain in question is anycasted



# How do we know it's anycast?



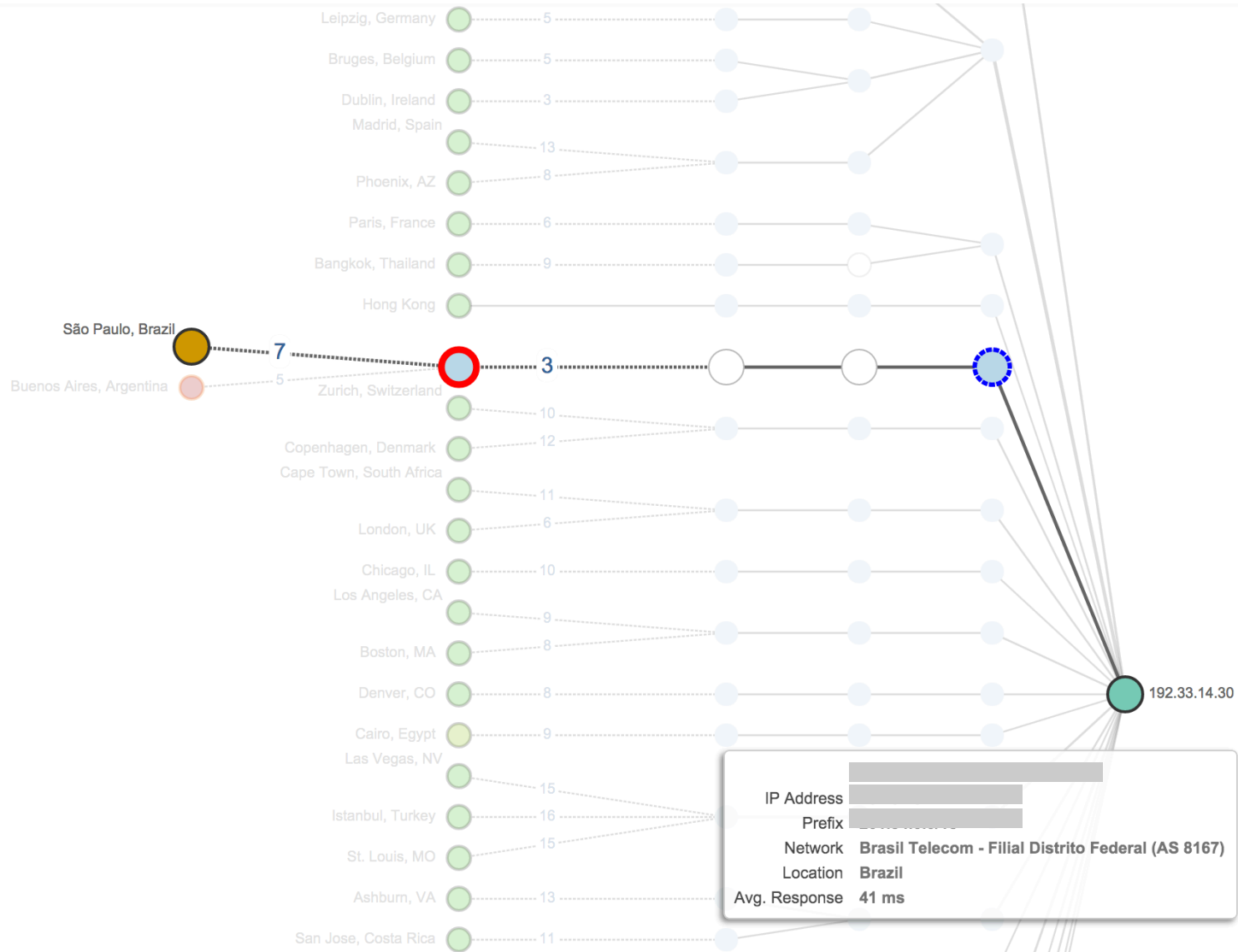
10 ms from Paris



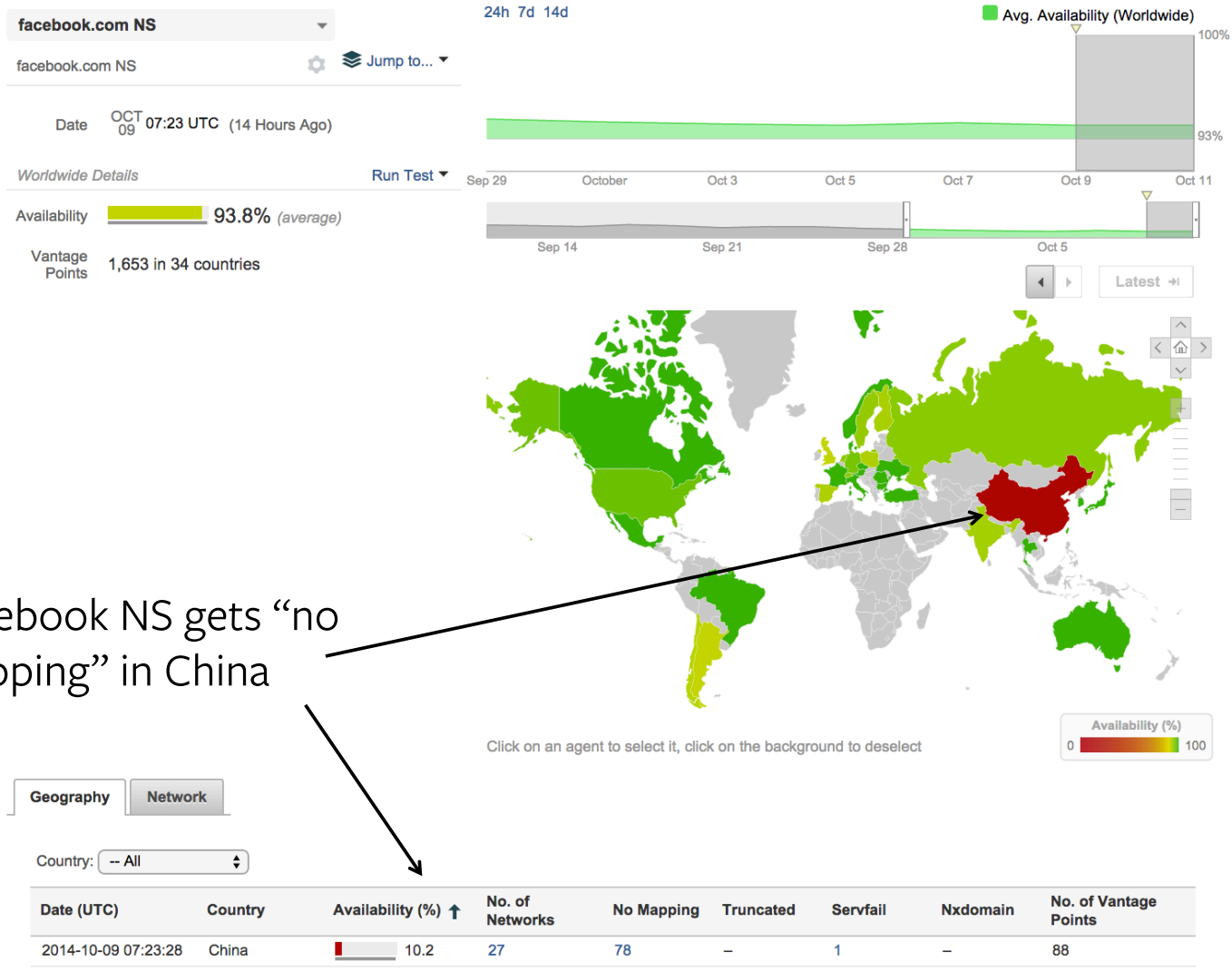
55 ms from Sao Paulo



# Identifying the problematic Anycast instance

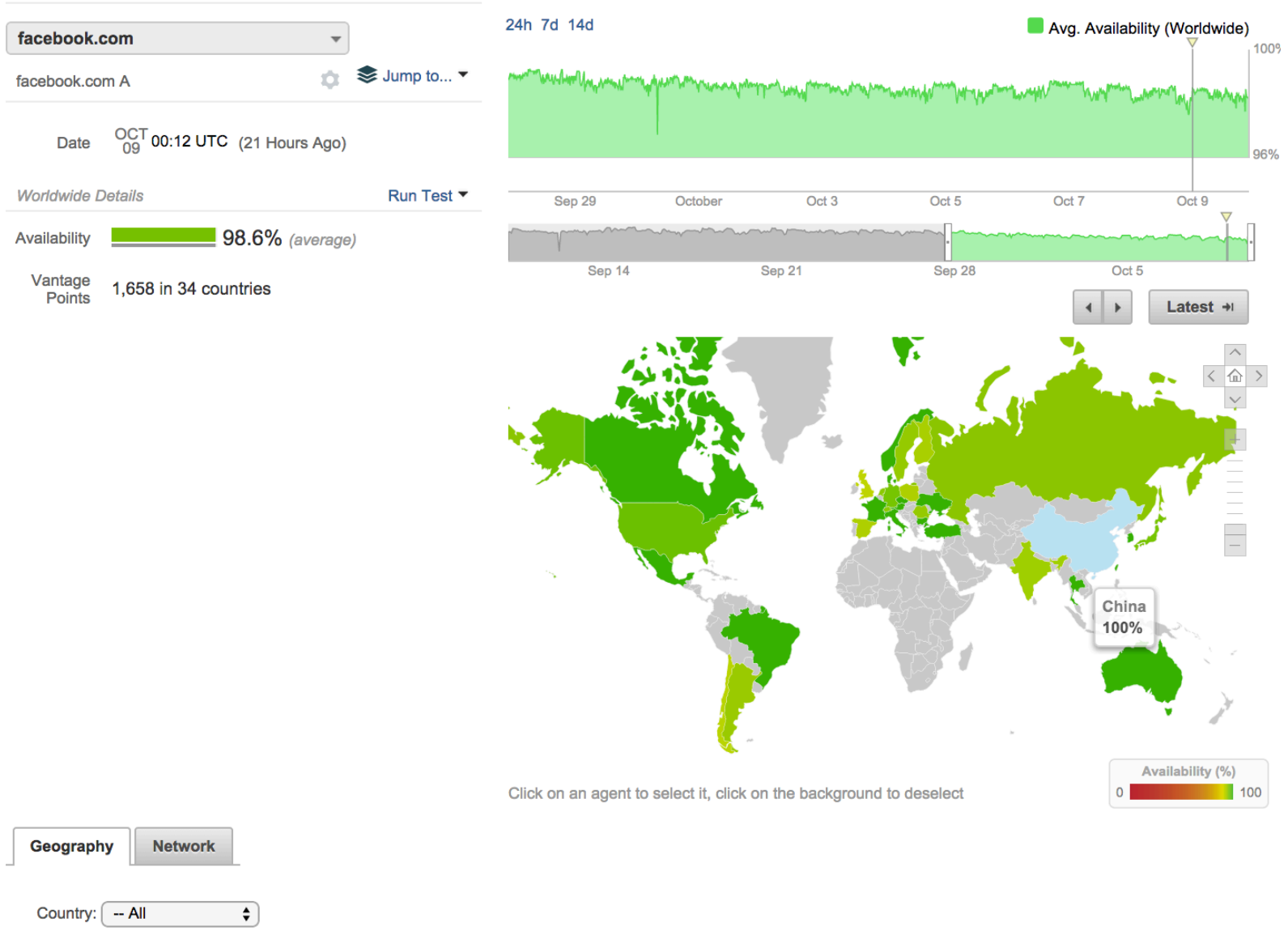


# So is everything ok if we get a DNS reply? Lets look at Facebook NS

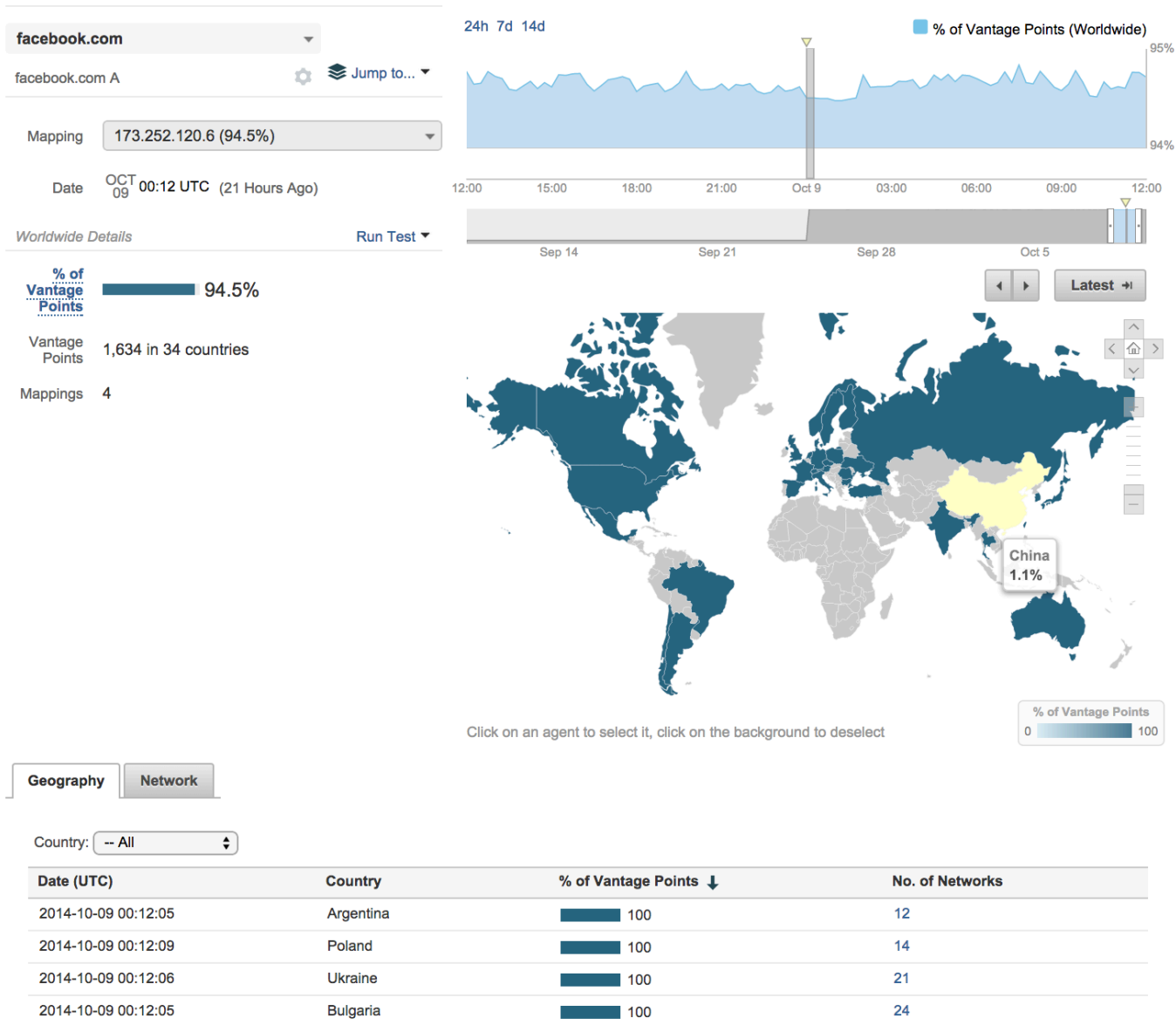


Facebook NS gets “no mapping” in China

# Facebook.com A record is 100% available in China



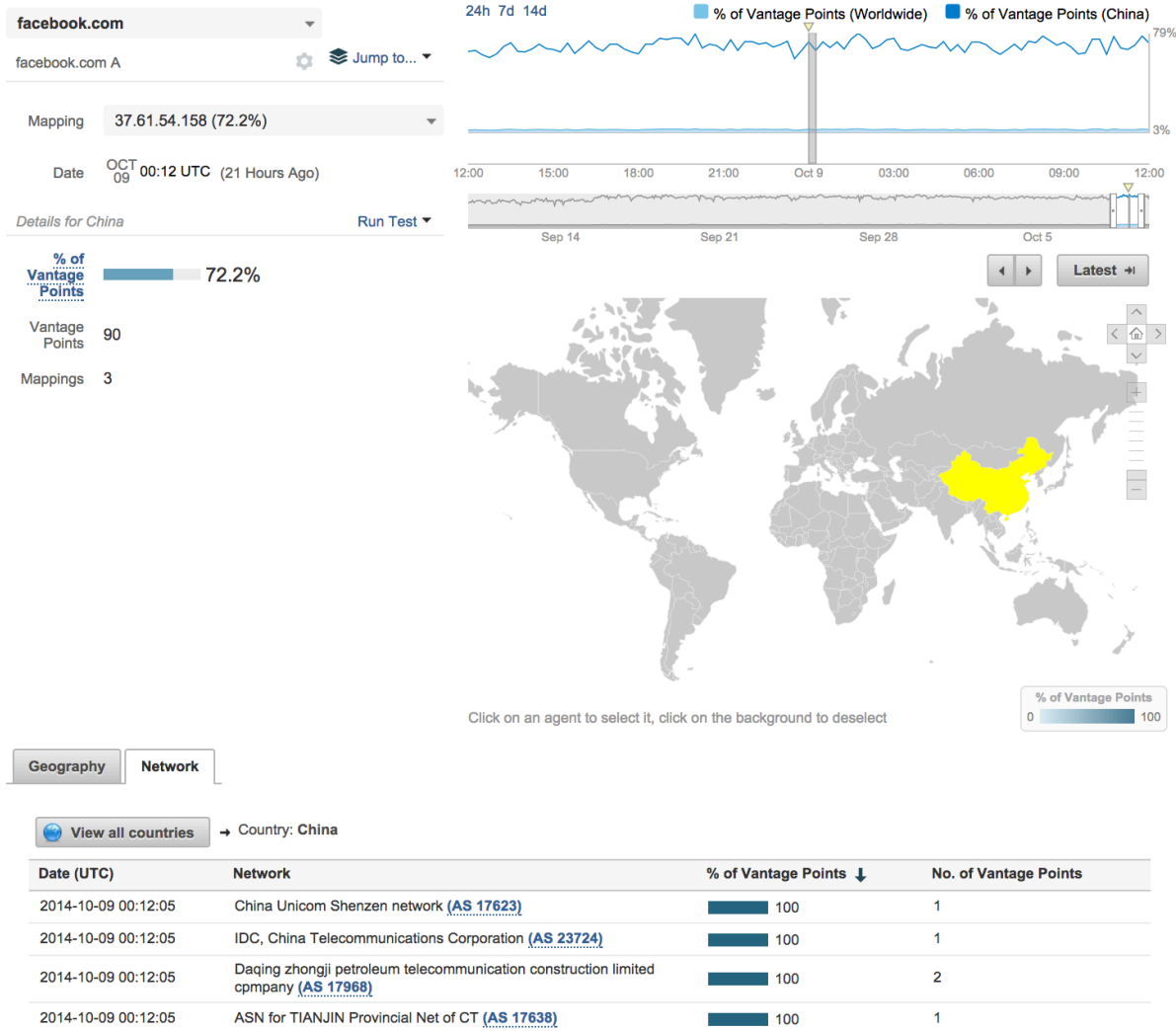
# Most of the world maps facebook.com to 173.252.120.6



## 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



## Who owns 37.61.54.158?

```
inetnum:      37.61.0.0 - 37.61.63.255
org:          ORG-BA2-RIPE
netname:      BAKINTER-NET-XDSL
descr:        Baktelekom
country:      AZ
admin-c:      SY5711-RIPE
admin-c:      NA3333
tech-c:       NA3333
status:       ASSIGNED PA
mnt-by:       AZ-BAKINTER-MNT
source:       RIPE # Filtered

organisation: ORG-BA2-RIPE
org-name:     Baktelekom
org-type:     LIR
address:      Bakinternet
address:      Seymur Yusifov
address:      131 str, Hasan Aliev
address:      AZ1110
address:      Baku
address:      AZERBAIJAN
phone:        +994125655565
fax-no:       +994125655564
mnt-ref:      AZ-BAKINTER-MNT
mnt-ref:      RIPE-NCC-HM-MNT
mnt-by:       RIPE-NCC-HM-MNT
admin-c:      NA3333
admin-c:      SY5711-RIPE
abuse-mailbox: support@bakinter.net
abuse-c:      SY5711
source:       RIPE # Filtered
```

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

Country Financial

Jump to...

https://www.countryfinancial.com/SiteController?url=/custo...

Agent: All agents

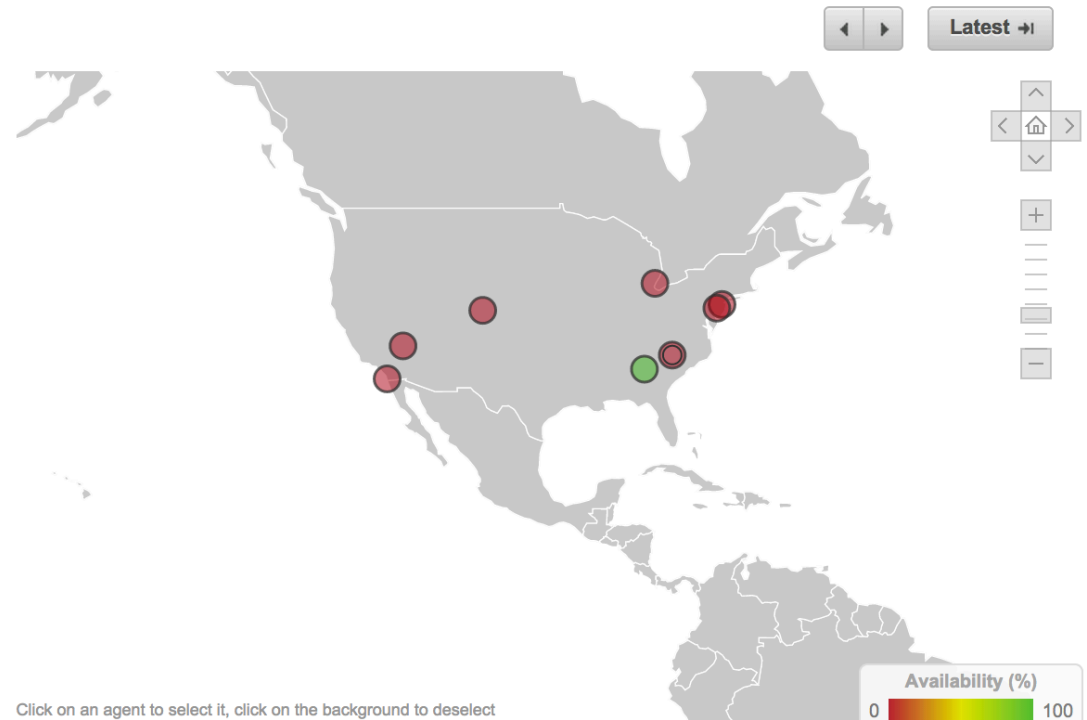
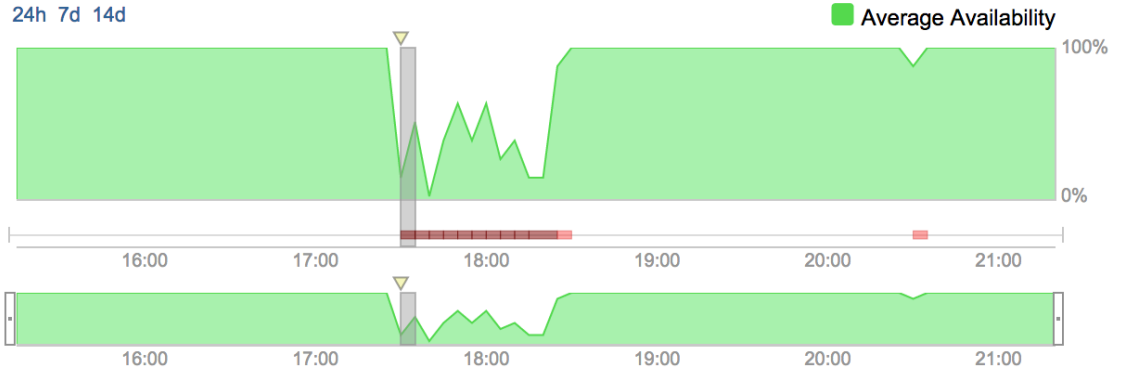
Metric: Availability Response Time Throughput

Date: SEP 04 17:30 UTC (35 Days Ago)

### Errors by Type

- DNS 0
- Connect 7
- SSL 0
- Send 0
- Receive 0
- HTTP 0

24h 7d 14d



Click on an agent to select it, click on the background to deselect

# Looking at the network

## Network – Path Visualization

www.countryfinancial.com:443 Jump to...

Country Financial

Agents  All agents visible  Group by continent

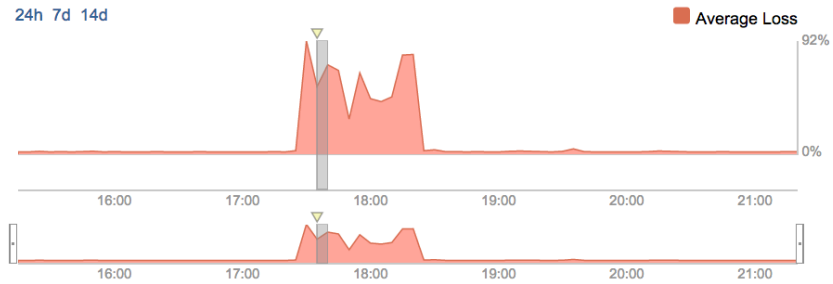
Metric **Loss** Latency Jitter Bandwidth

Date SEP 04 17:35 UTC (35 Days Ago)

### Quick Selection

- 5 nodes with forwarding loss > 0%
- 5 links are part of an MPLS tunnel
- 3 agents with failed path MTU discovery

24h 7d 14d



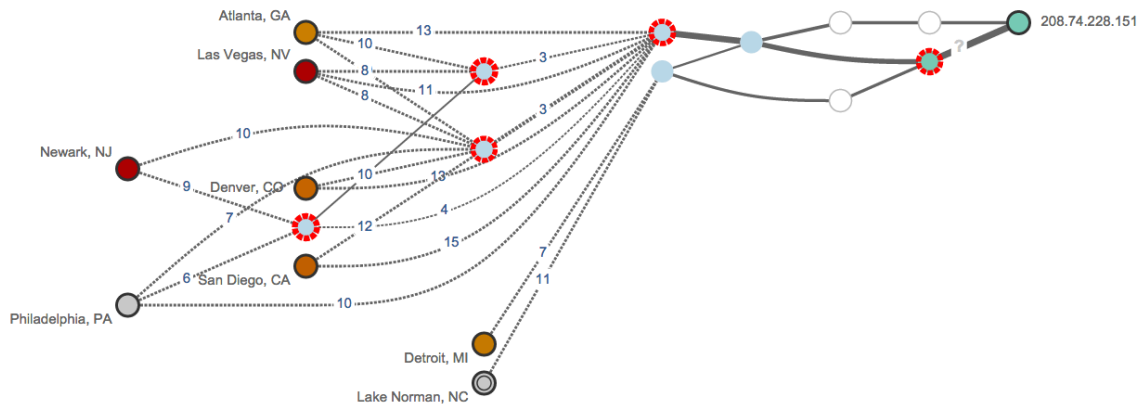
Group interfaces [Manage groups]

Search Find nodes by network or country...

Source Destination  
 Show 0 hops Show 3 hops

Color links with delay > 100 ms  
 Mark nodes with loss > 0%

5 nodes selected Deselect All



# Looking at the network

5 nodes selected

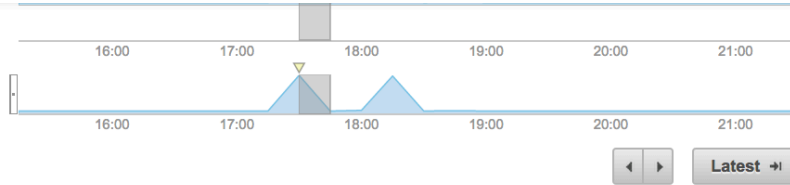
**Nodes**

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

Metric **Path Changes** Reachability Updates

Date **SEP 04 17:30 UTC** (35 Days Ago)

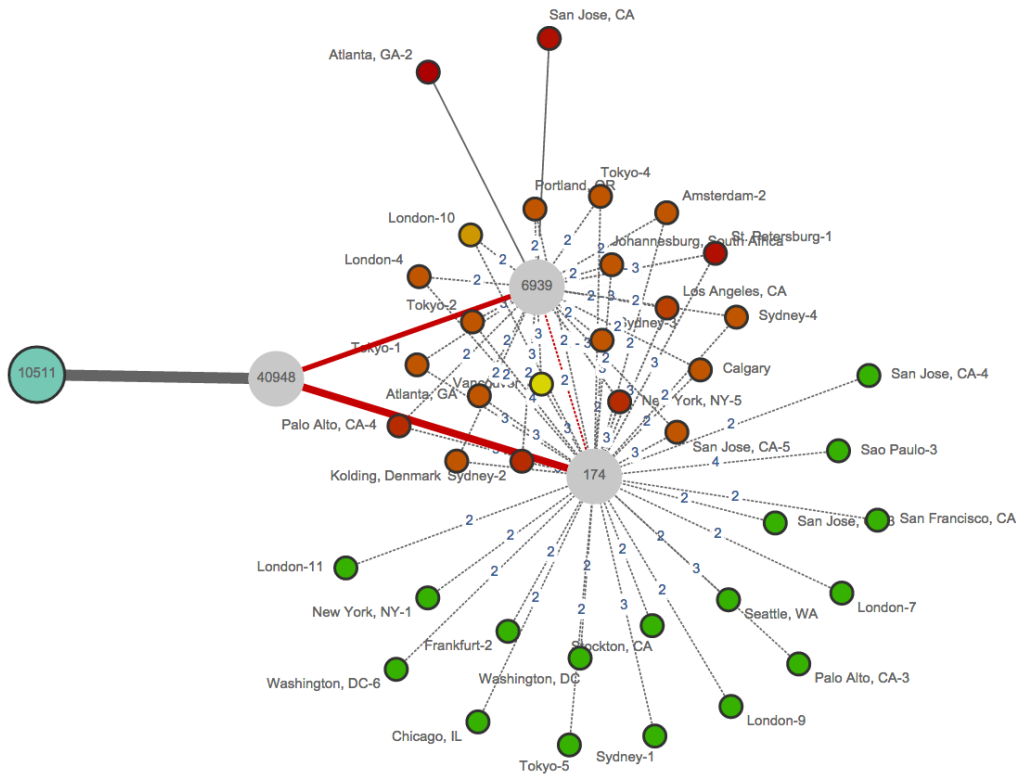


Quick Selection

56 links involved in path changes

Monitors Origin →  
Show 0 hops Show 2 hops  Show only monitors with path changes

No Selection (click on a node or link to select it) Deselect All





# Lets look at a DDoS attack

Web – HTTP Server

HSBC DDoS Jump to...  
http://www.us.hsbc.com

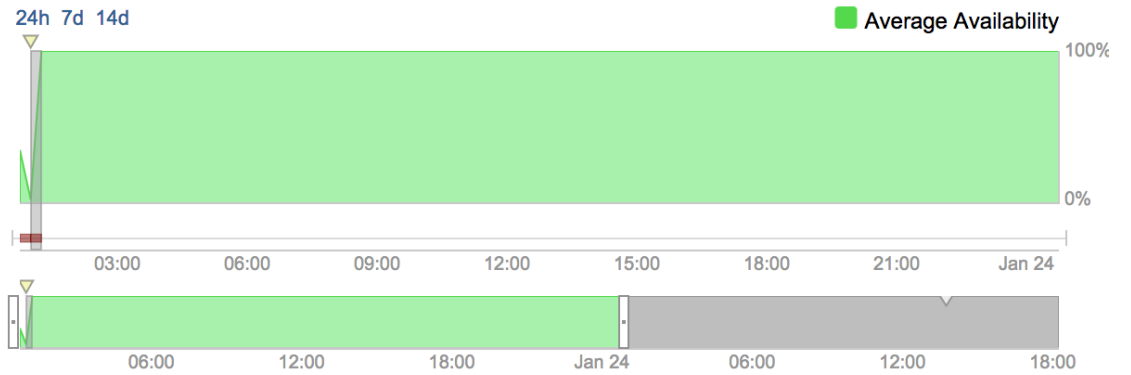
Agent All agents

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

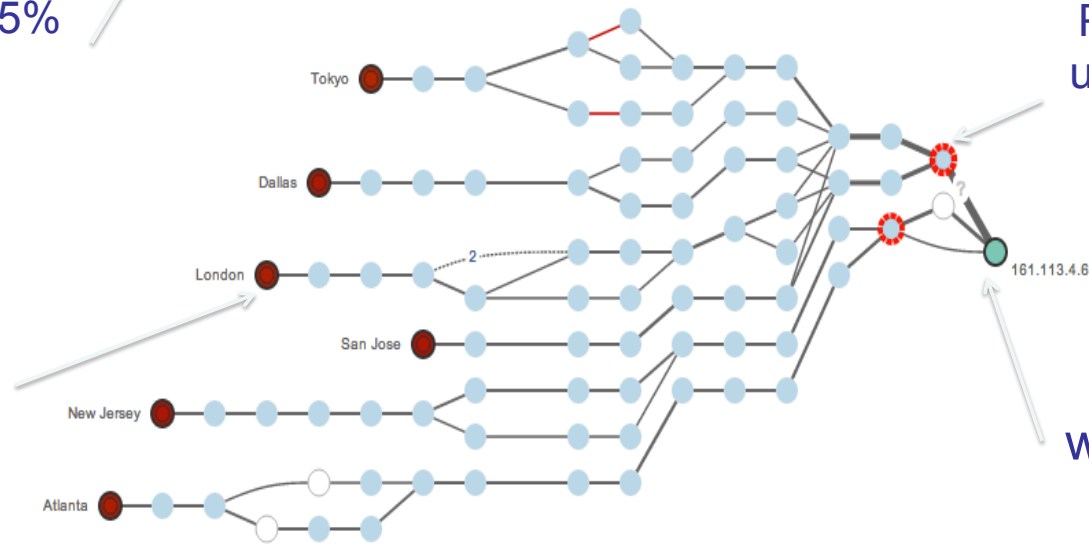
▼ 2 nodes selected    Deselect All

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

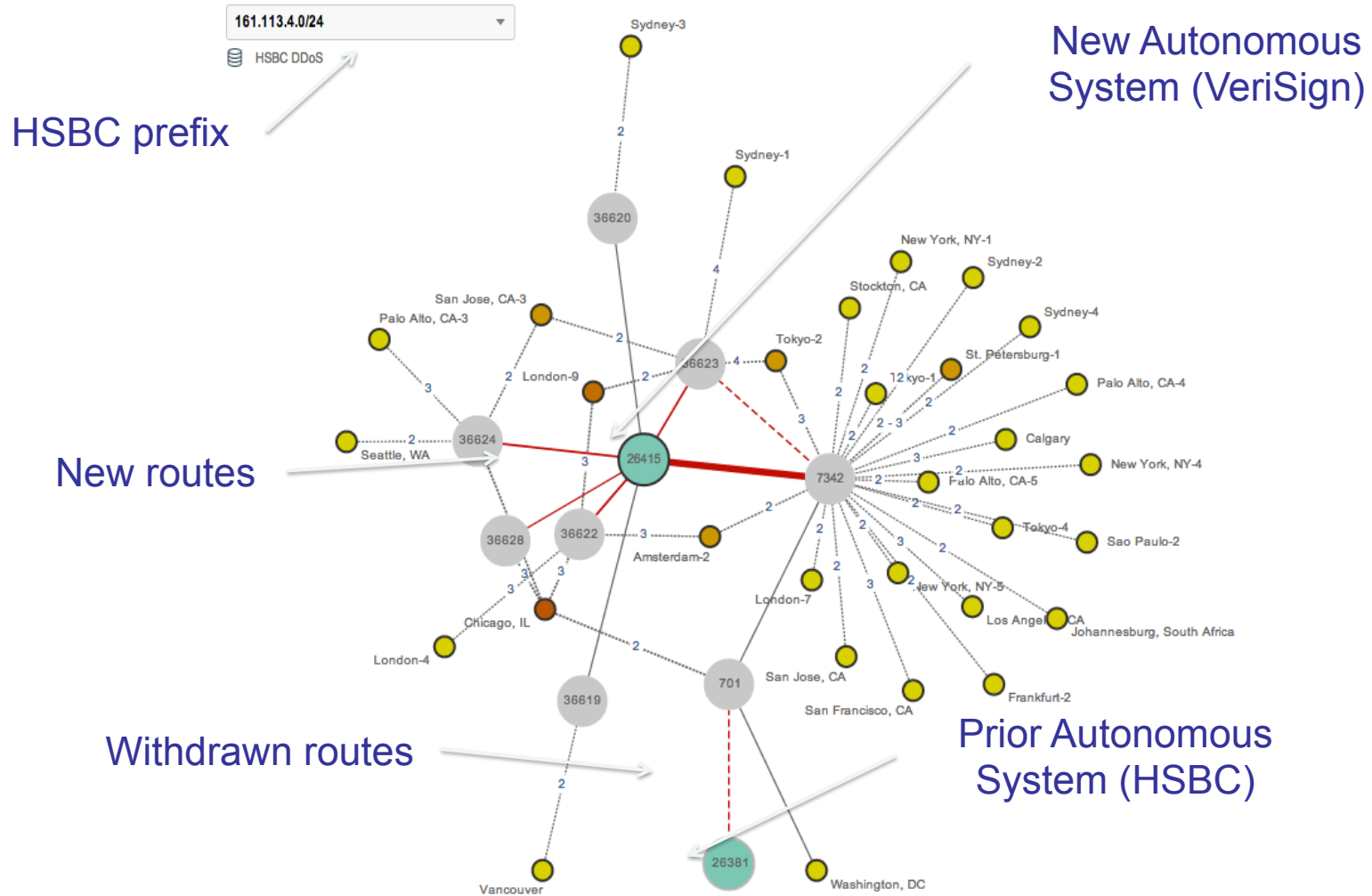
High packet loss from all testing points



Packet loss in upstream ISPs Verizon and AT&T

HSBC bank website under attack

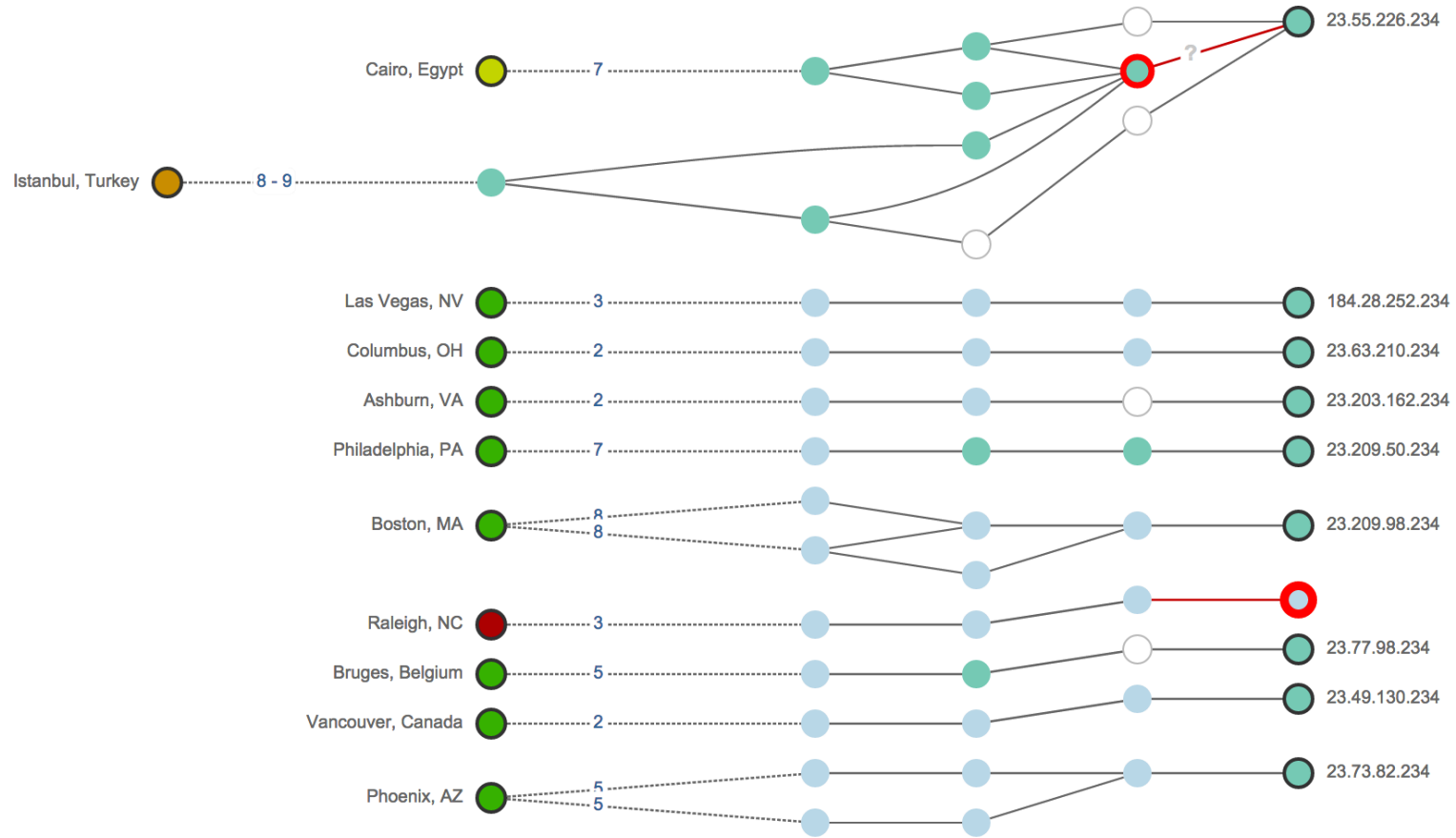
# DDoS Attack: Mitigation Handoff Using BGP





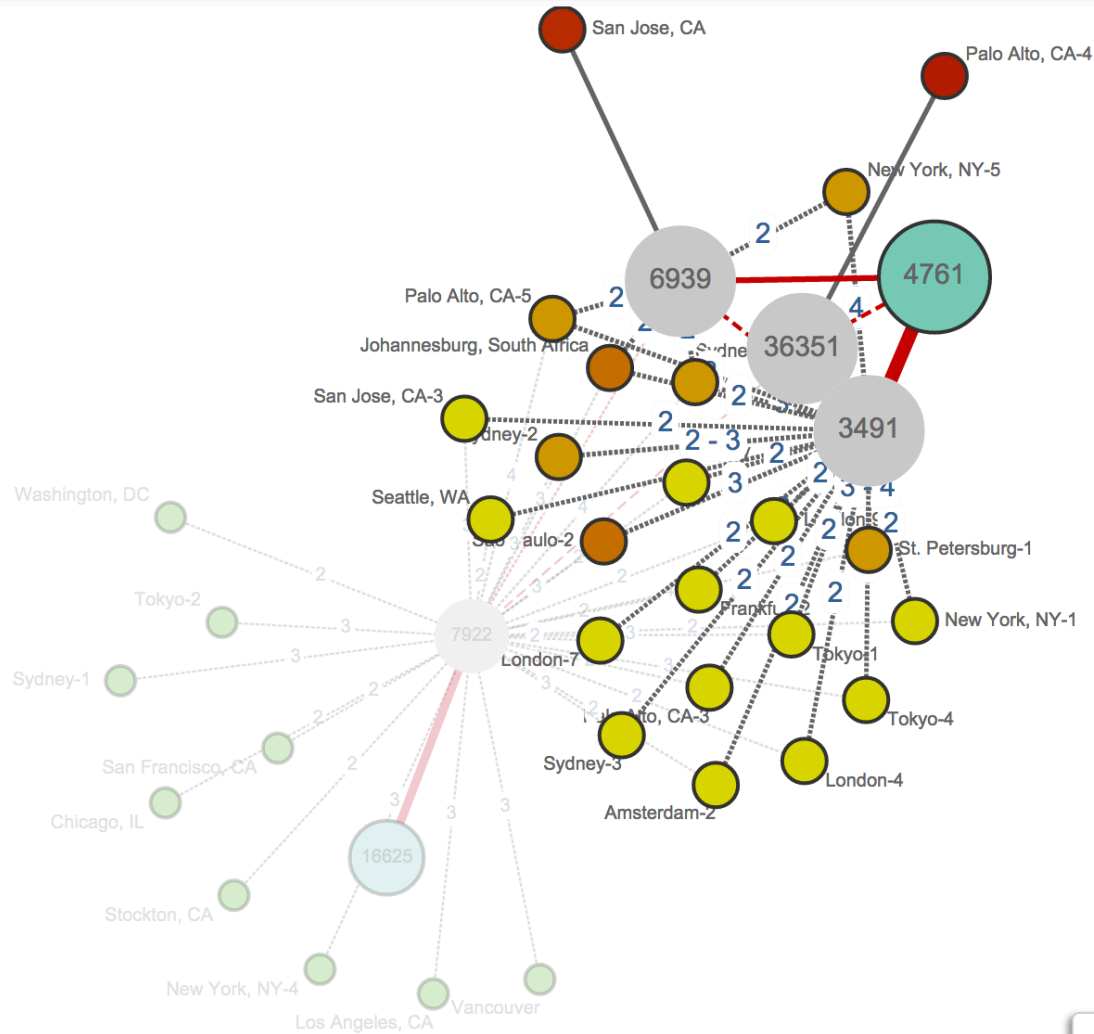


# Lets look at the network





# Indosat advertising the same prefix block



INDOSAT (AS 4761) (Origin)	
Primary Country	Indonesia
Global Network Rank	136
Prefixes Announced	349

# Thanks !

---

[mohit@thousandeyes.com](mailto:mohit@thousandeyes.com)