ThousandEyes

UKNOF39

The Challenges of DNS Resolution in China

Tim Hale, Solutions Engineer

Why China?

“ In 2008 China became the largest population on the Internet.

As of July 2016, 730,723,960 people (53.2% of the country's total population) were Internet users.

"The World Factbook — Central Intelligence Agency". www.cia.gov.

A Different Internet: A different strategy

Frequent Congestion

- 10 backbone access points
- 2 dominant, government-controlled ISPs
  - China Unicom
  - China Telecom

The Great Firewall

- IP blocking
- Keyword filtering
- DNS tampering

ThousandEyes

Views > Tests

51

Demo - Tim Hale

Dashboard
Views
Alerts
Reports
Sharing
Saved Events

SETTINGS

Agents
Devices
Tests
Alerts
Labels
BGP Monitors

Current Test

A - Github DNS Server (China)

Run Now

Save

Share

Views

DNS
DNS Server

NETWORK
Overview
Path Visualization

ROUTING
BGP Route Visualization

Metric: Availability

Server: ns-1283.awsdns-32.or...

Agent: All agents

24h 7d 14d

Average Availability

100%

99%

08:00

08:00

Target Domain
github.com A

Showing data from **Tue, Jan 16 07:55 - 07:57 UTC** (2 Minutes Ago)

Latest

Map Servers Agents (to ns-1283.awsdns-32.org.)

Details for ns-1283.awsdns-32.org.

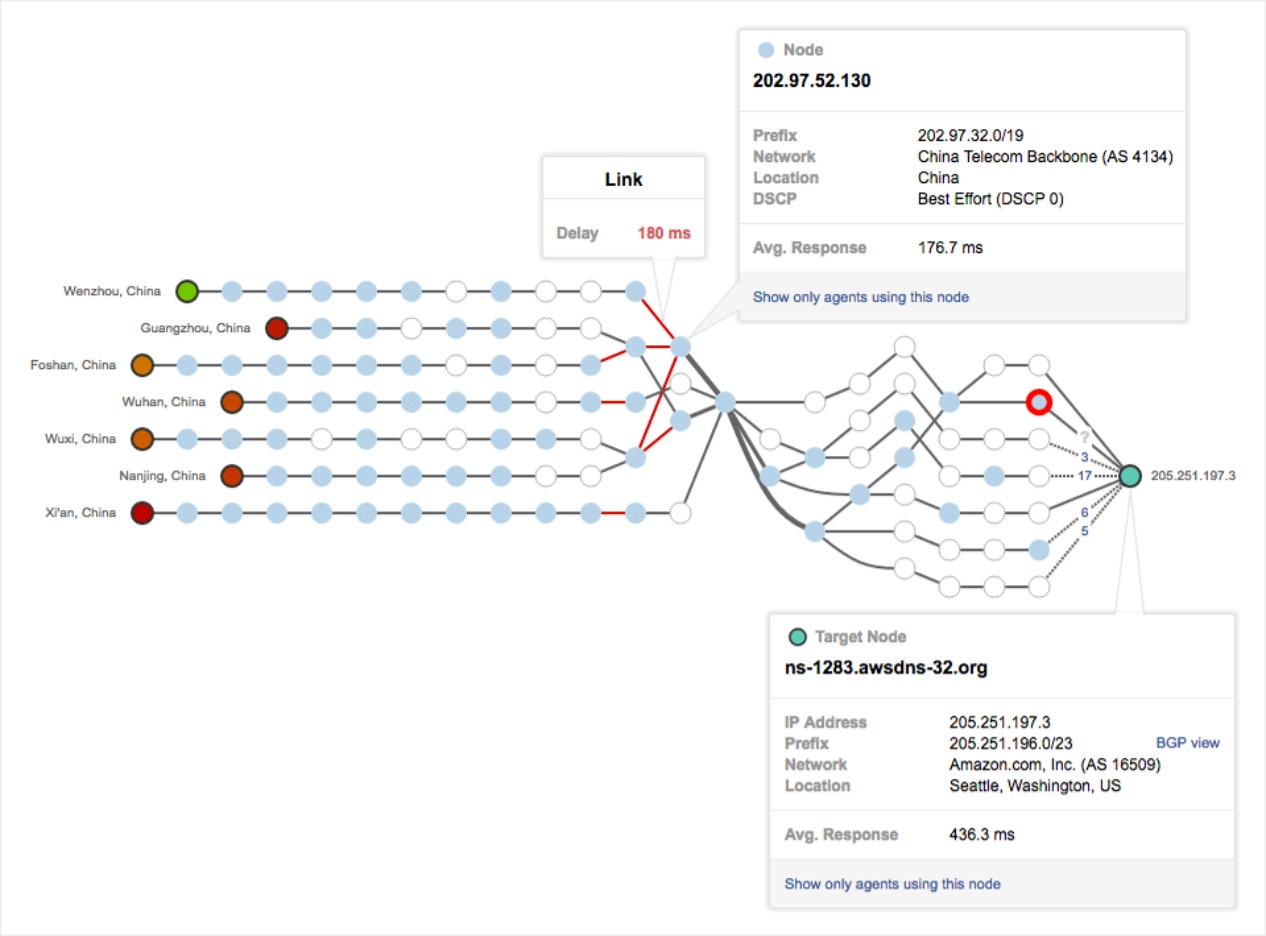
Availability 100%

Resolution Time 157 ms

Availability (%)

0 100

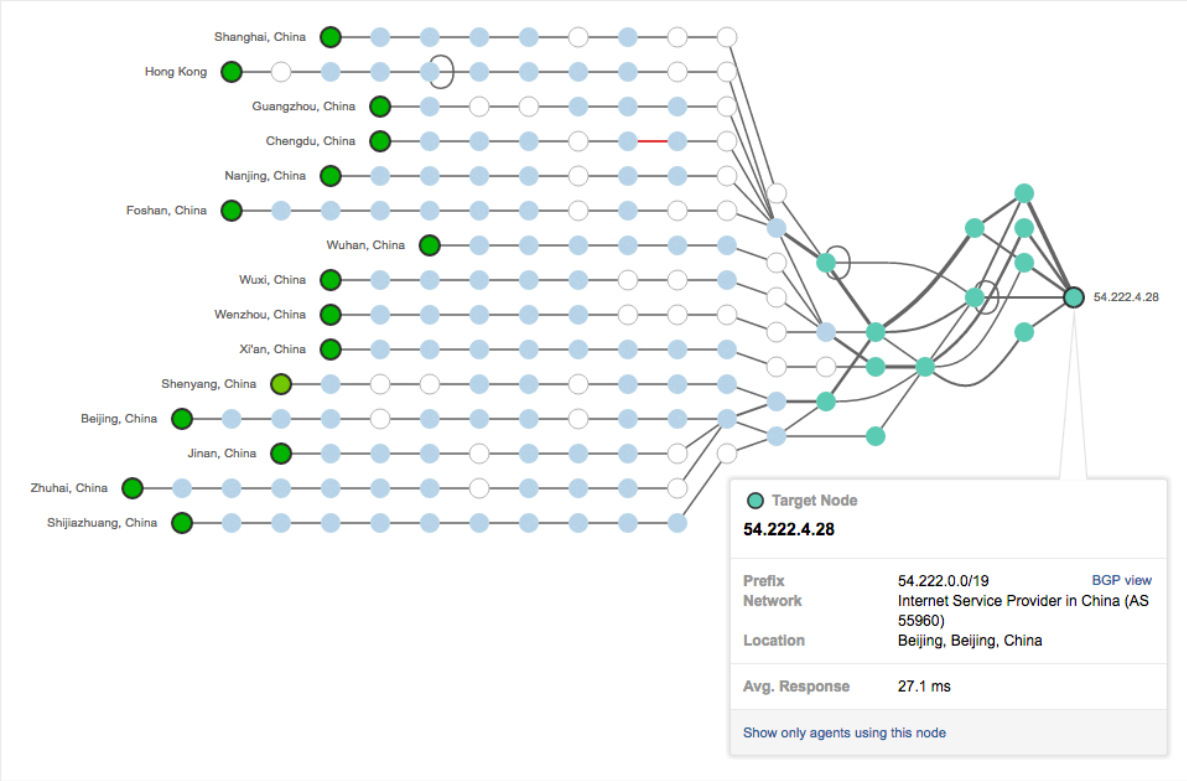
Outside China



Frequent Congestion

Packet loss

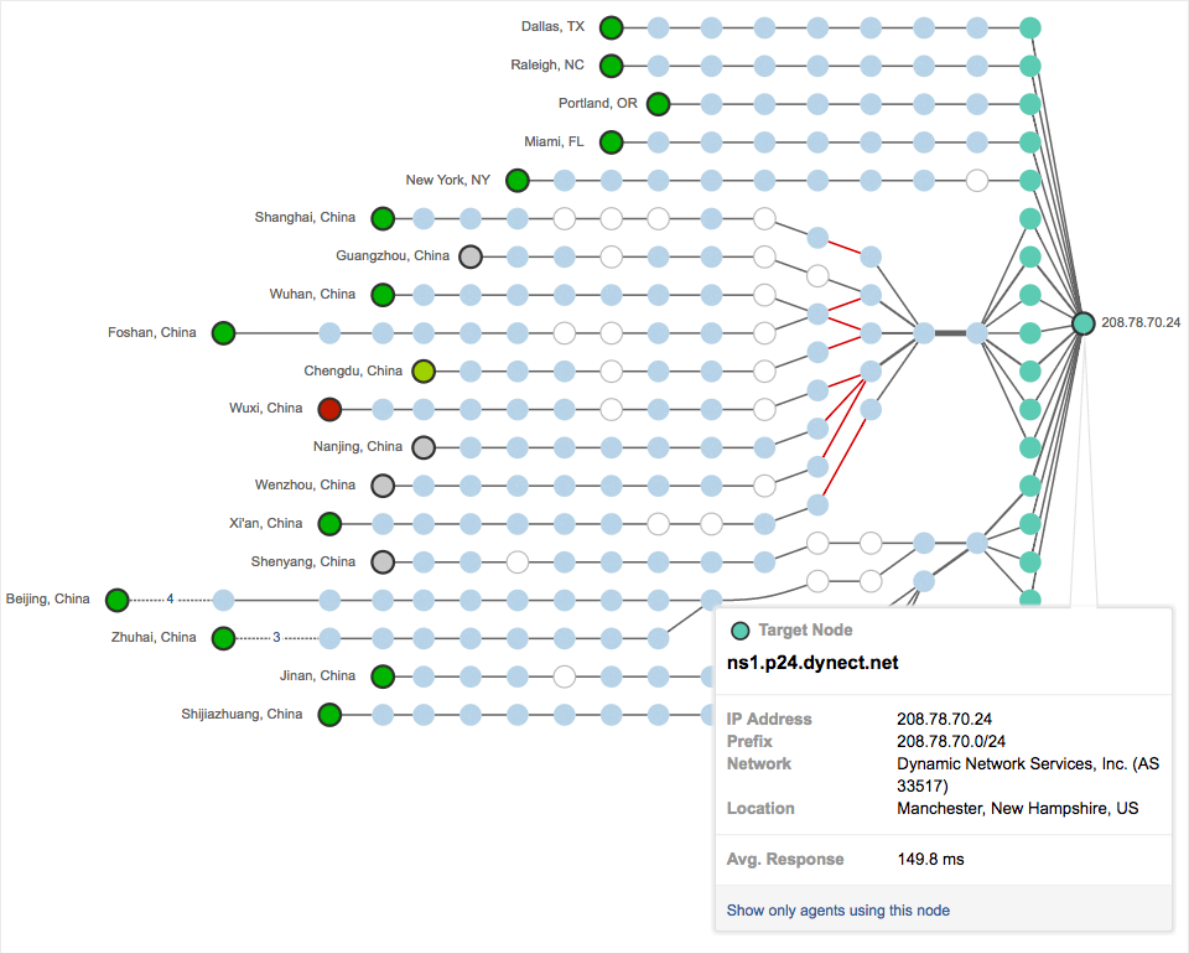
Inside China



Lower latency

Less packet loss

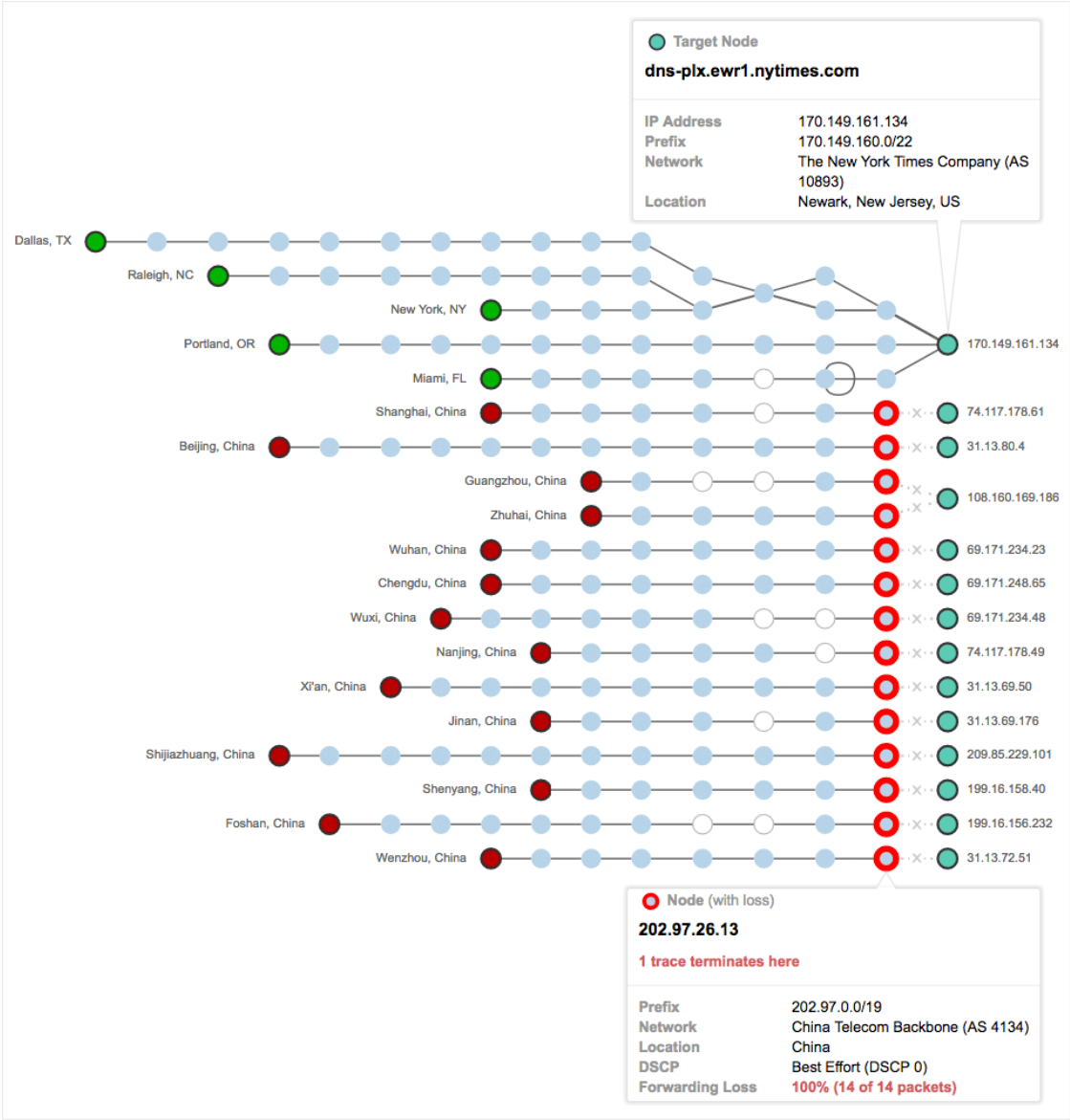
Uncensored?



nytimes.com

ns1.p24.
dynect.net

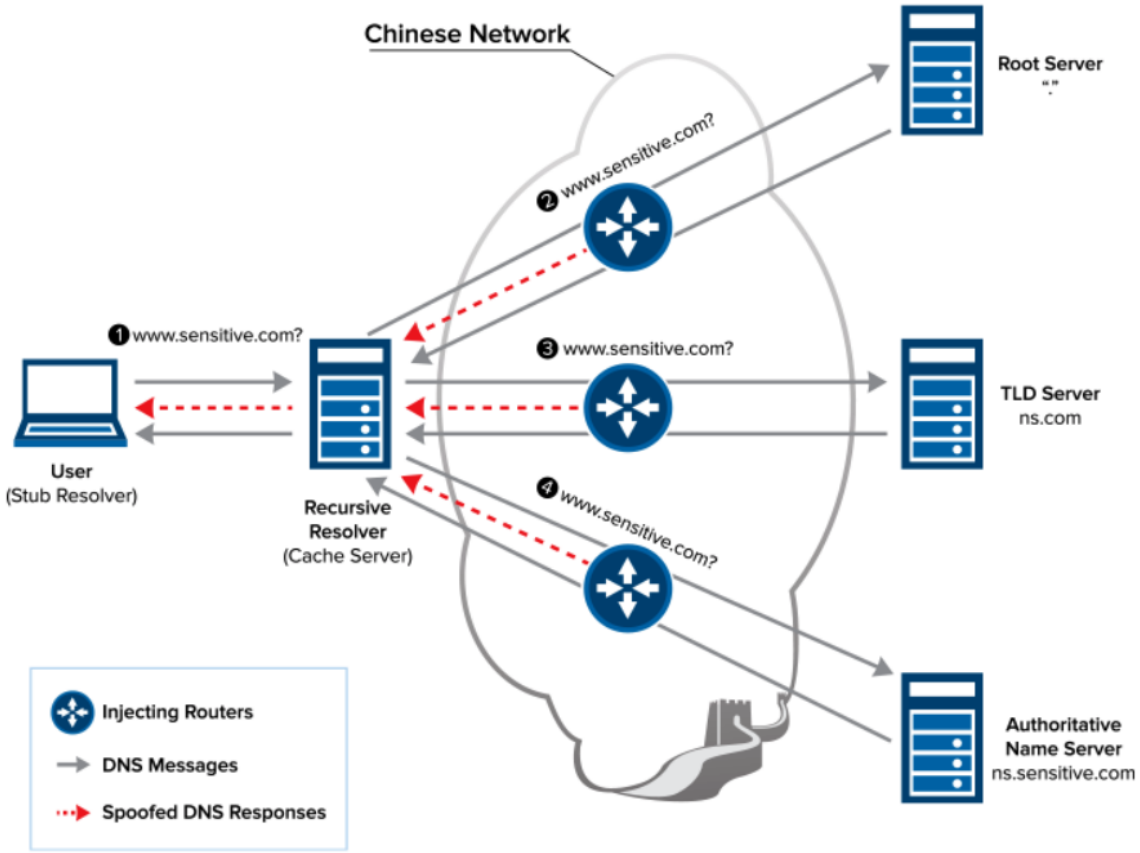
Censored



nytimes.com

dns-plx.ewr1.
nytimes.com

DNS Tampering



Cache poisoning

Keyword based hijacking

DNS Tampering

Map Servers **Agents (to dns-plx.ewr1.nytimes.com.)**

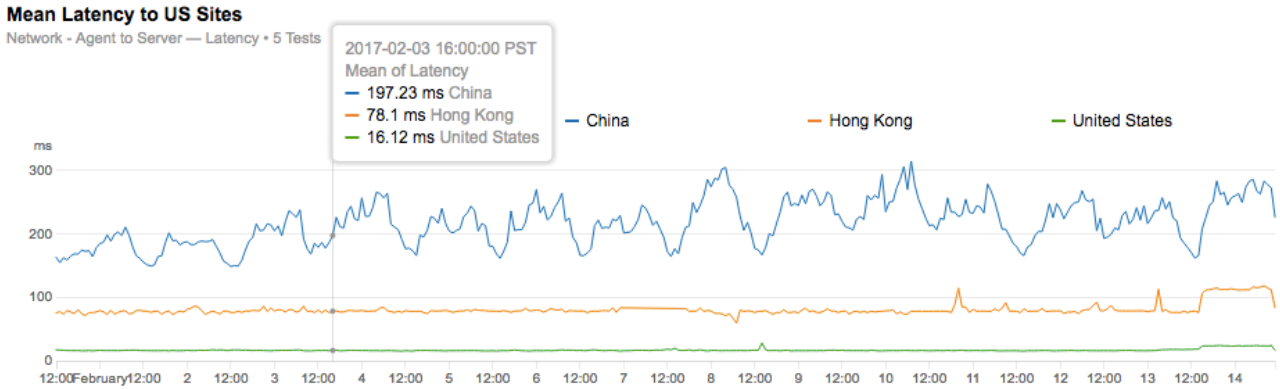
Agent	Date (EDT)	Mappings	Resolution Time (ms)
Wuhan, China	2017-03-14 19:23:25	31.13.78.66	19
Wenzhou, China	2017-03-14 19:23:50	31.13.76.8	9
Chengdu, China	2017-03-14 19:24:16	69.171.237.16	27
Dallas, TX	2017-03-14 19:22:47	151.101.1.164 151.101.65.164 151.101.129.164 151.101.193.164	41
Portland, OR	2017-03-14 19:23:11	151.101.1.164 151.101.65.164 151.101.129.164 151.101.193.164	73
Raleigh, NC	2017-03-14 19:23:01	151.101.193.164 151.101.1.164 151.101.65.164 151.101.129.164	15
Wuxi, China	2017-03-14 19:23:49	168.143.162.123	7
Detroit, MI	2017-03-14 19:22:58	151.101.129.164 151.101.193.164 151.101.1.164 151.101.65.164	34

Suspiciously Low latency

IPs returned are from other blocked destinations

What to Expect

- Incorrect mappings
  - DNS poisoning and hijacking
- Volatile conditions with high latency and loss
  - Evolving censorship mechanisms (keyword filtering, IP blocking)
  - Frequent congestion, especially when crossing the GFW
- Diurnal patterns in latency and loss for outbound traffic



What to Do About It

- Continuously monitor DNS tests and alerts to check if records:
  - Are always available
  - Have the correct mappings
  - Are served up quickly
- Benchmark performance metrics like latency, packet loss
  - Adjust your expectations and alerts accordingly

ThousandEyes

Thank You