

Pinpointing Anomalies in Large-Scale Traceroute Measurements

Romain Fontugne & Kenjiro Cho

November 10, 2016

On going research work conducted at IIJ-II

In collaboration with:

- Emile Aben (RIPE NCC)
- Cristel Pelsser (University of Strasbourg)
- Randy Bush (IIJ)

Agenda

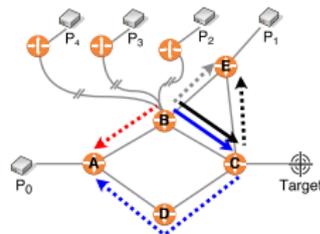
Background:

- Understanding Internet health
- Challenges



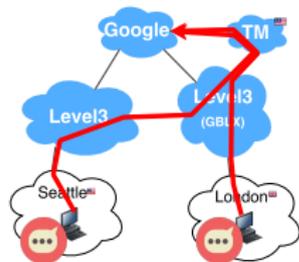
Detect and locate Internet congestion:

- Analysis of traceroutes from RIPE Atlas
- Differential RTT and robust statistics

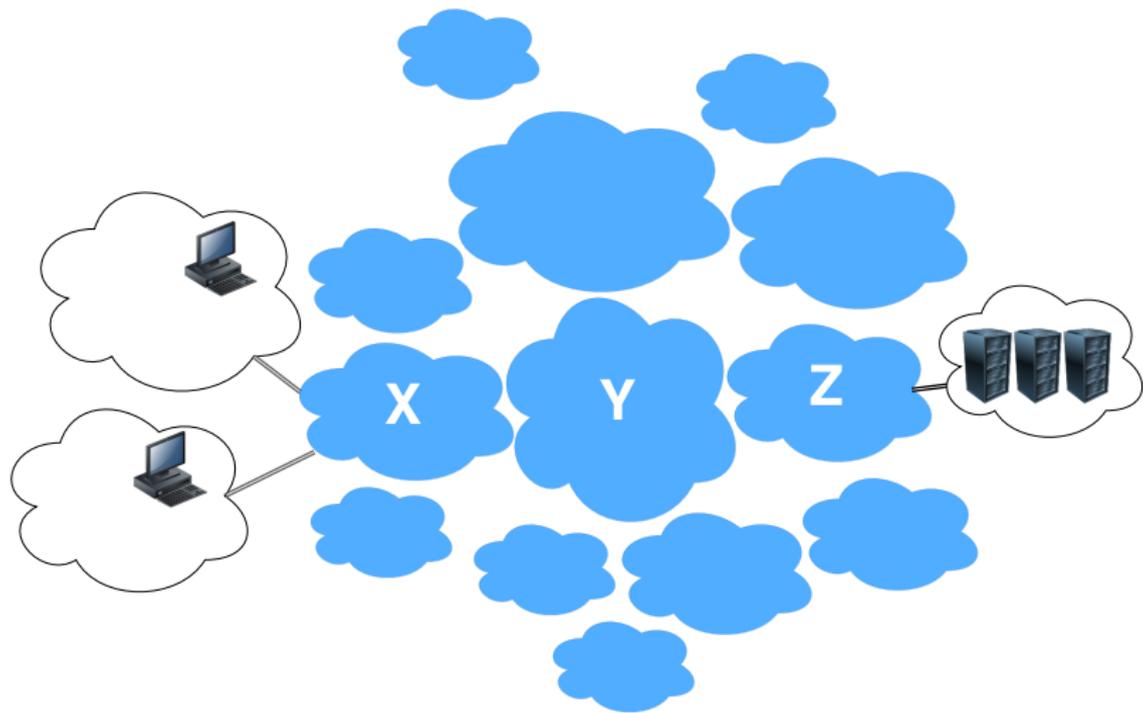


Results:

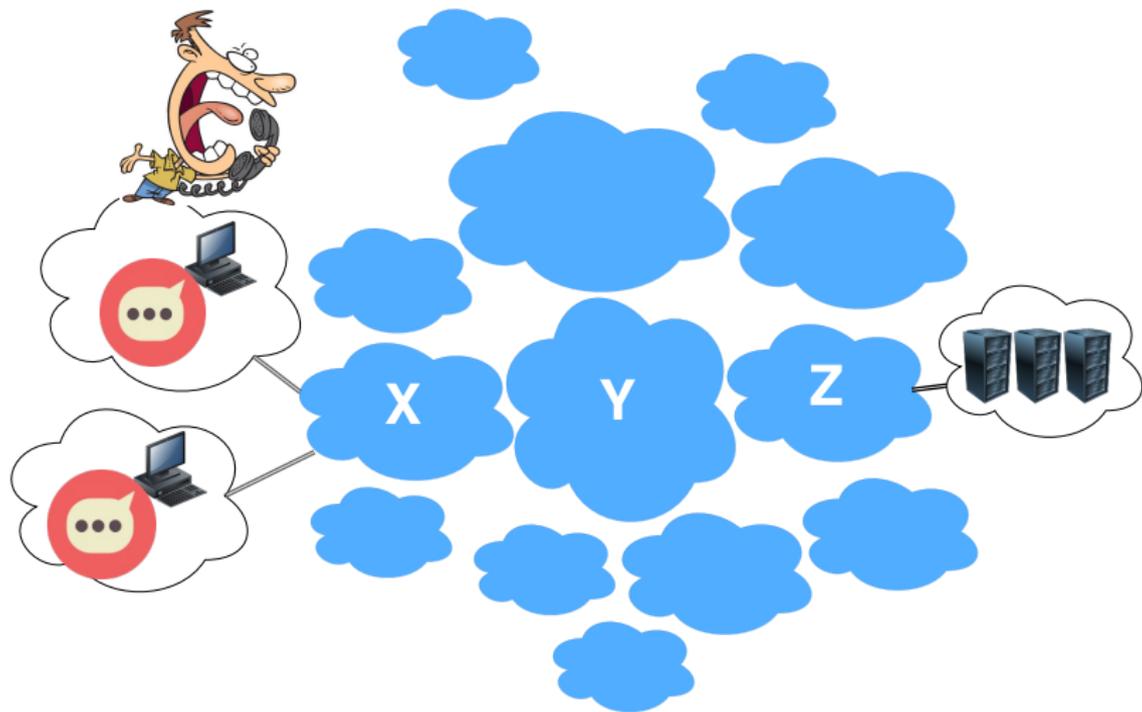
- Study cases: DDoS attack and BGP leak



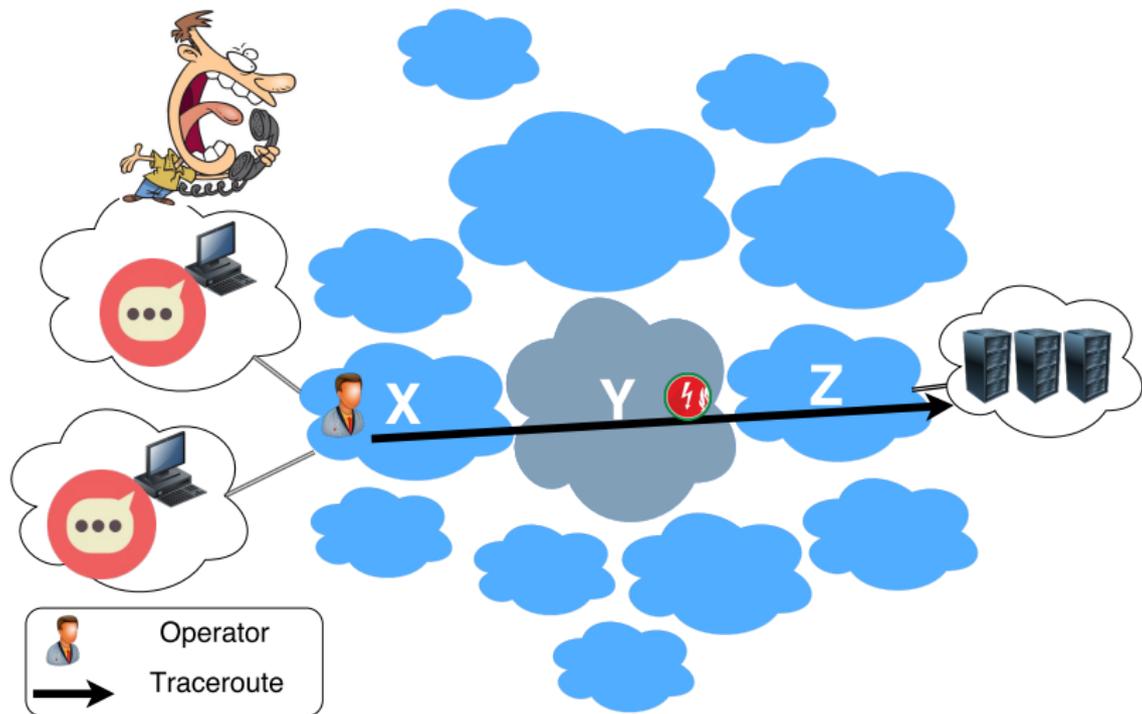
Understanding Internet health?



Understanding Internet health?



Understanding Internet health?



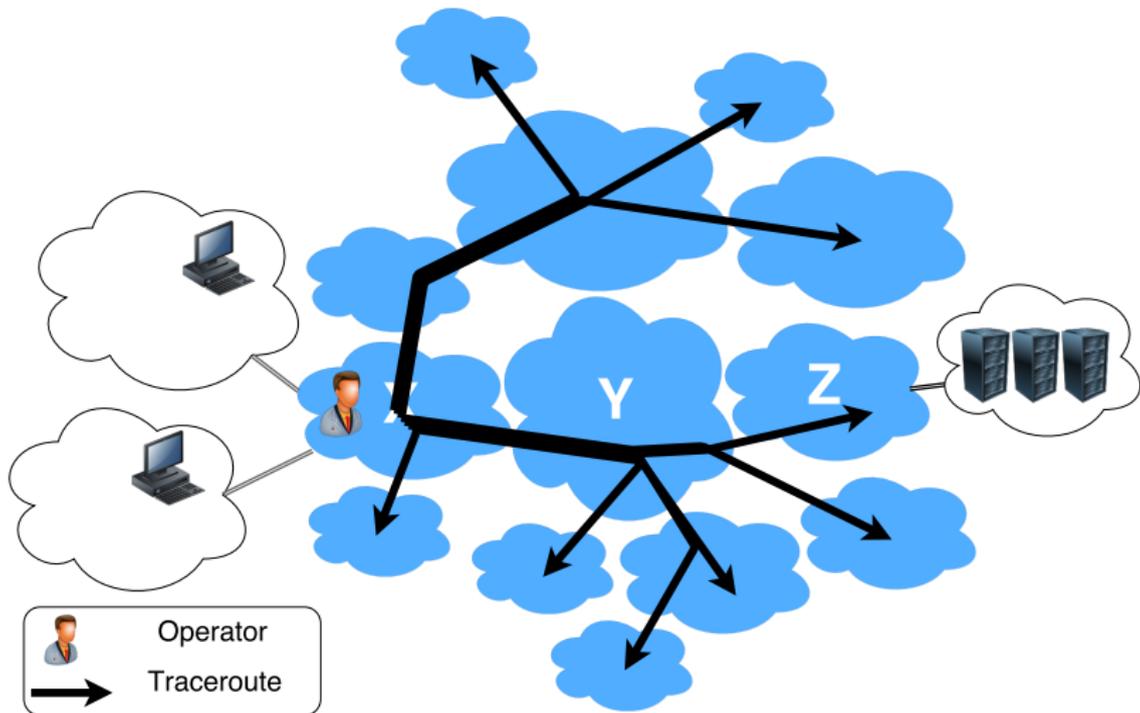
Understanding Internet health? (Problems)

Manual observations and operations

- Traceroute / Ping / Operators' group mailing lists
- Time consuming
- Slow process
- Small visibility

→ **Our goal: Pinpointing network disruptions (i.e. congestion and packet loss)**

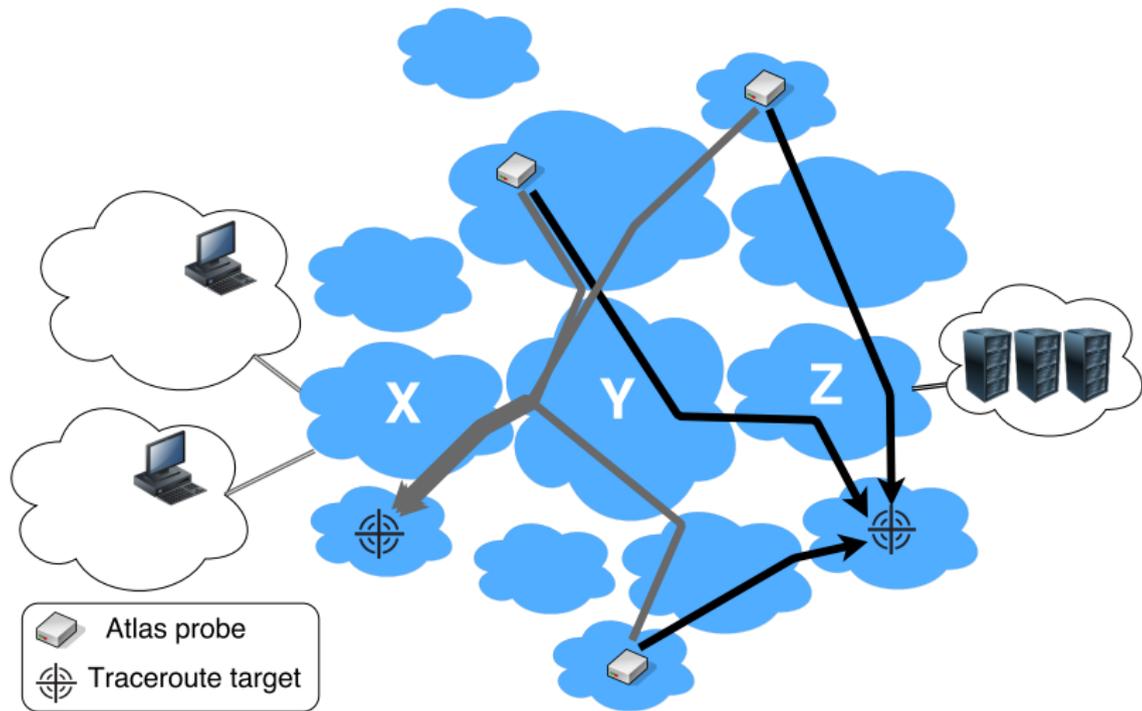
Silly solution: frequent traceroutes to the whole Internet!



→ Doesn't scale

→ Overload the network

Better solution: mine results from deployed platforms



→ Cooperative and distributed approach

→ Using existing data, no added burden to the network

Actively measures Internet connectivity

- Ethernet port
- Automatically perform active measurements: ping, **traceroute**, DNS, SSL, NTP and HTTP
- All results are collected by RIPE NCC



RIPE Atlas: coverage

9300+ active probes!



Two repetitive large-scale measurements

- *Builtin*: traceroute every 30 minutes to all DNS root servers (\approx 500 server instances)
- *Anchoring*: traceroute every 15 minutes to 189 collaborative servers

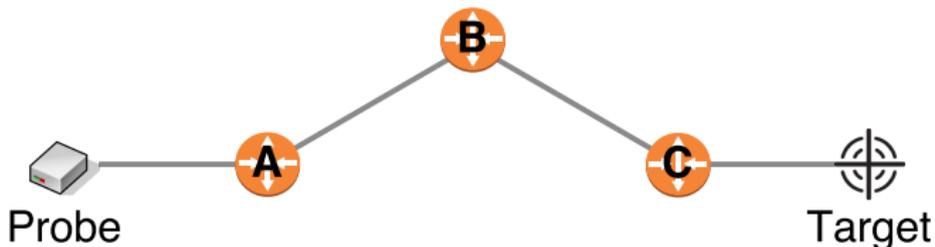
Analyzed dataset

- May to December 2015
- 2.8 billion IPv4 traceroutes
- 1.2 billion IPv6 traceroutes

Monitor delays with traceroute?

Traceroute to “www.target.com”

```
~$ traceroute www.target.com
traceroute to target, 30 hops max, 60 byte packets
 1  A          0.775 ms  0.779 ms  0.874 ms
 2  B          0.351 ms  0.365 ms  0.364 ms
 3  C          2.833 ms  3.201 ms  3.546 ms
 4  Target     3.447 ms  3.863 ms  3.872 ms
```



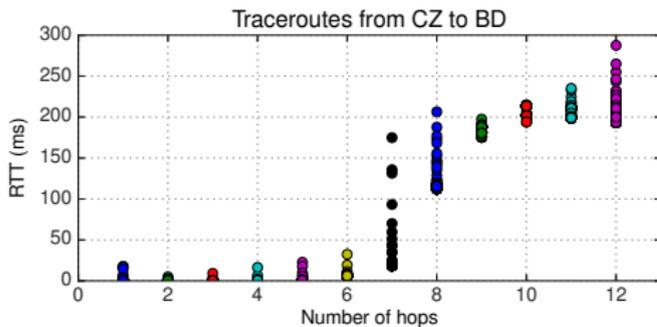
Round Trip Time (RTT) between B and C?

Report abnormal RTT between B and C?

Monitor delays with traceroute?

Challenges:

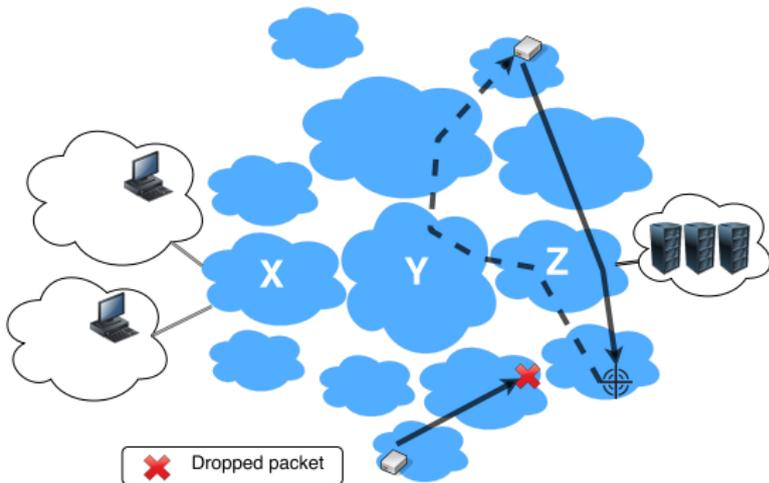
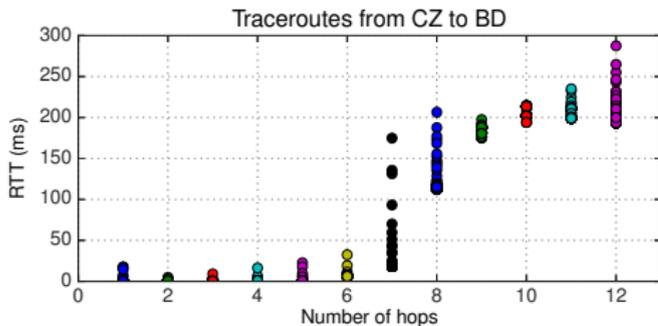
- Noisy data



Monitor delays with traceroute?

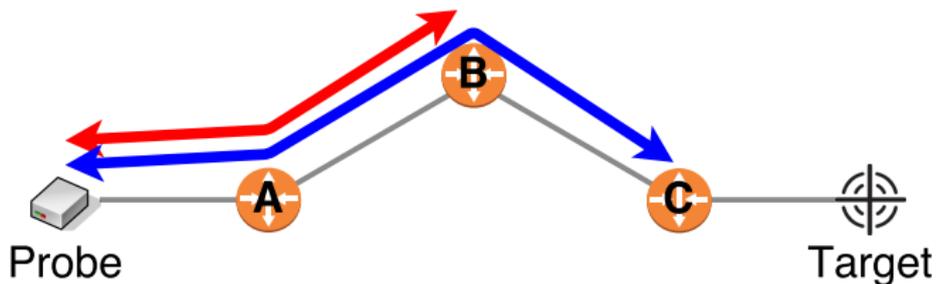
Challenges:

- Noisy data
- Traffic asymmetry
- Packet loss



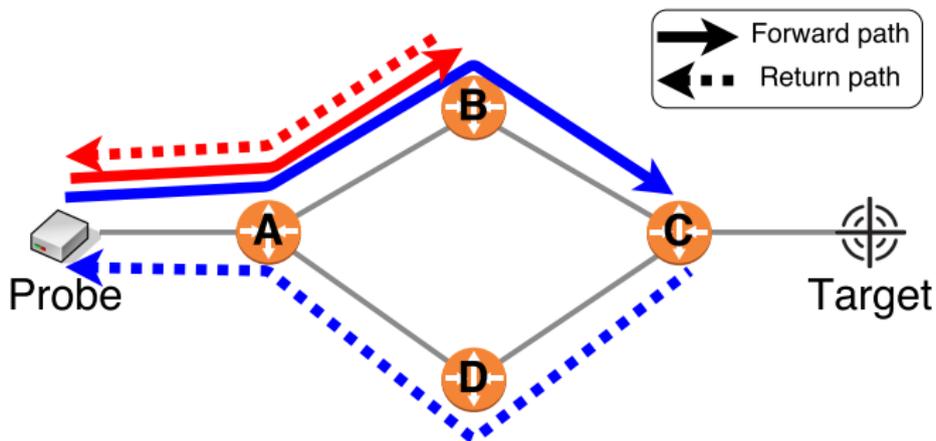
What is the RTT between B and C?

```
~$ traceroute www.target.com
traceroute to target, 30 hops max, 60 byte packets
 1  A           0.775 ms  0.779 ms  0.874 ms
 2  B           0.351 ms  0.365 ms  0.364 ms
 3  C           2.833 ms  3.201 ms  3.546 ms
 4  Target      3.447 ms  3.863 ms  3.872 ms
```



$$RTT_C - RTT_B = RTT_{CB}?$$

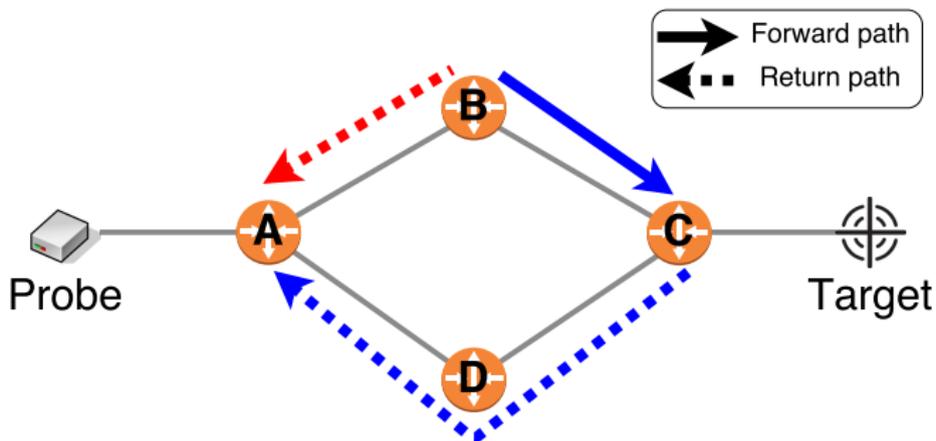
What is the RTT between B and C?



$$RTT_C - RTT_B = RTT_{CB}?$$

- No!
- Traffic is asymmetric
- RTT_B and RTT_C take **different return paths!**

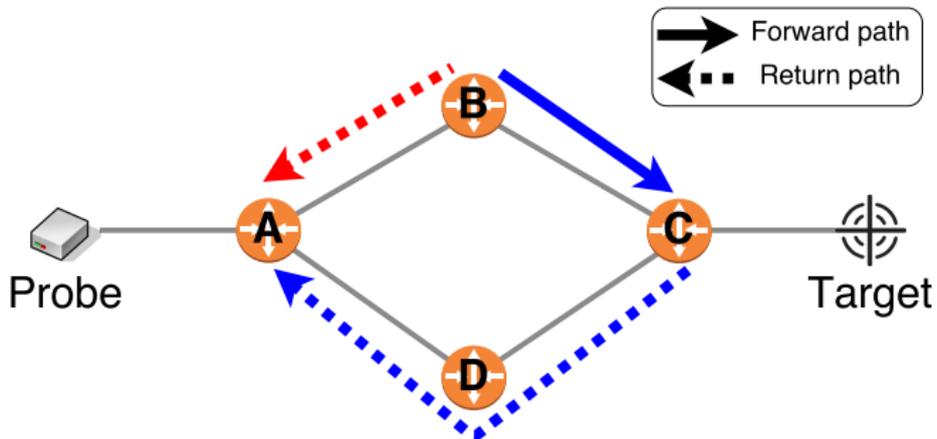
What is the RTT between B and C?



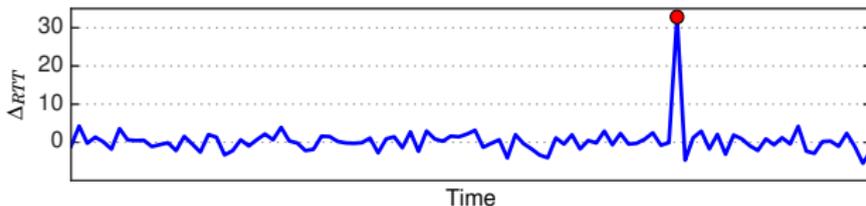
$$RTT_C - RTT_B = RTT_{CB}?$$

- No!
- Traffic is asymmetric
- RTT_B and RTT_C take **different return paths!**
- **Differential RTT:** $\Delta_{CB} = RTT_C - RTT_B = d_{BC} + e_p$

Problem with differential RTT



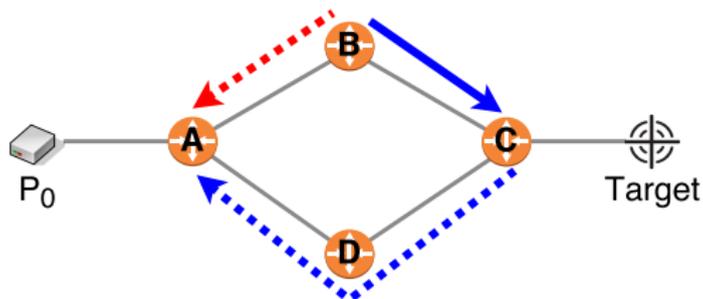
Monitoring Δ_{CB} over time:



→ Delay change on BC? CD? DA? BA???

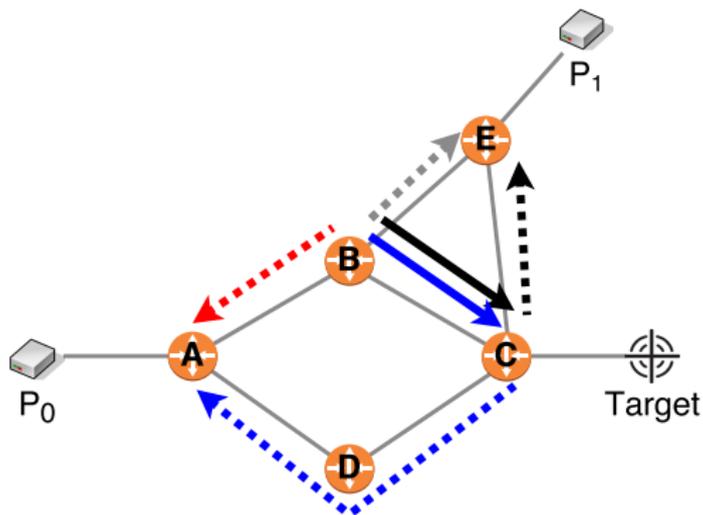
Proposed Approach: Use probes with different return paths

Differential RTT: $\Delta_{CB} = x_0$



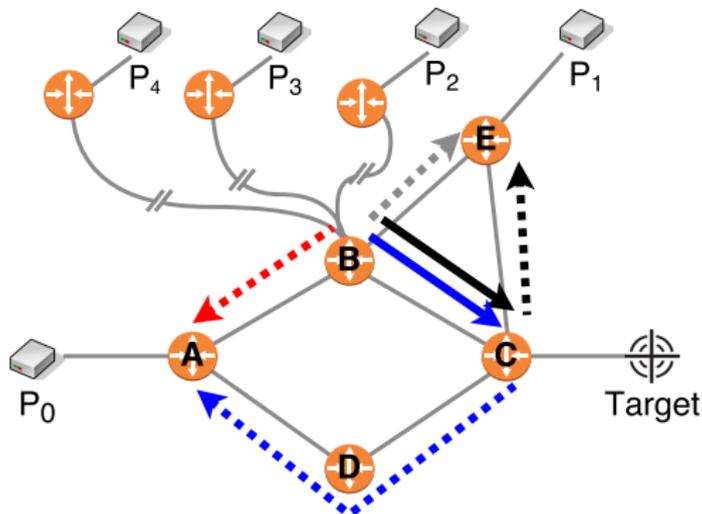
Proposed Approach: Use probes with different return paths

Differential RTT: $\Delta_{CB} = \{x_0, x_1\}$



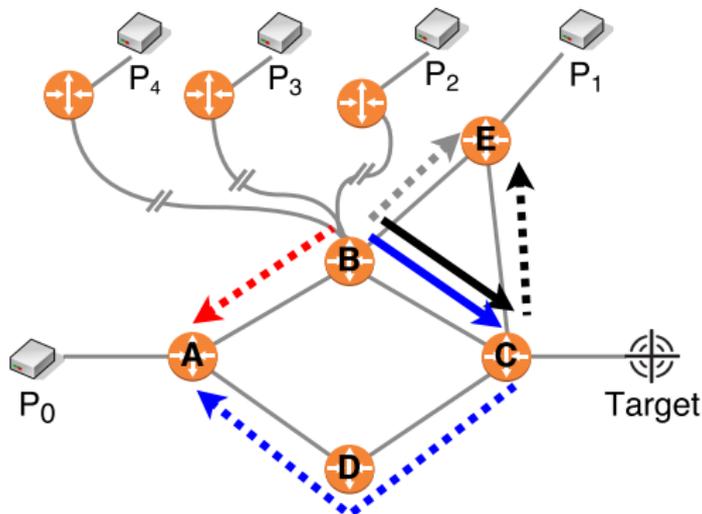
Proposed Approach: Use probes with different return paths

Differential RTT: $\Delta_{CB} = \{x_0, x_1, x_2, x_3, x_4\}$



Proposed Approach: Use probes with different return paths

Differential RTT: $\Delta_{CB} = \{x_0, x_1, x_2, x_3, x_4\}$

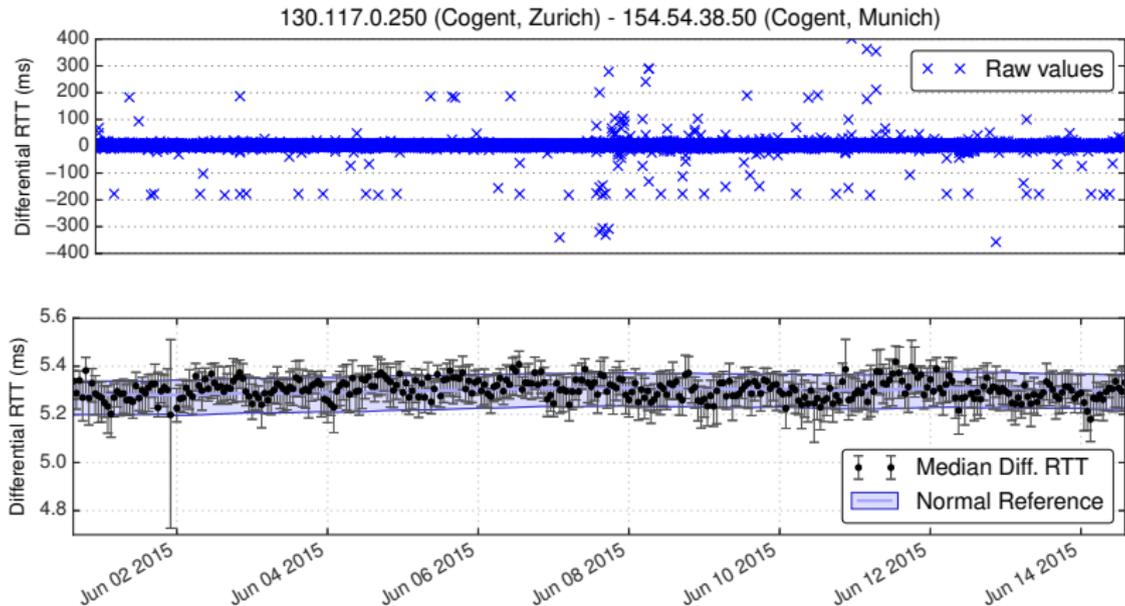


Median Δ_{CB} :

- Stable if a few return paths delay change
- Fluctuate if delay on BC changes

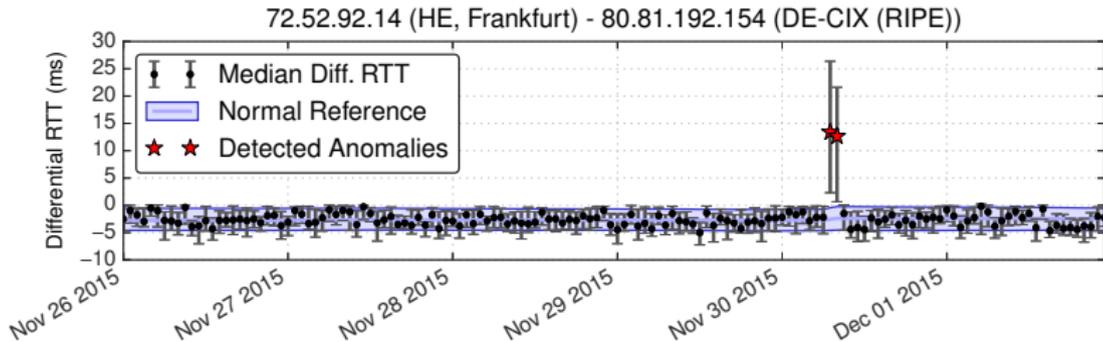
Median Diff. RTT: Example

Tier1 link, 2 weeks of data, 95 probes:



- **Stable** despite noisy RTTs (not true for average)
- Normally distributed

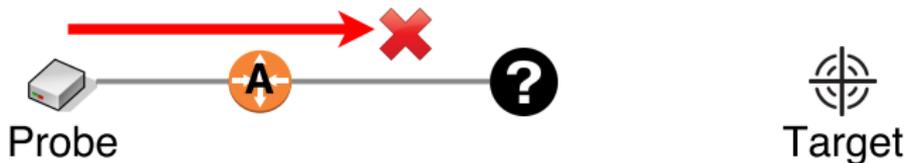
Detecting congestion



Significant RTT changes:

Confidence interval not overlapping with the normal reference

Packet loss

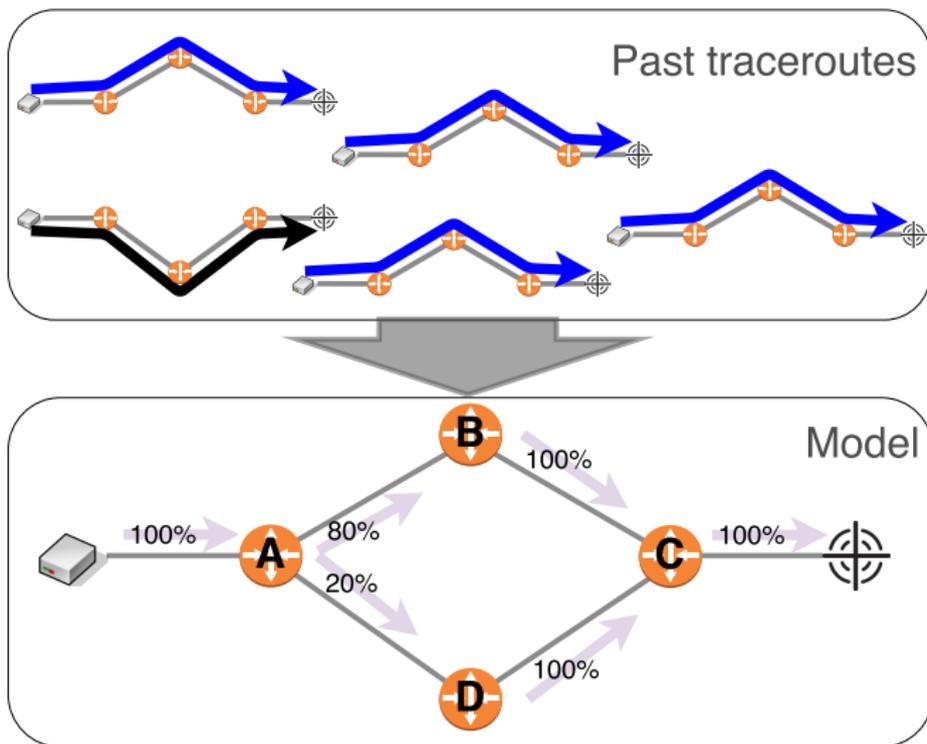


Worst case: router is not responding

- Cannot obtain RTT values
- Need to identify the faulty link

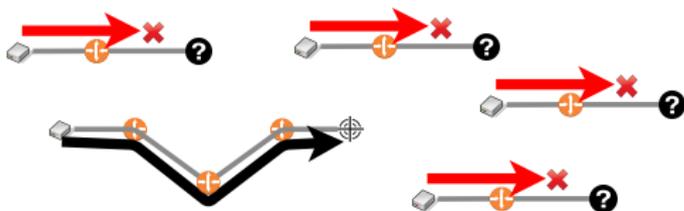
Packet forwarding model

Learn usual paths from past traceroutes:

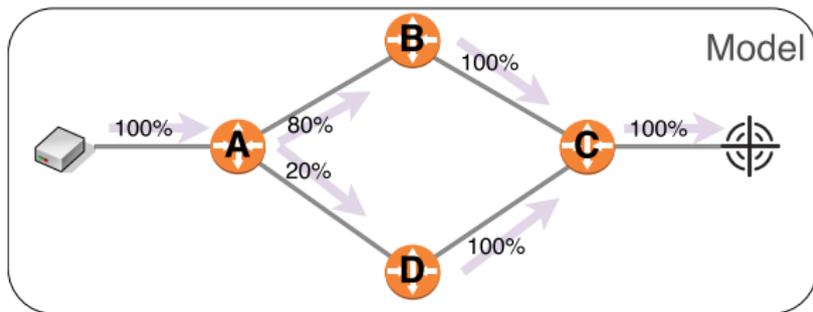


Identifying faulty links

In case of packet loss:



Query the model for the expected next hop



→ Link AB is dropping packets!

Analyzed dataset

- Atlas *builtin/anchoring* measurements
- From May to Dec. 2015
- Observed 262k IPv4 and 42k IPv6 links

We found a lot of congested links!

Let's see only two significant examples

Study case: DDoS on DNS root servers

Two attacks:

- Nov. 30th 2015
- Dec. 1st 2015

Almost all server are anycast

- Congestion at the 531 sites?
- Found 129 instances altered by the attacks



The Register
Hit the head that leads it

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWARE

Networks

Internet's root servers take hit in DDoS attack

Who's testing the limits of the DNS system?

8 Dec 2015 at 23:10, Karen McCarthy

The internet's root servers came under a o effectively knocked three of the 13 critical p

The attack came just days before the Janet

According to a first analysis of the root serv attack occurred on November 30, 2015 bet

Many, but not all, of the root servers receive flood network connections and cause time messages for a single domain name; the s

Ultimately, the operators affected by the atts proper analysis is now underway to discov

Of perhaps most concern is the fact that in deal with such an attack, a number of the s

The root servers themselves make up the g as a sort of global directory for all the other

Due to the internet's design, the servers th you compare it to what companies like Goog introduce problems for the wider internet, thousands of other servers.

That said, any attack on the DNS' infrastru larger than a day, it would start causing sig

0.66% 99% Data resolution: 10 minutes

The Hacker News
Security in a serious way

Someone Just Tried to Take Down Internet's Backbone with 5 Million Queries/Sec

Wednesday, December 09, 2015

112 1 Like 1.5K Shares 650K 1049 58 1437

The Internet's Backbone

DNS Root Servers Hit by a Massive Cyber Attack

Someone just DDoSed one of the most critical organs of the internet anatomy - **The Internet's DNS Root Servers**.

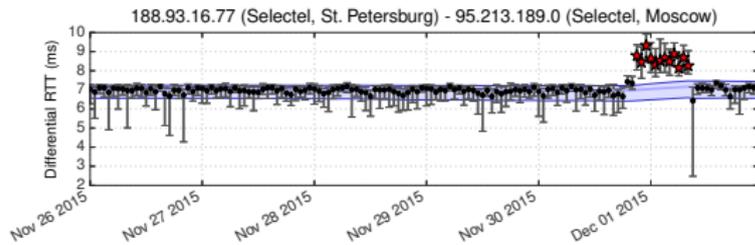
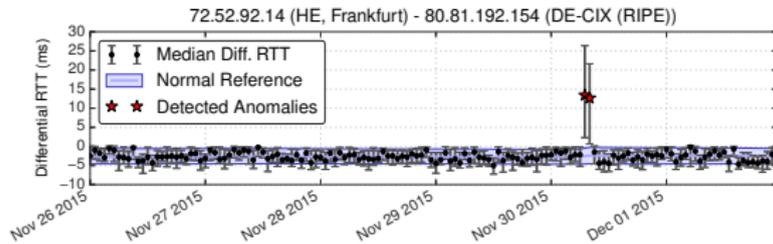
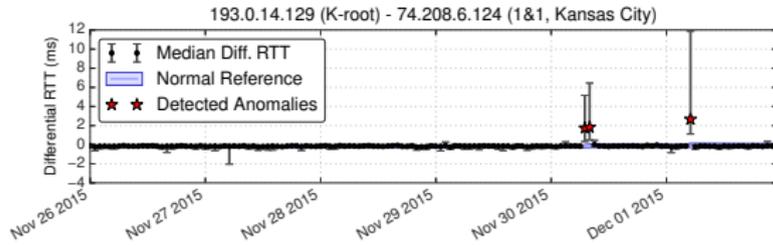
Early last week, a flood of as many as 5 Million queries per second hit many of the Internet's DNS (Domain Name System) Root Servers that act as the authoritative reference for mapping domain names to IP addresses and are a total of 13 in numbers.

The attack, commonly known as **Distributed Denial of Service (DDoS)** attack, took place on two separate occasions.

The first DDoS attack to the Internet's backbone root servers launched on *November 30* that lasted 160 minutes (*almost 3 hours*), and the second one started on *December 1* that lasted almost an hour.

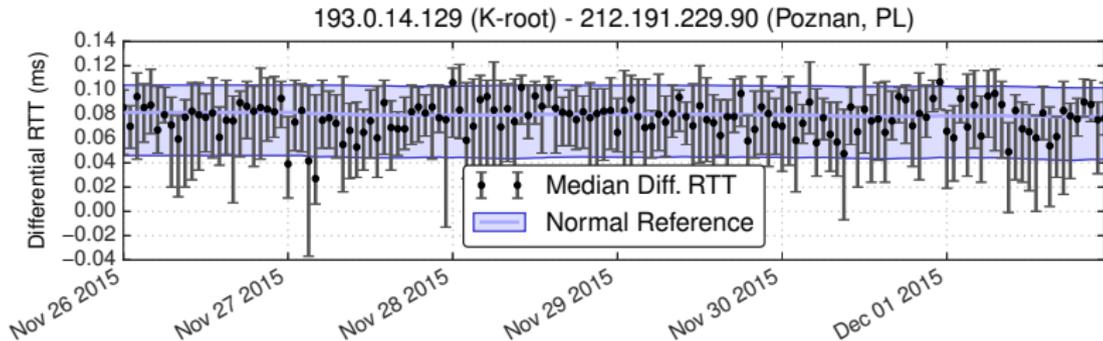
Massive Attacks Knocked Many of the 13 Root Servers Offline

Observed congestion



- Certain servers are affected only by one attack
- Continuous attack in Russia

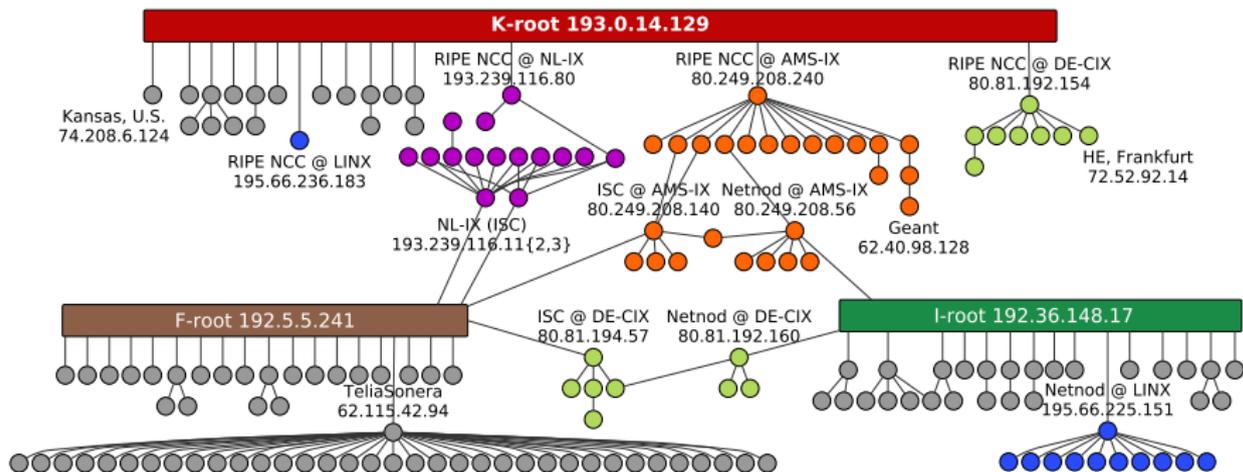
Unaffected root servers



Very stable delay during the attacks

- Thanks to anycast!
- Far from the attackers

Congested links for servers F, I, and K



→ **Concentration of malicious traffic in IXPs**

Study case: Telekom Malaysia BGP leak

itnews GOVERNMENT IT INFOSEC FINANCEIT TELCO

Benchmark Awards Reports Blogs Tutorials CIO Challenge Whitepapers What's On

Australia's internet hit hard by massive Malaysian route leak

By Jaha Saarenen
Jun 15 2015
11:45AM

Telekom Malaysia apologises for BGP bungle.

Related Articles:

- Rainlink locates interconnector cable fault
- Australian plan high-speed fibre research tested
- US govt to place export restrictions on China's 5TE
- NSN to deploy skinnier fibre to lower build costs

Previous Story

Massive route leak causes Internet slowdown

www.bgpmon.net/massive-route-leak-cause-internet-slowdown/

BGPMON Now part of **OpenBG**

HOME BLOG ABOUT US PRODUCTS AND SERVICES NEWS AND PRESS CLIENT PORT

Massive route leak causes Internet slowdown

Posted by Andree Tooni - June 12, 2015 - BGP Instability - No Comments

Earlier today a massive route leak initiated by Telekom Malaysia (AS4788) caused significant network problems for the global routing system. Primarily affected was Level3 (AS3549 - formerly known as Global Crossing) and their customers. Below are some of the details as we know them now.

Starting at 08:43 UTC today June 12th, AS4788 Telekom Malaysia started to announce about 179,000 of prefixes to Level3 (AS3549, the Global crossing AS), whom in turn accepted

Global Collateral Damage of TMnet leak

research.dyn.com/2015/06/global-collateral-damage-of-tmnet-leak/

Dyn Research
THE NEW HOME OF **renesys**

HOME TOPICS PRESENTATIONS ABOUT OUTAGES DYN CONTENT HUB

JUNE 12, 2015 COMMENTS (1) VIEWS: 4114 SECURITY, UNCLASSIFIED DUAL PRIORITY

Global Collateral Damage of TMnet leak

Previous Story

The Washington Post recently published a [great piece](#) about the development and current weaknesses of the Border Gateway Protocol (BGP, which is used to route all internet traffic). This morning [Telekom Malaysia](#) (a.k.a TMnet) helped to illustrate the point made in the article by leaking almost half of the global multi-tenant site [Level3](#) at 08:43 UTC.

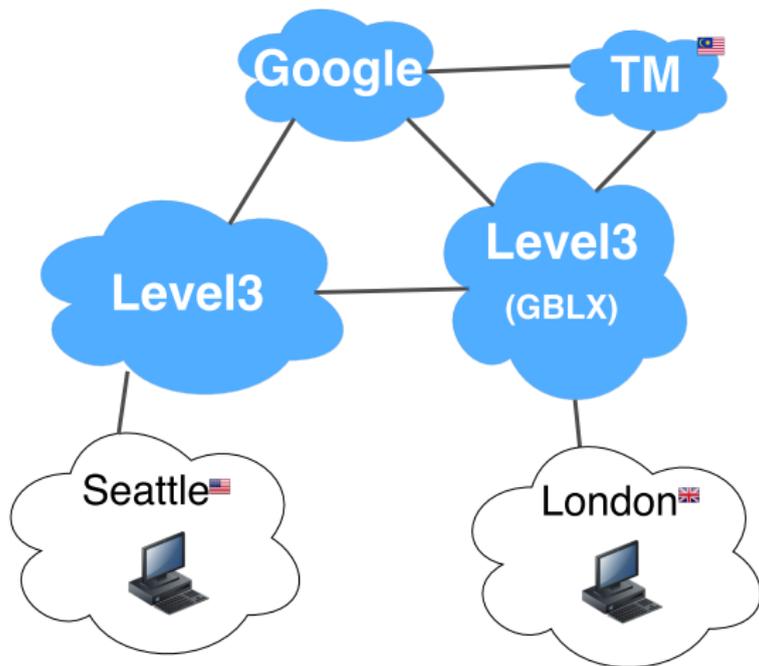
Popular Authors Archives

The New Threat: Targeted Internet Traffic Misdirection
DECEMBER 18, 2014

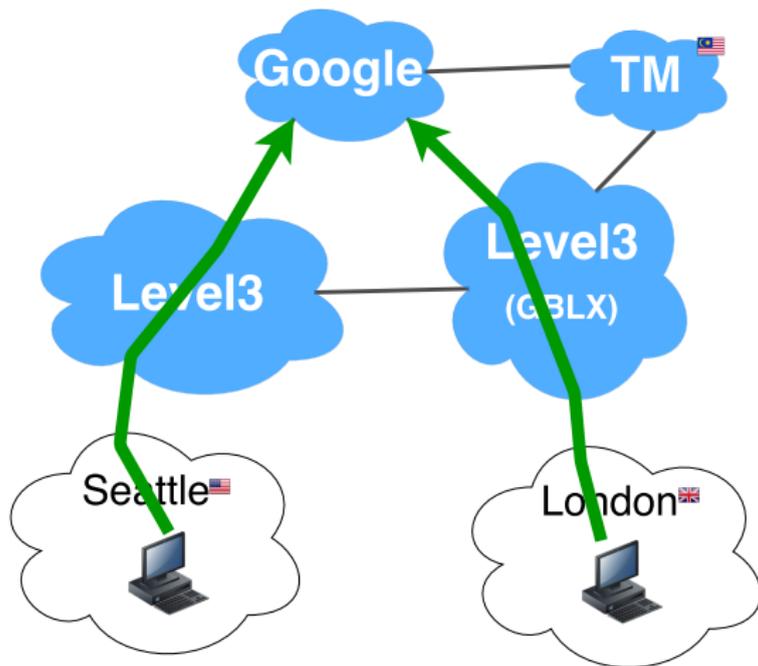
Egypt Leaves the Internet
JANUARY 20, 2011

Next Story =

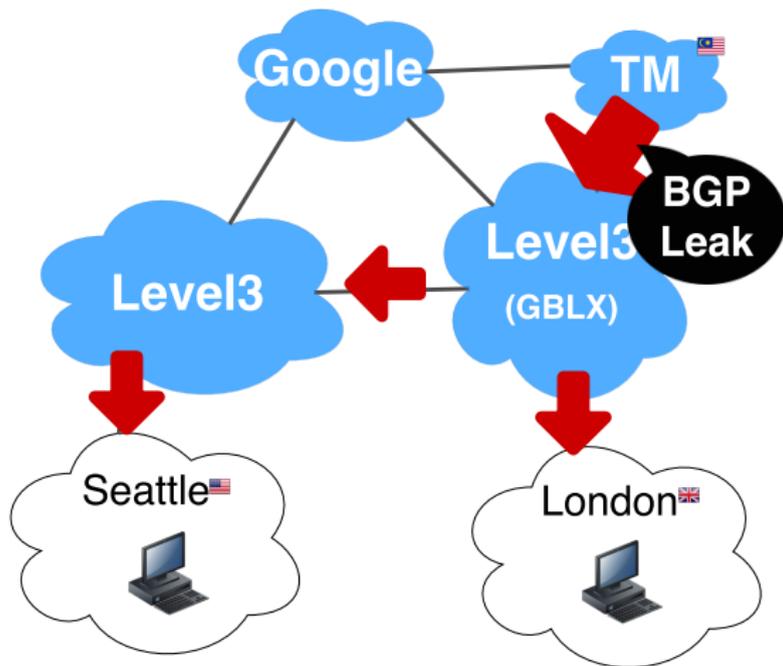
Study case: Telekom Malaysia BGP leak



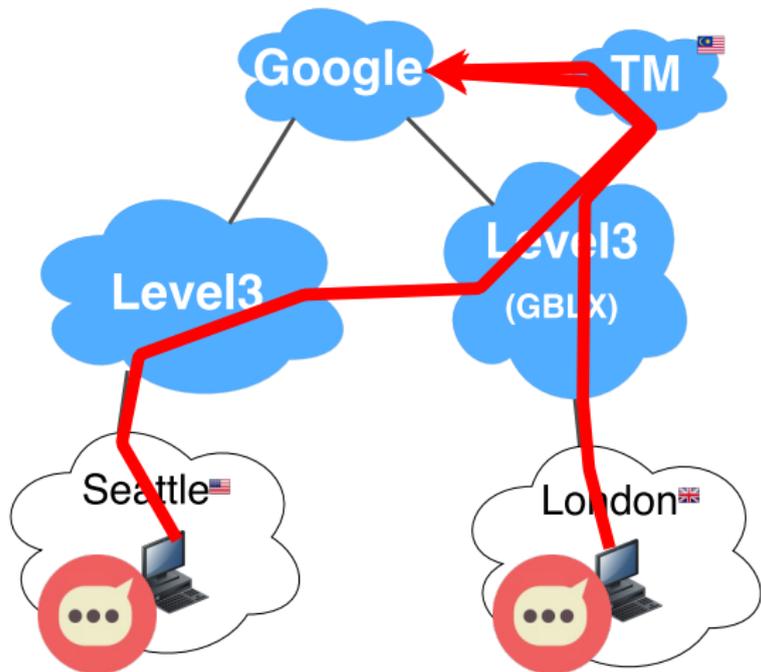
Study case: Telekom Malaysia BGP leak



Study case: Telekom Malaysia BGP leak



Study case: Telekom Malaysia BGP leak

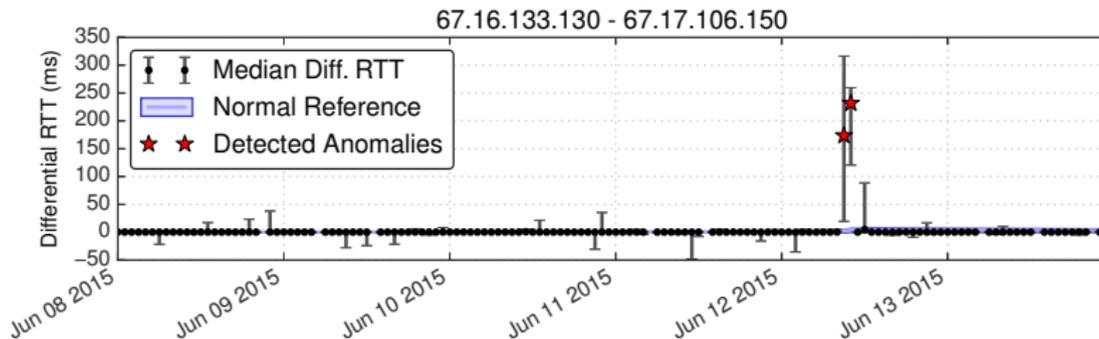


Not only with Google... but about **170k prefixes!**

Congestion in Level3

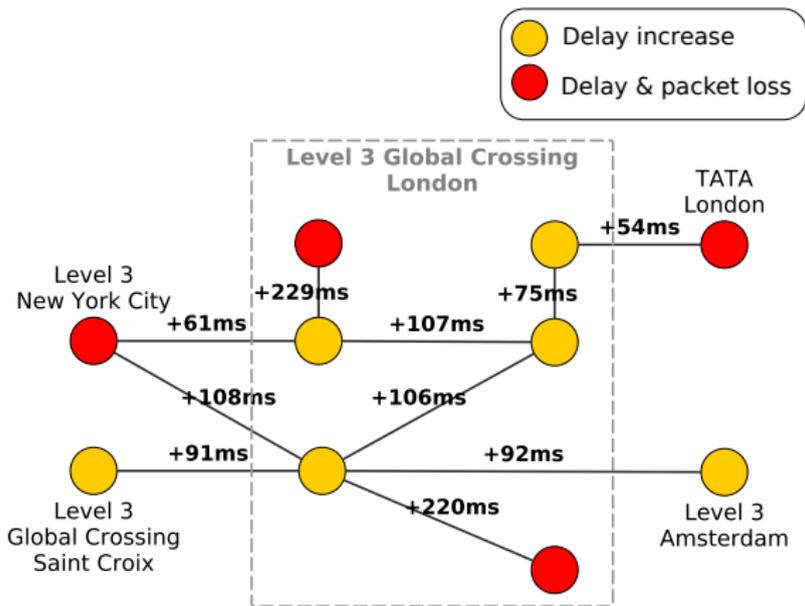
Rerouted traffic has congested Level3 (120 reported links)

- Example: 229ms increase between two routers in London!



Congestion in Level3

Reported links in London:



→ Traffic staying within UK/Europe may also be altered

Monitor delays with the Atlas platform

- Billions of (noisy) traceroutes

Detect and locate Internet congestion

- Robust statistical analysis
- Diverse root causes: remote attacks, routing anomalies, etc...
- Give a lot of new insights on reported events

On going work with RIPE NCC:

- Online detection and reports for network operators

References: <http://romain.iijlab.net/ihr/>