大規模tracerouteデータを使った異常発生箇所の特定

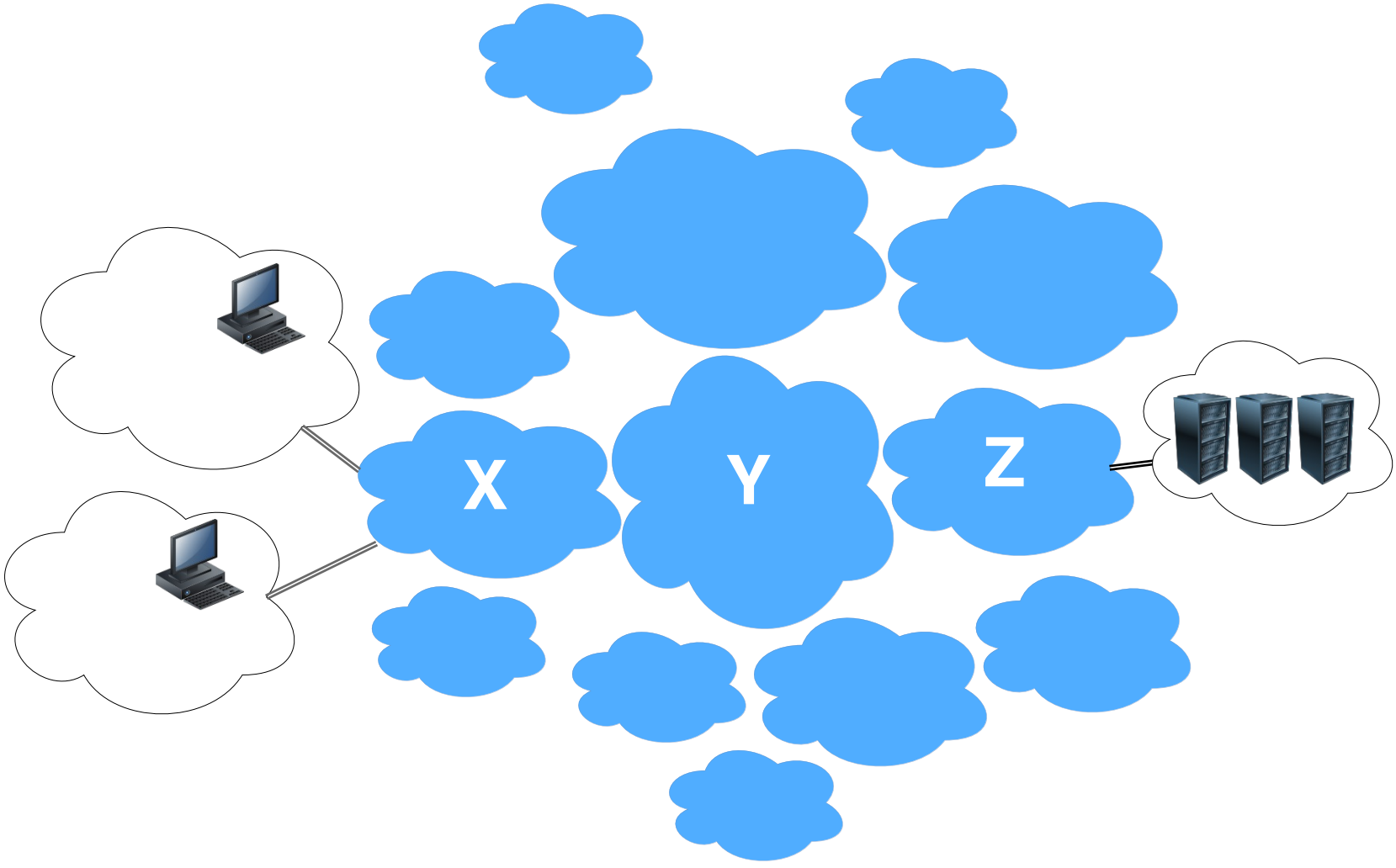
Romain Fontugne (ロマン), IIJ Research Lab

in collaboration with E.Aben (RIPE NCC), C.Pelsser (U.Strasbourg), R.Bush (IIJ)

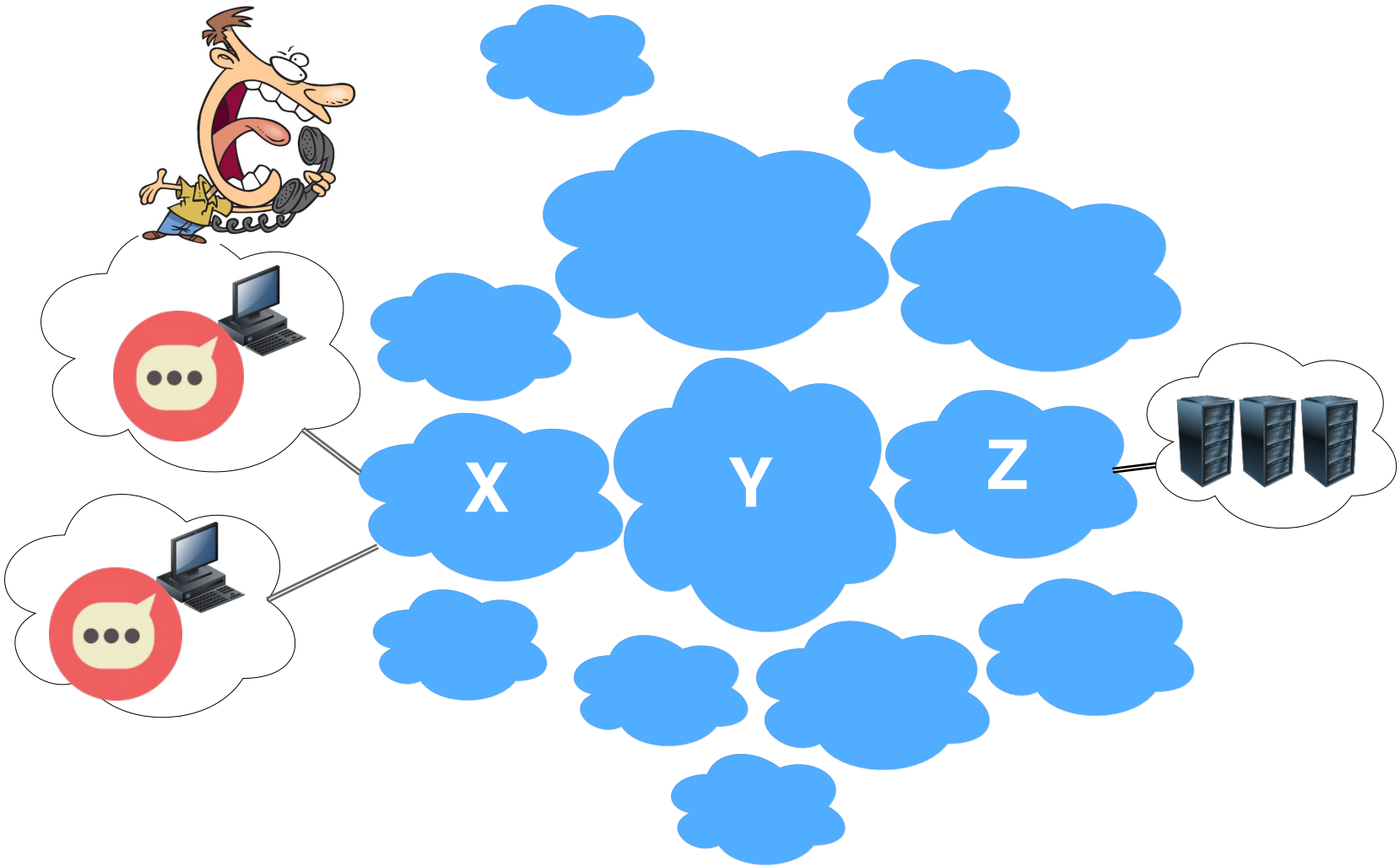
日本語訳: Matsuzaki ‘maz’ Yoshinobu

26 January 2018, JANOG 41, Hiroshima

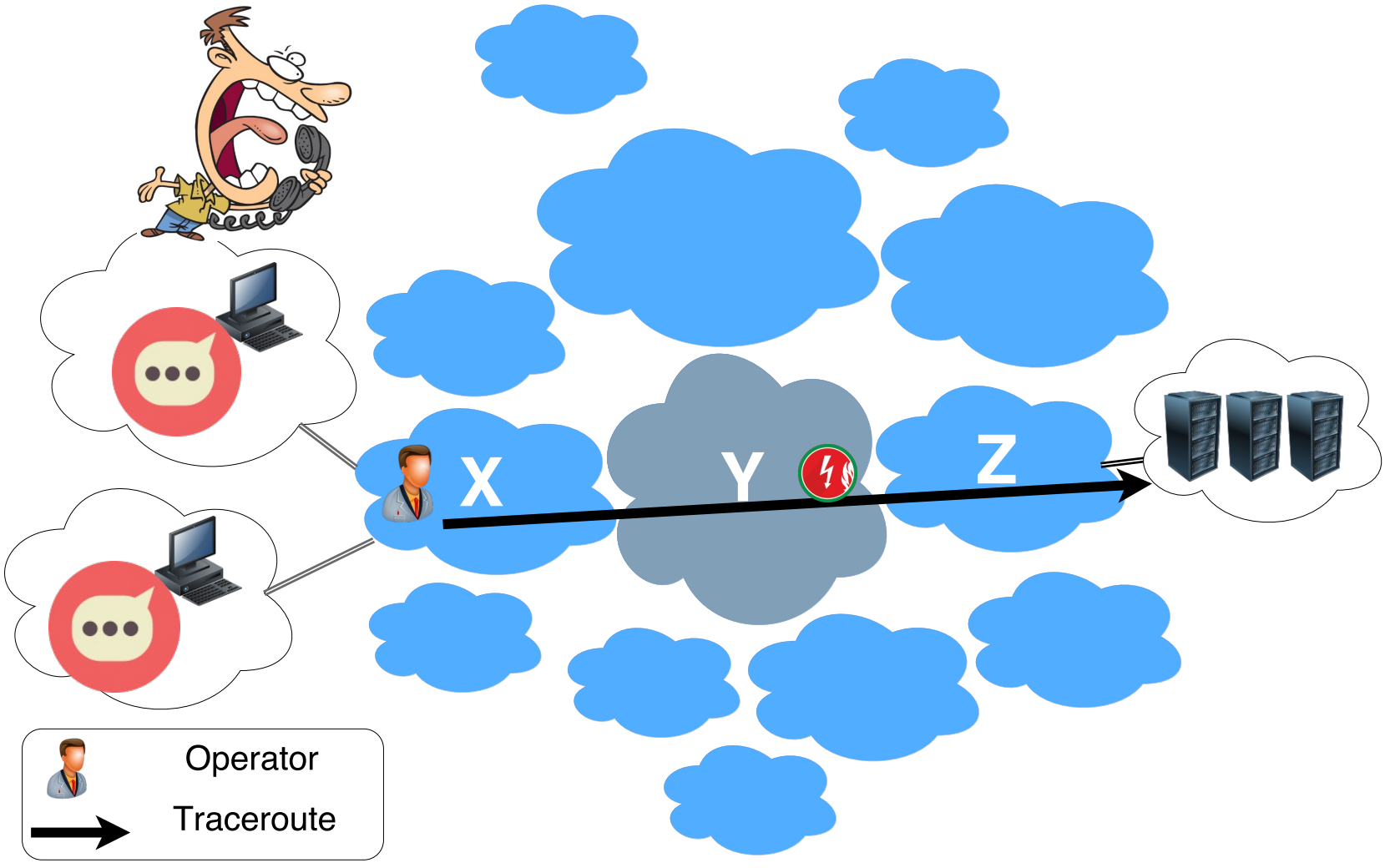
インターネット遅延の監視？



インターネット遅延の監視？



インターネット遅延の監視？



インターネット遅延の監視？

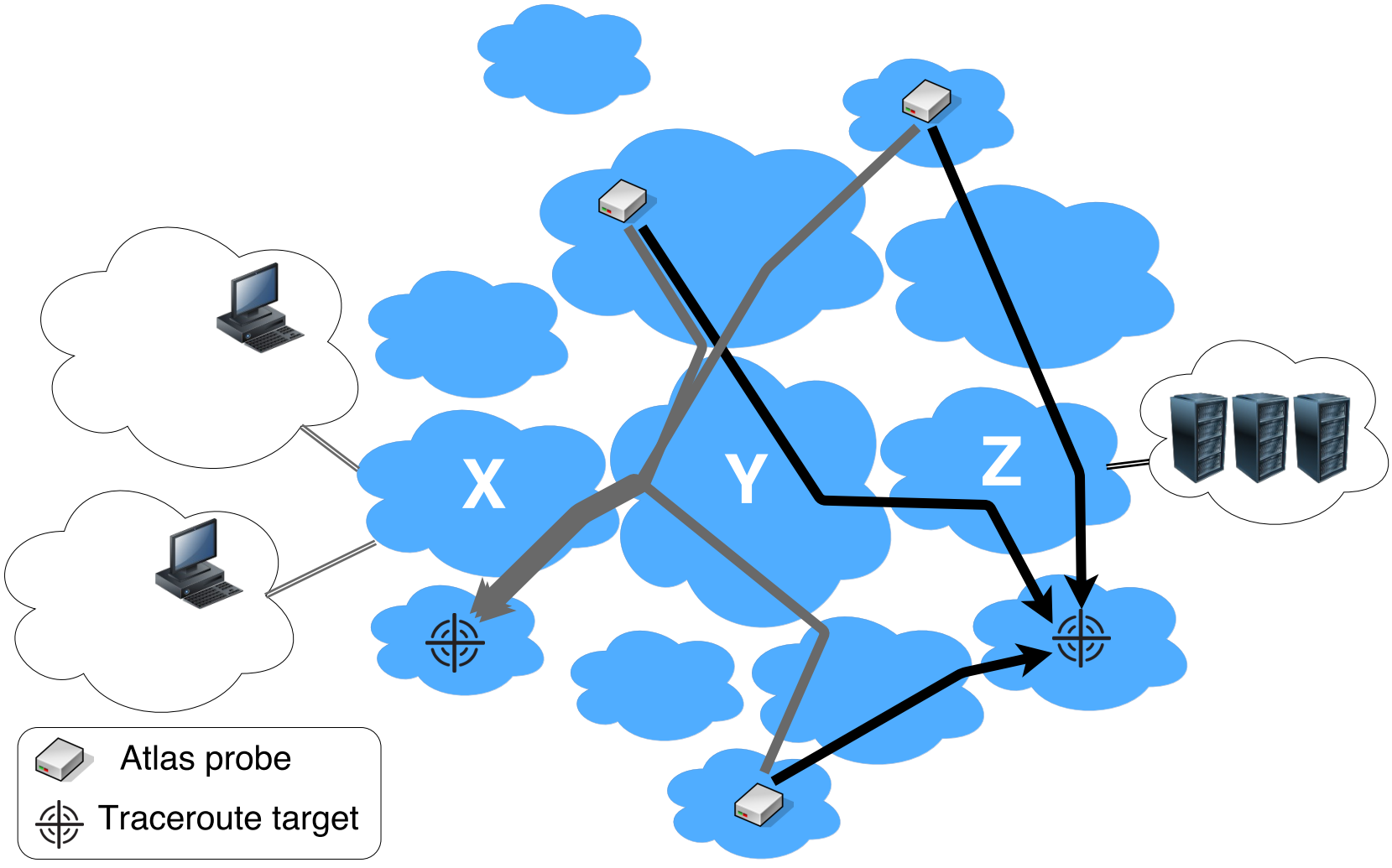
モチベーション

- 到達性は他の AS への依存により確保
- 他の AS の遅延を把握したい

問題

- 他のネットワークの知識がない
- 手動にての検査（traceroute, ping）
- 観測点に依存した一部の状態した見えない

アプローチ：RIPE Atlas での traceroute の分析



→ 協調・分散アプローチ

→ 既存のデータを使用

RIPE Atlas

能動的にインターネット接続を測定

- 複数の測定手法：ping、traceroute、DNS、SSL、NTP、HTTP
- 1万アクティブプローブ！
- 多数の測定データが公開され、利用可能

RIPE Atlas: traceroutes

2 つの大規模な測定

- *Builtin*：30 分ごとに DNS ルートサーバーへの traceroute（≈ 500 サーバーインスタンス）
- *Anchoring*：15 分ごとに 200+のコラボレーションサーバーへの traceroute

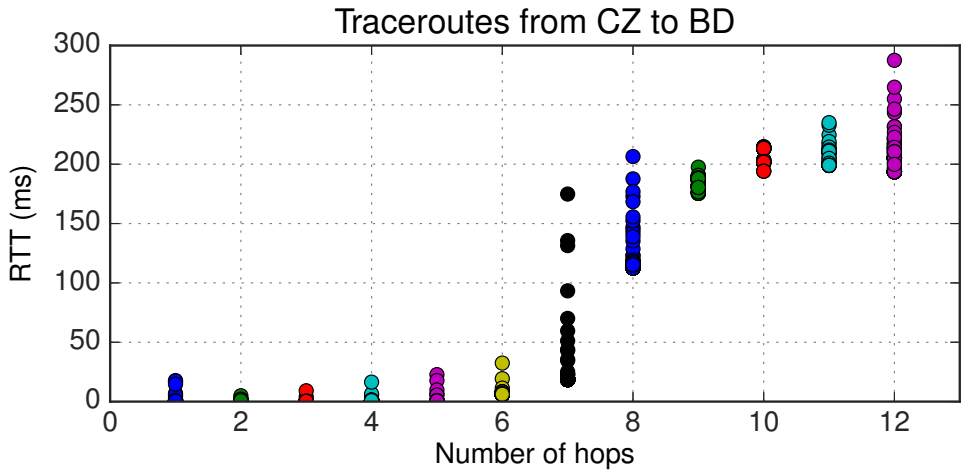
分析対象のデータセット

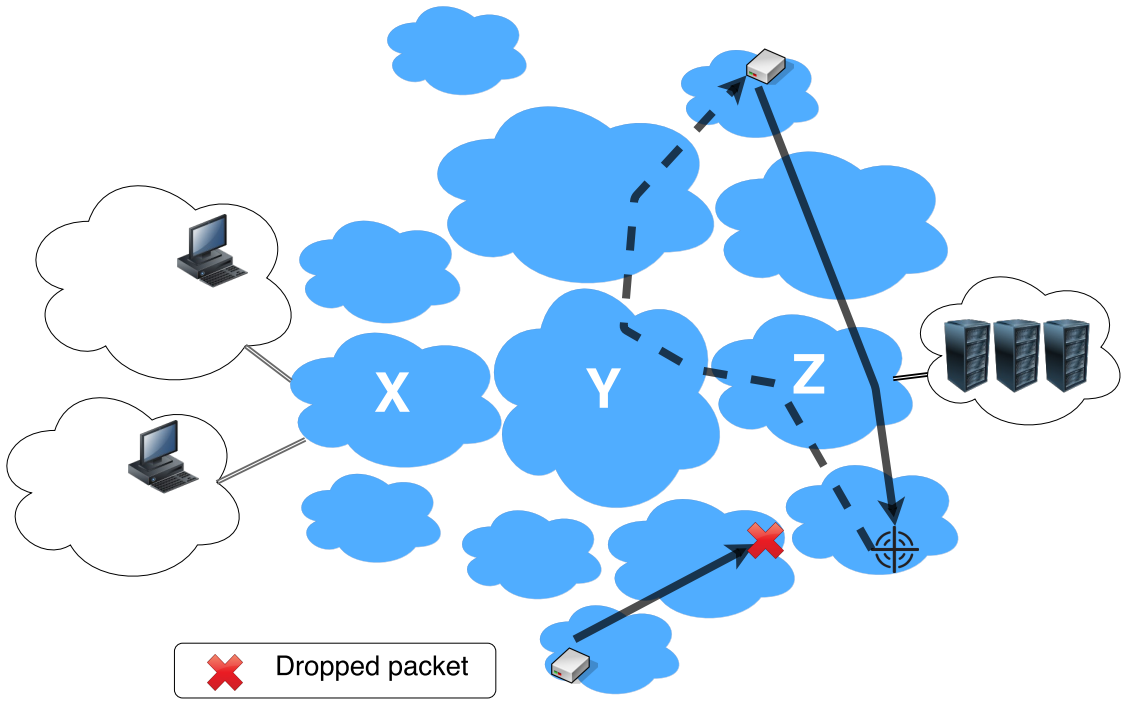
- 2015 年 5 月～12 月
- 28 億の IPv4 traceroutes
- 12 億の IPv6 traceroutes

traceroute で遅延を監視する際の課題

課題：

- ノイズの多いデータ
- 非対称のトラフィック
- パケットロス

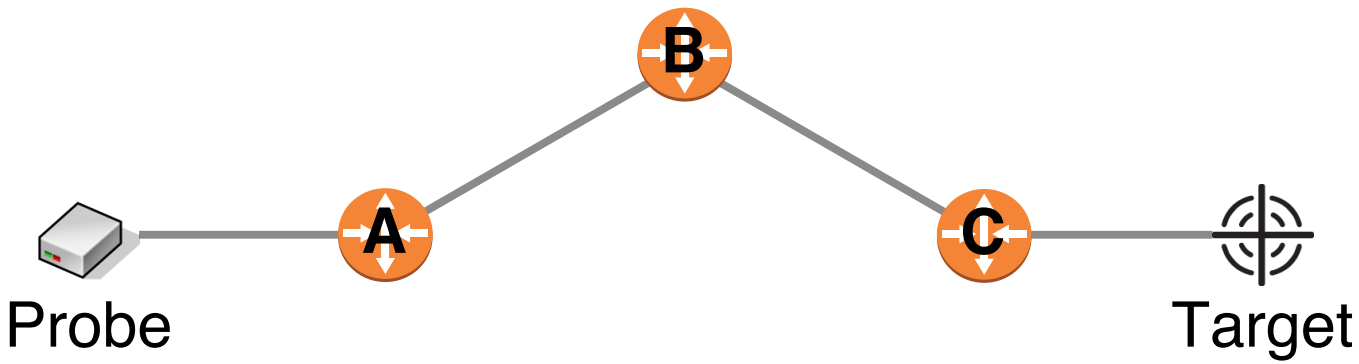




traceroute で遅延を監視する際の課題

”www.target.com” への traceroute

```
~$ 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
```

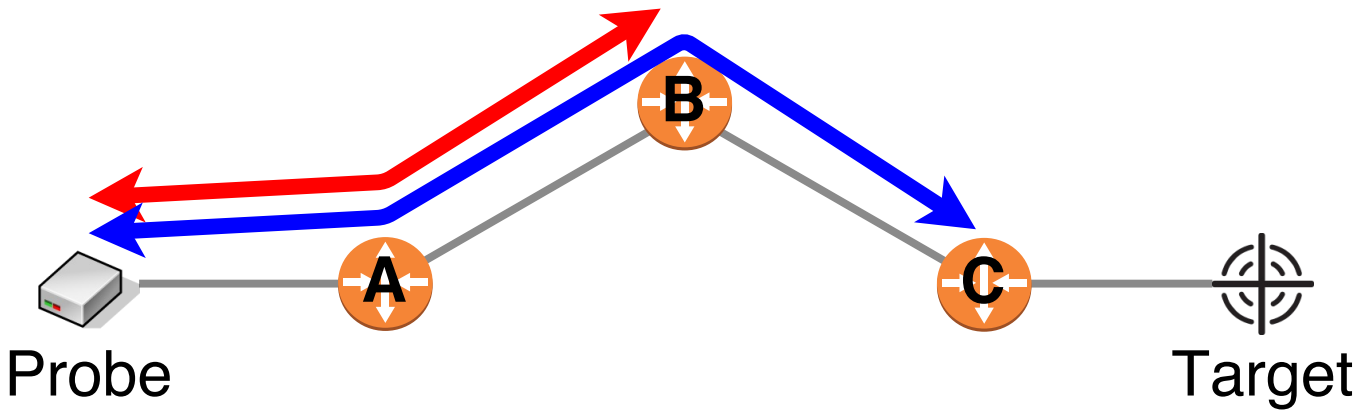


B と C の間の往復時間（RTT）？

B と C の RTT に異常があったと言えるのか？

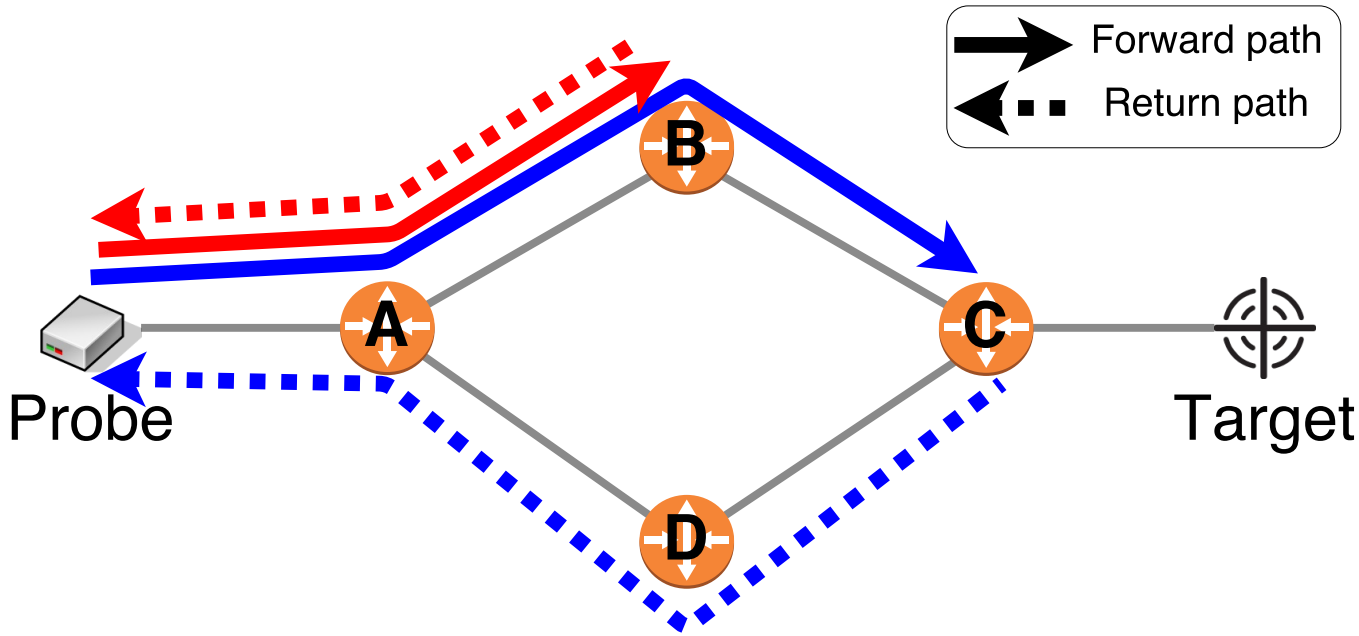
B と C の間の RTT？

```
~$ 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
```



Differential RTT: $\Delta_{CB} = RTT_C - RTT_B \stackrel{?}{=} RTT_{CB}$

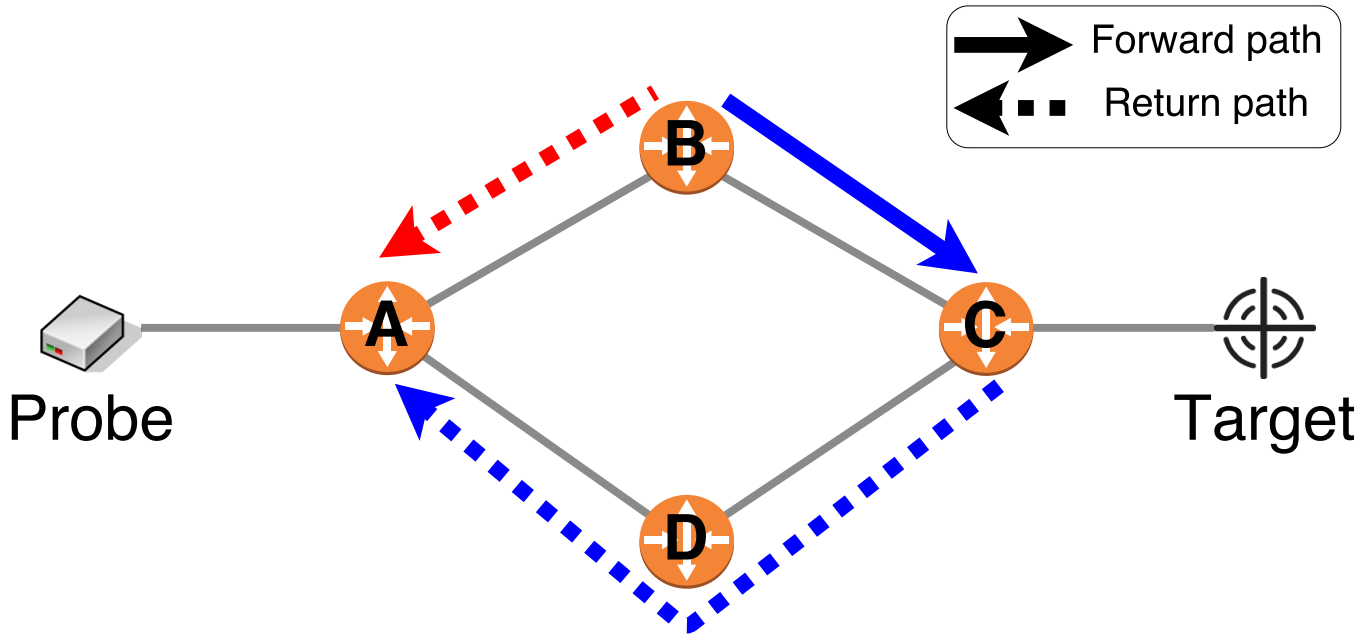
B と C の間の RTT？



$RTT_C - RTT_B = RTT_{CB}$?

- いいえ！
- トラフィックが非対称
- RTT_B と RTT_C が異なるリターンパスを取る!

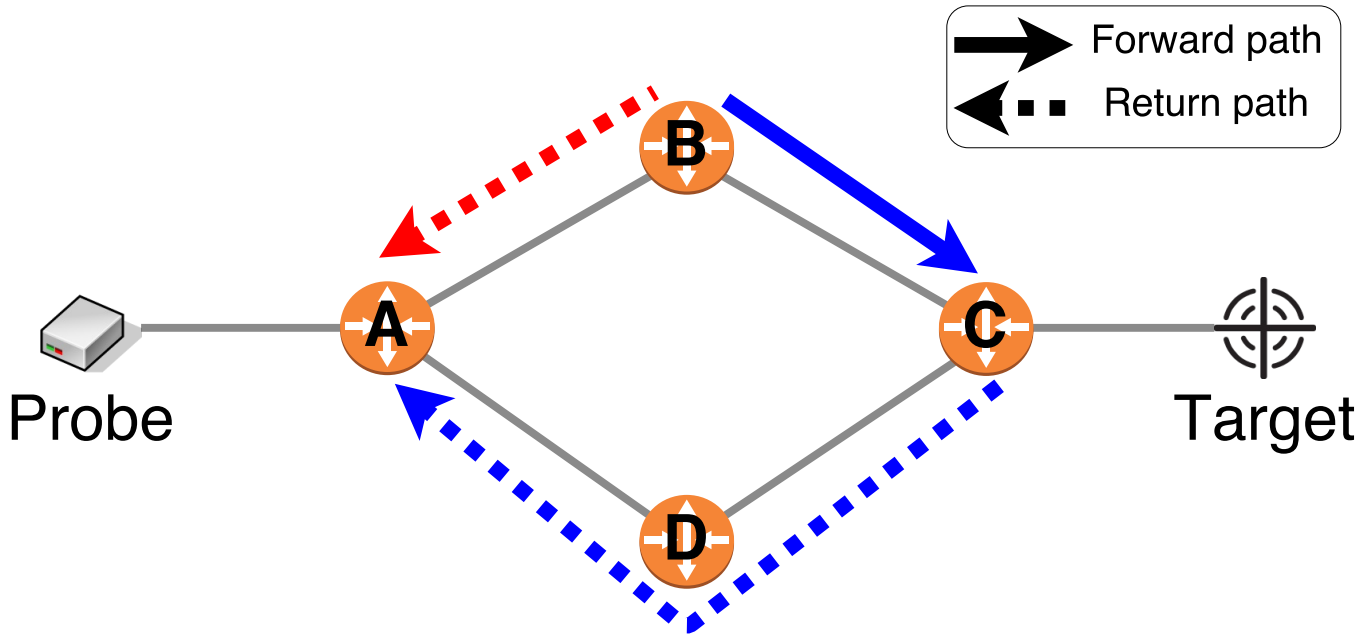
B と C の間の RTT？



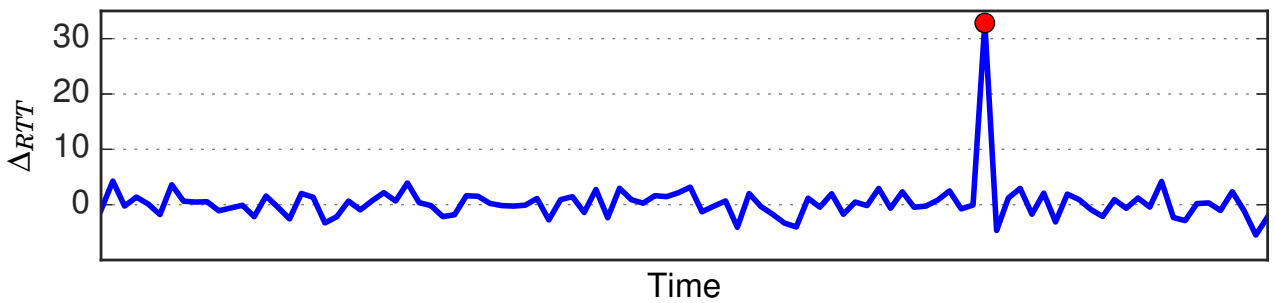
RTT_C - RTT_B = RTT_{CB}?

- いいえ！
- トラフィックが非対称
- RTT_B と RTT_C が異なるリターンパスを取る!
- Differential RTT: $\Delta_{CB} = RTT_C - RTT_B = d_{BC} + e_p$

Differential RTT の問題



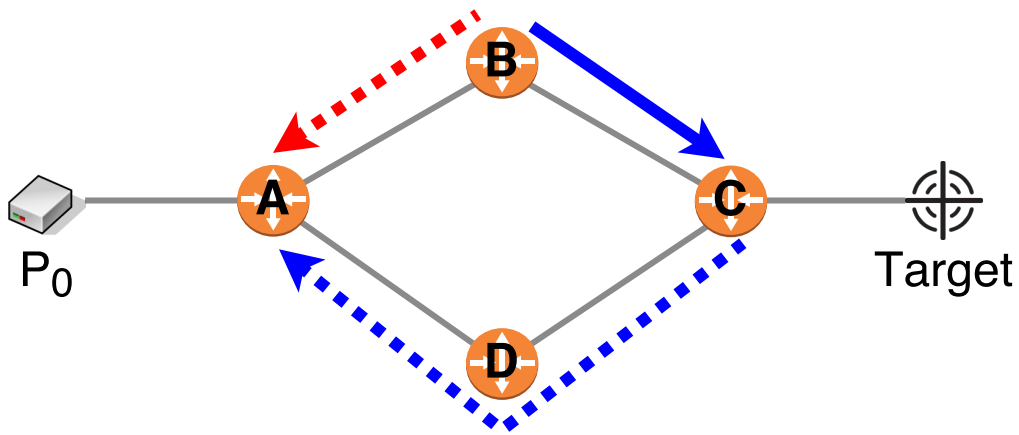
Δ_{CB} の長時間モニタリング：



→ BC の遅延が変ったのか？ それとも CD？ DA？ BA？？

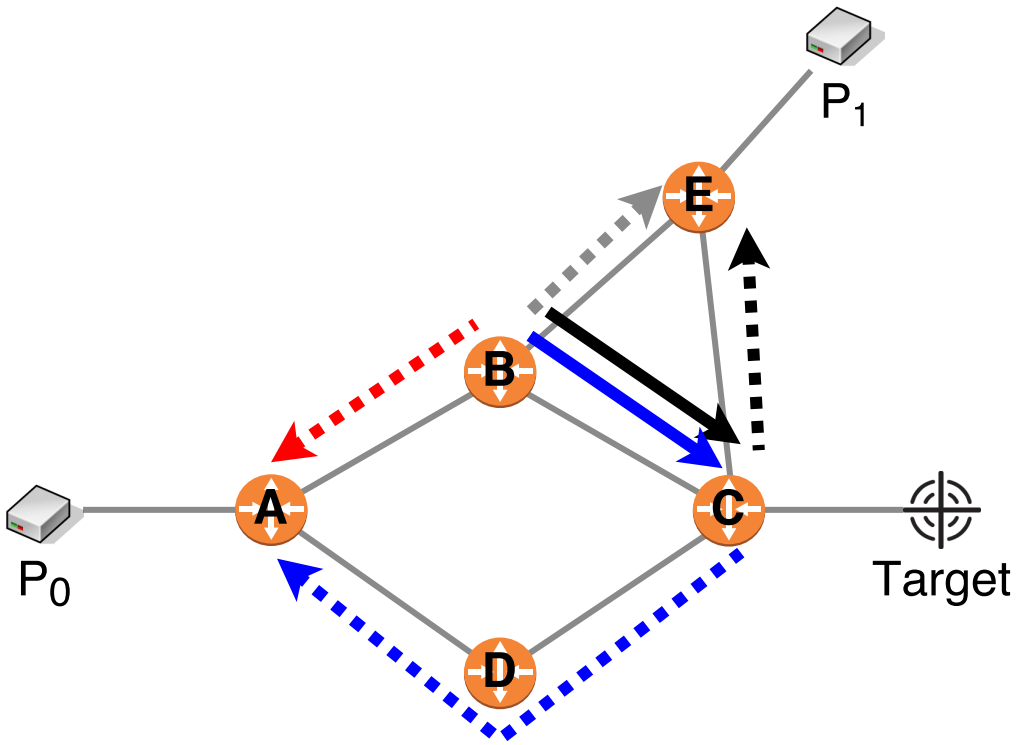
アプローチ：異なるリターンパスを持つプローブを使用する

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



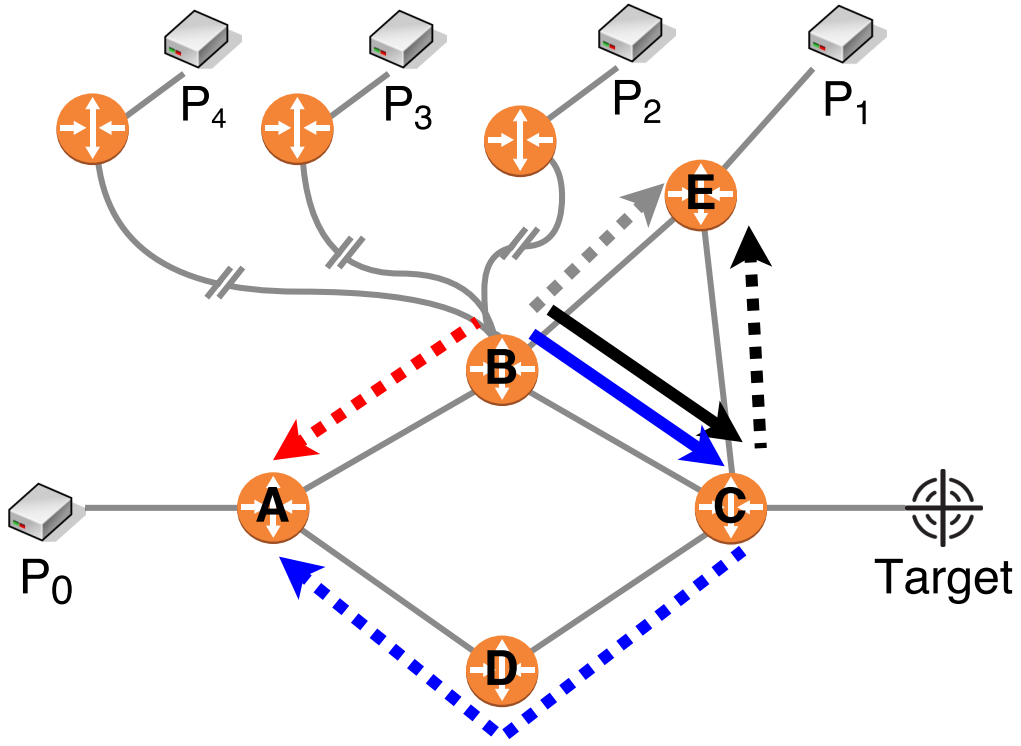
アプローチ：異なるリターンパスを持つプローブを使用する

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



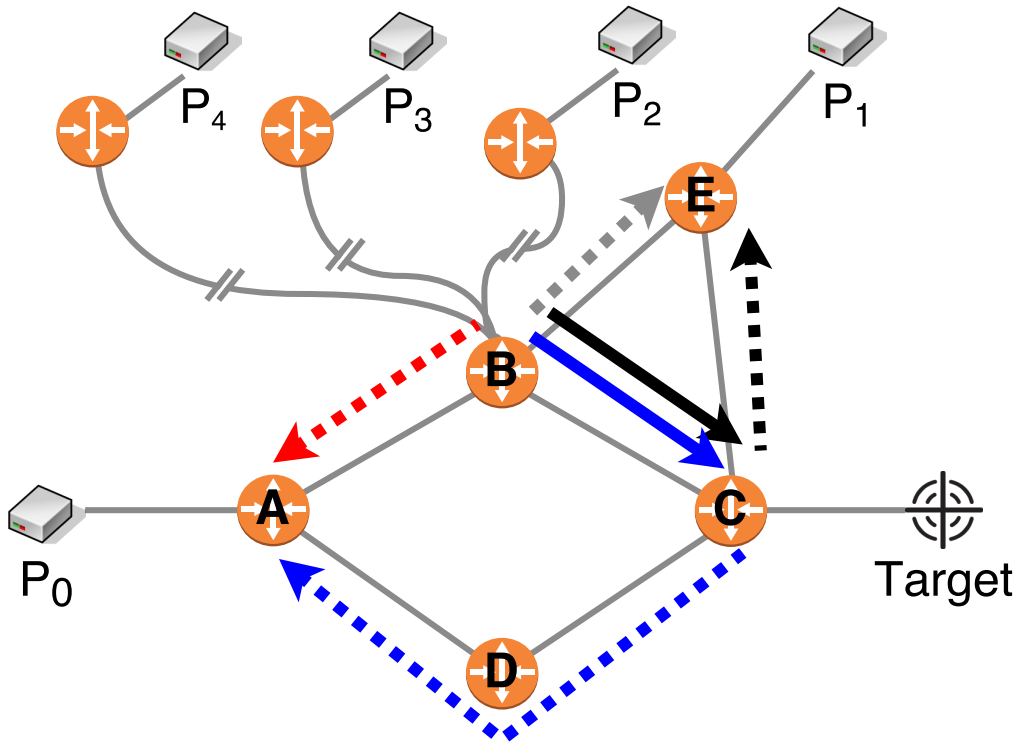
アプローチ：異なるリターンパスを持つプローブを使用する

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



アプローチ：異なるリターンパスを持つプローブを使用する

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

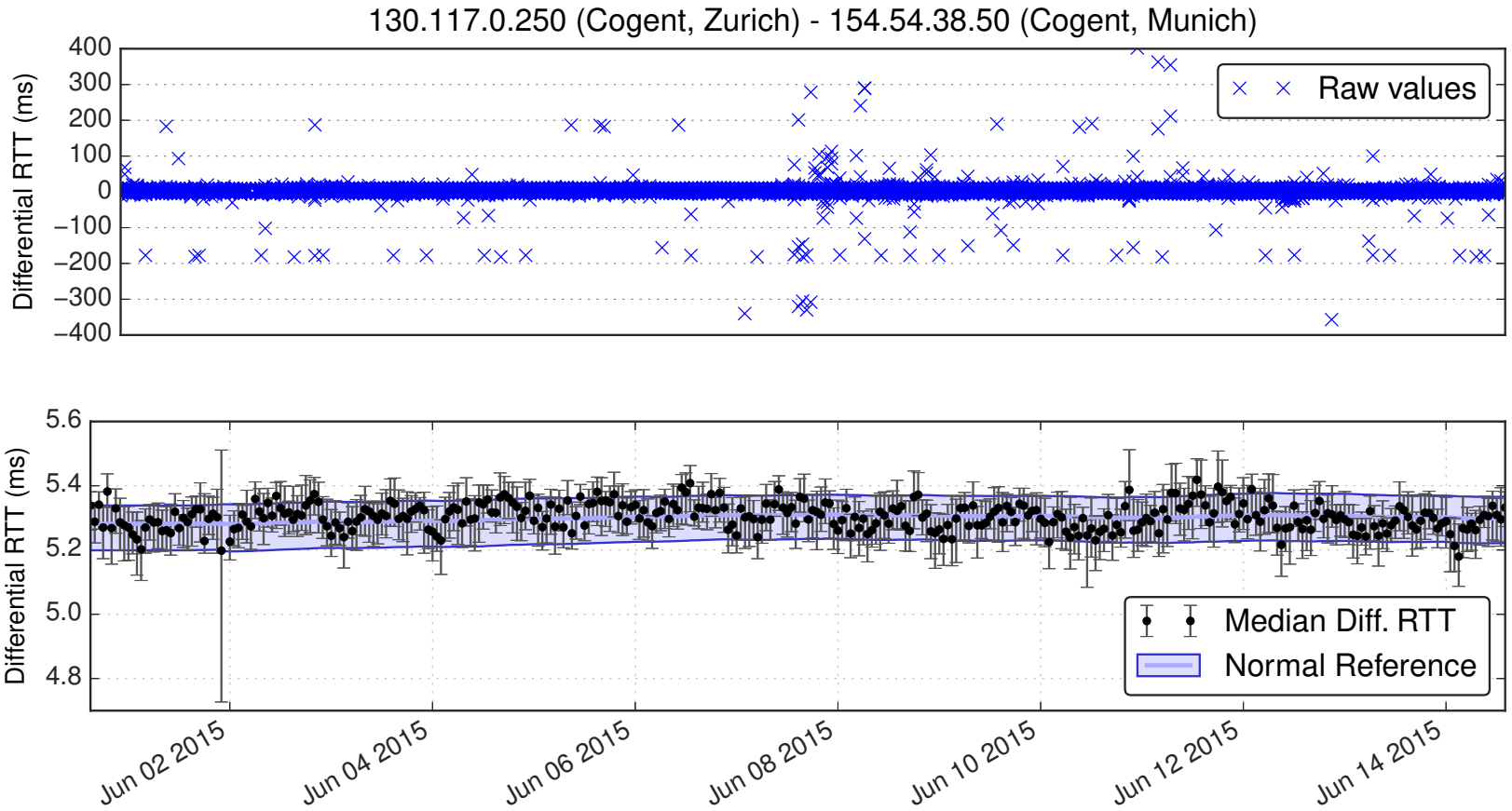


中央値 Δ_{CB}:

- リターンパスの遅延変動が少ない場合は安定
- BC の遅延が変化した場合に変動する

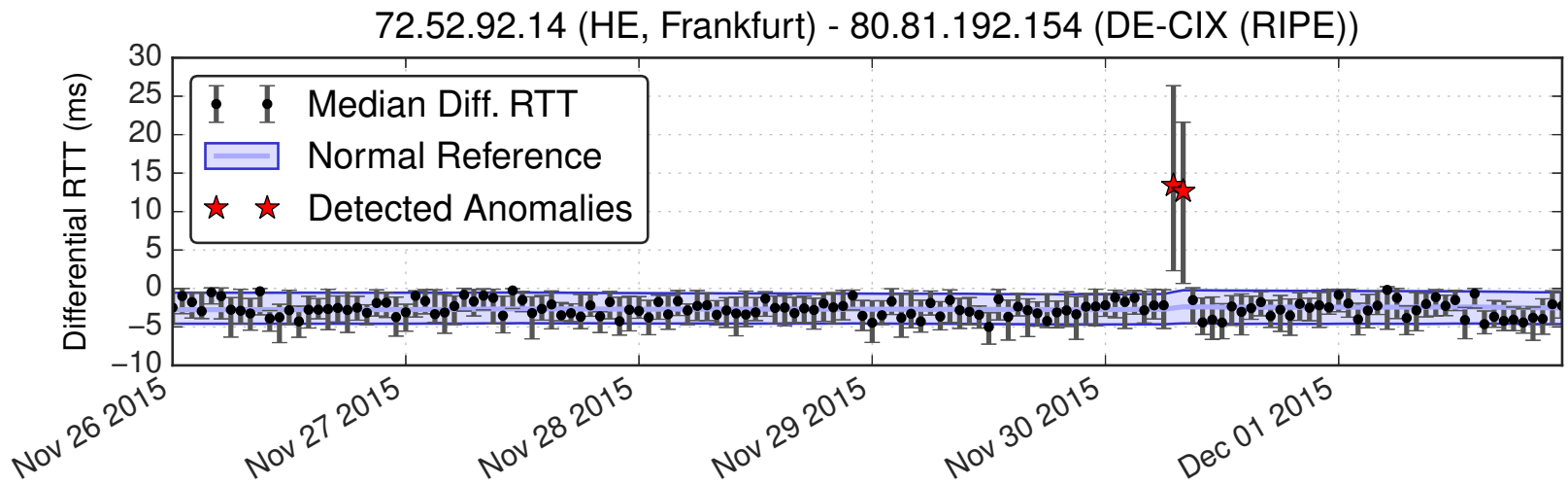
例：中央値 Differential RTT

Cogent リンク、2 週間のデータ、95 プローブ：



- ノイズの多い RTT にもかかわらず安定
- 正規化基準と信頼区間

遅延変動の検出



重要な RTT の変動：

- 信頼区間が通常の参照と重複しない

結果

データセット

- Atlas の Builtin/Anchoring 測定
- 2015 年 5 月から 12 月まで
- 262k の IPv4 および 42k の IPv6 リンクの監視

多くの遅延の変動を発見しました！
2 つの顕著な例を見てみましょう

DNS ルートサーバー上の DDoS

2 つの攻撃：

- 2015 年 11 月 30 日
- 2015 年 12 月 1 日

ほぼすべてのサーバーは エニーキャスト

- 531 サイトでの輻輳検知？
- 攻撃によって変更された 129 のインスタンスが見つかりました

The Register®
Biting the hand that feeds 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, Kieren McCarthy

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

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 timec
messages for a single domain name; the s

Ultimately, the operators affected by the atta
proper analysis is now underway to discove

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

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

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

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

≤ 66% > 99% Data resolution: 10 minutes

Home Hacking Tech Cyber Attacks Vulnerabilities Malware Spying

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 Swati Khandelwal

G+1 192 Like 5.9K Share 6538 Tweet 1049 Share 58 share 8417

The Internet's Backbone

DNS Root Servers Hit by a Massive Cyber Attack

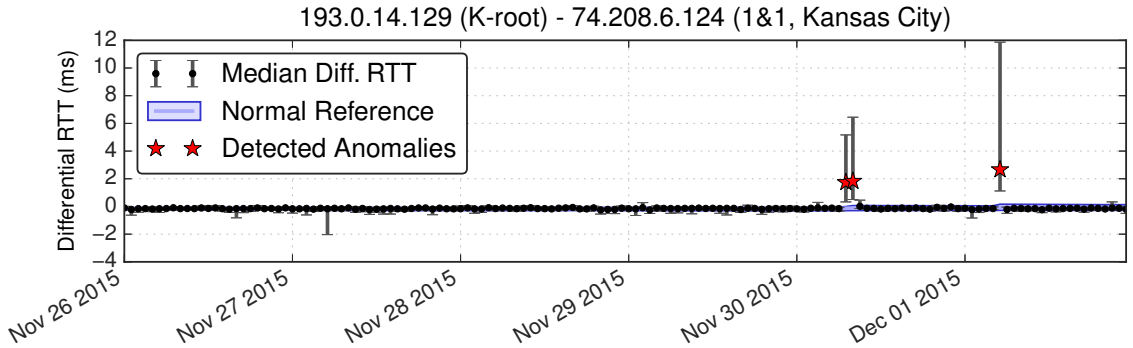
Someone just DDoSed one of the most critical organs of the Internet anatomy – **The Internet's DNS Root Servers**.

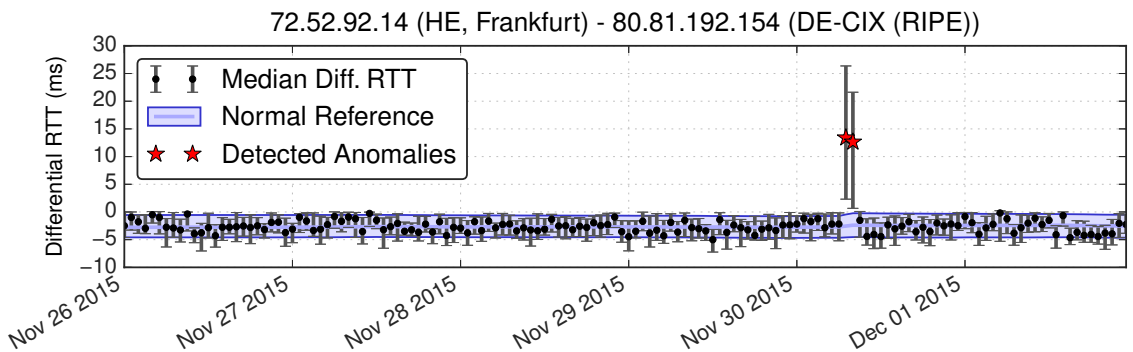
Early last week, a flood of as many as 5 Million queries per second hit many of the Internet's DNS (*Domain Name System*) Root Servers that act as the authoritative reference for mapping domain names to IP addresses and are a total of 13 in numbers.

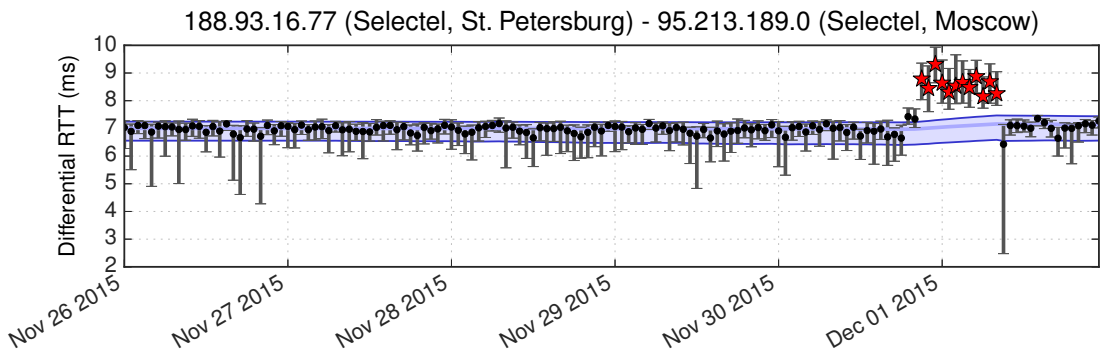
The attack, commonly known as **Distributed Denial of Service** (DDoS) attack, took place on two separate occasions.

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.

観測された遅延の変化

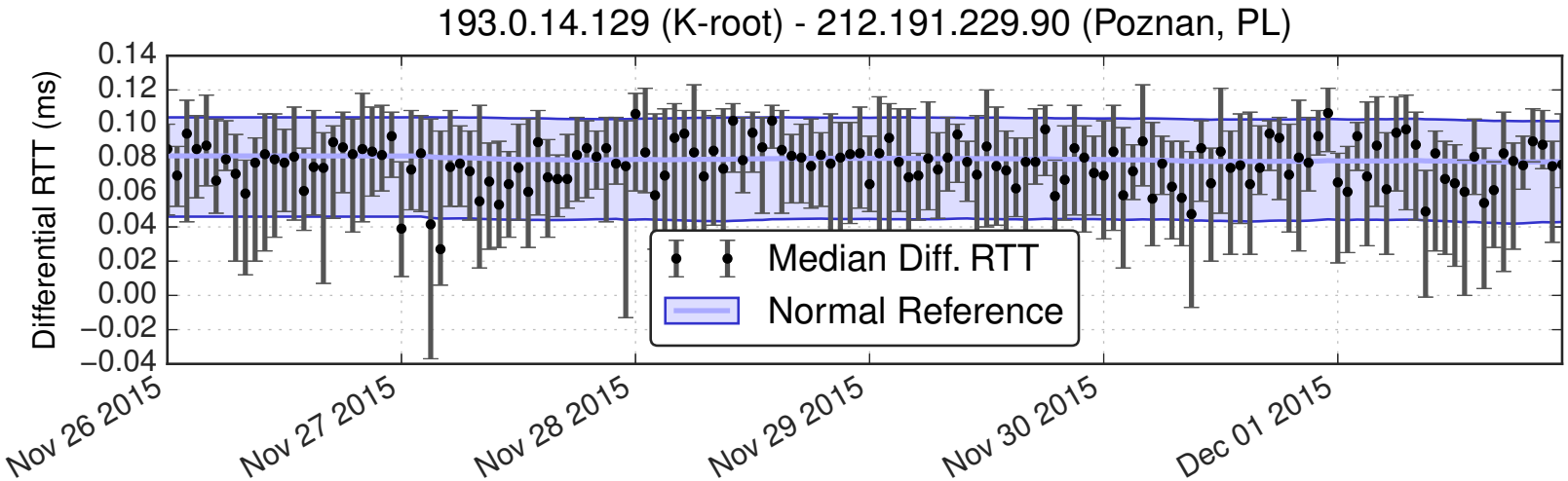






- 特定のサーバーは1つの攻撃によってのみ影響
- ロシアでの継続的攻撃

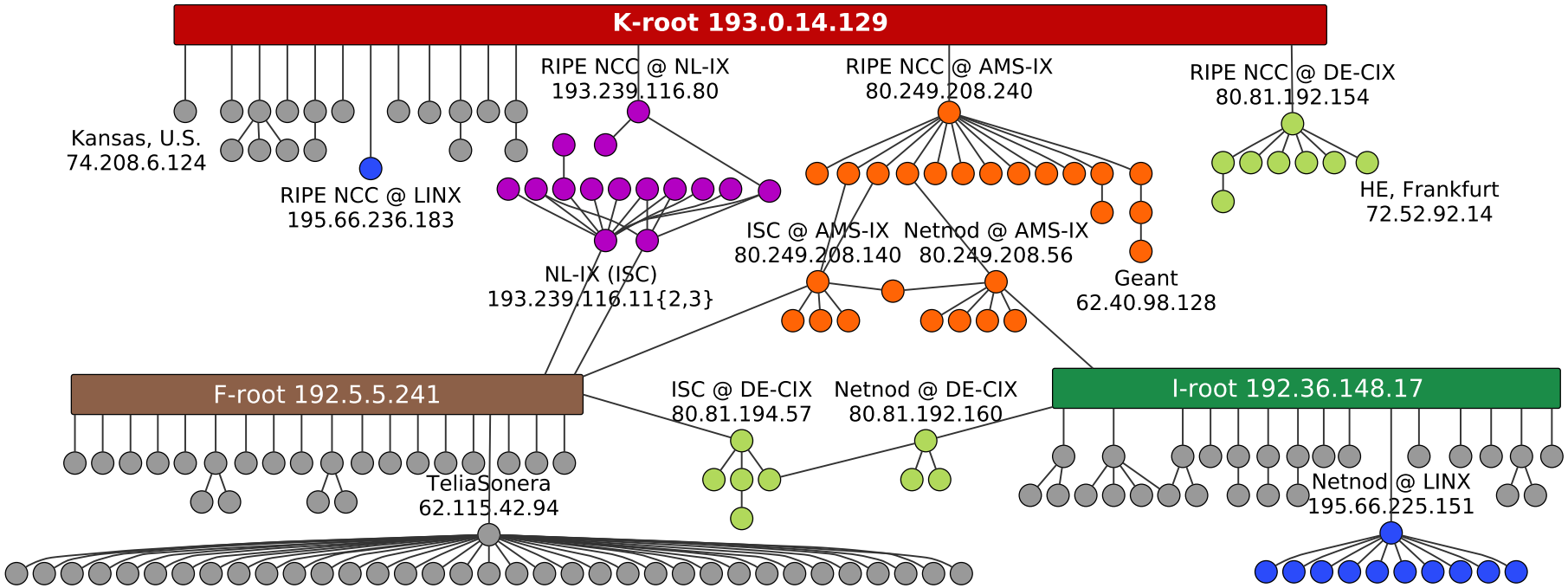
影響を受けていないサーバー



攻撃中の非常に安定した遅延

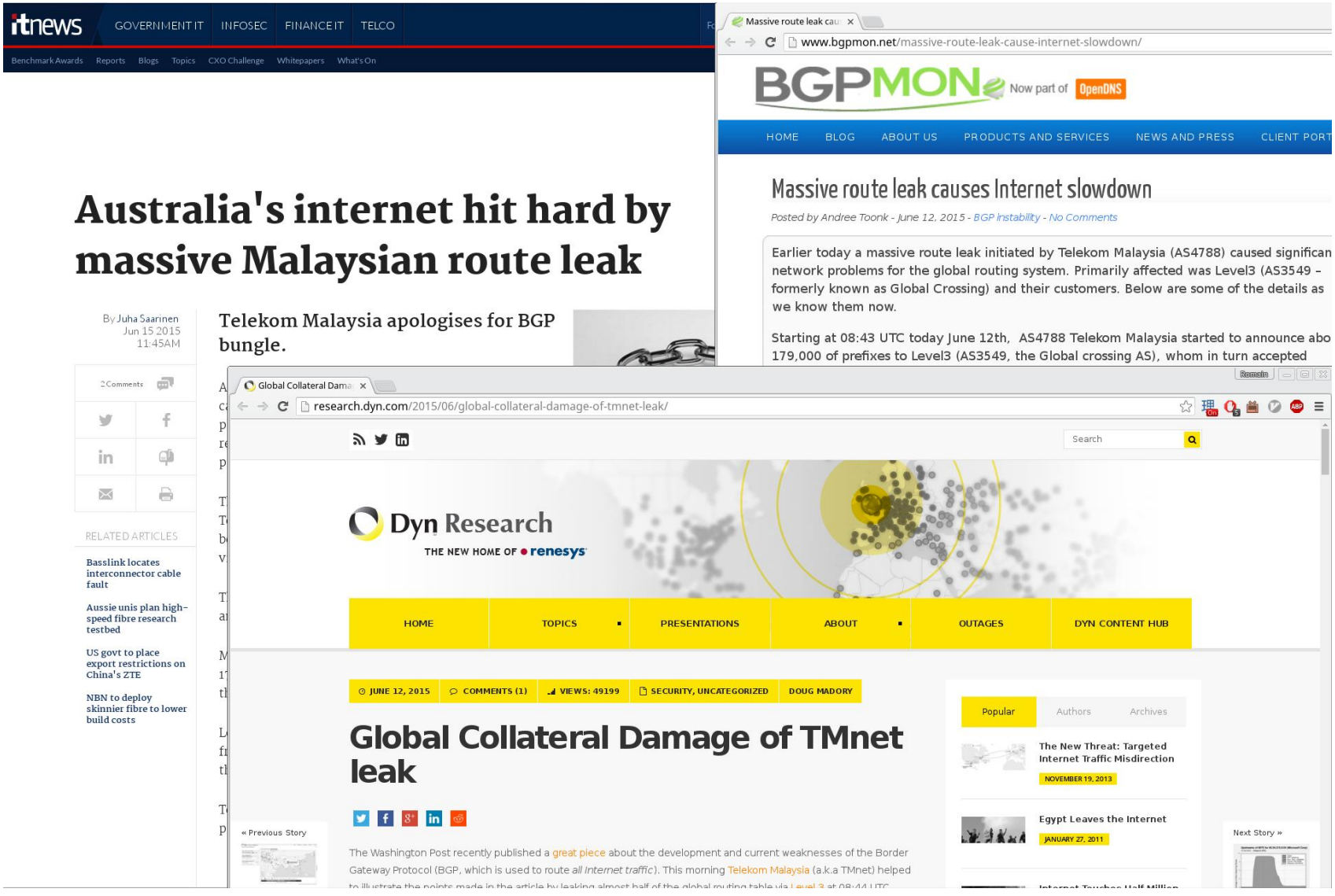
- エニーキャストのおかげで！
- 攻撃者から遠い

F、I、Kの混雑したリンク

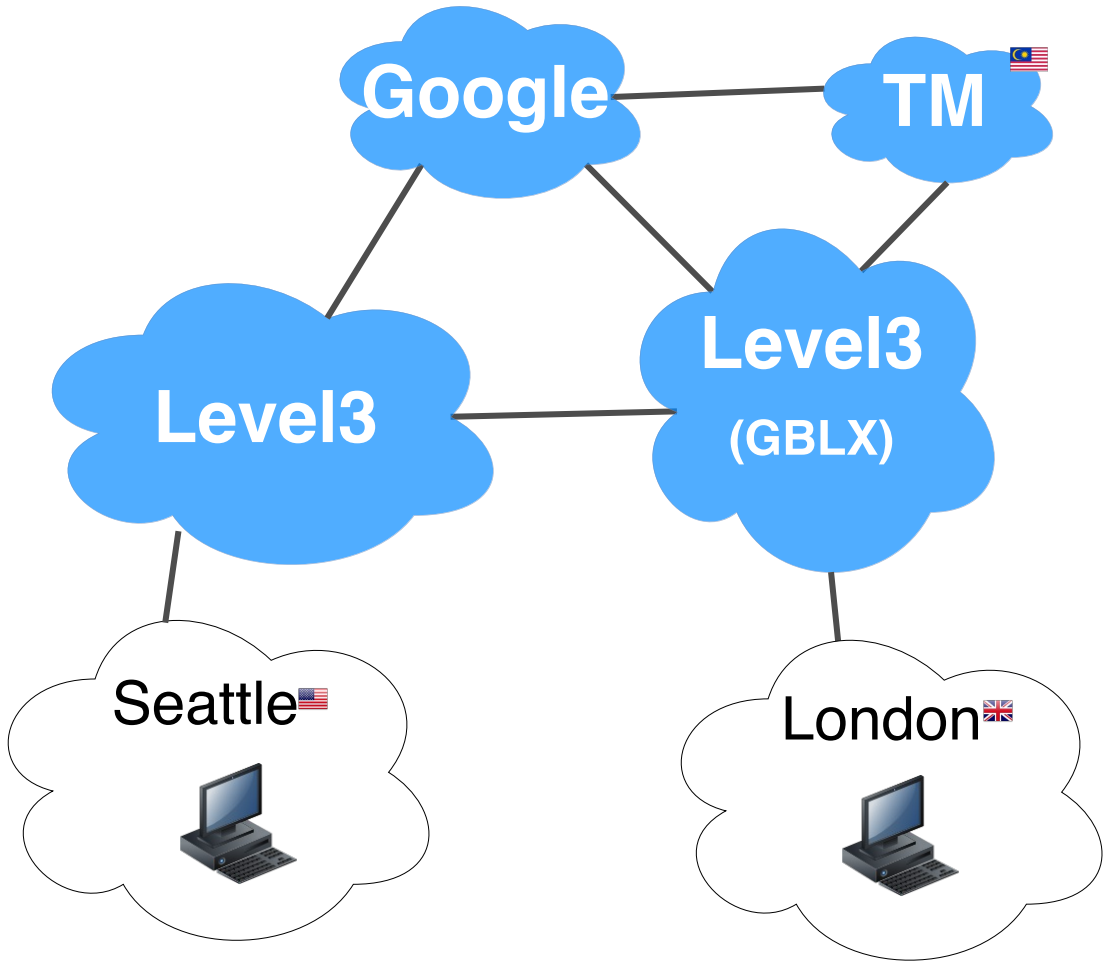


→ IXP での悪意のあるトラフィックの集中

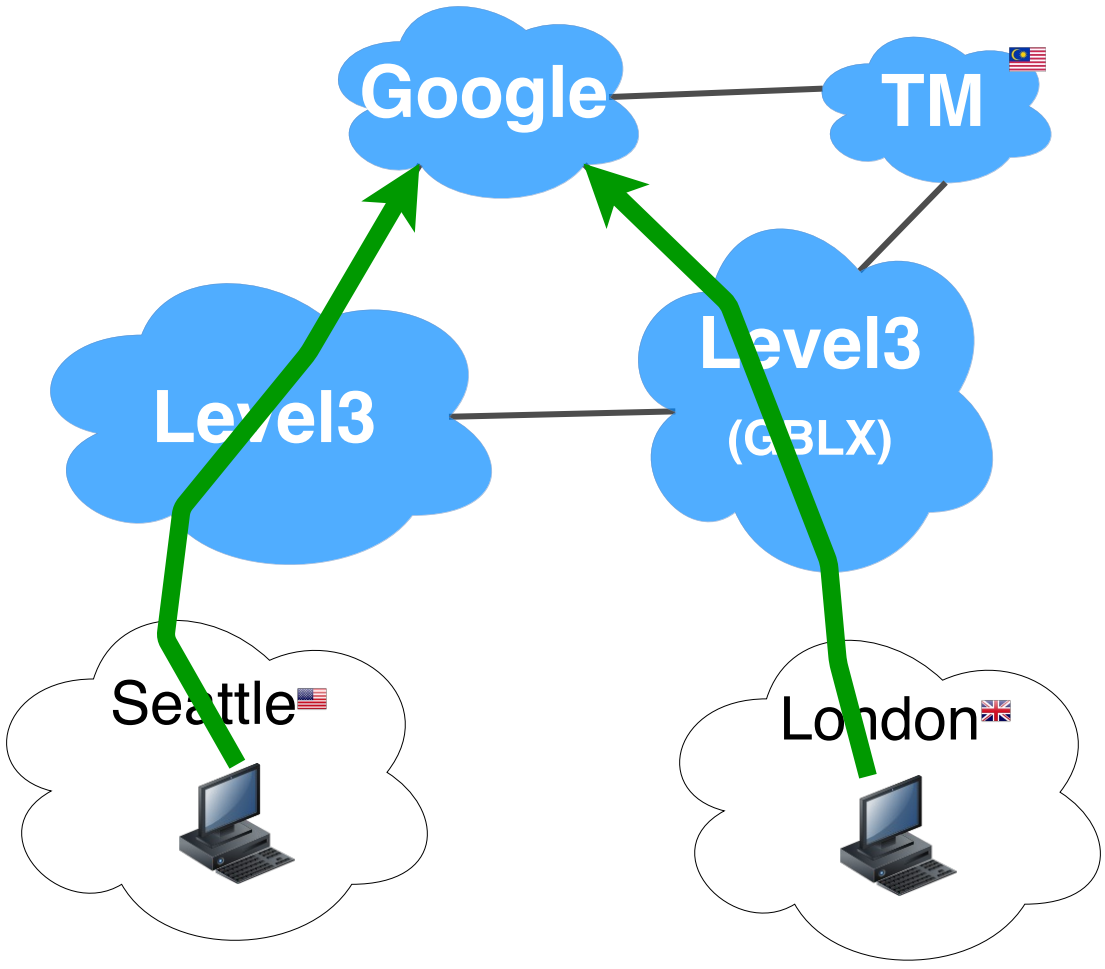
Telekom Malaysia の BGP リーク



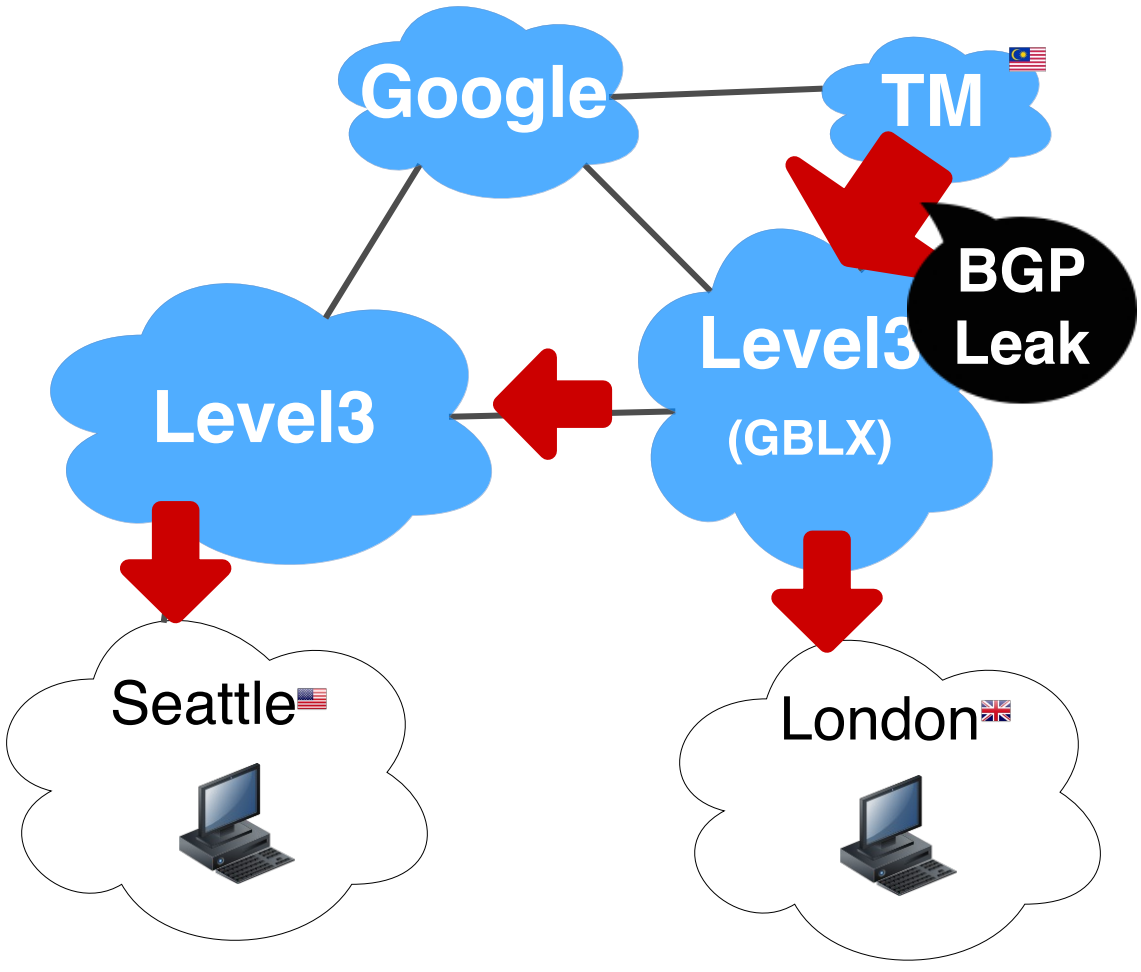
Telekom Malaysia の BGP リーク



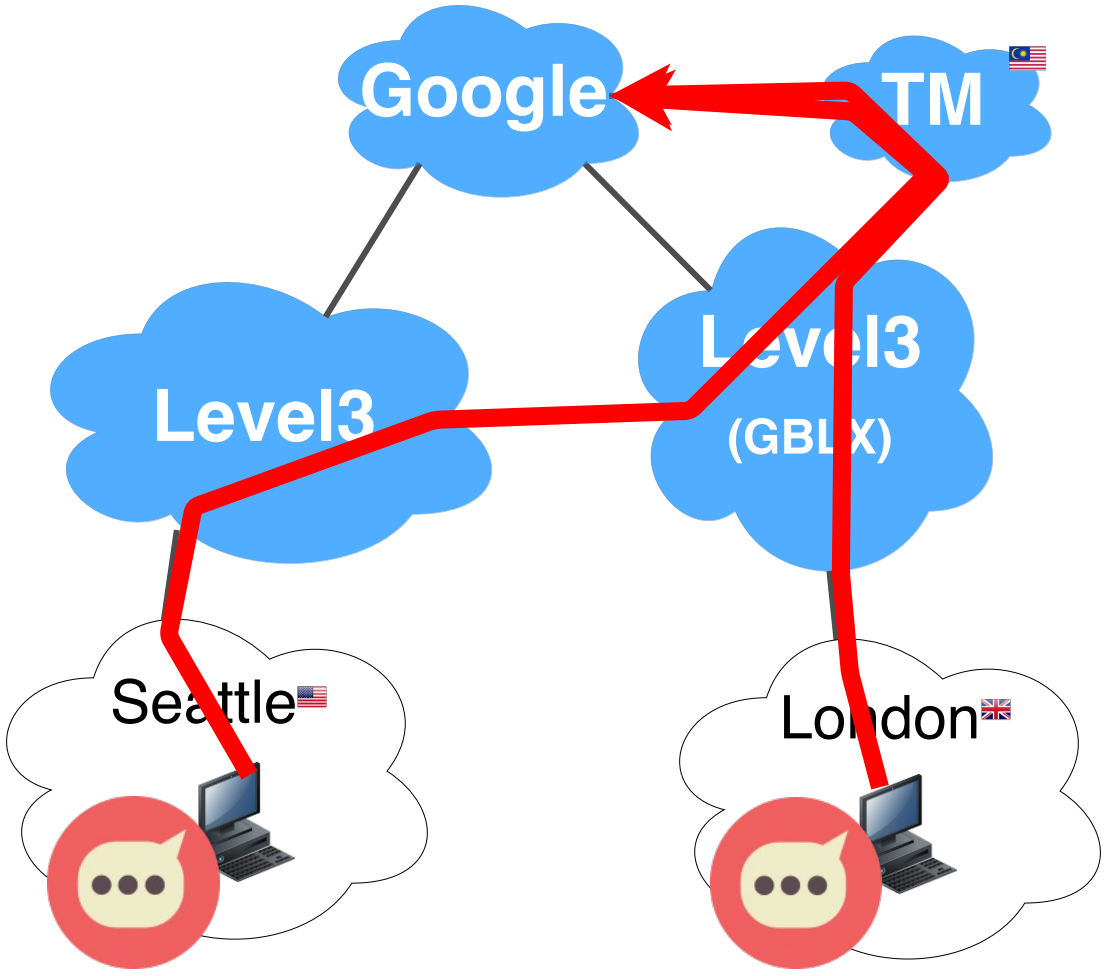
Telekom Malaysia の BGP リーク



Telekom Malaysia の BGP リーク



Telekom Malaysia の BGP リーク

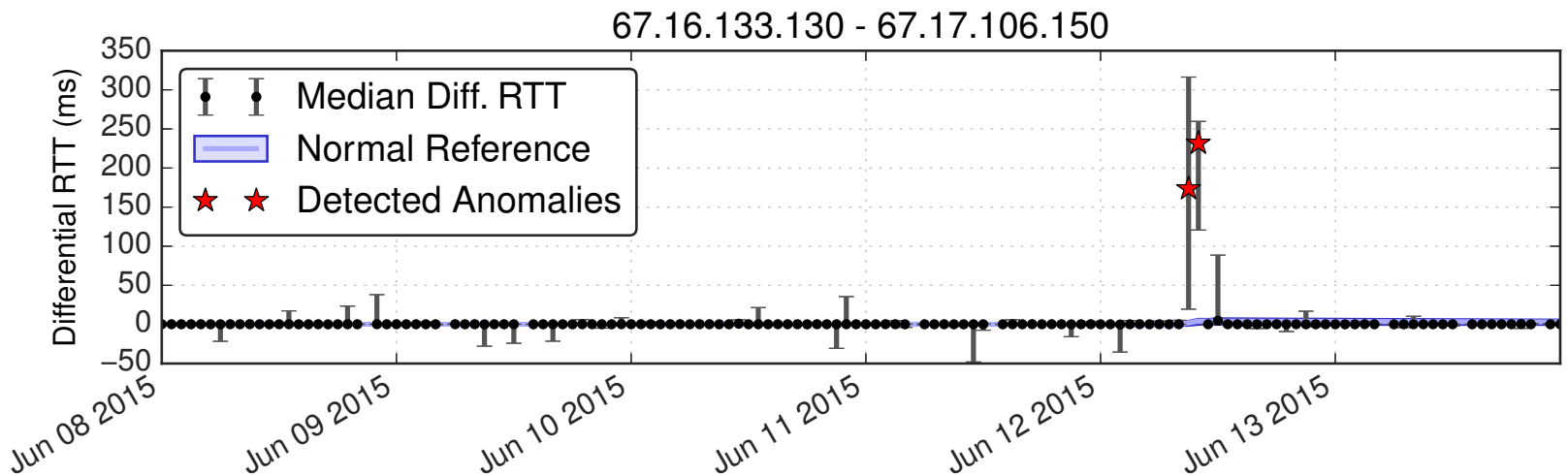


Google だけでなく、約 170k のプレフィクス！

Level(3) での混雑

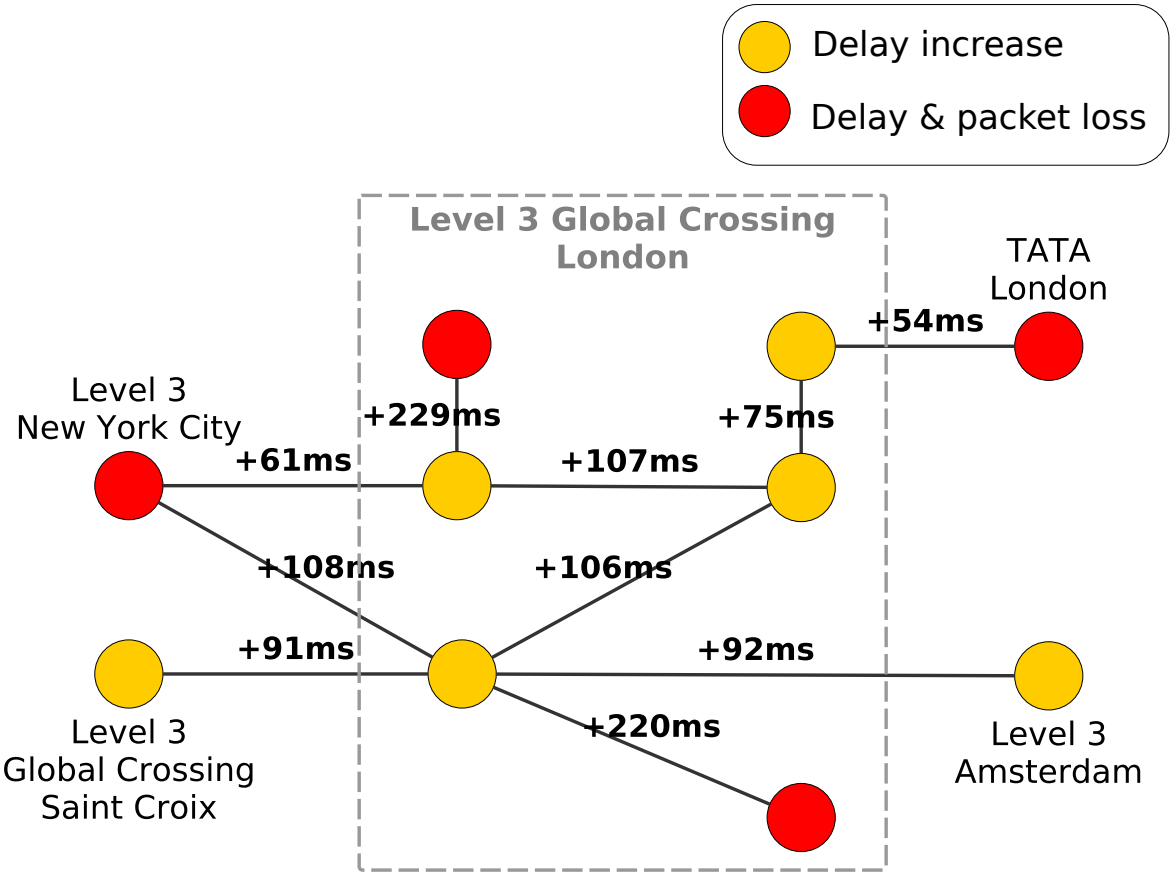
リルートされたトラフィックによって Level3 が輻輳 (報告された 120 のリンク)

- 例：ロンドンの 2 台のルータ間で 229ms の増加！



Level(3) での混雑

ロンドンで報告されたリンク：



→ 英国/ヨーロッパ内のインターネットトラフィックも変更される可能性

まとめ

数十億の traceroute で遅延異常を検出

- ノンパラメトリックな統計
- さまざまな原因：
  リモート攻撃、ルーティング異常など
- 報告されたイベントについて多くの新しい見識を提示できた

オペレータのためのオンライン検出

- `http://ihr.iijlab.net/`
- romain@iij.ad.jp

論文:`https://conferences.sigcomm.org/imc/2017/papers/imc17-final106.pdf`

Backup slides

http://ihr.iijlab.net

Delay Anomalies:

- Congested link in Level(3)
- Hot link in Comcast

Forwarding Anomalies:

- Hanging in Cogent

Outage:

- Iran disconnections
- OVH outage

AS interdependency

- `http://ihr.iijlab.net/ihr/hegemony/`