Detecting Peering Infrastructure Outages in the Wild

Vasileios Giotsas, Christoph Dietzel, Georgios Smaragdakis, Anja Feldmann, Arthur Berger, Emile Aben

vasilis@inet.tu-berlin.de
Peering Infrastructures are critical part of the interconnection ecosystem

**Internet Exchange Points** (IXPs) provide a shared switching fabric for layer-2 bilateral and multilateral peering.

- Largest IXPs support > 100 K of peerings, > 5 Tbps peak traffic
- Typical SLA 99.99% (~52 min. downtime/year)

Carriernutral **co-location facilities** (CFs) provide infrastructure for physical co-location and cross-connect interconnections.

- Largest facilities support > 170 K of interconnections
- Typical SLA 99.999% (~5 min. downtime/year)

---

1. [https://ams-ix.net/services-pricing/service-level-agreement](https://ams-ix.net/services-pricing/service-level-agreement)
2. [http://www.telehouse.net/london-colocation/](http://www.telehouse.net/london-colocation/)
Outages in peering infrastructures can severely disrupt critical services and applications

BT, other ISPs hit by second major Internet outage—power failure blamed

Equinix cooling outage leads to flight delays in Australia

Equinix Outage Means Downtime for Zoho

Telecity London data centre outage borks VoIP, websites, AWS...

LINX reports sudden sharp traffic drop, Amazon Direct Connect goes TITSUP
Outages in peering infrastructures can severely disrupt critical services and applications.

Outage detection crucial to improve **situational awareness**, **risk assessment** and **transparency**.
Current practice: “Is anyone else having issues?”

- ASes try to crowd-source the detection and localization of outages.
- Inadequate transparency/responsiveness from infrastructure operators.
Symbiotic and interdependent infrastructures

https://www.franceix.net/en/technical/infrastructure/
Remote peering extends the reach of IXPs and CFs beyond their local market

Global footprint of AMS-IX
https://ams-ix.net/connect-to-ams-ix/peering-around-the-globe
Our Research Goals

1. Outage detection:
   ○ *Timely*, at the *finest granularity* possible

2. Outage localization:
   ○ Distinguish *cascading effects* from outage *source*

3. Outage tracking:
   ○ Determine duration, shifts in routing paths, geographic spread
Challenges in detecting infrastructure outages
Challenges in detecting infrastructure outages
Challenges in detecting infrastructure outages
Challenges in detecting infrastructure outages

Actual incident

Observed paths

Before outage

During outage
Challenges in detecting infrastructure outages

1. Capturing the infrastructure-level hops between ASes
Challenges in detecting infrastructure outages

1. Capturing the infrastructure-level hops between ASes
Challenges in detecting infrastructure outages

1. Capturing the infrastructure-level hops between ASes
2. Correlating the paths from multiple vantage points
Challenges in detecting infrastructure outages

1. Capturing the infrastructure-level hops between ASes
2. Correlating the paths from multiple vantage points
3. Continuous monitoring of the routing system
Challenges in detecting infrastructure outages

1. Capturing the infrastructure-level hops between ASes
2. Correlating the paths from multiple vantage points
3. Continuous monitoring of the routing system

Can we combine **continuous passive** measurements with **fine-grained** topology discovery?
Deciphering location metadata in BGP

PREFIX: 1.0.0.0/24
ASPATH: 2 1 0
COMMUNITY: 2:200
Deciphering location metadata in BGP

**BGP Communities:**
- Optional attribute
- 32-bit numerical values
- Encodes *arbitrary* metadata

**PREFIX:** 1.0.0.0/24
**ASPATH:** 2 1 0
**COMMUNITY:** 2:200
Deciphering location metadata in BGP

The BGP Community 2:200 is used to tag routes received at Facility 2.

PREFIX: 1.0.0.0/24
ASPATH: 2 1 0
COMMUNITY: 2:200
Deciphering location metadata in BGP

Prefix: 1.0.0.0/24
ASPATH: 2 1 0
Community: 2:200

Prefix: 3.3.3.3/24
ASPATH: 4 3
Community: 4:8714 4:400

Prefix: 2.2.2.2/24
ASPATH: 4 2
Community: 4:8714 4:400
Deciphering location metadata in BGP

When a route changes ingress point, the community values will be updated to reflect the change.

PREFIX: 1.0.0.0/24
ASPATH: 2 1 0
COMMUNITY: 2:100

PREFIX: 3.3.3.3/24
ASPATH: 4 3
COMMUNITY: 4:400

PREFIX: 2.2.2.2/24
ASPATH: 4 2
COMMUNITY: 4:8714 4:400
Interpreting BGP Communities

- Community values **not standardized**.
- Documentation in public data sources:
  - WHOIS, NOCs websites
- Natural Language Tools to extract the interpretations
Topological coverage

- 3,049 communities by 468 ASes.
- \(\sim 50\%\) of IPv4 and \(\sim 30\%\) of IPv6 paths annotated with at least one Community in our dictionary.
- 24% of the facilities in PeeringDB, 98% of the facilities with at least 20 members.
Passive outage detection: **Initialization**

For each vantage point (VP) collect all the **stable** BGP routes tagged with the communities of the target facility (Facility 2)
Passive outage detection: **Initialization**

For each vantage point (VP) collect all the **stable** BGP routes tagged with the communities of the target facility (Facility 2)
Passive outage detection: Monitoring

Track the BGP updates of the stable paths for changes in the communities values that indicate ingress point change.
Passive outage detection: **Outage signal**

- Concurrent changes of communities values for the same facility.
- **Indication** of outage but not final inference yet!

---

**AS_PATH**: 1 x  
**COMM**: 1:FAC1

**AS_PATH**: 2 1 0  
**COMM**: 2:FAC1

**AS_PATH**: 4 x  
**COMM**: 4:FAC4  
4:IXP
Passive outage detection: **Outage signal**

- Concurrent changes of communities values for the same facility.
- **Indication** of outage but not final inference yet!
Passive outage detection: **Outage signal**

- Concurrent changes of communities values for the same facility.
- **Indication** of outage but not final inference yet!
Partial outage? De-peering of large ASes? Major routing policy change?

Signal investigation:

- Targeted active measurements.
- How disjoint are the affected paths?
- How many ASes and links have been affected?
Passive outage detection:  Outage tracking

End of outage inferred when the majority of paths return to the original facility.
Outage source disambiguation and localization

Paths not investigated in aggregated manner, but at the granularity of separate (AS, Facility) co-locations.
De-noising of BGP routing activity

The aggregated activity of BGP messages (updates, withdrawals, states) provides no outage indication.
De-noising of BGP routing activity

The aggregated activity of BGP messages (updates, withdrawals, states) provides no outage indication.

The BGP activity filtered using communities provides strong outage signal.
Detecting peering infrastructure outages in the wild

- **159** outages in 5 years of BGP data
  - **76%** of the outages not reported in popular mailing lists/websites
- Validation through status reports, direct feedback, social media
  - **90%** accuracy, **93%** precision (for trackable PoPs)
Effect of outages on Service Level Agreements

~70% of failed facilities below 99.999% uptime
~50% of failed IXPs below 99.99% uptime
5% of failed infrastructures below 99.9% uptime!
Measuring the impact of outages

> 56% of the affected links in different country, > 20% in different continent!

50% increase in the number of paths with end-to-end RTT > 100 ms during the AMS-IX outage.
Conclusions

- **Timely** and **accurate** infrastructure-level outage detection through **passive** BGP monitoring

- Majority of outages not (widely) reported

- Remote peering and infrastructure interdependencies **amplify** the impact of local incidents

- **Hard evidence** on outages can improve accountability, transparency and resilience strategies
Detecting Peering Infrastructure Outages in the Wild

Vasileios Giotsas  
CAIDA/TU Berlin  
vgiotsas@ucsd.edu

Christoph Dietzel  
TU Berlin/DE-CIX  
christoph@inet.tu-berlin.de

Georgios Smaragdakis  
MIT/TU Berlin  
gsmaragd@csail.mit.edu

Anja Feldmann  
TU Berlin  
anja@inet.tu-berlin.de

Arthur Berger  
MIT/Akamai  
awberger@csail.mit.edu

Emile Aben  
RIPE NCC  
emile.aben@ripe.net

ABSTRACT
Peering infrastructures, namely, colocation facilities and Internet exchange points, are located in every major city, have hundreds of network members, and support hundreds of thousands of interconnections around the globe. These infrastructures are well provisioned and managed, but outages have to be expected, e.g., due to power failures, human errors, attacks, and natural disasters. However, little is known about the frequency and impact of outages at these critical infrastructures with high peering concentration.

1 INTRODUCTION
Today, our economy as well as our social life, rely on the smooth and uninterrupted operation of the Internet. While the Internet has shown an amazing resilience as a whole, even short outages can have a significant impact on a subset of the Internet user population. Past major Internet outages have been studied in depth, including outages due to network component failure, e.g., hardware, software, and configuration failures in routers [98], optical layer outages [47], natural disasters [20, 23, 35, 56, 84], and nation-wide censorship [23,