Detecting Peering Infrastructure Outages in the Wild

Vasileios Giotsas †, Christoph Dietzel †§, Georgios Smaragdakis ‡†, Anja Feldmann †, Arthur Berger ¶‡, Emile Aben #

†TU Berlin  *CAIDA  §DE-CIX  ¶MIT  ¶¶Akamai  #RIPE NCC
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)\(^1\)

Carrier-neutral 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)\(^2\)

\(^1\) [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.
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

Actual incident

Observed paths

Before outage
Challenges in detecting infrastructure outages

Actual incident

VP

Observed paths

Before outage
Challenges in detecting infrastructure outages
Challenges in detecting infrastructure outages

1. Capturing the infrastructure-level hops between ASes

![Diagram showing actual incident and observed paths before and during outage. AS path does not change!](image-url)
Challenges in detecting infrastructure outages

1. Capturing the infrastructure-level hops between ASes

Before outage

During outage

IXP or Facility 2 failed
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

France-IX topology
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
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

IP-to-Facility\(^3,4\) and IP-to-IXP\(^5\) mapping **possible** but **expensive**!

---

\(^3\) Giotsas, Vasileios, et al. "Mapping peer ing interconnections to a facility", CoNEXT 2015
Challenges in detecting infrastructure outages

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

Can we combine **continuous passive** measurements with **fine-grained** topology discover?
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

- BGP: ✓
- Traceroute: ✗
Deciphering location metadata in BGP

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

BGP Communities:
- Optional attribute
- 32-bit numerical values
- Encodes arbitrary metadata
Deciphering location metadata in BGP

PREFIX: 1.0.0.0/24
ASPATH: 2 1 0
COMMUNITY: 2:200

Top 16 bits: ASN that sets the community.
Bottom 16 bits: Numerical value that encodes the actual meaning.
Deciphering location metadata in BGP

The BGP Community 2:200 is used to tag routes received at Facility 2.
Deciphering location metadata in BGP

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

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

Multiple communities can tag different types of ingress points.

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**: 3.3.3.3/24
  - **ASPATH**: 4 3
  - **COMMUNITY**: 4:400

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

- Community values not standardized.
- Documentation in public data sources:
  - WHOIS, NOCs websites
- 3,049 communities by 468 ASes
Topological coverage

- ~50% of IPv4 and ~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: Monitoring

We don’t care about AS-level path changes if the ingress-tagging communities remain the same.
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!
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

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

The BGP activity filtered using communities provides strong outage signal.
The location of community values that trigger outage signals may **not** be the outage source!

- Communities encode the ingress point closest to our VPs (near-end infrastructure)
  - ASes may be interconnected over multiple intermediate infrastructures
  - Failures in intermediate infrastructures may affect the near-end infrastructure paths
Outage localization is more complicated!
Outage localization is more complicated!
Outage localization is more complicated!

Outage in Facility 2 causes drop in the paths of Facility 4!
Outage localization is more complicated!
Outage localization is more complicated!

Outage in Facility 3 causes drop in the paths of Facility 4!
Outage source disambiguation and localization

- Create **high-resolution co-location maps:**
  - AS to Facilities, AS to IXPs, IXPs to Facilities
  - Sources: PeeringDB, DataCenterMap, operator websites

- Decorrelate the behaviour of affected ASes based on their infrastructure colocation.
Outage localization is more complicated!

Far-end ASes colocated in Facility 2
Outage localization is more complicated!

Far-end ASes colocated in Facility 3
Outage source disambiguation and localization

Paths not investigated in aggregated manner, but at the granularity of separate (AS, Facility) co-locations.
Paths not investigated in aggregated manner, but at the granularity of separate (AS, Facility) co-locations.
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!

Median RTT rises by > 100 ms for rerouted paths during 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
Thank you!
Tracking the progress of outages

Passive tracking:
Monitor how location-tagging BGP Communities change during the outage.

Active tracking:
Execute targeted traceroutes based on the hints of the BGP signals.
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

Before outage

The initial hops changed

No hop changes
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

Before outage

During outage

Passive BGP monitoring

BGP encodes AS paths

The initial hops changed

No hop changes
Deciphering location-metadata in BGP

- BGP not entirely information-hiding!

- **Communities BGP attribute:**
  - Optional, tags BGP routes with arbitrary metadata
  - Often encodes the **ingress location** of prefixes