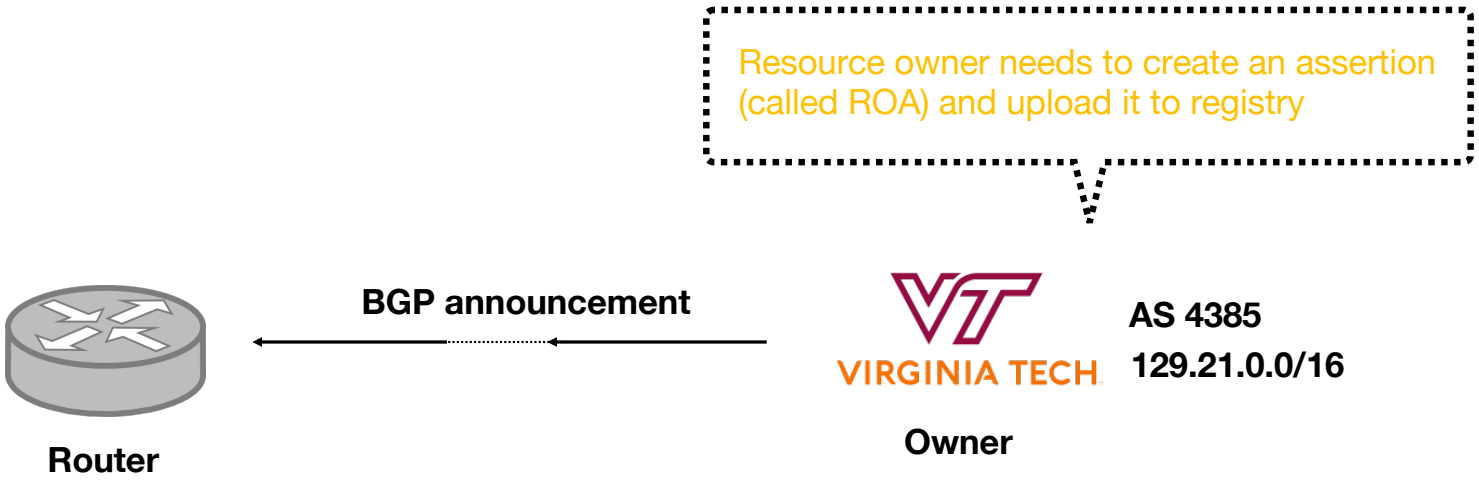
RoVista+: Mapping Real ROV Deployments, Dependencies, and Delays

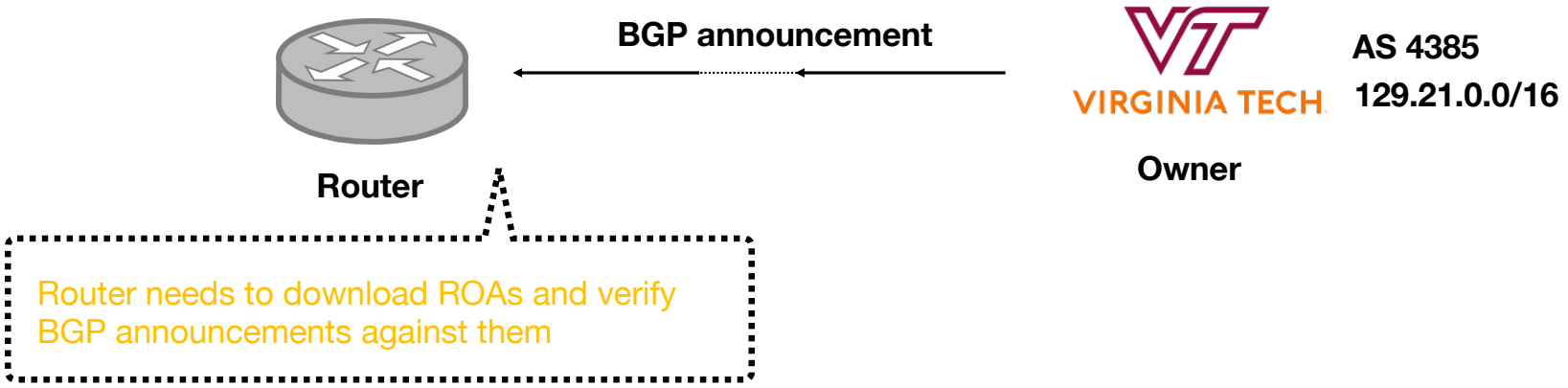
Tijay Chung (https://tijay.github.io)
Associate Professor at VT

VIRGINIA TECH

Route Origin Authorization vs. Route Origin Validation



Route Origin Authorization vs. Route Origin Validation



Two questions

- How do network operators use RPKI to “claim” their IP addresses?
- How do network operators also use RPKI to “filter” invalid BGP announcements?

Two questions

Answering this question is “relatively” straightforward

- How do network operators use RPKI to “claim” their IP addresses?
- How do network operators also use RPKI to “filter” invalid BGP announcements?

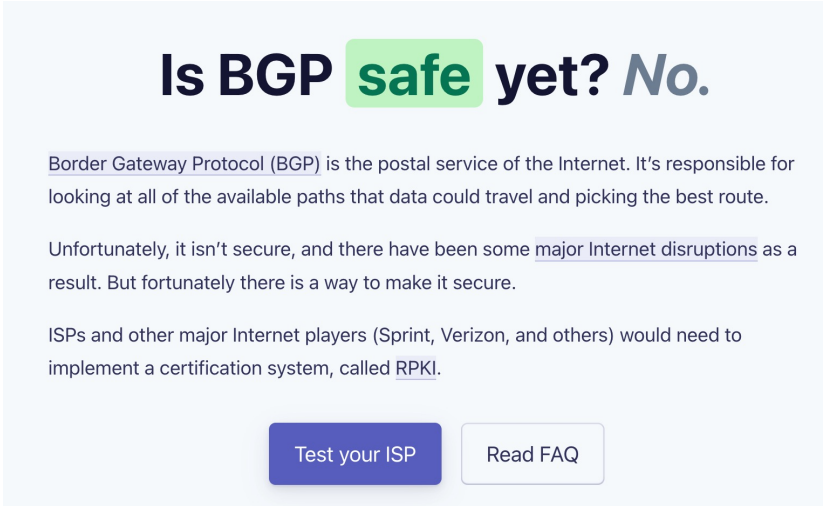
Two questions

- How do network operators use RPKI to “claim” their IP addresses?
- How do network operators also use RPKI to “filter” invalid BGP announcements?

This is **not** straightforward

Previous approaches (1)

https://isbgpsafeyet.com/



valid.rpki.cloudflare.com

Announced By		
Origin AS	**Announcement**	**Description**
AS13335	104.16.0.0/12	Cloudflare, Inc.
AS13335	104.18.32.0/19	Cloudflare, Inc.
AS13335	104.18.32.0/20	Cloudflare, Inc.
AS13335	104.18.47.0/24	Cloudflare, Inc.

invalid.rpki.cloudflare.com

Announced By		
Origin AS	**Announcement**	**Description**
AS13335	103.21.244.0/24	Cloudflare, inc.

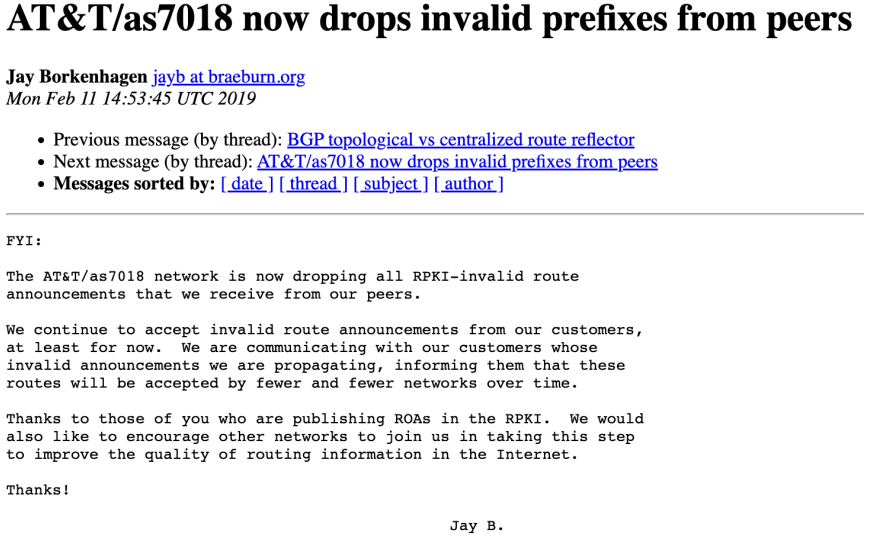
Previous approaches (2)

- Crowd-source based spreadsheet managed by network operators
  - http://rpki.exposed

	May 4th 2020	*Rejecting invalids*	*Rejecting invalids*	*Rejecting invalids*		
Carrier	**ASN**	**Transits**	**Peers**	**Customers**	**ROAs**	**Status**
NTT	2914	n/a	yes	yes	done	done
GTT	3257	n/a	yes	yes	done	done
AT&T	7018	n/a	yes	no	in progress	in progress
Telia	1299	n/a	yes	yes	done	done
Workonline	37271	yes	yes	yes	done	done
Seacom	37100	yes	some	yes		done
KPN Eurorings	286	n/a // yes (*)	yes	yes	done	done
Freethought	41000	yes	yes	yes	done	done
Fusix	57866	yes	yes	yes	done	done
BIT	12859	yes	yes	yes	done	done
Tuxis	197731	yes	yes	yes	done	done
MaxiTEL (NL)	61349	yes	yes	yes	done	done
ColoClue	8283	yes	yes	no	done	done
Fiber Telecom	41327	yes	yes	yes	done	done
Sentia BV	8315	yes	yes	yes	done	done
Cadence Networks	47638	yes	yes	yes	done	done
Atom86	8455	yes	yes	yes	done	done
AMS-IX	6777	n/a	yes	n/a	done	done
NetNod	52005	n/a	yes	n/a		done

Previous approaches (3)

- Official blogpost, mailing list, and so on.



AT&T/as7018 now drops invalid prefixes from peers

Jay Borkenhagen jayb at braeburn.org
Mon Feb 11 14:53:45 UTC 2019

- Previous message (by thread): BGP topological vs centralized route reflector
- Next message (by thread): AT&T/as7018 now drops invalid prefixes from peers
- **Messages sorted by:** [date] [thread] [subject] [author]

```
FYI:

The AT&T/as7018 network is now dropping all RPKI-invalid route
announcements that we receive from our peers.

We continue to accept invalid route announcements from our customers,
at least for now.  We are communicating with our customers whose
invalid announcements we are propagating, informing them that these
routes will be accepted by fewer and fewer networks over time.

Thanks to those of you who are publishing ROAs in the RPKI.  We would
also like to encourage other networks to join us in taking this step
to improve the quality of routing information in the Internet.

Thanks!

                                                        Jay B.
```

Previous Approach (4)
RoVista: Measuring RPKI ROV status at Scale [NANOG'90]

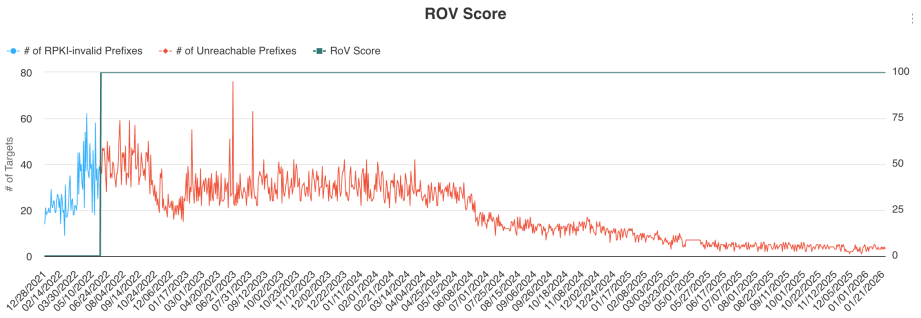
- Goal: Assess if ASes drop RPKI-invalid routes.
- Technique: Remote Connectivity Inference (called "IP-ID Side Channel").
  - Target: Live servers located in ``in-the-wild'' RPKI-invalid prefixes.
  - Source: Sampled vantage points (e.g., 10 hosts) within the Subject AS.
- Detection Logic:
  - No Connectivity → ROV filtering (Local or Upstream)
  - Connectivity Established → No ROV (Traffic allowed)
- Dataset: 3-year longitudinal data available at https://rovista.netsecurelab.org (around 32K ASes); All measurement hosts are available upon approved registration.

RoV Scores

Search By: Organization | Search: Comcast

Rank	ASN	Country	Organization	ROV-Score	Last updated on
34	7922	United States	Comcast Cable Communications, LLC	100.0%	2026-01-25
197	33491	United States	Comcast Cable Communications, LLC	100.0%	2026-01-25
255	7015	United States	Comcast Cable Communications, LLC	100.0%	2026-01-25
272	33651	United States	Comcast Cable Communications, LLC	100.0%	2026-01-25

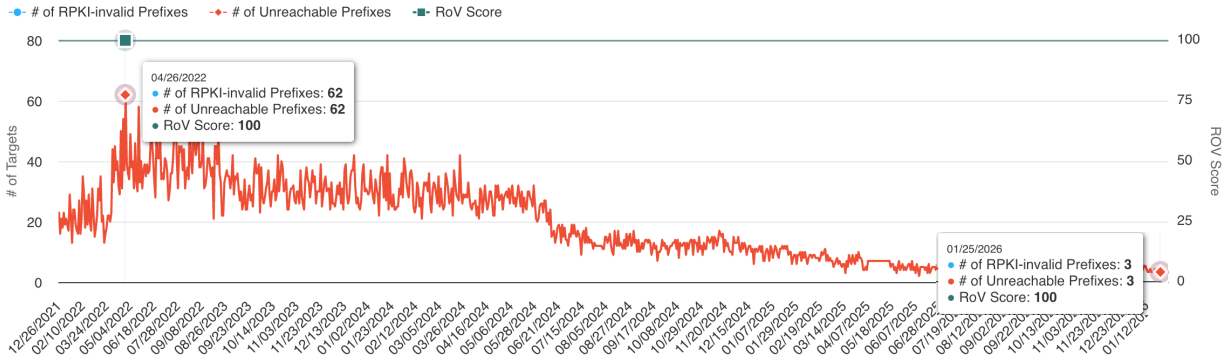
AS 5511



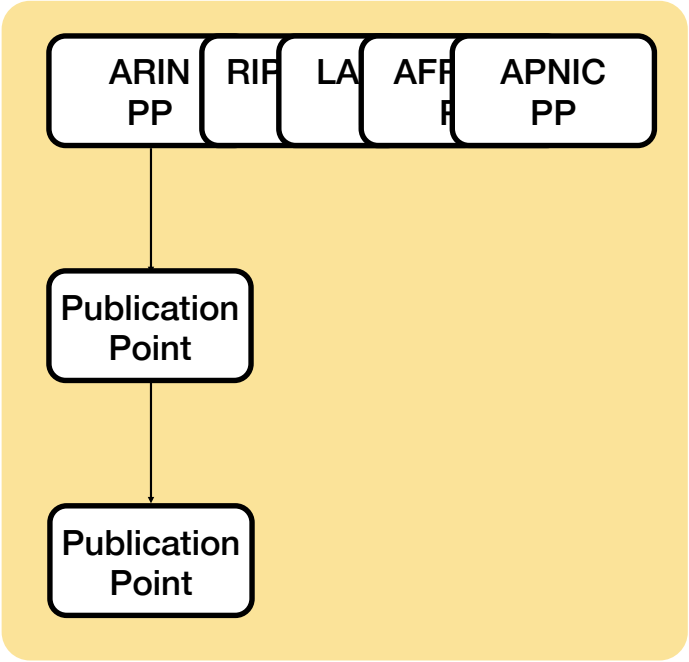
Challenges of RoVista

- Visibility: RoVista cannot determine who has actively deployed ROV. For an AS, if one of their upstream providers has deployed it, some RPKI-invalid prefixes may be filtered, while others may not.

- Reduction in RPKI-invalid prefixes: As ROV deployment expands, the number of visible RPKI-invalid prefixes decreases significantly, dropping from approximately 40–50 to around 5.

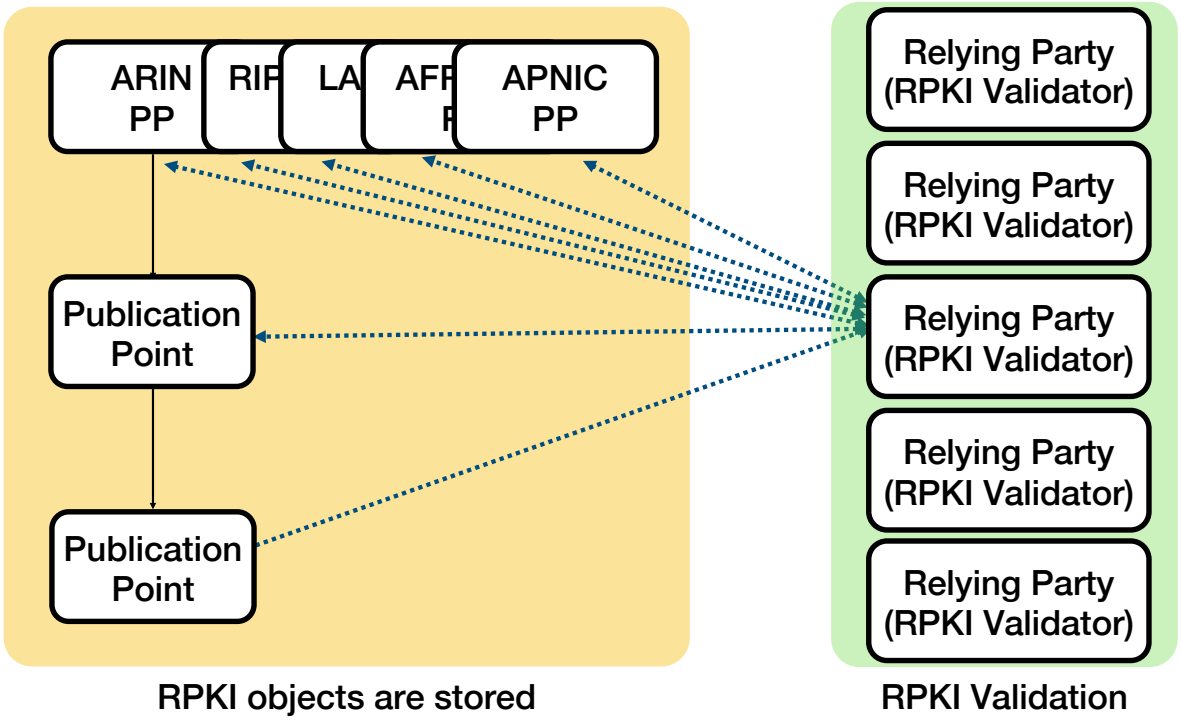


ROV Ecosystem

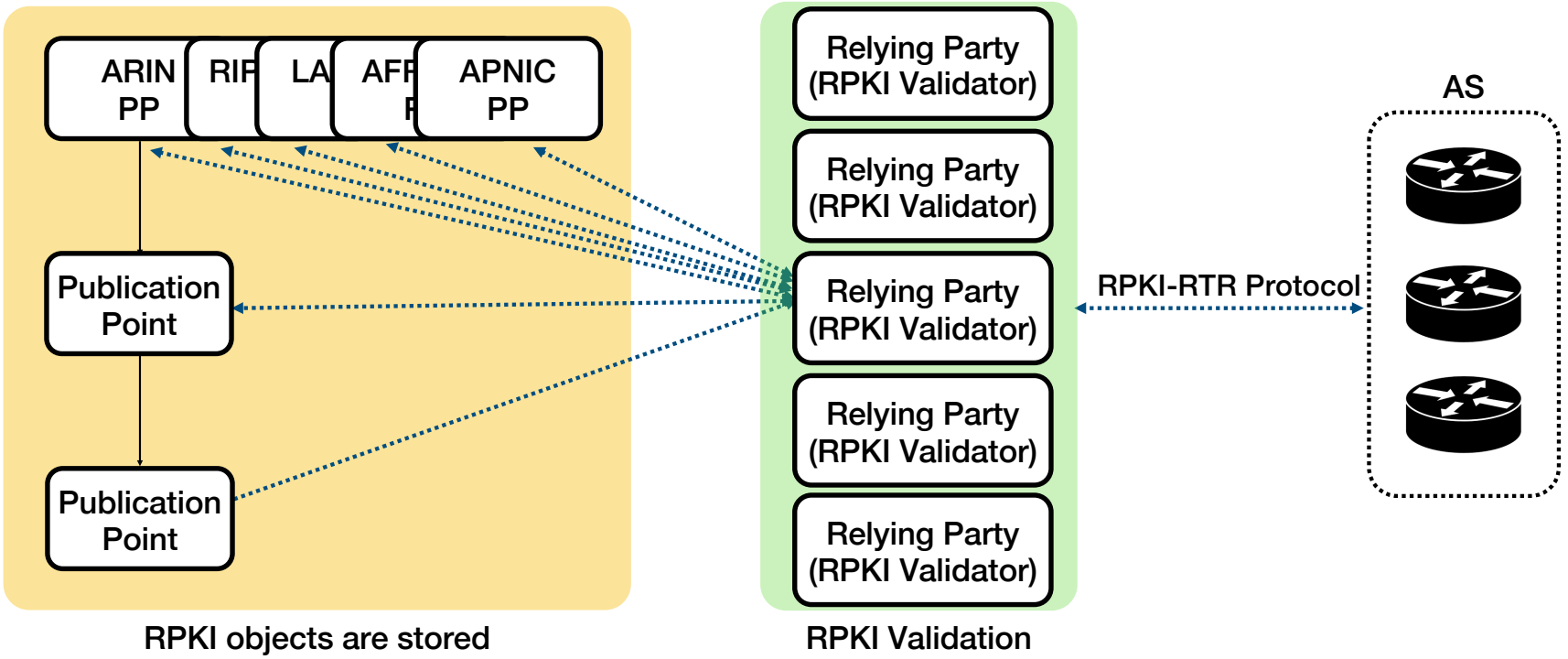


RPKI objects are stored

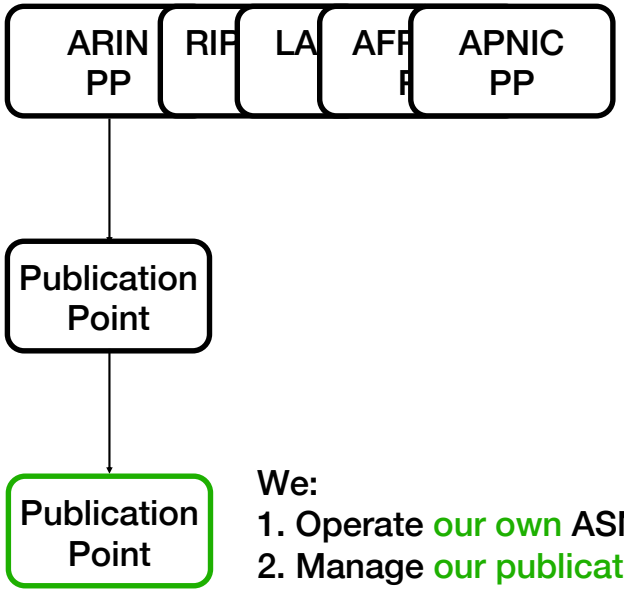
ROV Ecosystem



ROV Ecosystem

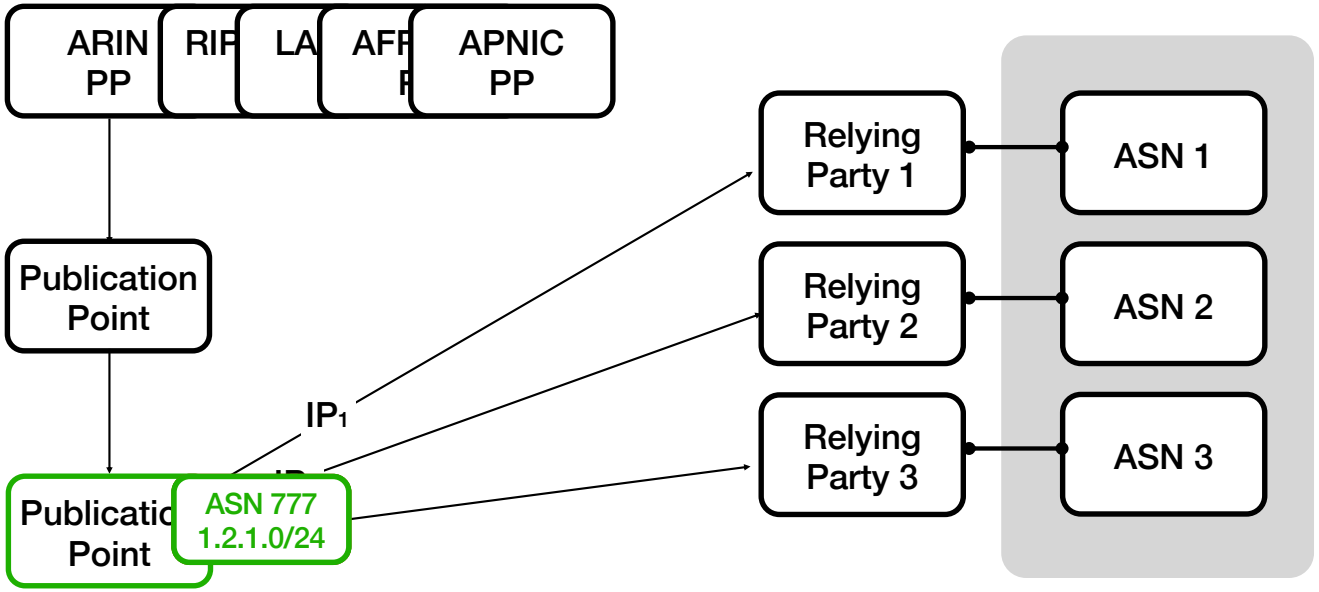


RoVista+: Measuring ROV Deployment at Scale



We:
1. Operate our own ASN and IP prefixes.
2. Manage our publication points, ensuring that all RPKI-relying parties must retrieve data directly from these points.

RoVista+: Measuring ROV Deployment at Scale



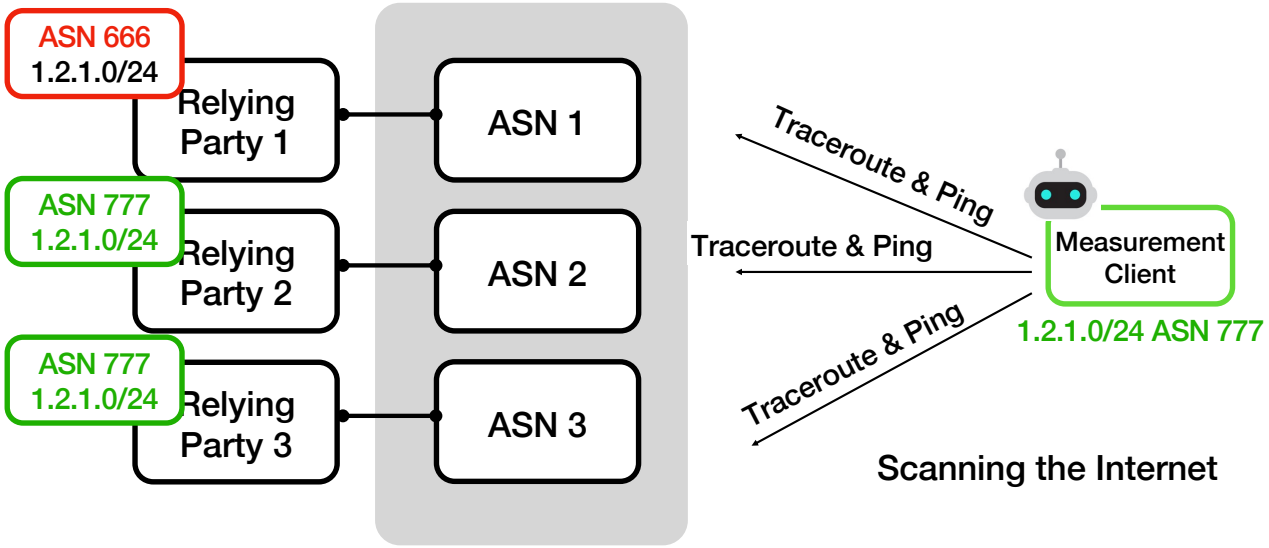
Operating publication points alone do not reveal which ASes are using specific RPs.

(1) We run our own ASN and IP prefixes ASN 777 and 1.2.0.0/24
(2) We announce 1.2.0.0/24 from ASN 777

3. We create two distinct ROAs for /24:
(a) A test ROA associated with ASN 666.
(b) A control ROA associated with ASN 777.

4. The test ROA is exclusively returned to RP1.

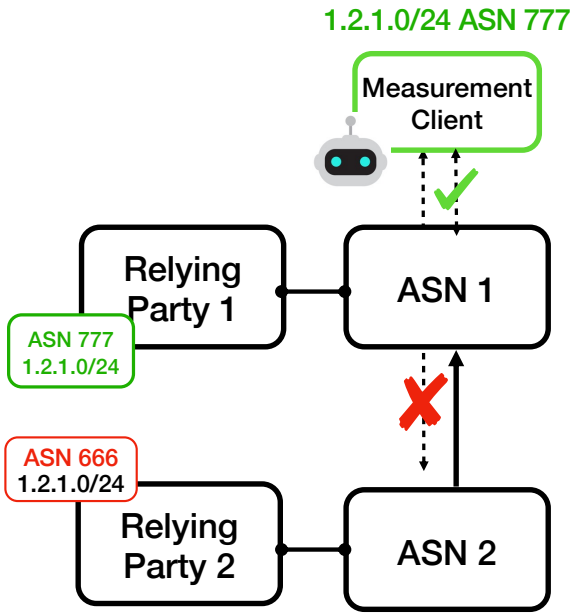
RoVista+: Measuring ROV Deployment at Scale



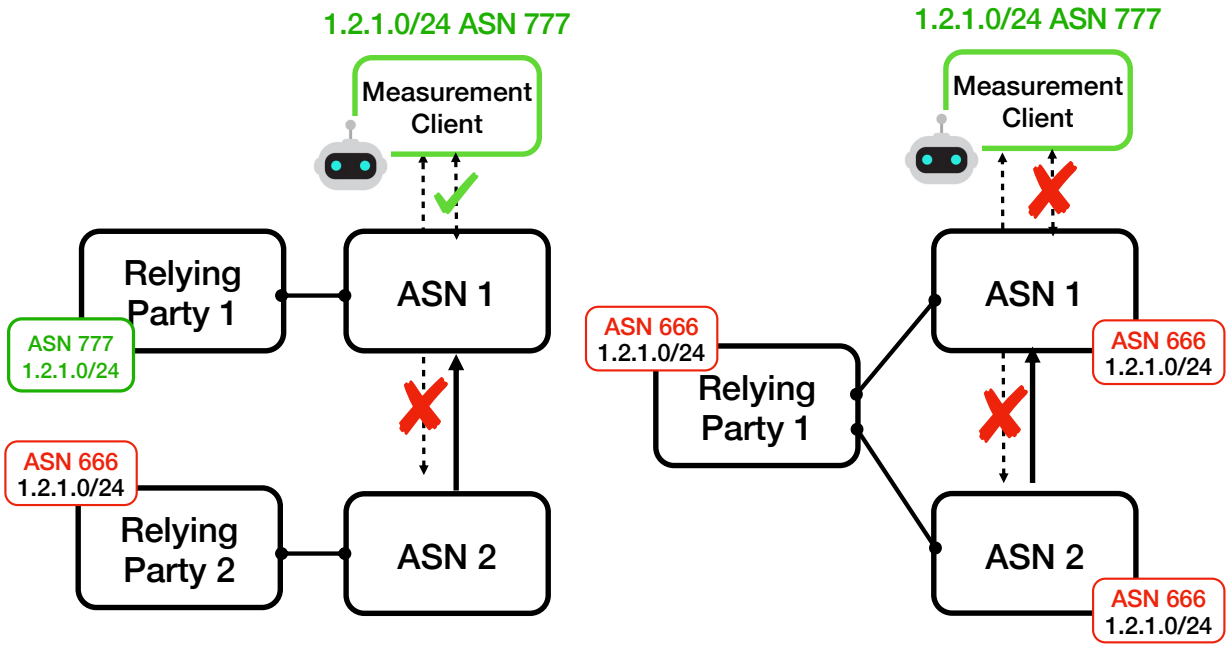
If ASN1 was previously able to reach (and respond) to our network but cannot after the introduction of a test-ROA, it suggests:

1. ASN1 has likely deployed ROV independently.
2. ASN1 is likely using RP1 for RPKI validation.

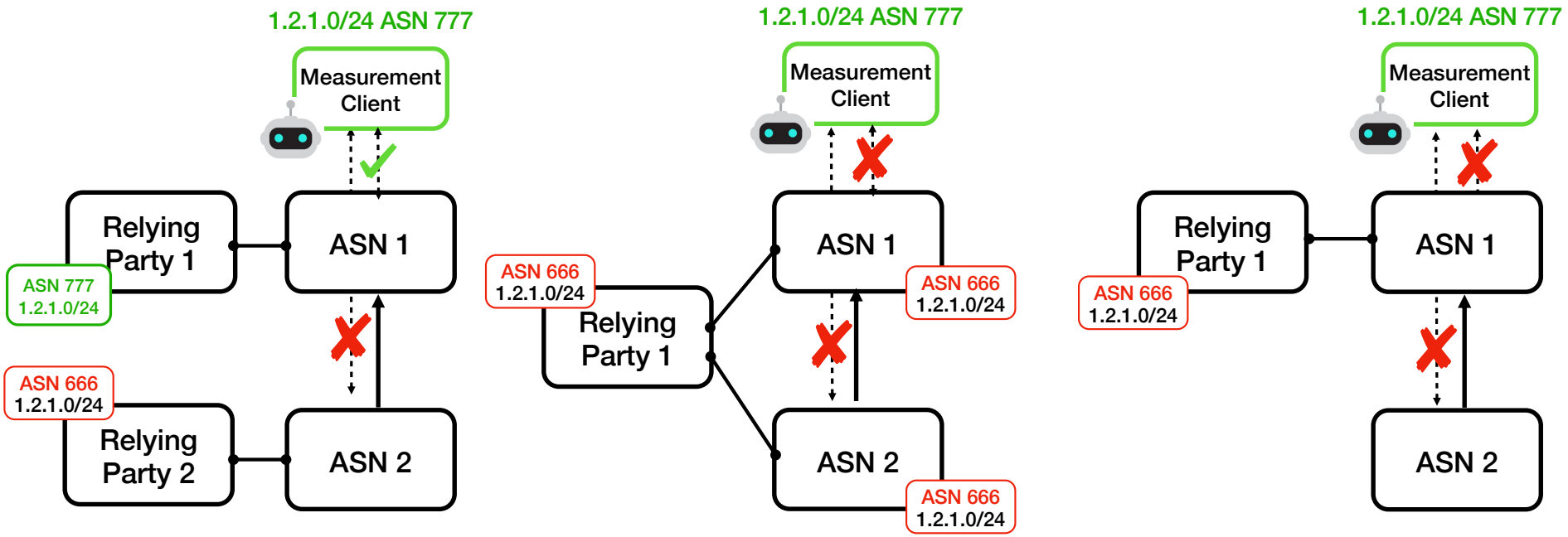
Challenge:
Distinguishing Local vs. Upstream Filtering in Single Upstream



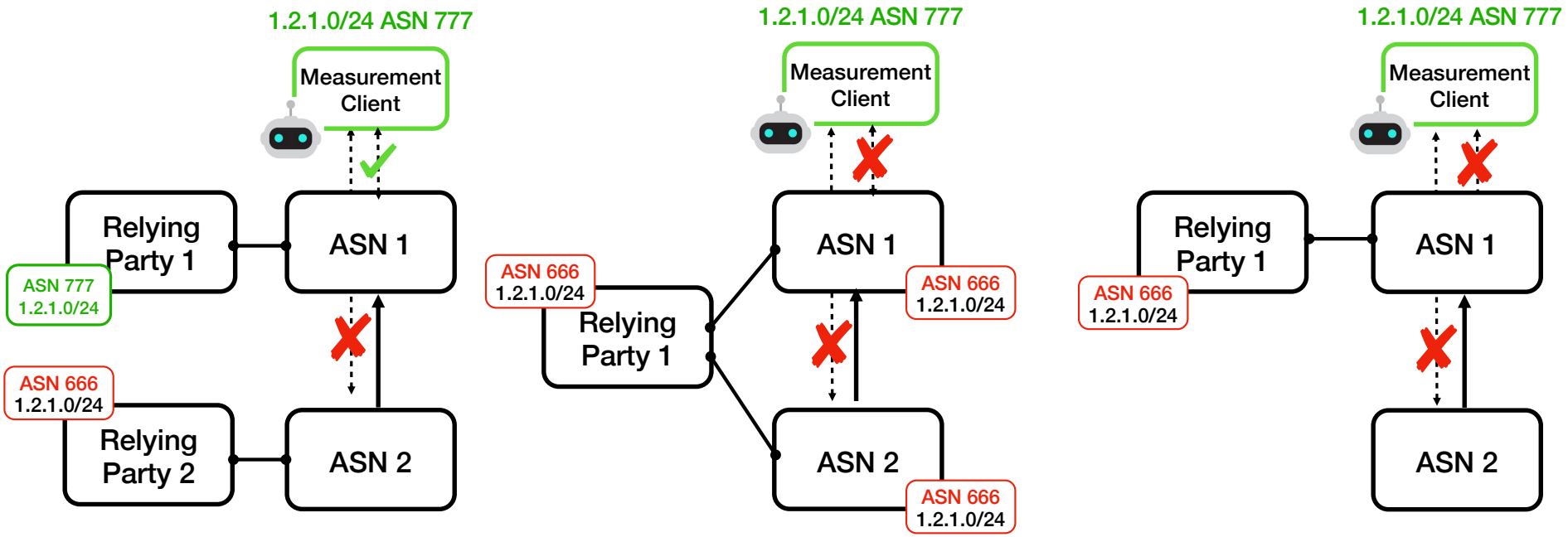
Challenge:
Distinguishing Local vs. Upstream Filtering in Single Upstream



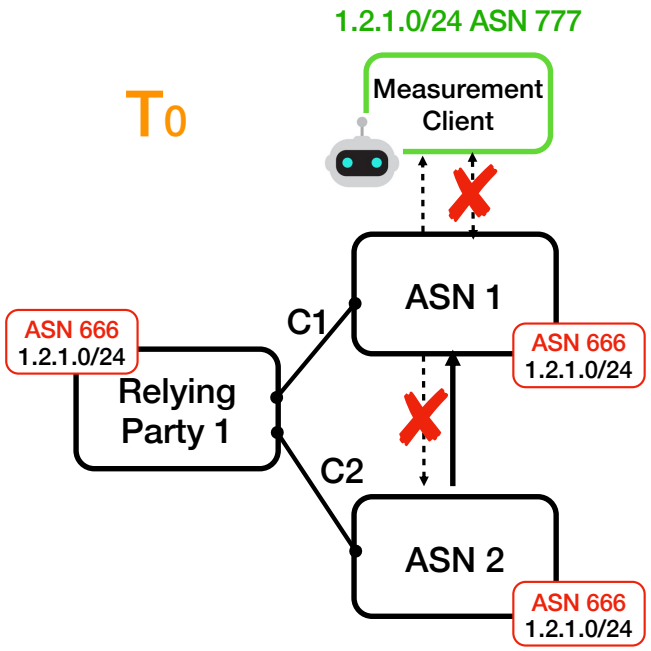
Challenge:
Distinguishing Local vs. Upstream Filtering in Single Upstream



Challenge:
Distinguishing Local vs. Upstream Filtering in Single Upstream



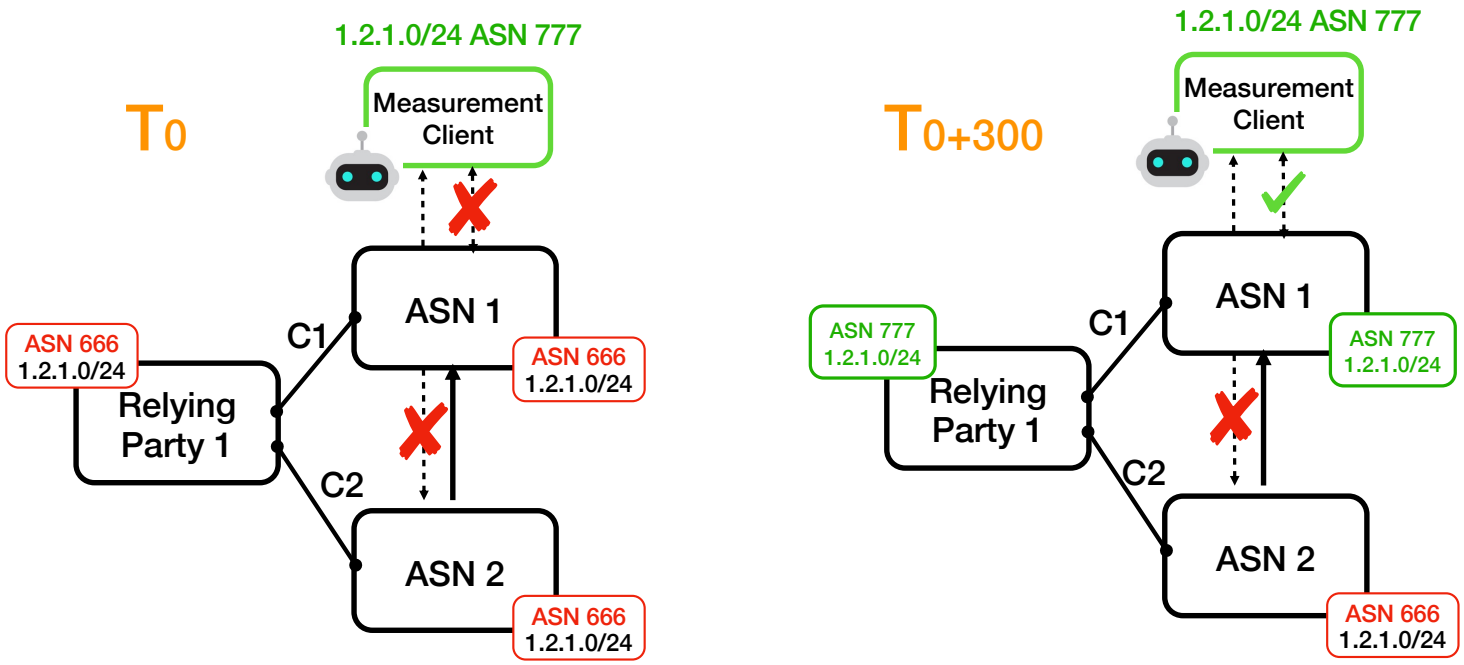
Distinguishing Local vs. Upstream Filtering (1) Shared Relying Party



C1 and C2:

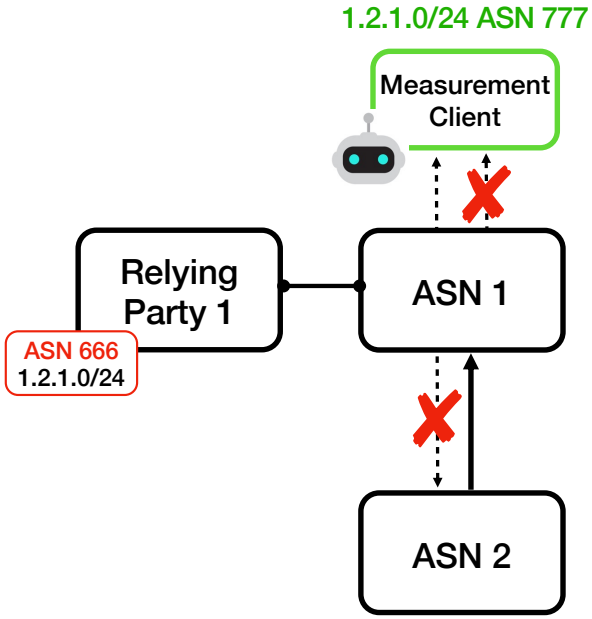
* RTR-Refresh Interval: The default is 600 seconds (10 minutes) [RFC 8210].
* two cycles are not synchronized, so synchronized behavior cannot always be expected.

Distinguishing Local vs. Upstream Filtering
(1) Shared Relying Party



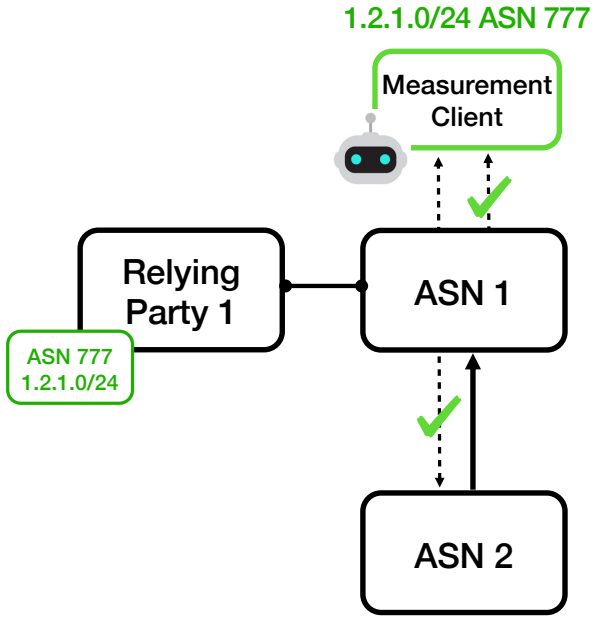
- RTR-Refresh Interval: The default is 600 seconds (10 minutes) [RFC 8210].
- It is highly likely that two cycles are not synchronized, so synchronized behavior cannot always be expected.
- We conduct multiple measurements, so the observed ROV status of AS1 and AS2 may not always appear synchronized.

Distinguishing Local vs. Upstream Filtering
(2) Upstream Filtering



The observed ROV status of AS1 and AS2 should always appear synchronized.

Distinguishing Local vs. Upstream Filtering
(2) Upstream Filtering



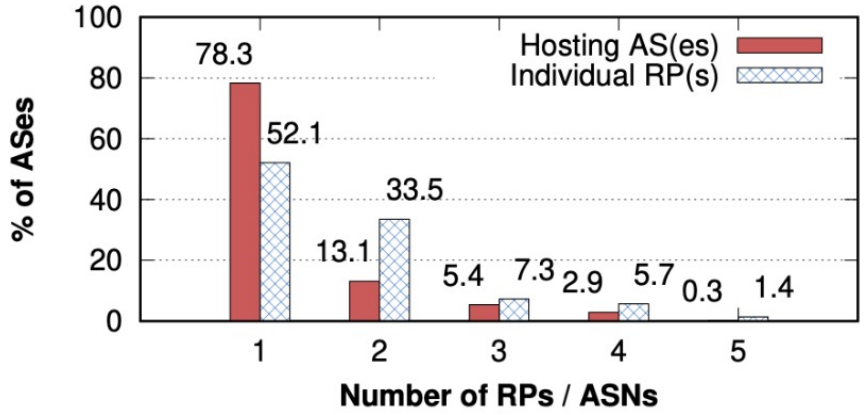
The observed ROV status of AS1 and AS2 should always appear synchronized.

Results

- Scale: 21,827 ASes measured.
- ROV Status:
  - Protected: 2,942 ASes (Total filtered).
  - Self-Deployed: 1,127 ASes
  - RP Infrastructure: 1,127 ASes rely on 1,672 RPs (hosted in 1,319 ASes).
- Duration: Continuous measurement since May 2025.

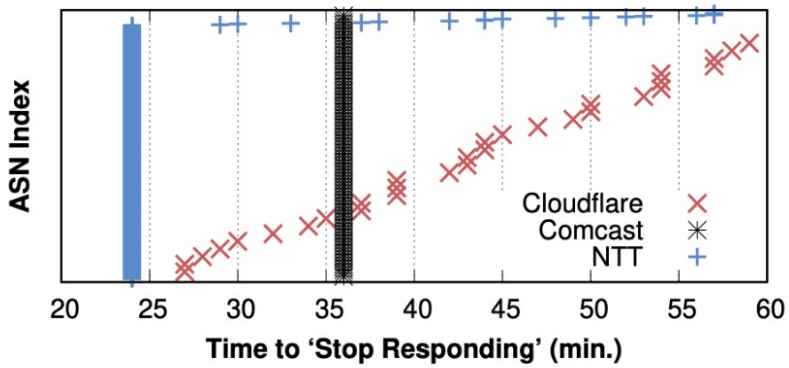
Observation
(1) Reliance on RPs

- 52% of ASes rely on exactly one RP server
- Only 14% deploy multiple RPs across different ASNs
- RFC 7115 recommends configuring multiple RPs to ensure resilience.



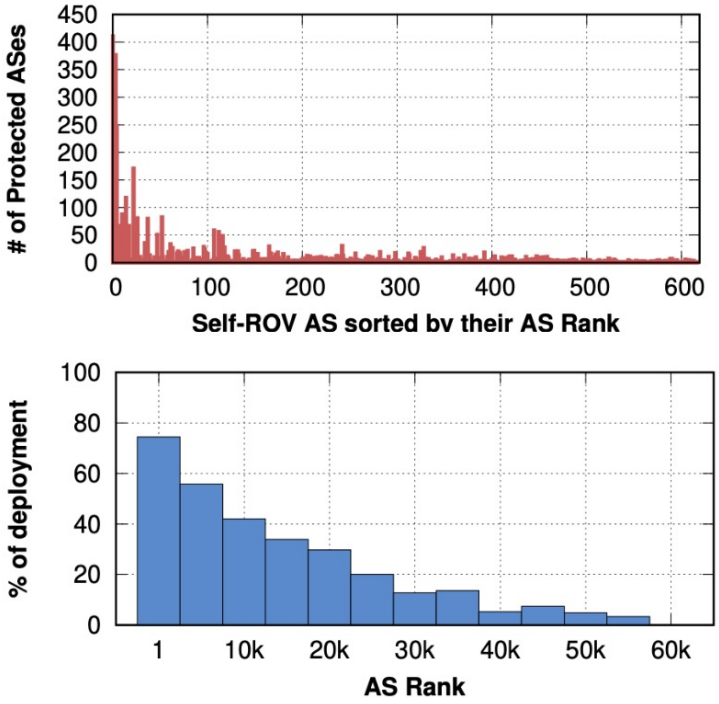
(2) Timing-Based ROV Detection

- Hypothesis: Drop Time Correlation
  - Upstream Protection: Downstream ASes lose connectivity precisely when the upstream filters (Synchronized).
  - Self-Deployment: Independent ASes drop at different times (due to unaligned RTR polling/router updates).
- Validation (Case Studies):
  - Comcast (Private RP): 94 ASes dropped simultaneously → Upstream Enforcement.
  - Cloudflare (Public RP): Client ASes dropped at varied times → Independent Self-ROV.
  - NTT (Hybrid): Shows both synchronized clusters (downstreams) and independent drops (public RP users).



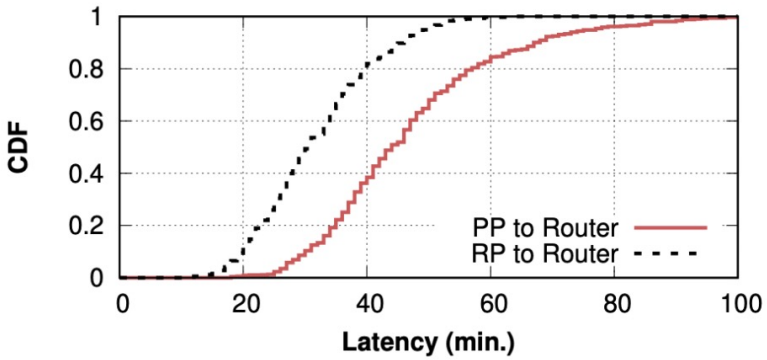
(3) ROV Protection and Deployment

- Higher-ranked ASes protect disproportionately large numbers of downstreams
- Top-tier ASes secure hundreds, while small ASes secure few
- ~74% of top 5,000 ASes self-deploy ROV
- Smaller ASes overwhelmingly depend on upstream filtering
- Implication:
  - Tier-1 and large ISPs drive global ROV effectiveness
  - ROV adoption is skewed toward large providers
  - Smaller networks remain vulnerable without upstream protection



(4) Validation Latency

- Observation:
  - End-to-end latency: 60–120 minutes
  - RP-to-router step alone adds ~37 minutes
- Implication:
  - Even after ROAs update, operational lag leaves invalid routes alive
  - Highlights need for faster RTR cycles and router enforcement



Summary

- RoVista+ is a framework that goes beyond RoVista to reveal how ASes truly deploy ROV, who they depend on, and how fast protection takes effect by running
  - Our own “dynamic” publication points
  - The Internet-wide scan
- We will release results at https://rovista.netsecurelab.org

RoVista+ is more than just a platform for measuring ROV deployment.

- With RoVista+, we expect to achieve the following:
  - Identify which ASes have deployed ROV.
  - Determine which RPs specific ASes rely on.
    - Assess the potential consequences of attacks on RPs (e.g., what happens if a public RP is compromised and experience outages?)
  - Gain deeper insights into AS paths.
    - Consider an AS path: AS 1, 2, 3, 777 (origin). If we are interested in exploring alternative paths, we can selectively return test ROAs to AS 2, causing only AS 2 to reject our announcement. This allows us to observe how AS 1 adjusts its path to reach us.
  - …

Q&A and Thanks

- Seeing unexpected ROV behavior? Let us know. We are actively looking for challenging problems and collaboration opportunities.
- This work is a joint effort with Weitong Li (VT), Yongzhe Xu (VT), Mingwei Zhang, and Vasileios Giotsas (Cloudflare).
- This research has been generously supported by NSF and Comcast Innovation Fund.