

RScope: Unveiling ROV Deployments and Dependencies in the Post-ROV Era (will appear at IMC'26)

Weitong Li, Yongzhe Xu, Mingwei Zhang, Vasileios Giotsas, and Tijay Chung
Virginia Tech and Cloudflare

Route Origin Authorization vs. Route Origin Validation



Route Origin Authorization vs. Route Origin Validation

Resource owner needs to create an assertion
(called ROA) and upload it to registry



Router

BGP announcement



Owner

AS 4385

129.21.0.0/16

Route Origin Authorization vs. Route Origin Validation



Router

BGP announcement



Owner

AS 4385

129.21.0.0/16

Router needs to download ROAs and
verify BGP announcements against them

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/>

Is BGP **safe** yet? *No.*

Border Gateway Protocol (BGP) is the postal service of the Internet. It's responsible for looking at all of the available paths that data could travel and picking the best route.

Unfortunately, it isn't secure, and there have been some major Internet disruptions as a result. But fortunately there is a way to make it secure.

ISPs and other major Internet players (Sprint, Verizon, and others) would need to implement a certification system, called RPKI.

[Test your ISP](#)

[Read FAQ](#)

Previous approaches (1)

<https://isbgpsafeyet.com/>

Is BGP **safe** yet? *No.*

Border Gateway Protocol (BGP) is the postal service of the Internet. It's responsible for looking at all of the available paths that data could travel and picking the best route.

Unfortunately, it isn't secure, and there have been some major Internet disruptions as a result. But fortunately there is a way to make it secure.

ISPs and other major Internet players (Sprint, Verizon, and others) would need to implement a certification system, called RPKI.

[Test your ISP](#)

[Read FAQ](#)

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.

Previous approaches (1)

<https://isbgpsafeyet.com/>

Is BGP **safe** yet? *No.*

Border Gateway Protocol (BGP) is the postal service of the Internet. It's responsible for looking at all of the available paths that data could travel and picking the best route.

Unfortunately, it isn't secure, and there have been some major Internet disruptions as a result. But fortunately there is a way to make it secure.

ISPs and other major Internet players (Sprint, Verizon, and others) would need to implement a certification system, called RPKI.

Test your ISP

Read FAQ

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

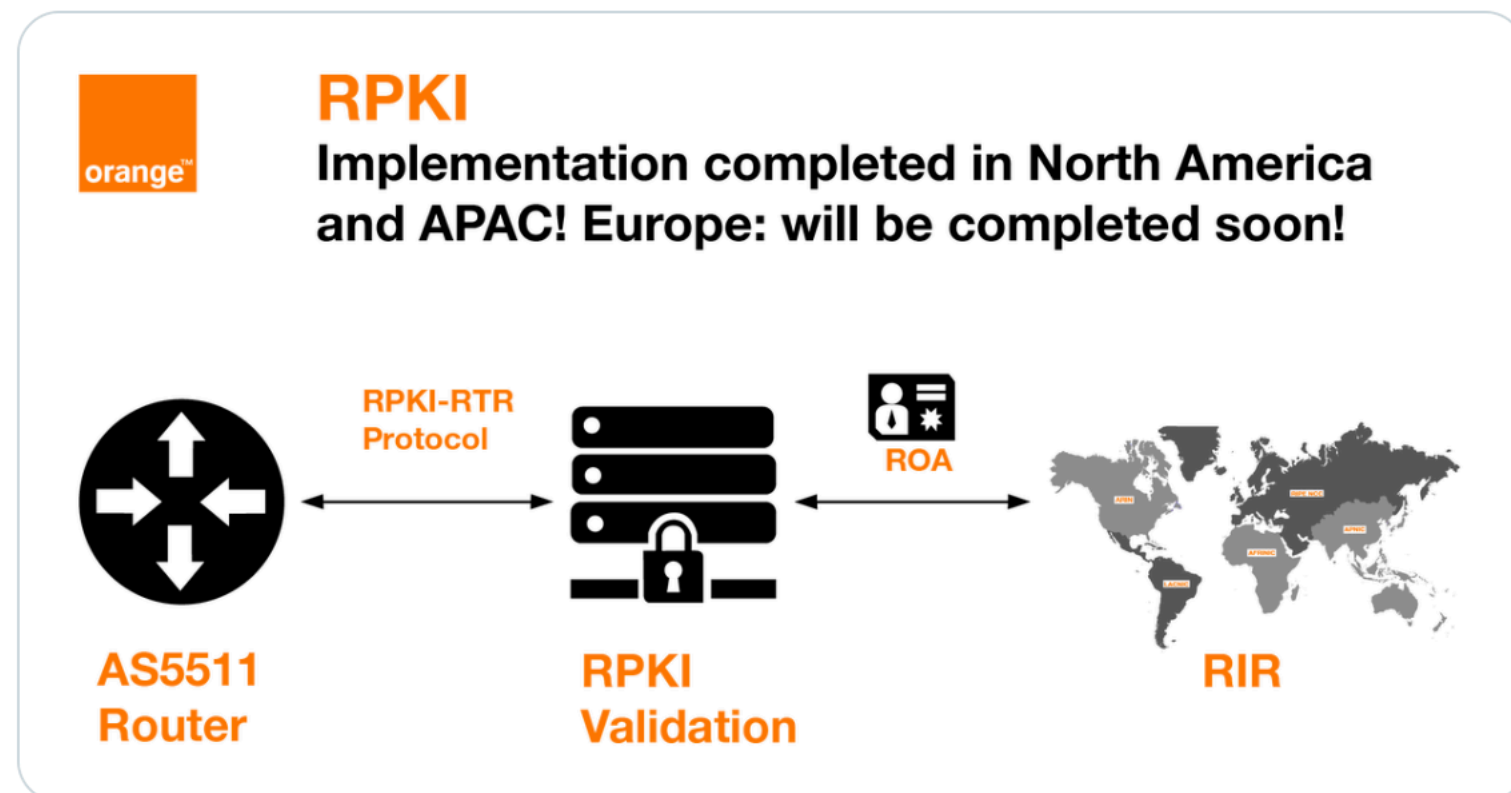
Announced By		
Origin AS	Announcement	Description
AS13335	103.21.244.0/24 🔑 ✓	Cloudflare, inc.

Previous approaches (2)

- Official blogpost, mailing list, and so on.

 **Orange Wholesale** 🌟
@OrangeWholesale

NEW We're glad to announce that we have now fully completed the **#RPKI** implementation in our **#IPTransit** network **NEW** ✓
Is your **#telecom** business ready? Already client? You can check your status via RPKI Monitor on our Customer Portal
Learn more about **#AS5511** 🖱️ oran.ge/39qZ1XI



11:00 AM · Jun 27, 2022

AT&T/as7018 now drops invalid prefixes from peers

Jay Borkenhagen [jayb at braeburn.org](mailto:jayb@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 (3)

RoVista: Measuring RPKI ROV status **at Scale** [IMC'23]

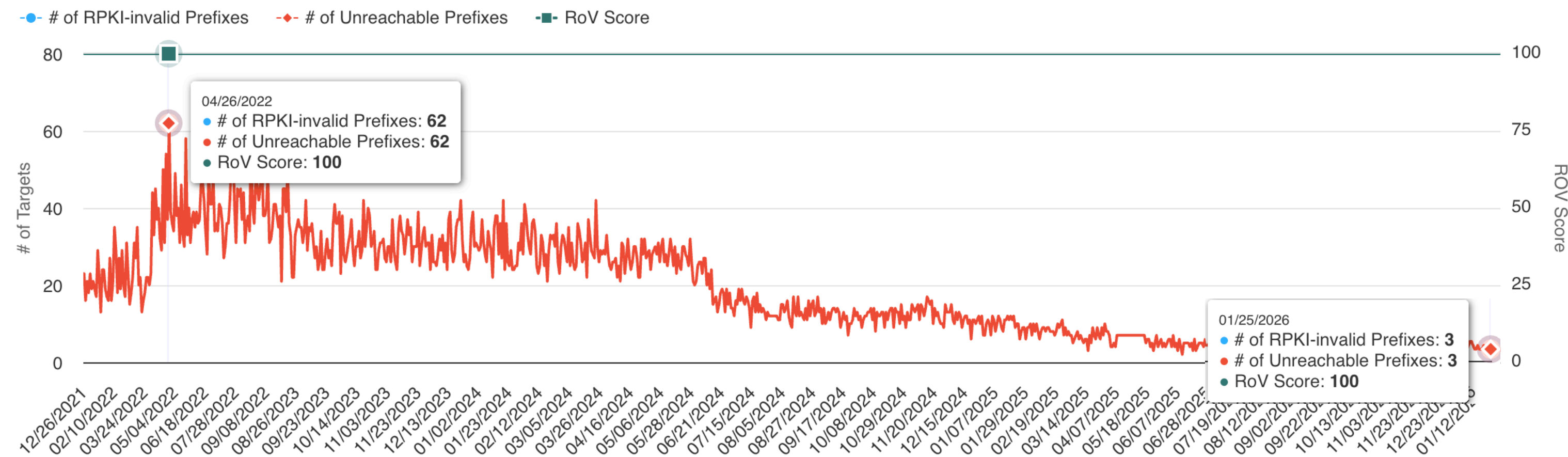
- Goal: Assess if ASes drop RPKI-invalid routes.
- Technique: Remote Connectivity Inference (called "IP-ID Side Channel").
 - Target: Live servers located in "in-the-wild" RPKI-invalid prefixes.
 - Source: Sampled vantage points (e.g., 10 hosts) within the Subject AS.
- Dataset: 3-year longitudinal data available at <https://rovista.netsecurelab.org> (around 32K ASes); All measurement hosts are available upon approved registration.

RoV Scores

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

Challenges

- Visibility: Data-plane measurements rely on the propagation of RPKI-invalid prefixes
- 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.

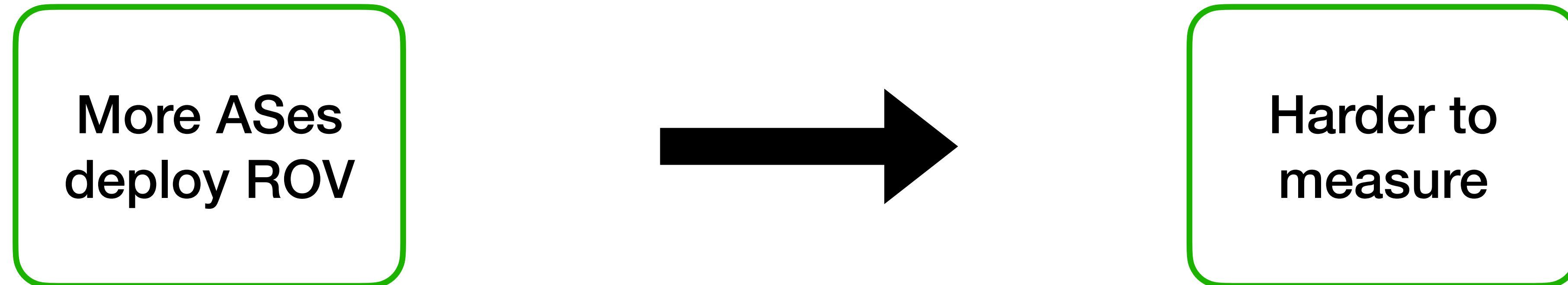


Challenges

- One RPKI-Invalid prefixes will be filtered in **ALL** ROV ASes

Challenges

- One RPKI-Invalid prefixes will be filtered in **ALL** ROV ASes



Challenges

- One RPKI-Invalid prefixes will be filtered in **ALL ROV ASes**

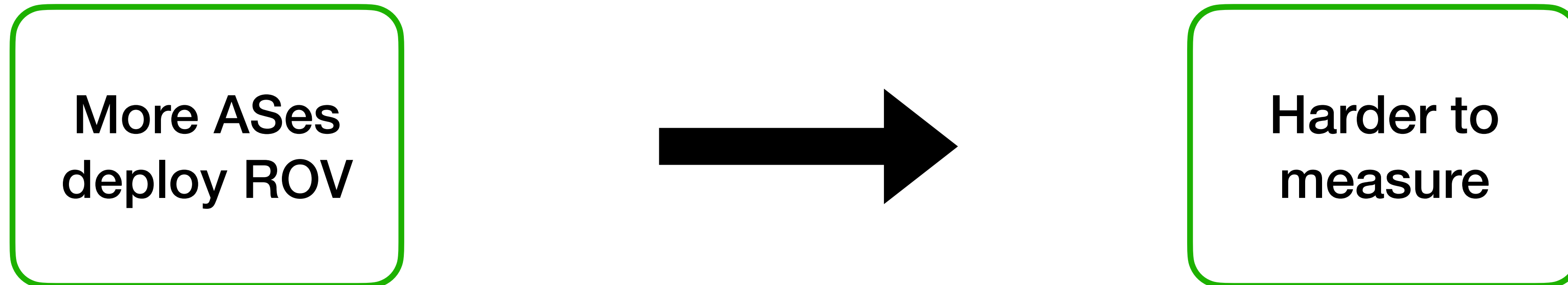
More ASes
deploy ROV



Harder to
measure

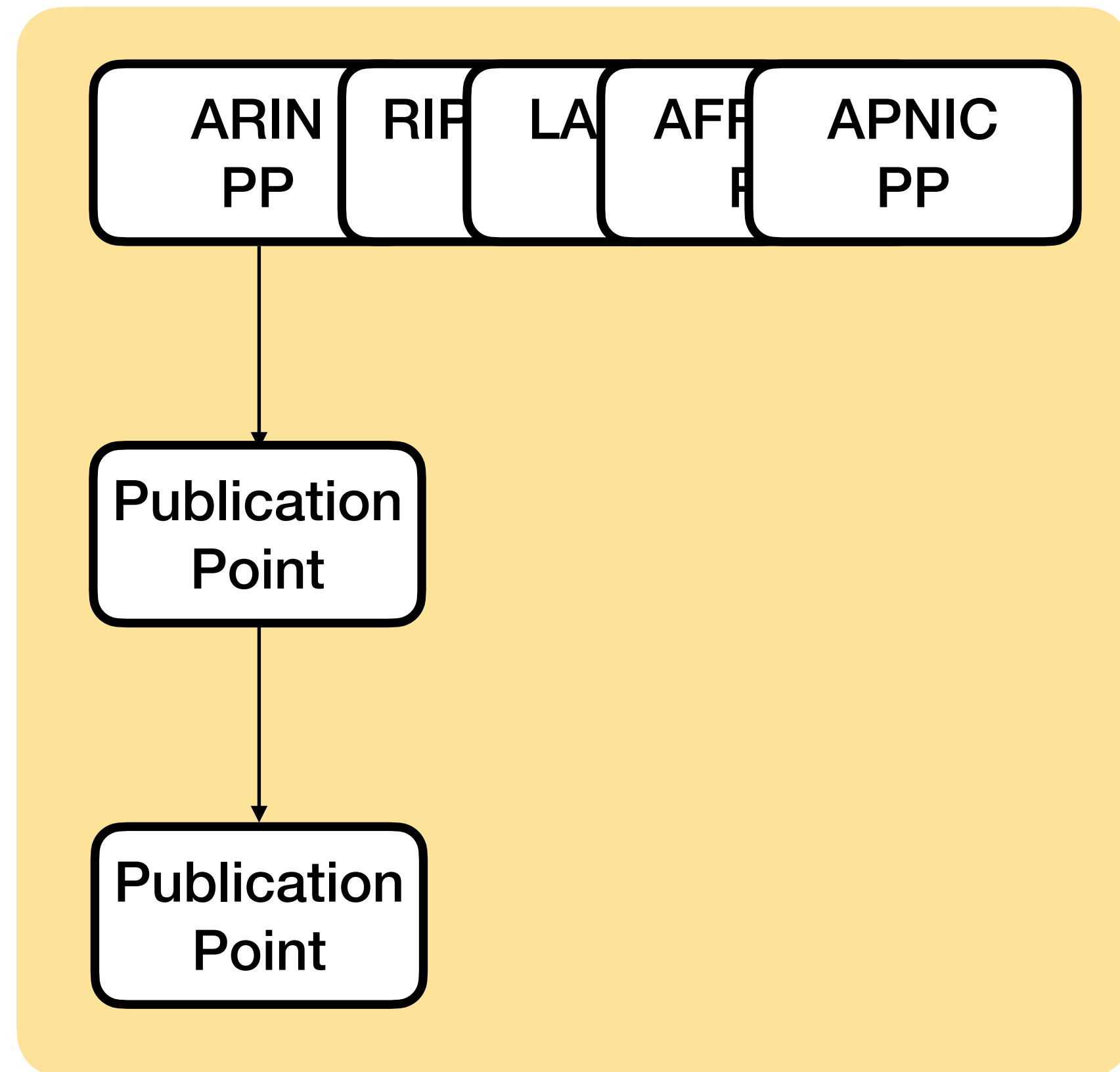
Challenges

- One RPKI-Invalid prefixes will be filtered in **ALL ROV ASes**



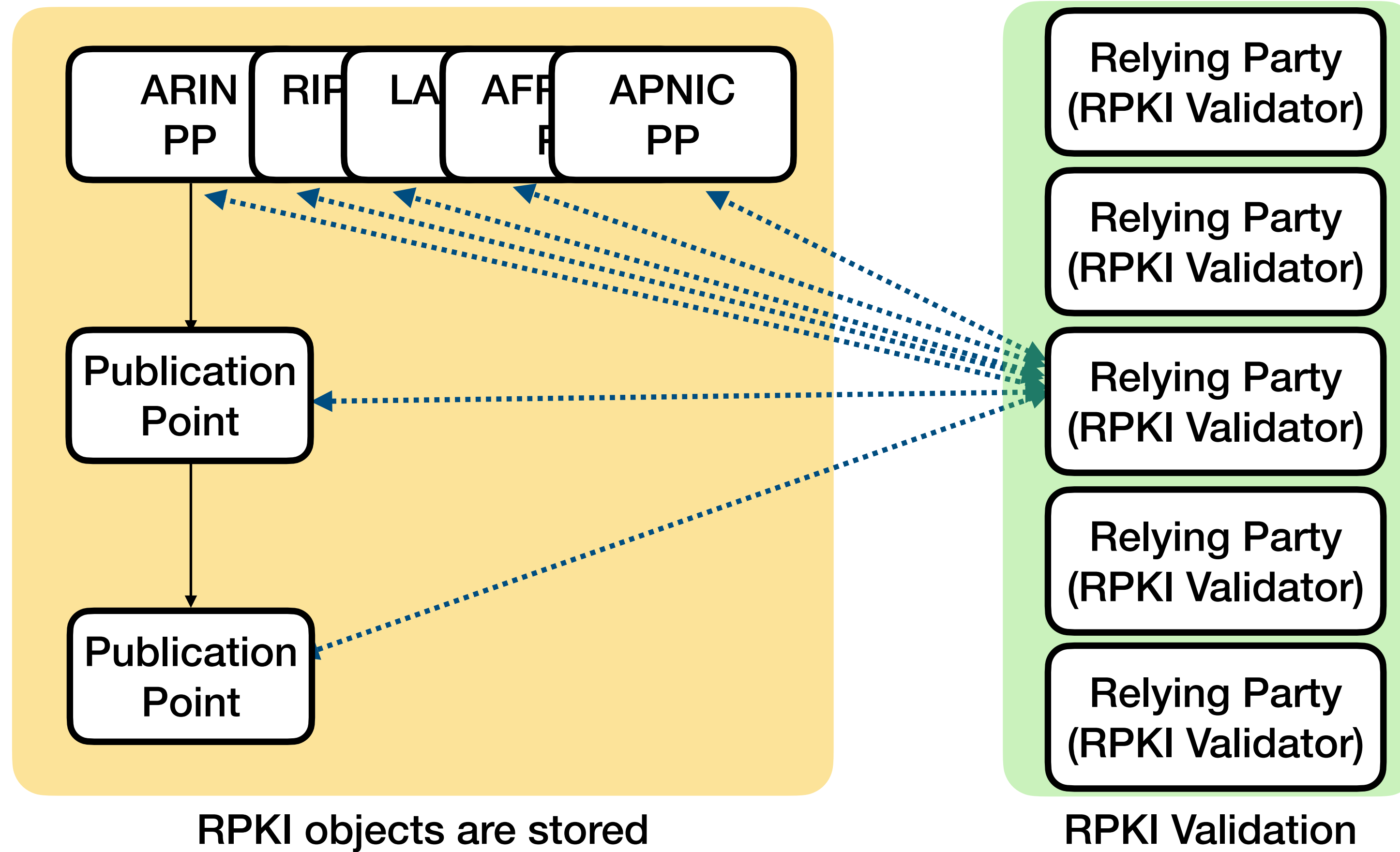
- Can we make our prefix only filter by one or few ROV AS(es)?

ROV Ecosystem

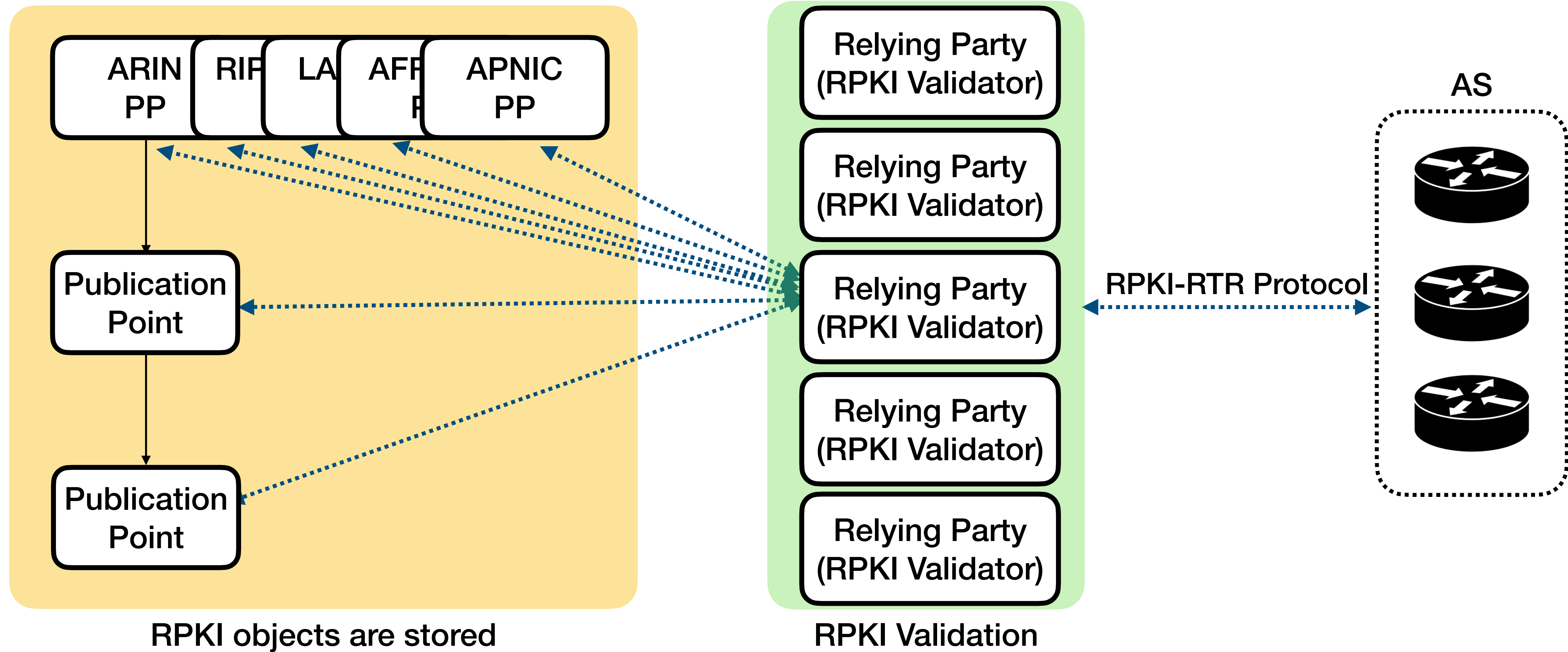


RPKI objects are stored

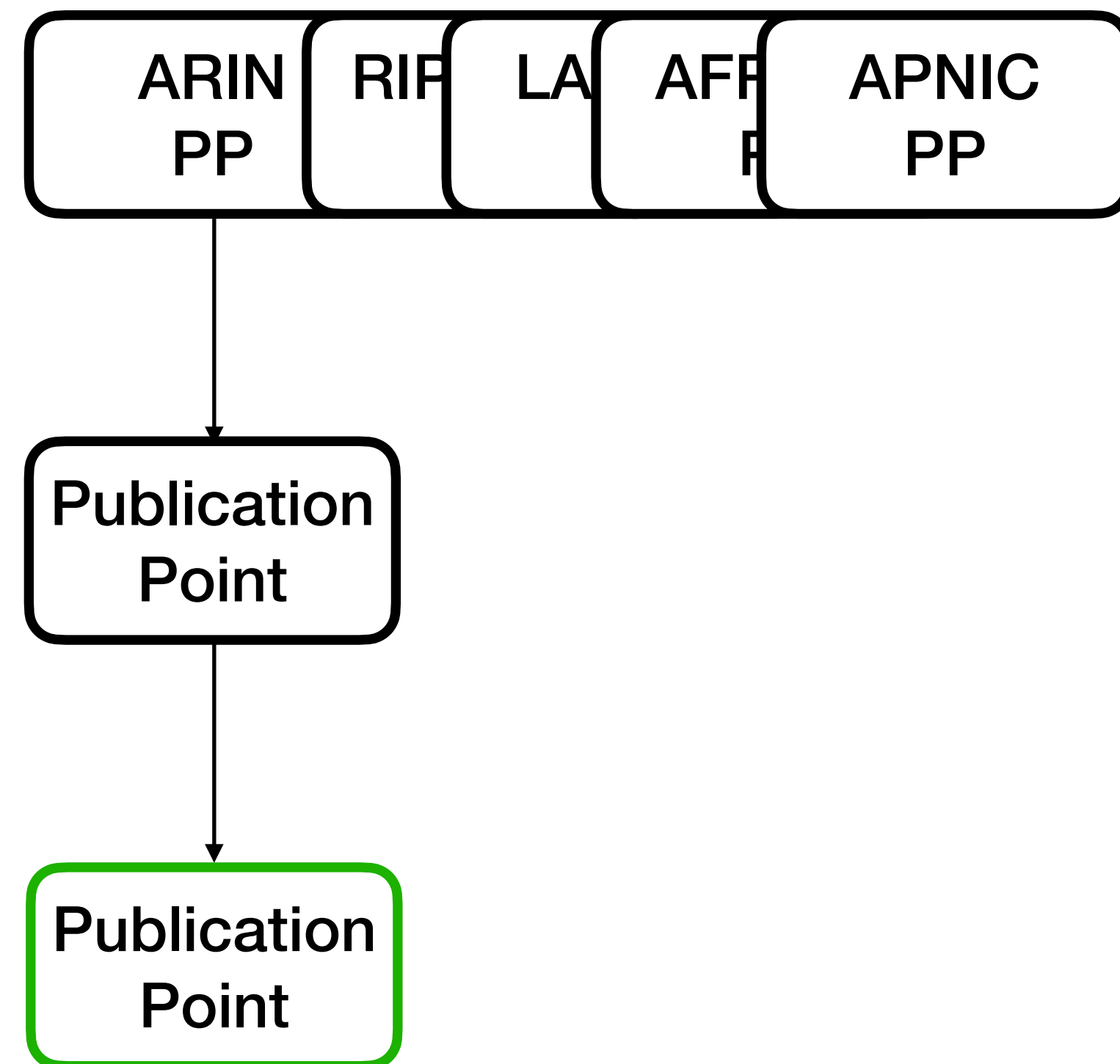
ROV Ecosystem



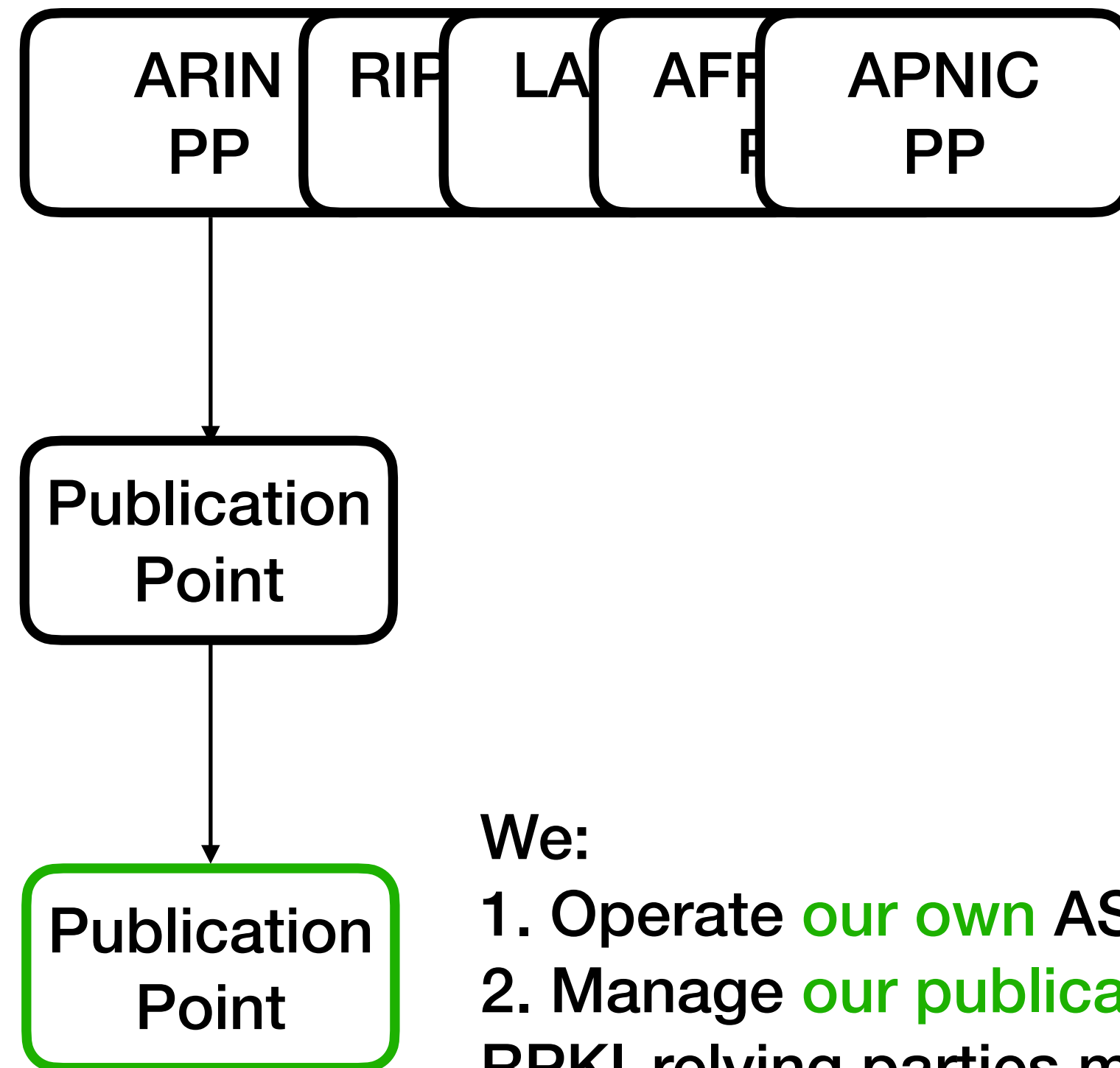
ROV Ecosystem



RScope: Measuring ROV Deployment at Scale



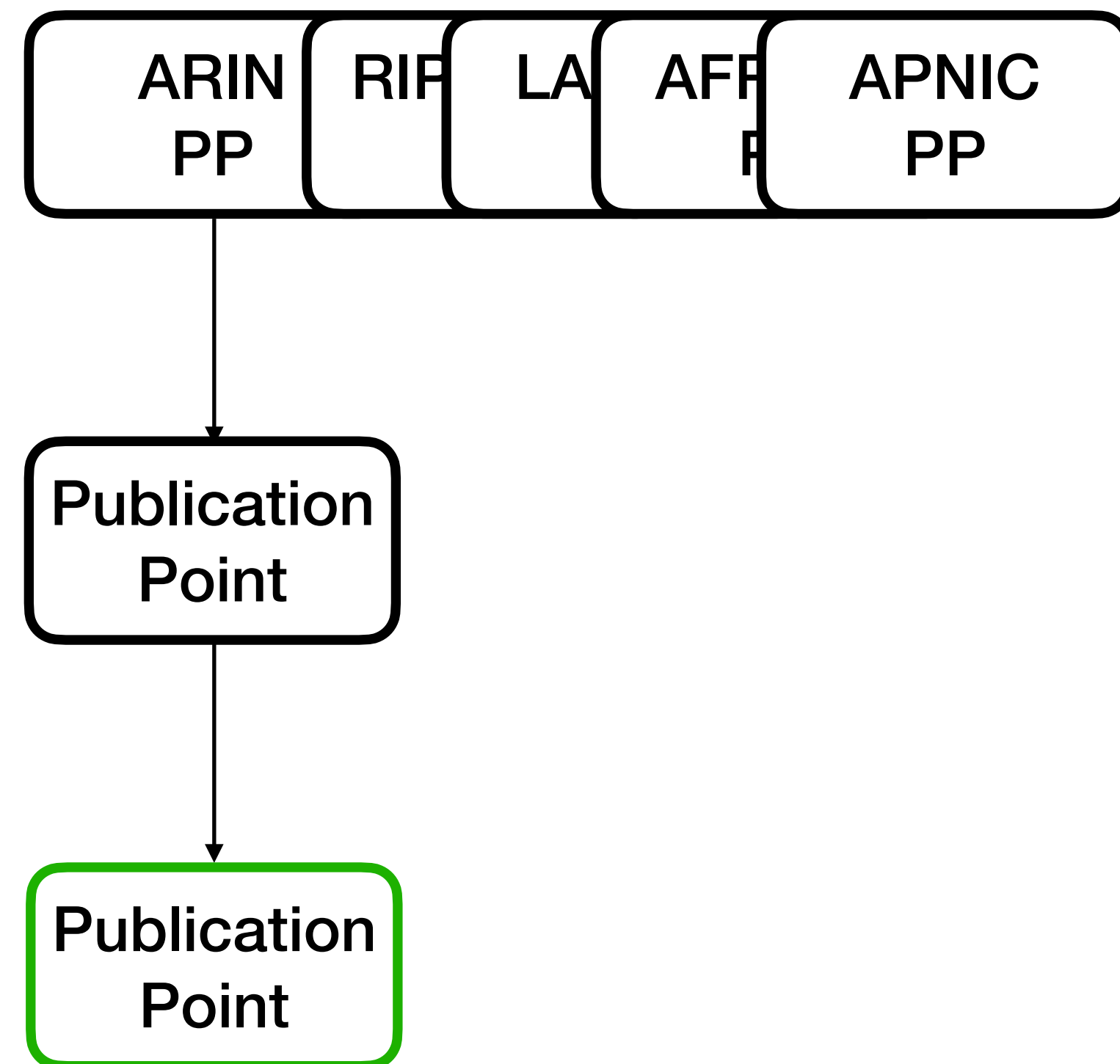
RScope: Measuring ROV Deployment at Scale



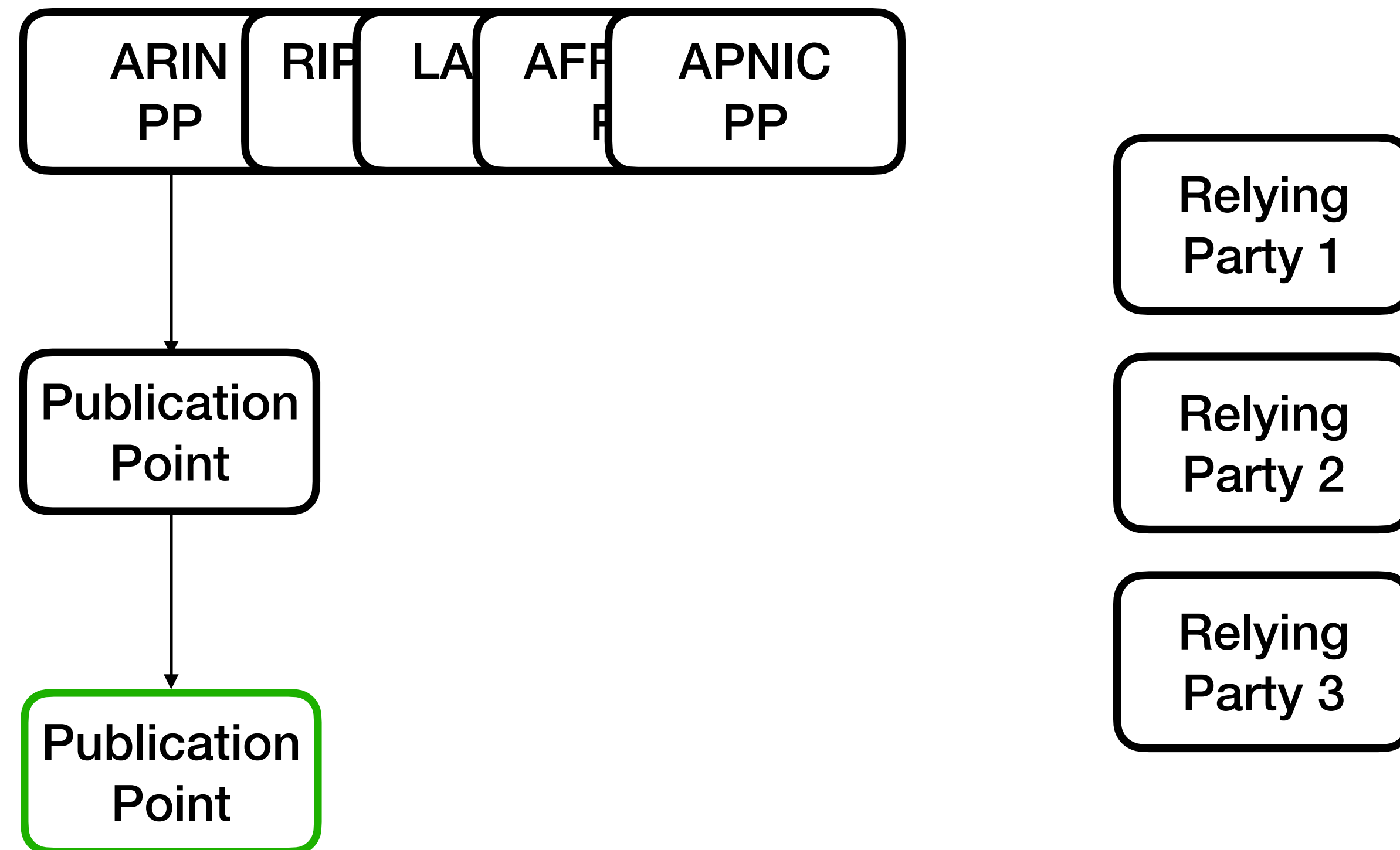
We:

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.

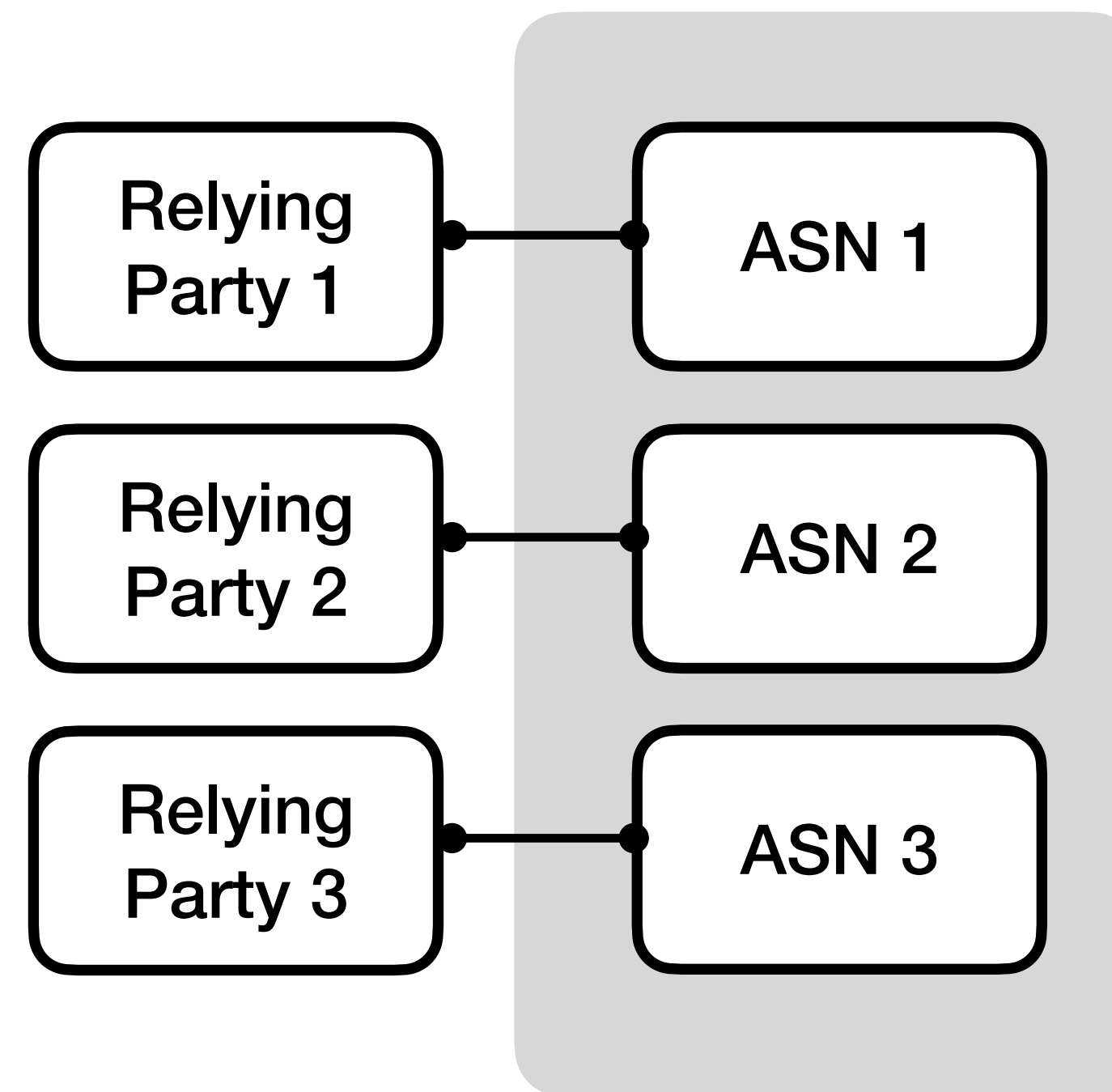
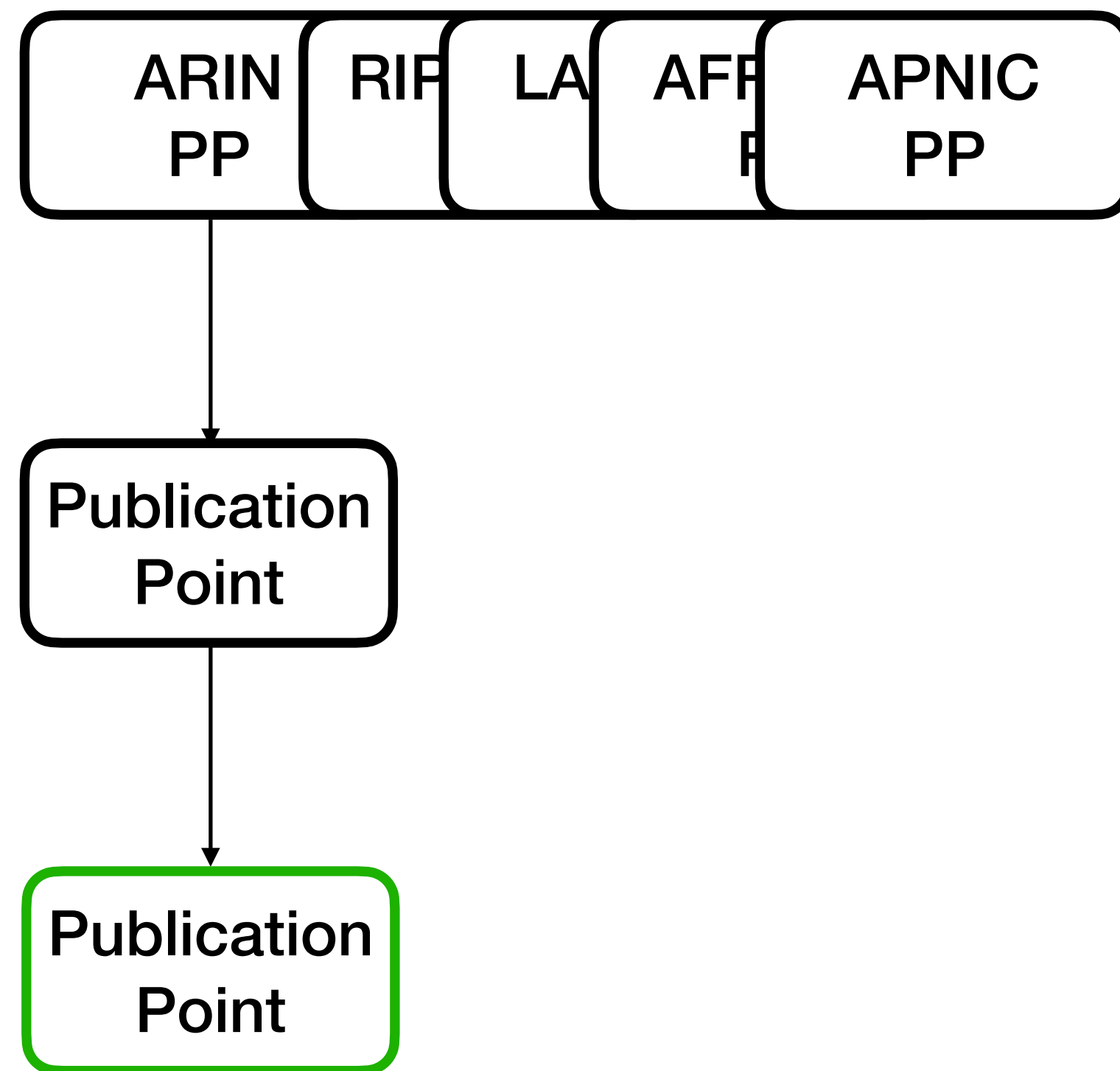
RScope: Measuring ROV Deployment at Scale



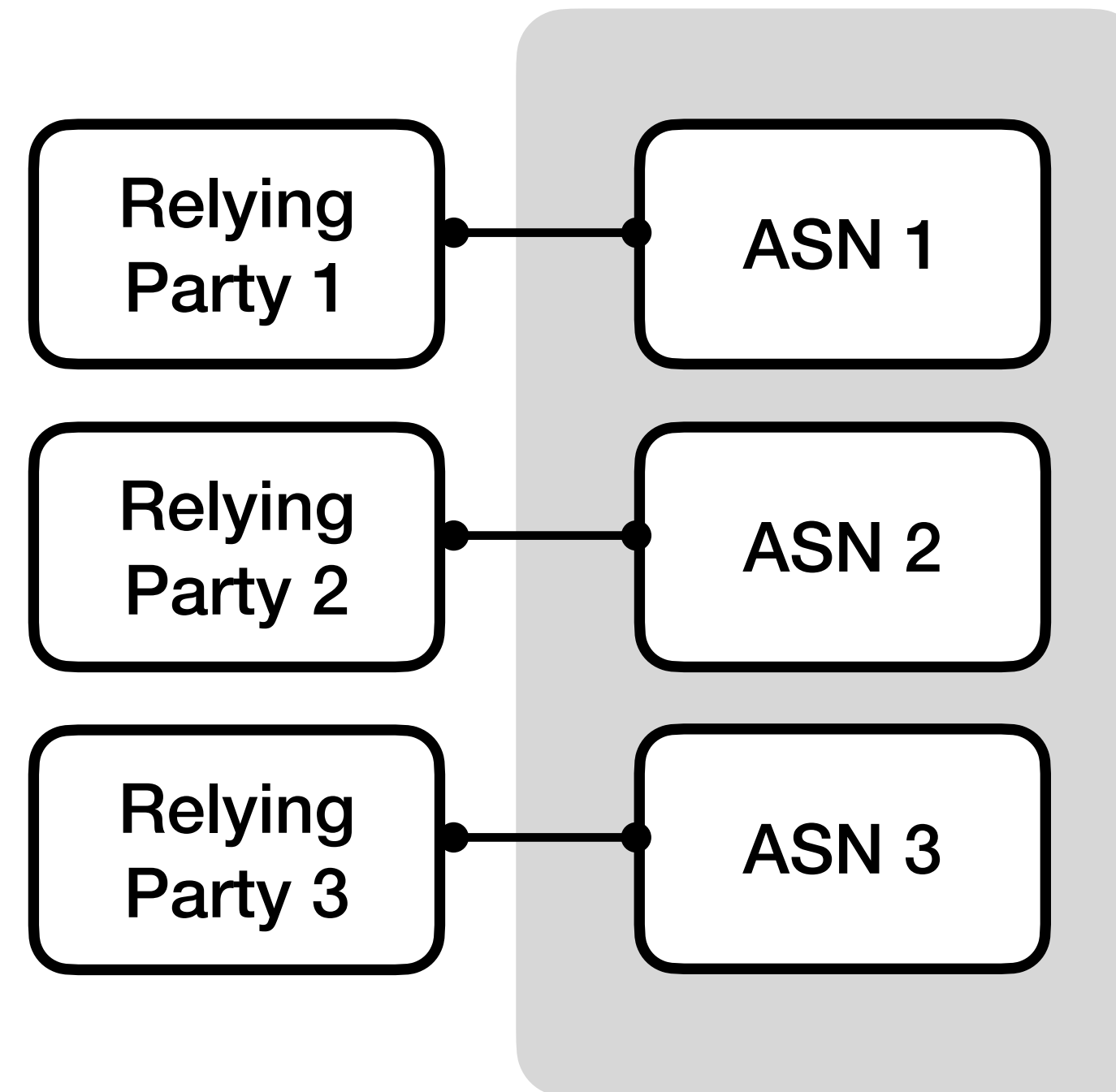
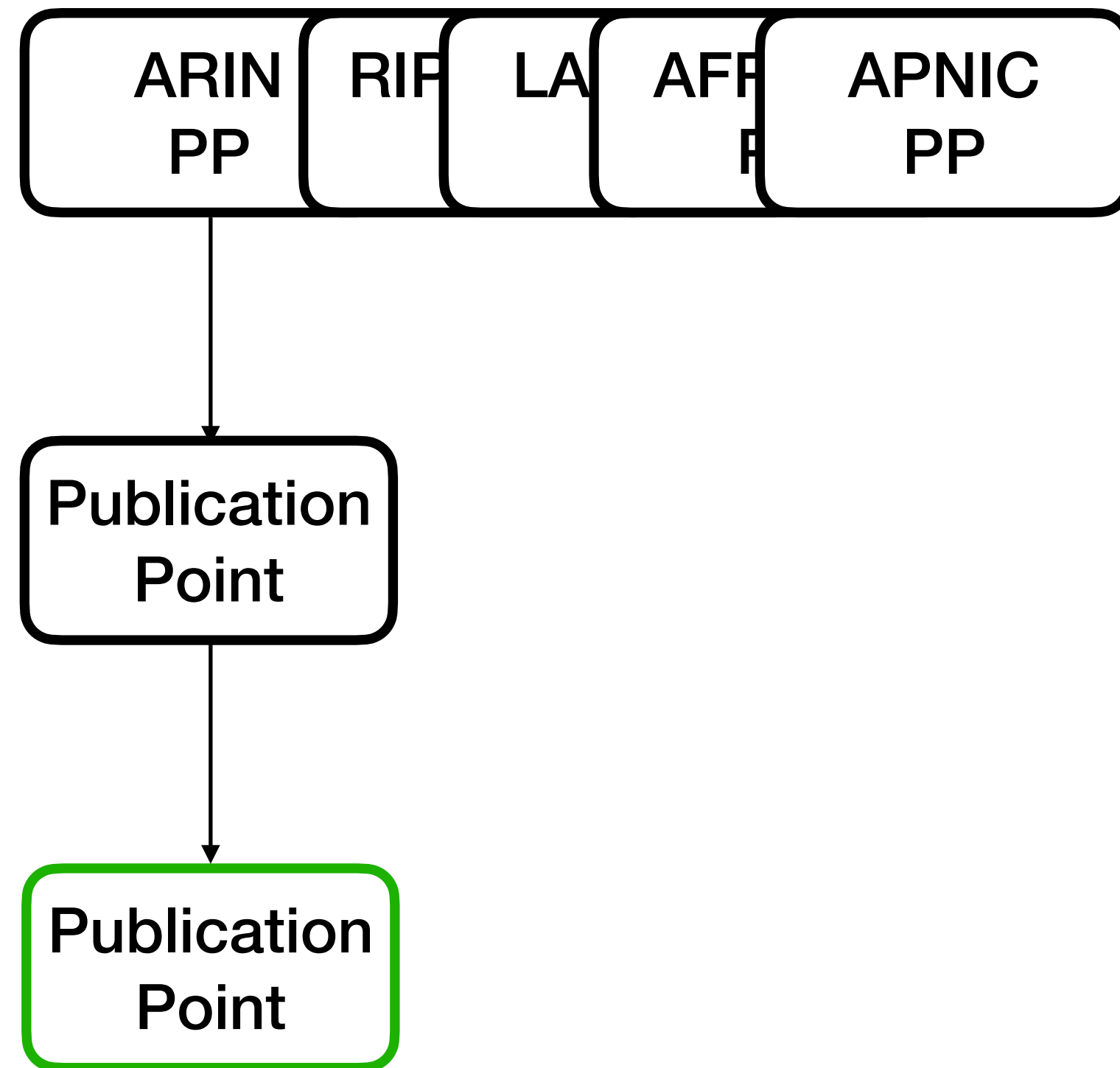
RScope: Measuring ROV Deployment at Scale



RScope: Measuring ROV Deployment at Scale

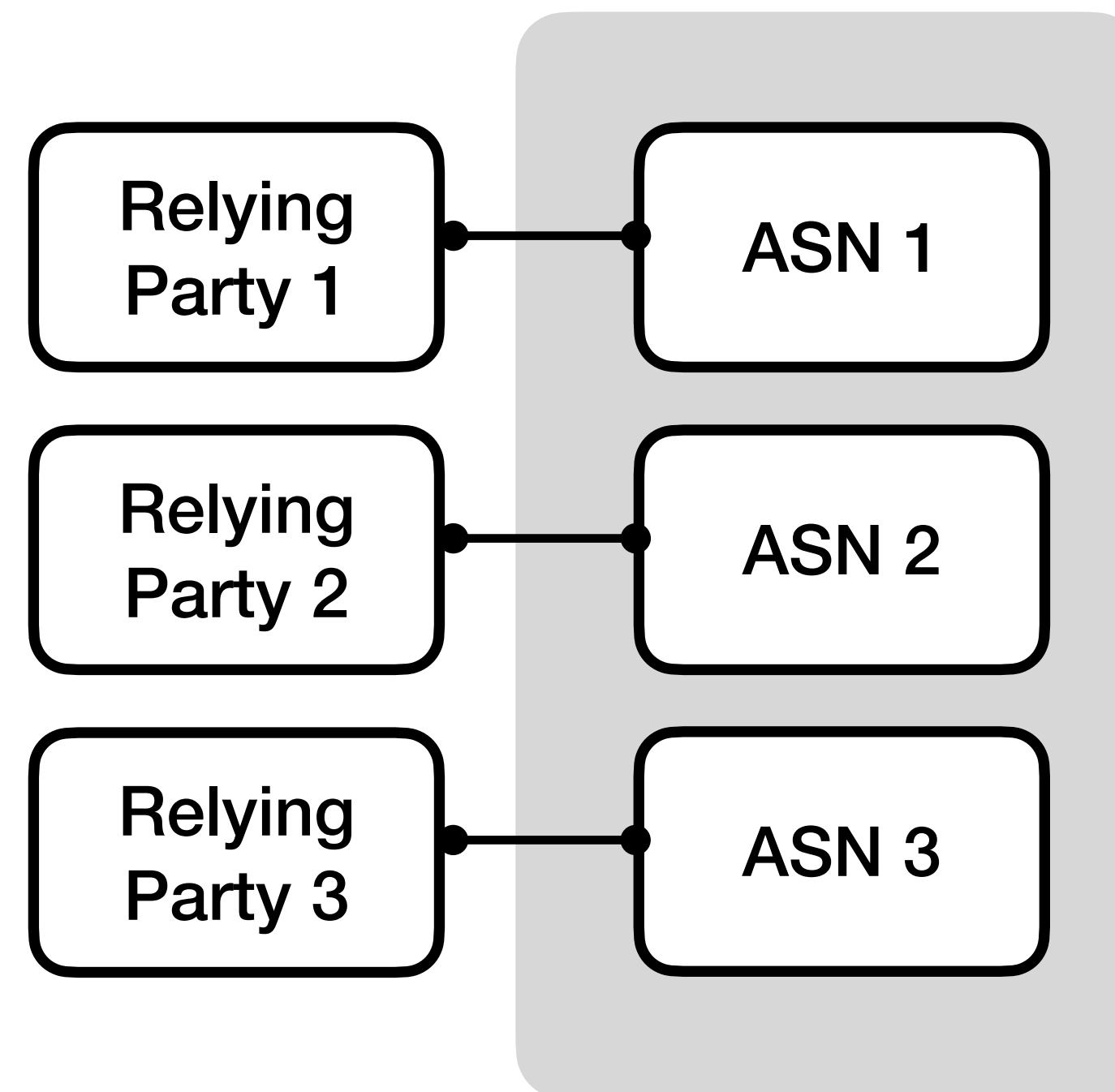
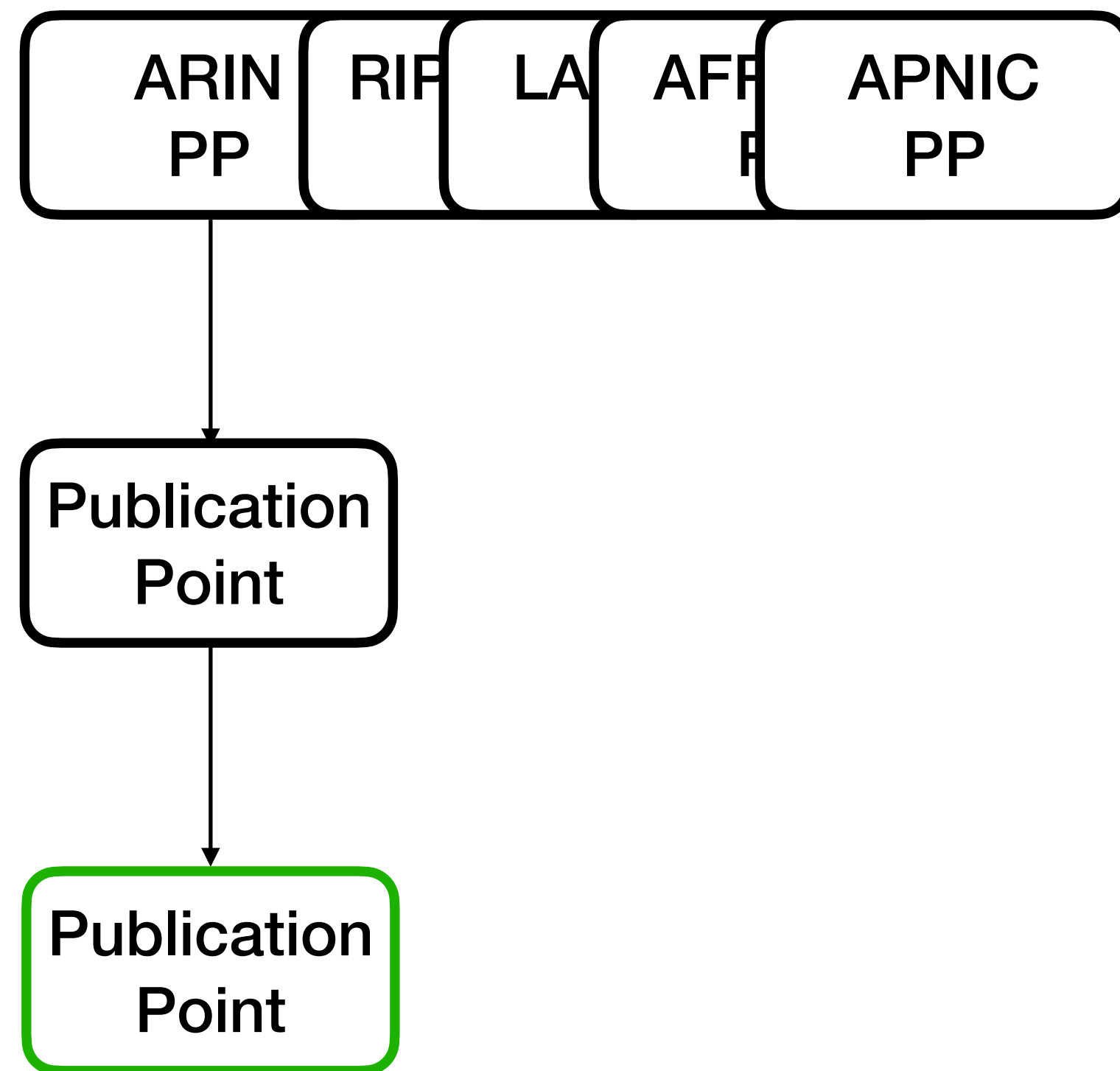


RScope: Measuring ROV Deployment at Scale



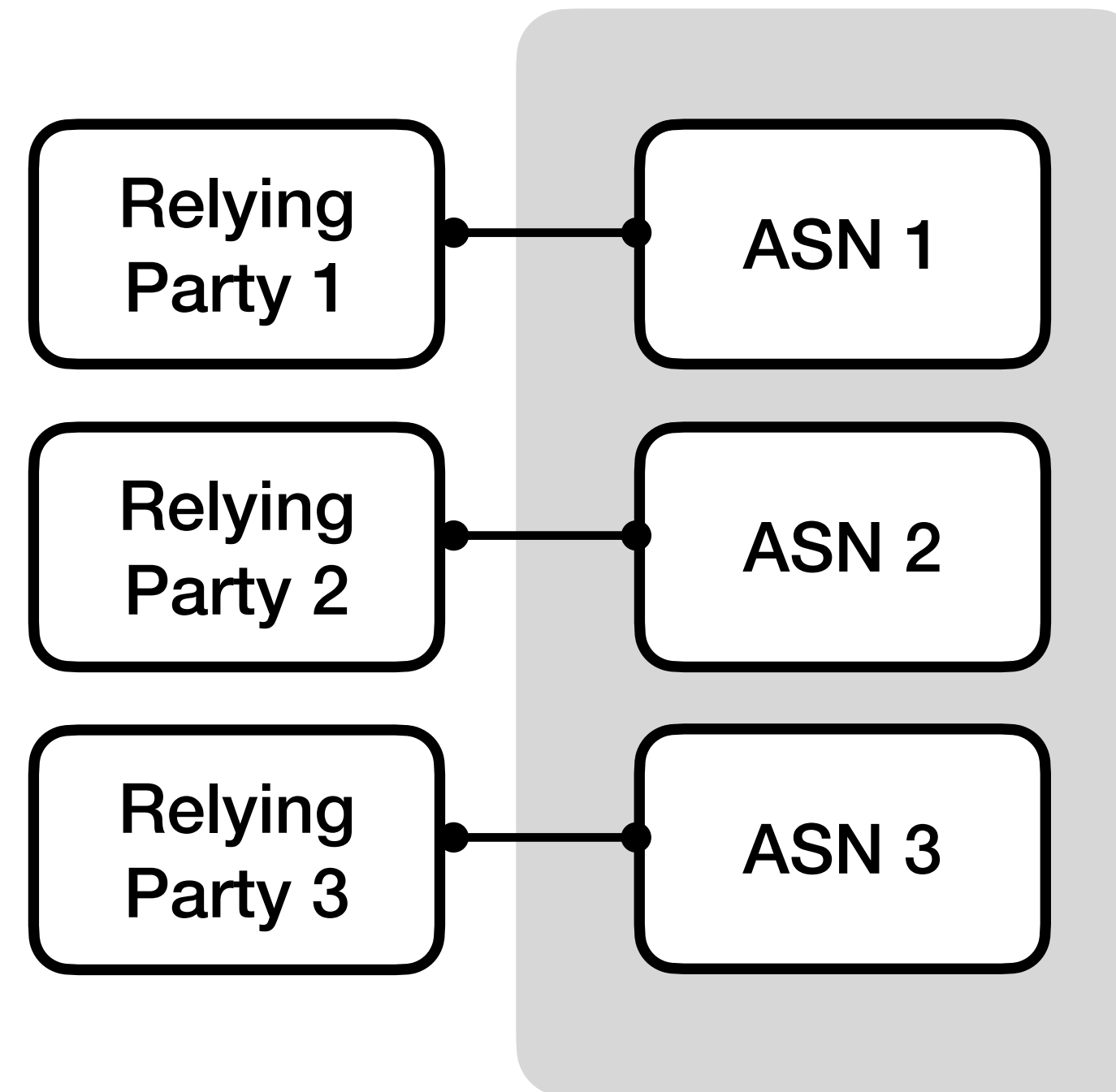
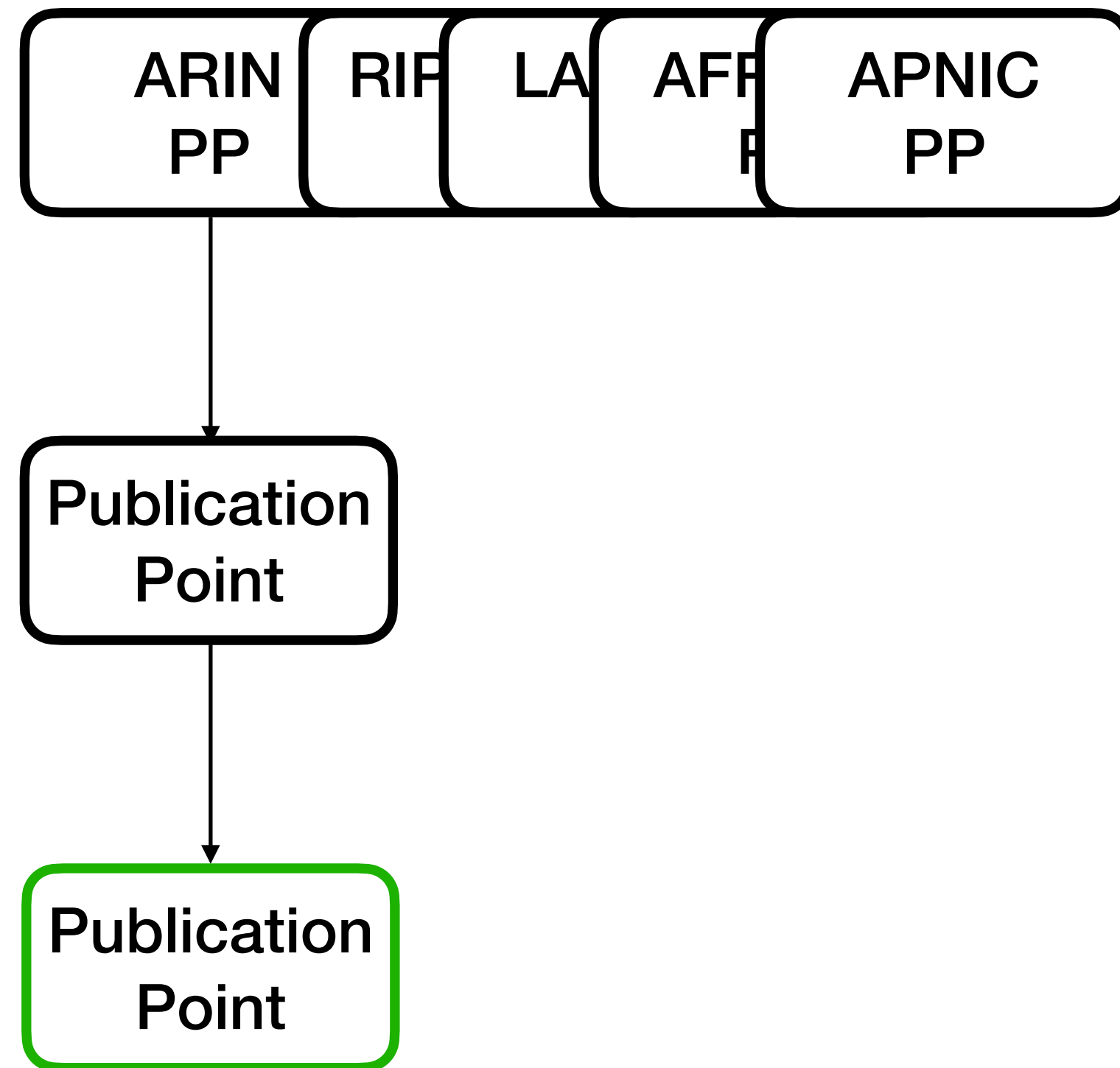
(1) We run our own ASN and IP prefixes
ASN 777 and 1.2.0.0/24

RScope: Measuring ROV Deployment at Scale



- (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

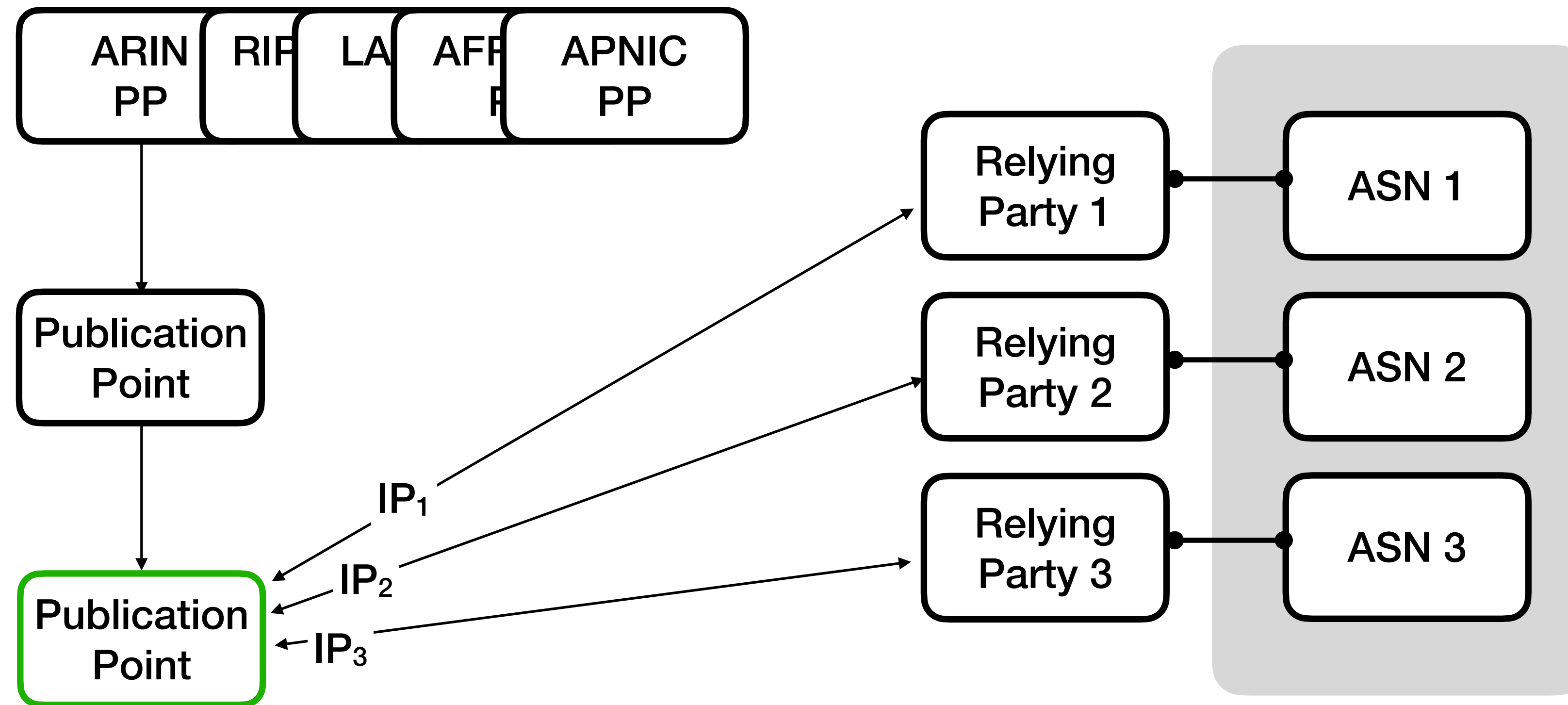
RScope: Measuring ROV Deployment at Scale



- (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**.

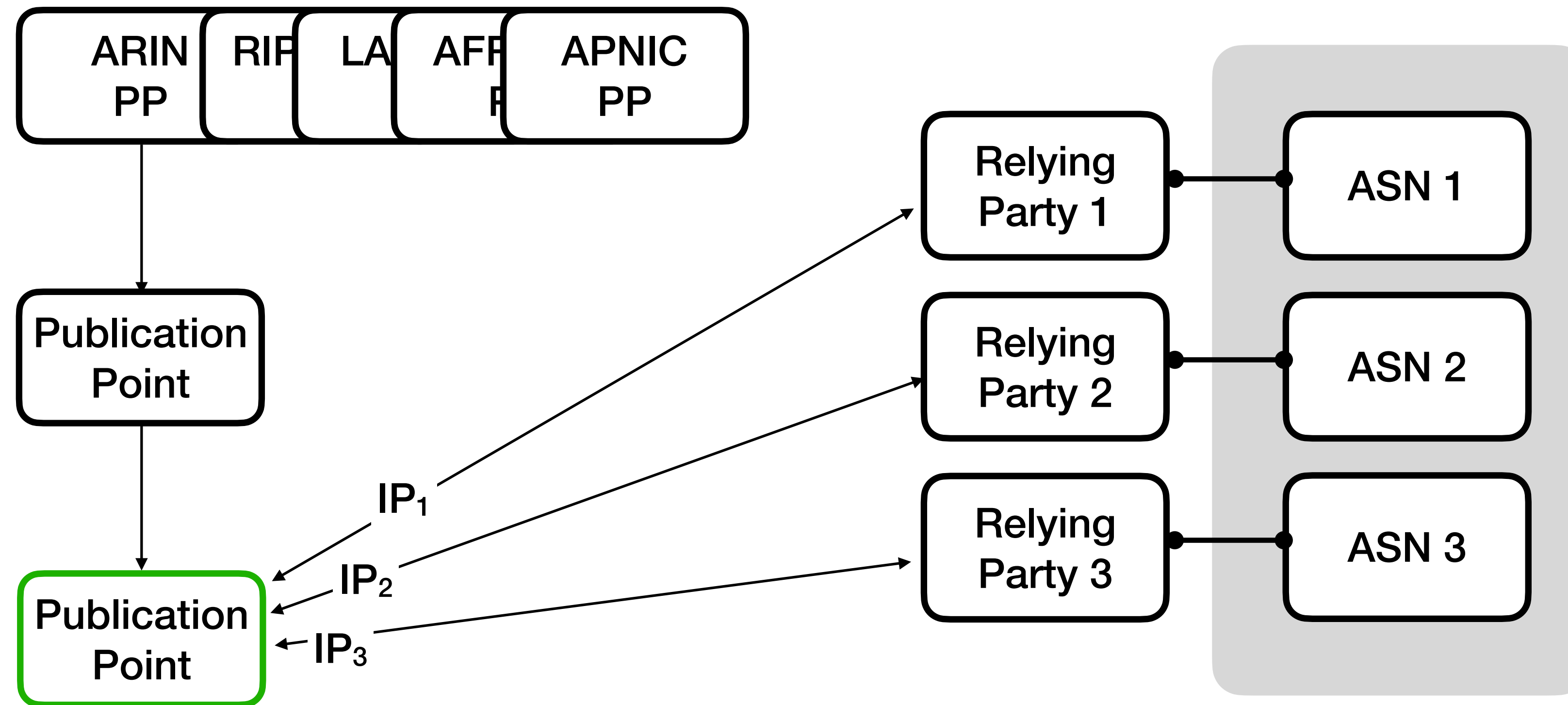
RScope: Measuring ROV Deployment at Scale



- (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.

RScope: Measuring ROV Deployment at Scale

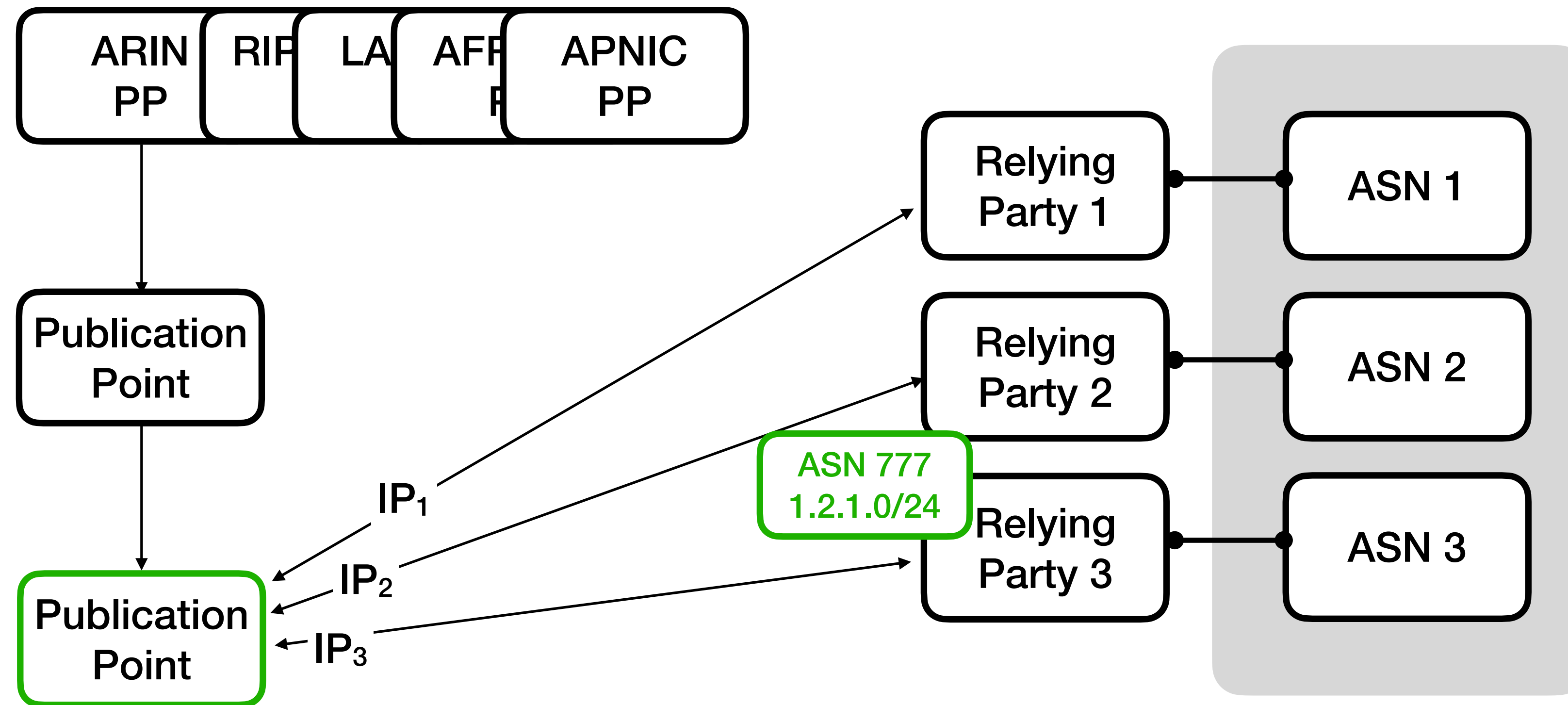


- (1) We run our own ASN and IP prefixes
ASN 777 and 1.2.0.0/24
- (2) We announce 1.2.0.0/24 from ASN 777

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.

RScope: Measuring ROV Deployment at Scale

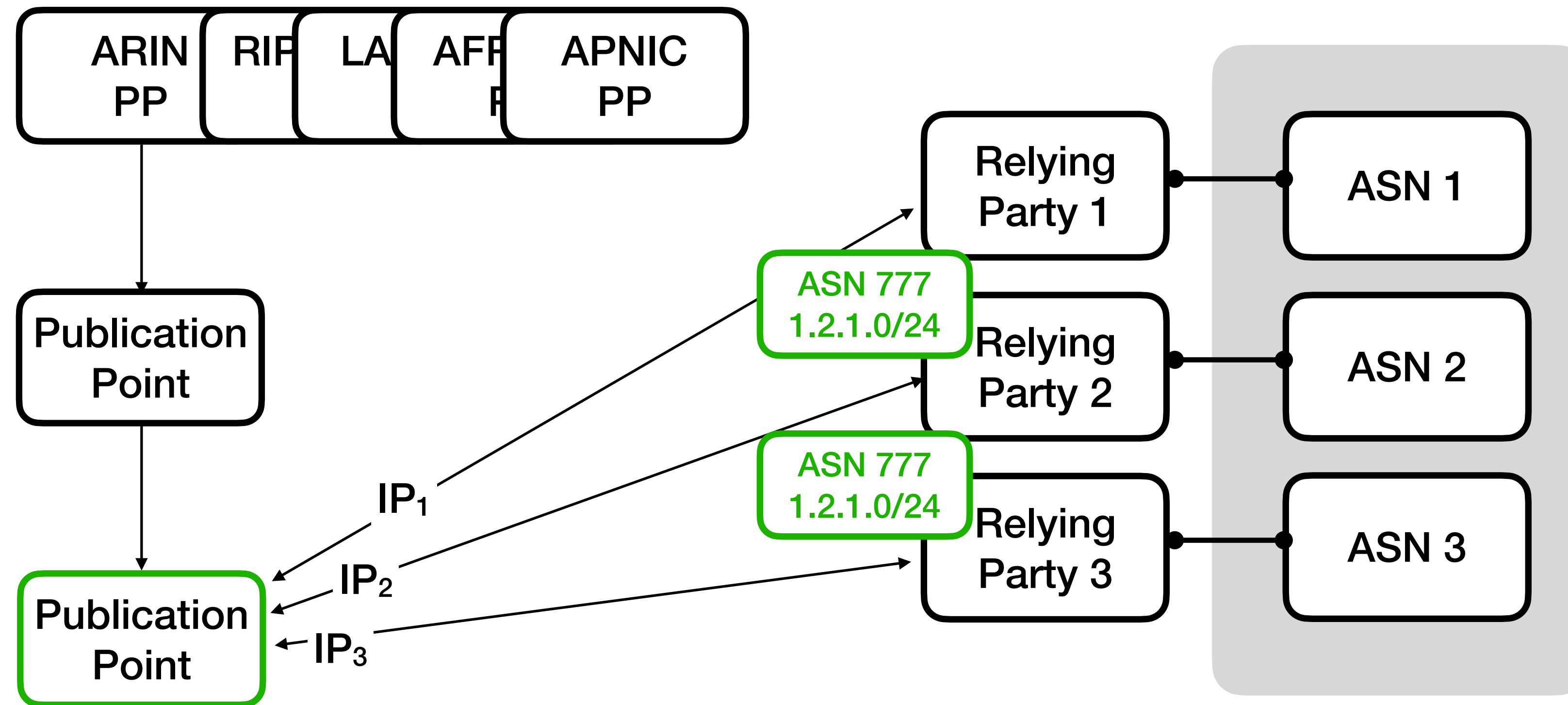


- (1) We run our own ASN and IP prefixes
ASN 777 and 1.2.0.0/24
- (2) We announce 1.2.0.0/24 from ASN 777

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

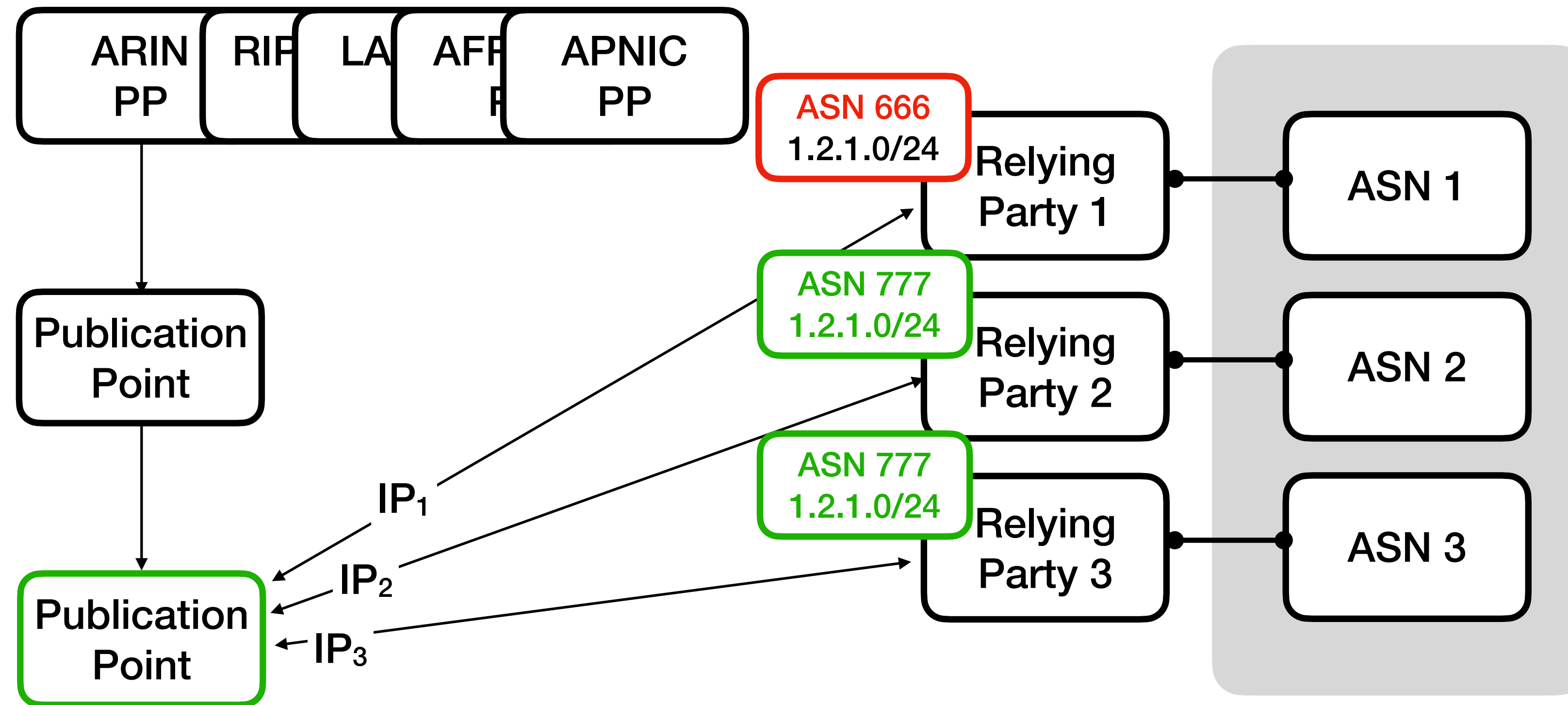
4. The test ROA is exclusively returned to RP1.

RScope: Measuring ROV Deployment at Scale



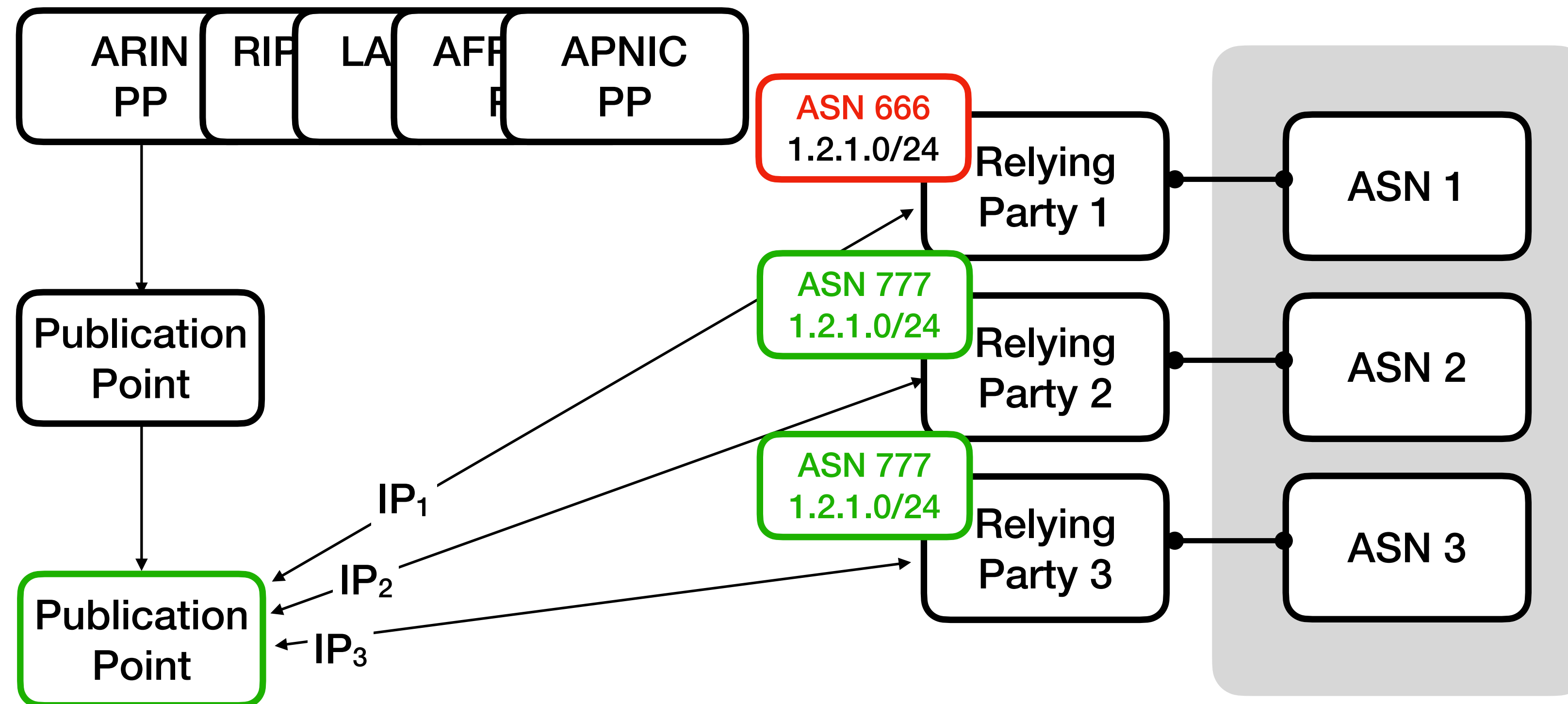
- (1) We run our own ASN and IP prefixes **ASN 777** and **1.2.0.0/24**
- (2) We announce 1.2.0.0/24 from ASN 777
3. We create two distinct ROAs for /24:
 - (a) A test ROA associated with **ASN 666**.
 - (b) A control ROA associated with **ASN 777**.
4. The test ROA is exclusively returned to RP1.

RScope: Measuring ROV Deployment at Scale



- (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.

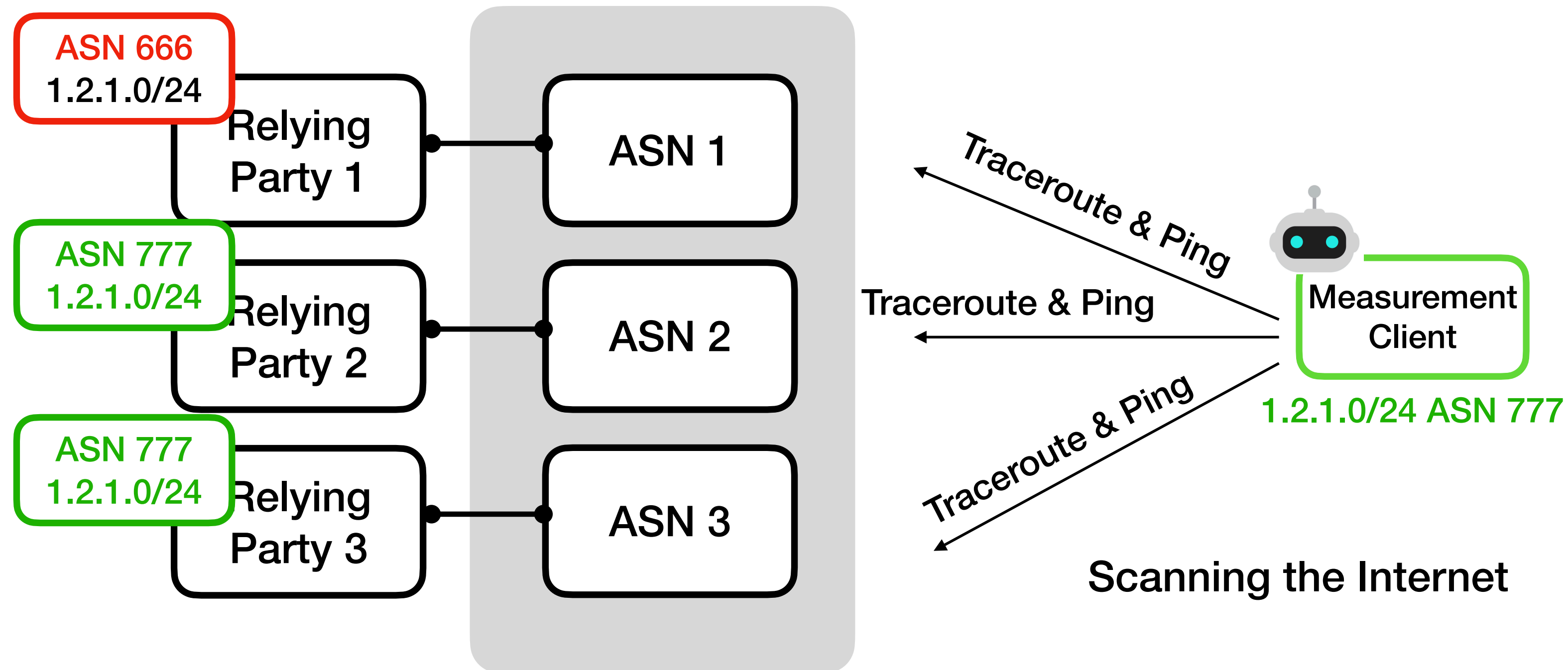
RScope: Measuring ROV Deployment at Scale



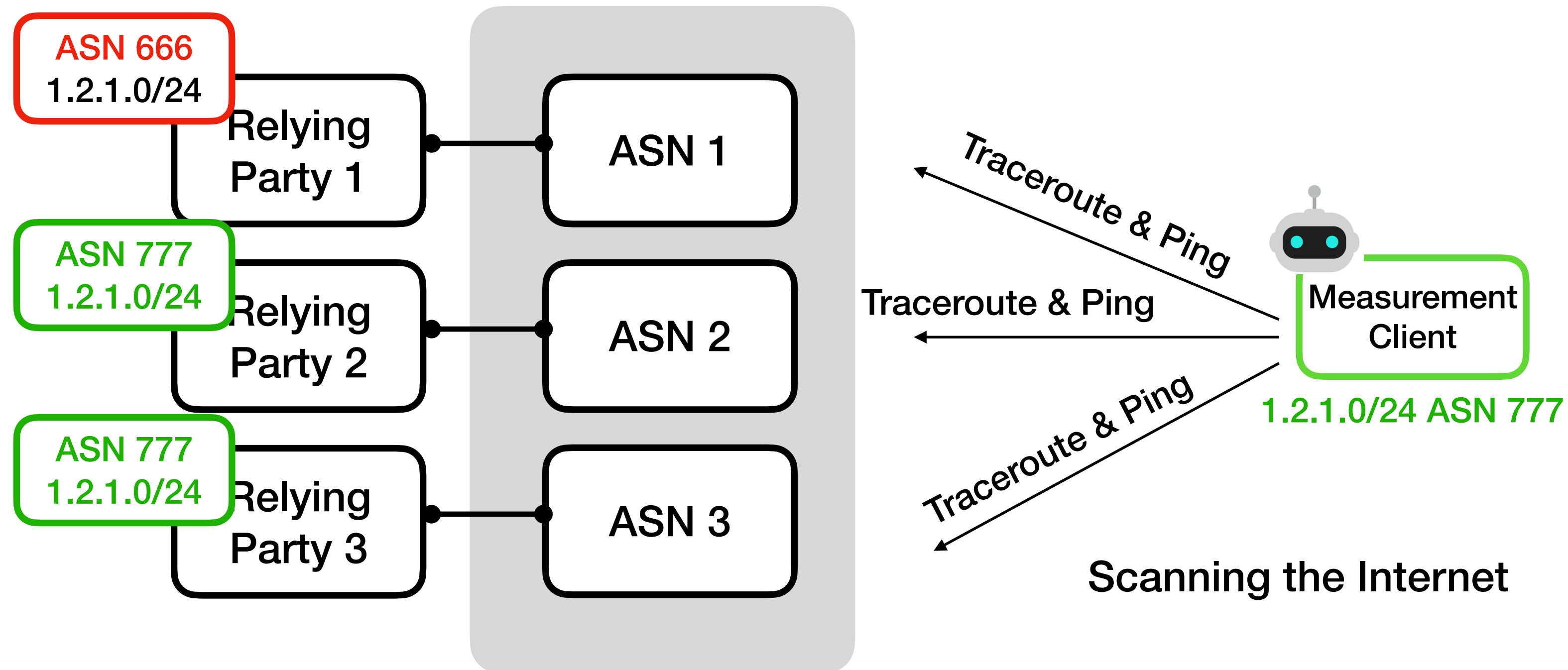
Operating publication points alone do not reveal which ASes are using specific RPs.

- (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.

RScope: Measuring ROV Deployment at Scale



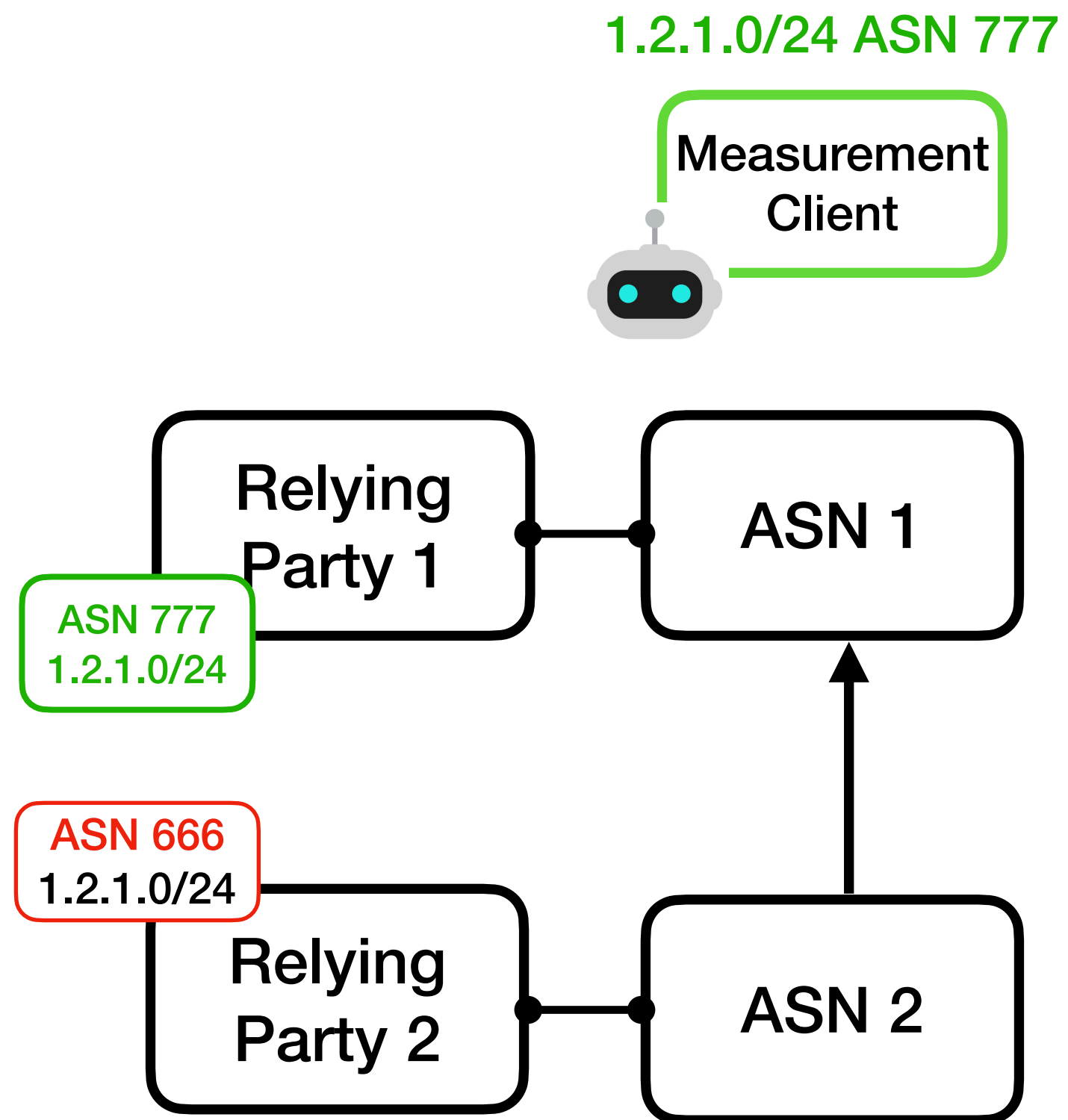
RScope: Measuring ROV Deployment at Scale



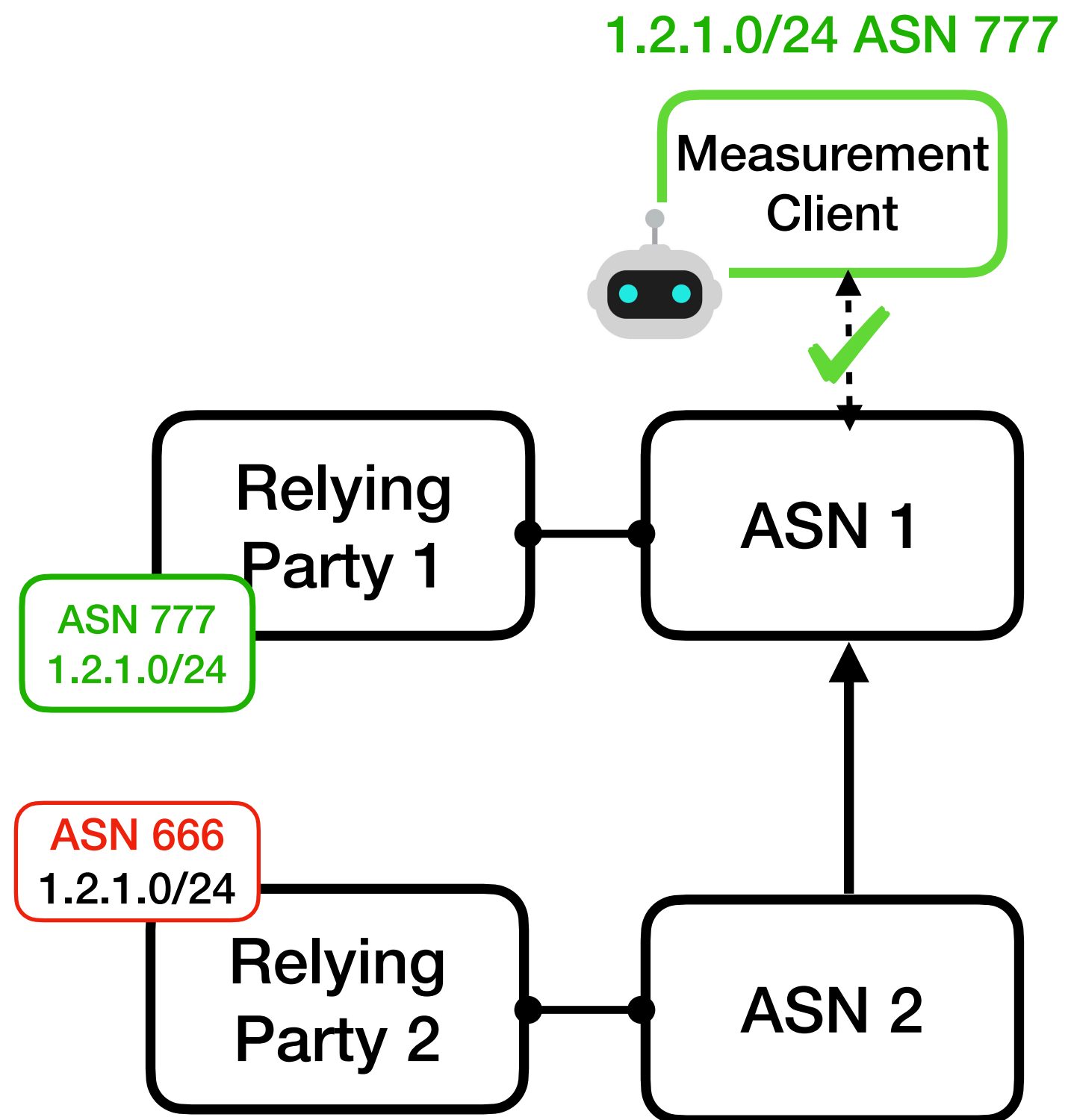
If ASN1 was previously able to reach (and respond) to our network but cannot after the introduction of a test-ROA, it suggests:

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

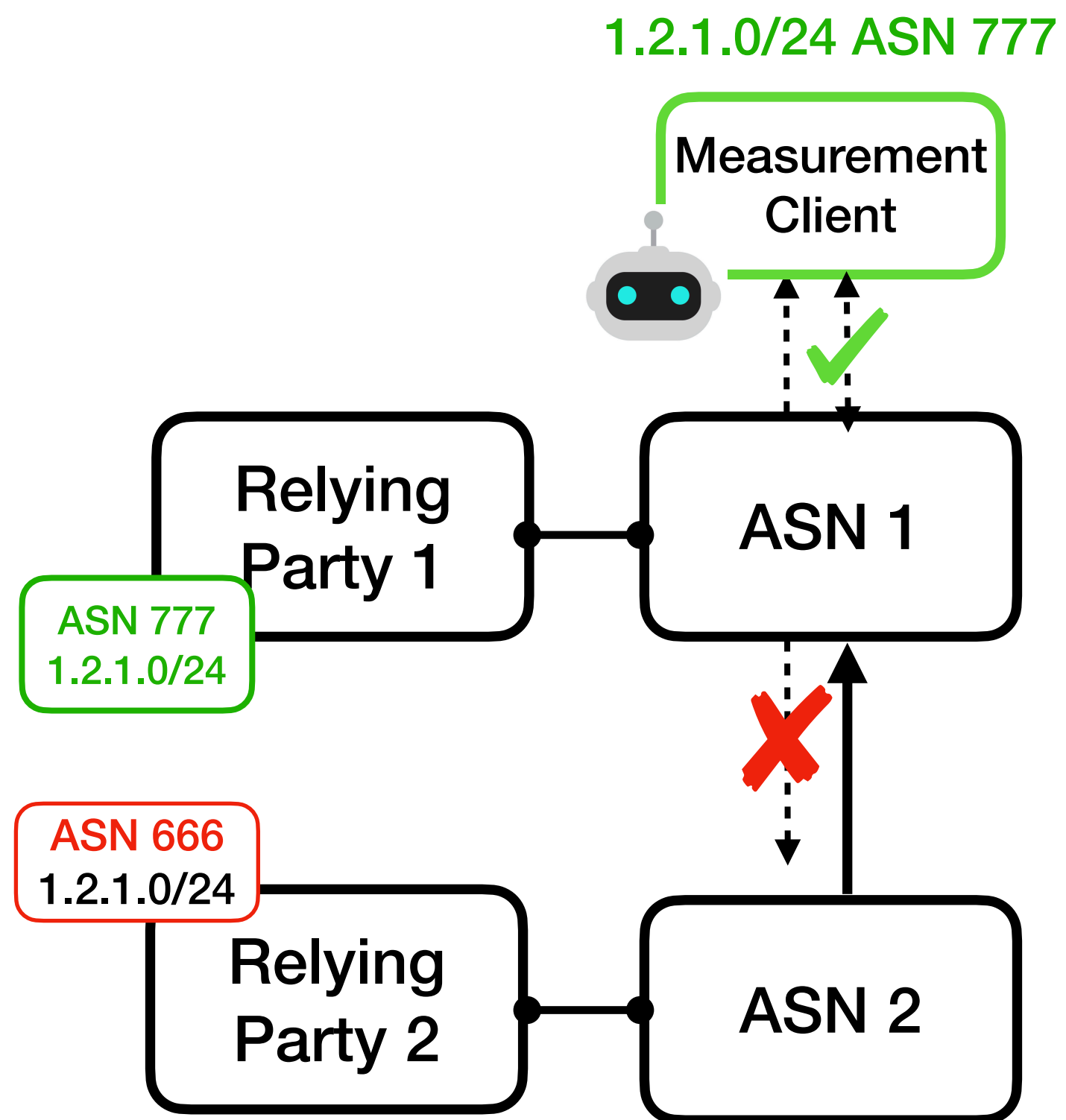
Challenge: Distinguishing Local vs. Upstream Filtering in Single Upstream



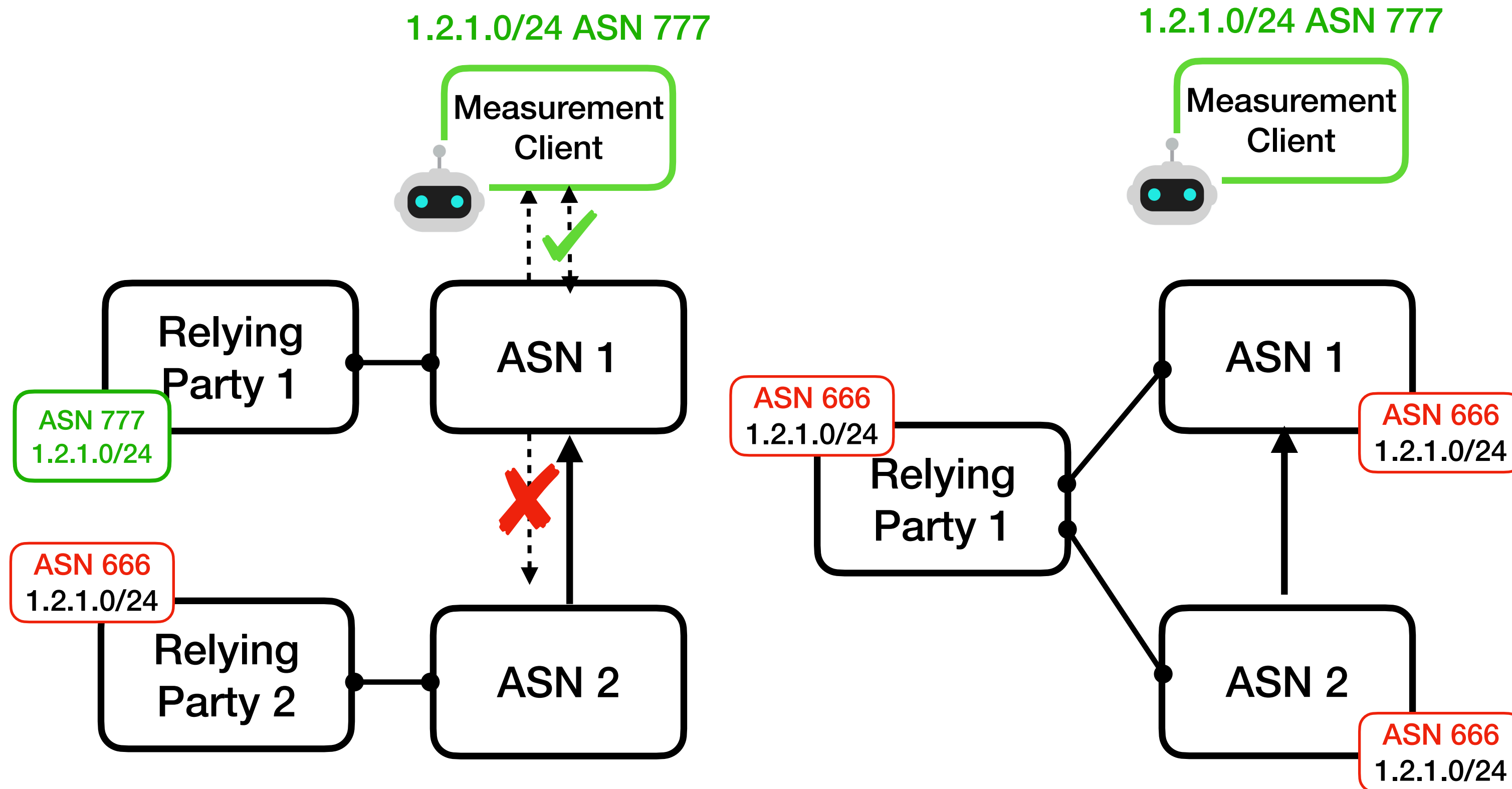
Challenge: Distinguishing Local vs. Upstream Filtering in Single Upstream



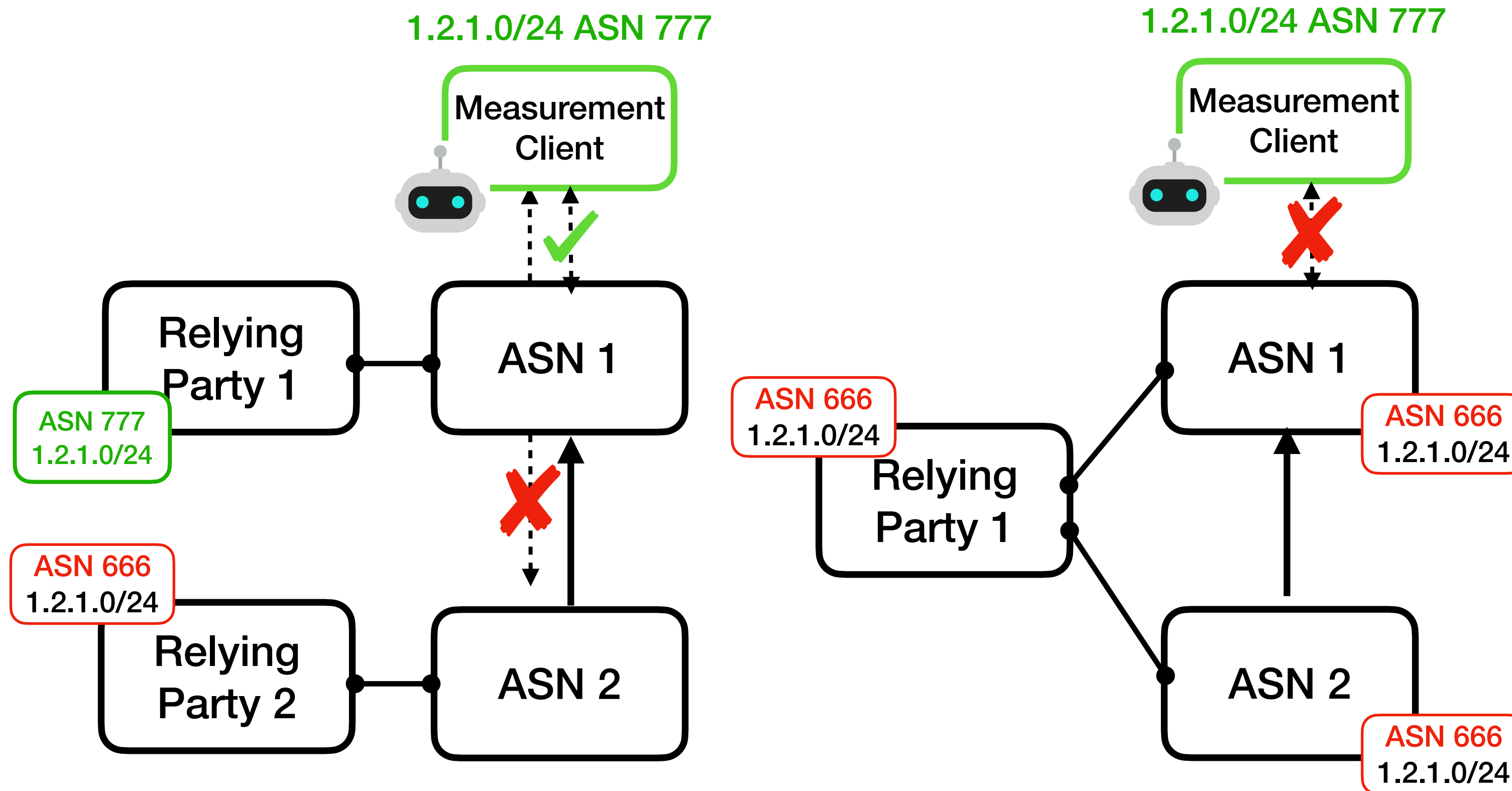
Challenge: Distinguishing Local vs. Upstream Filtering in Single Upstream



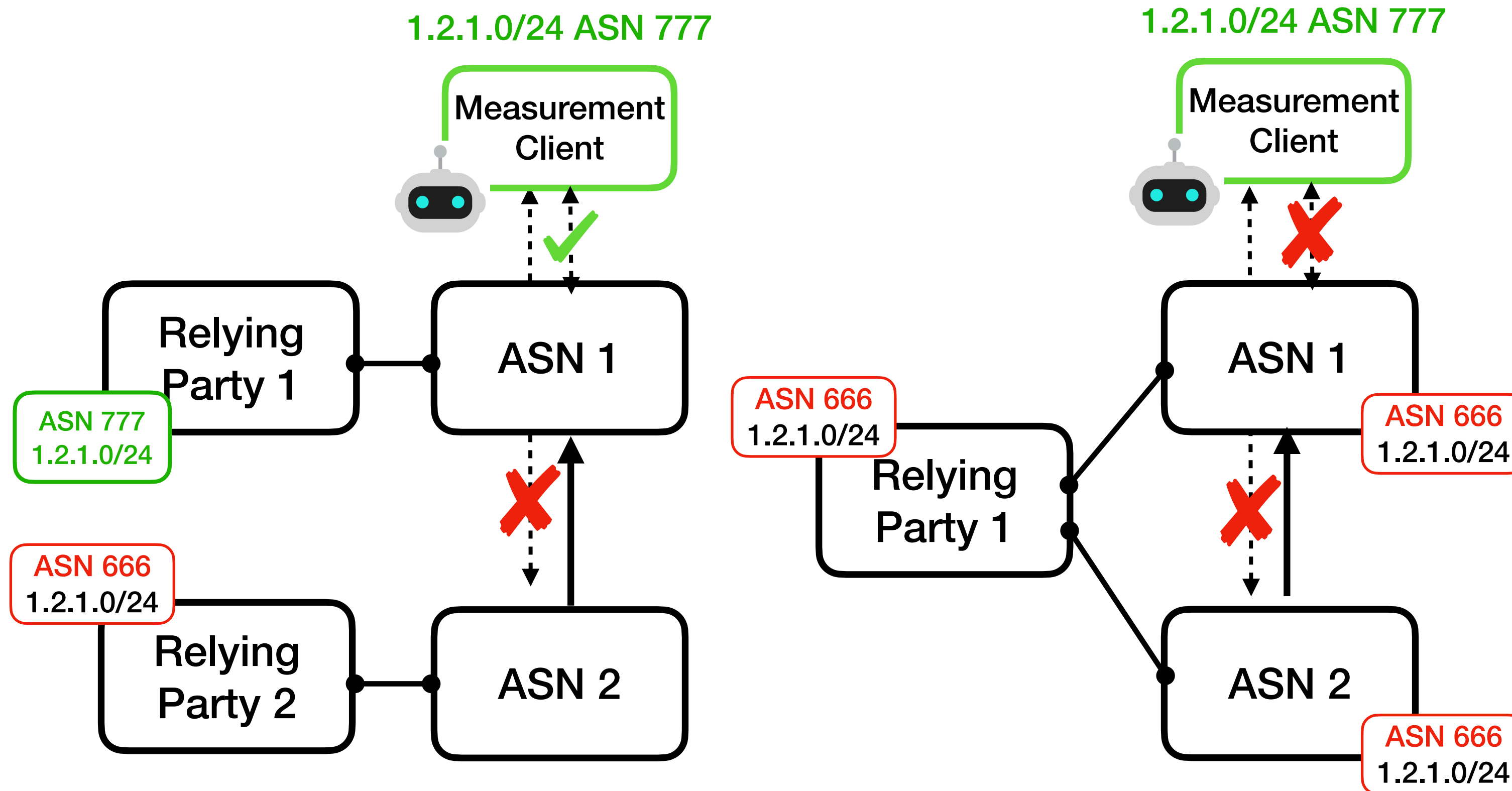
Challenge: Distinguishing Local vs. Upstream Filtering in Single Upstream



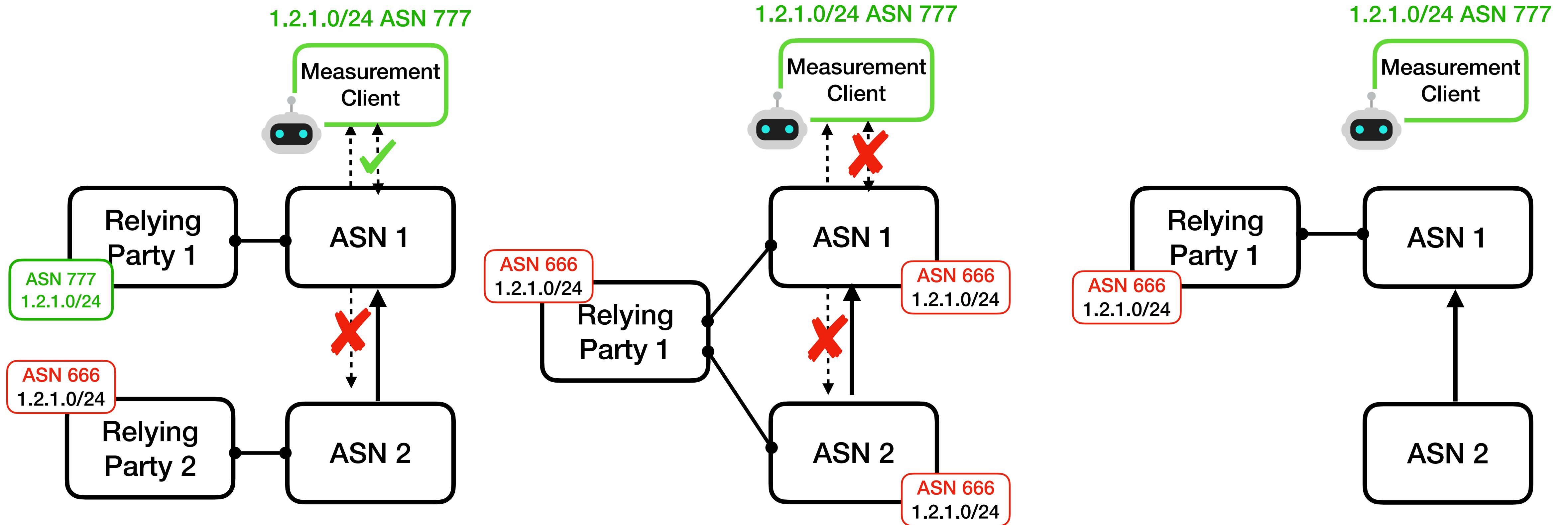
Challenge: Distinguishing Local vs. Upstream Filtering in Single Upstream



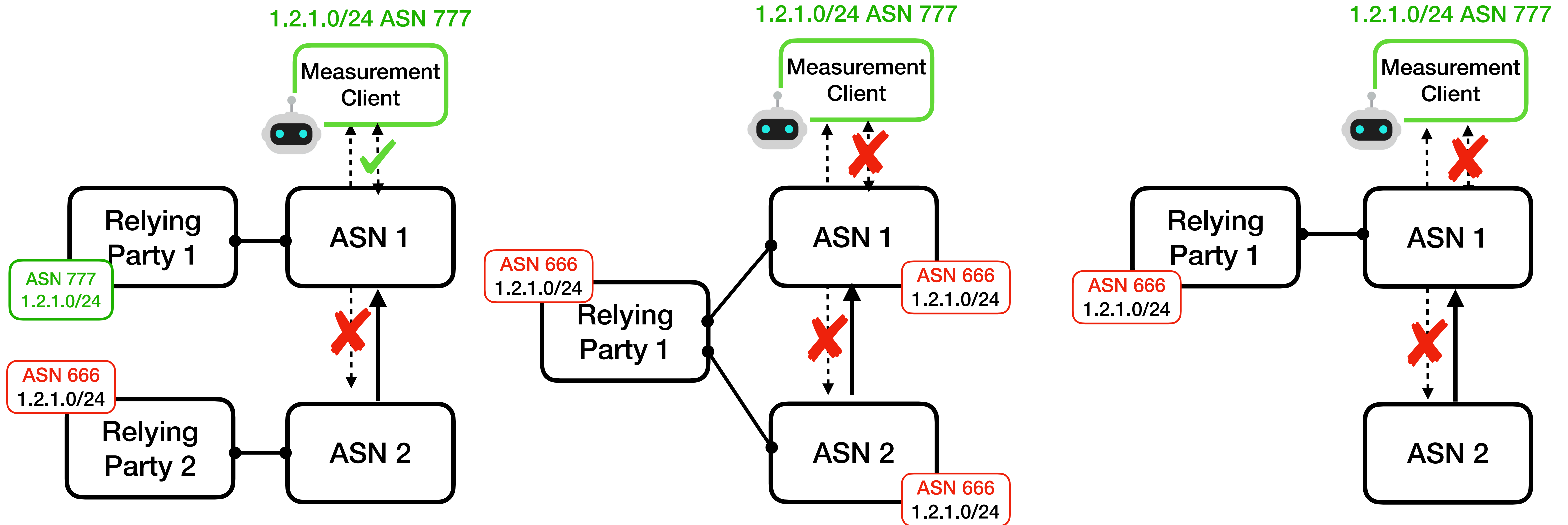
Challenge: Distinguishing Local vs. Upstream Filtering in Single Upstream



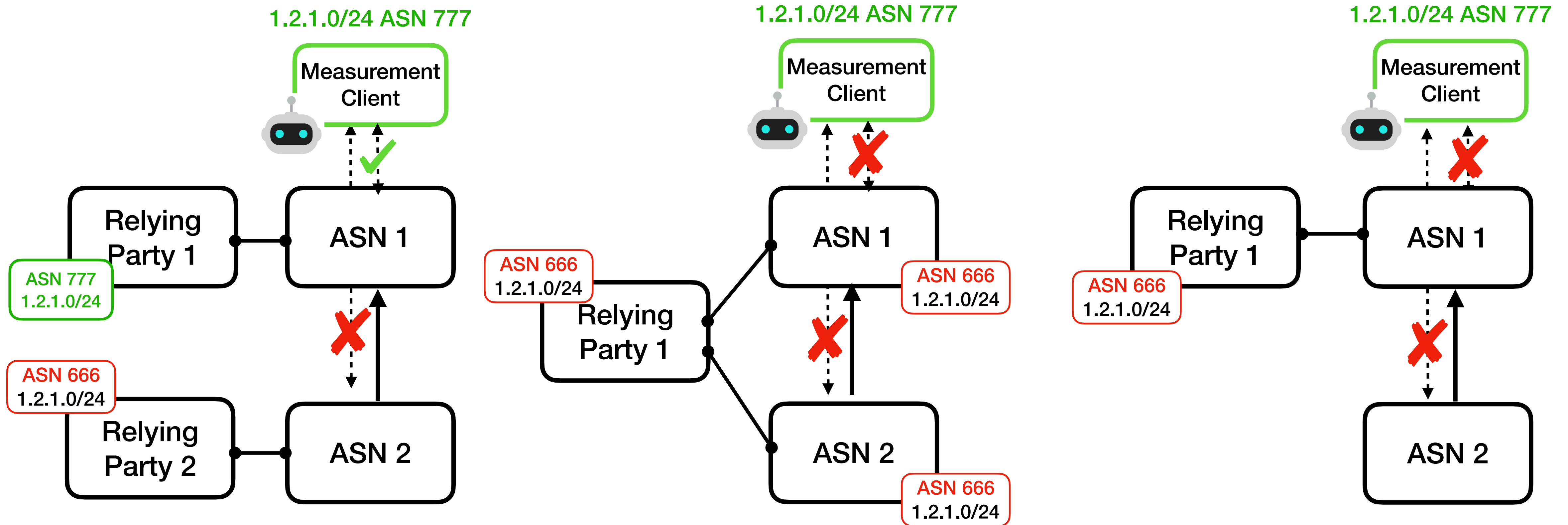
Challenge: Distinguishing Local vs. Upstream Filtering in Single Upstream



Challenge: Distinguishing Local vs. Upstream Filtering in Single Upstream

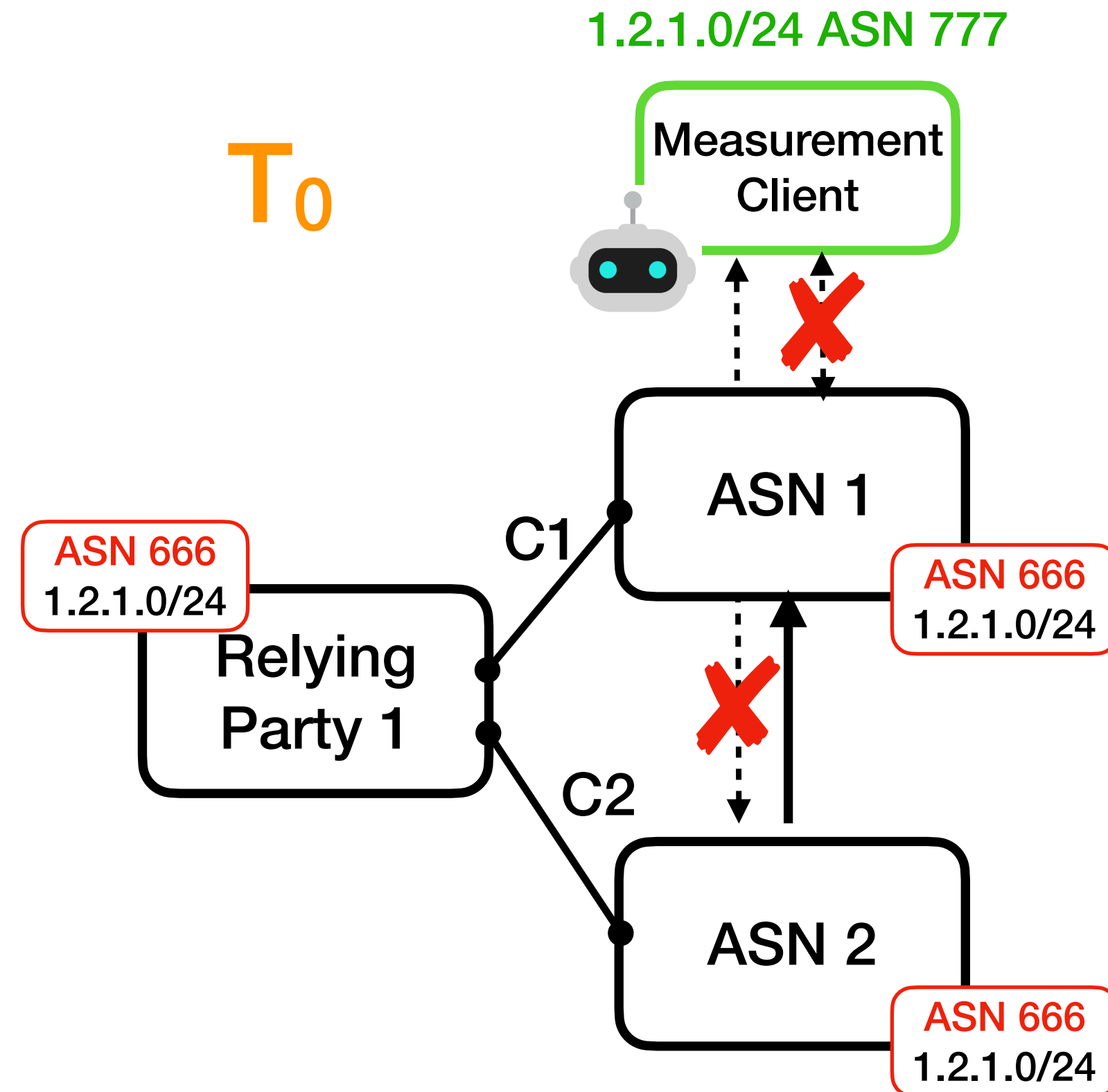


Challenge: Distinguishing Local vs. Upstream Filtering in Single Upstream



Distinguishing Local vs. Upstream Filtering

(1) Shared Relying Party

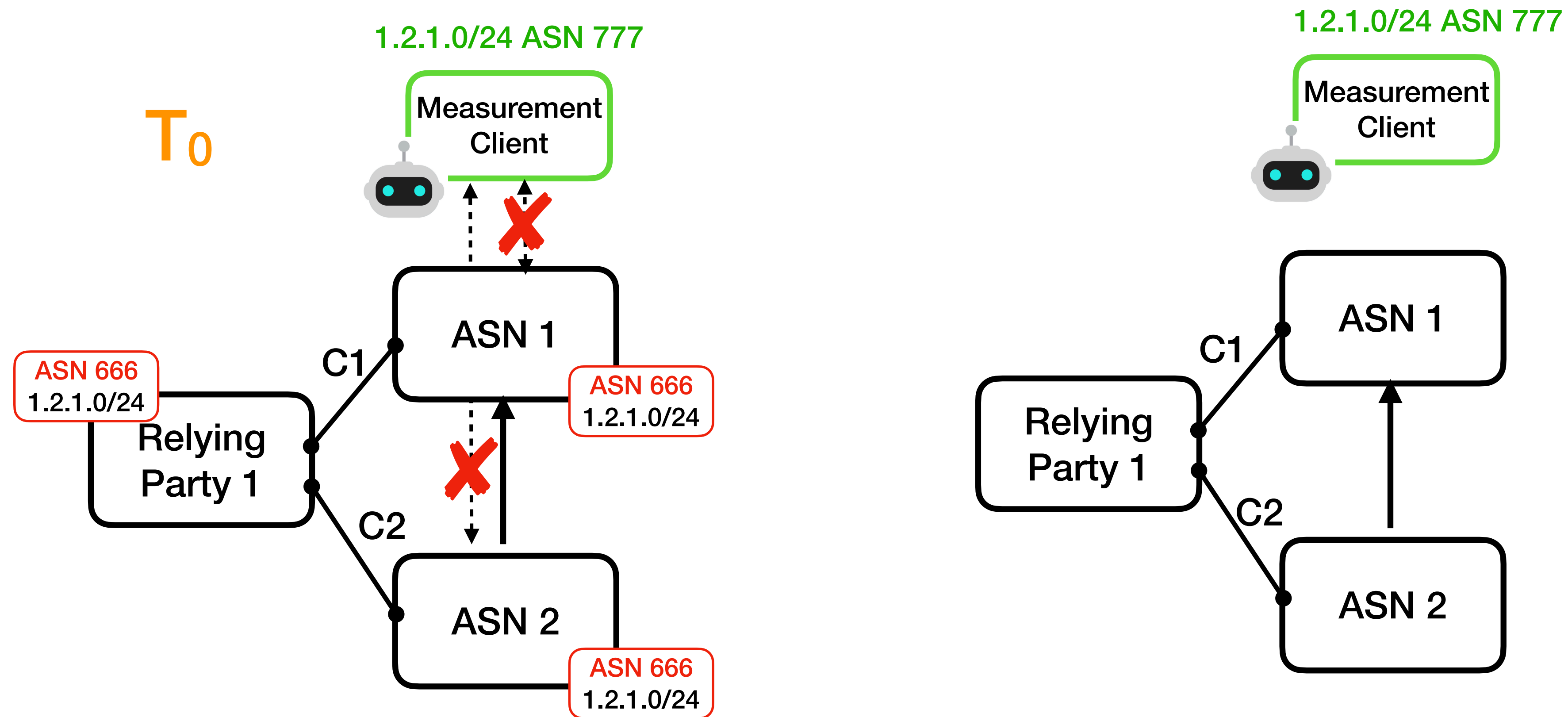


C1 and C2:

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

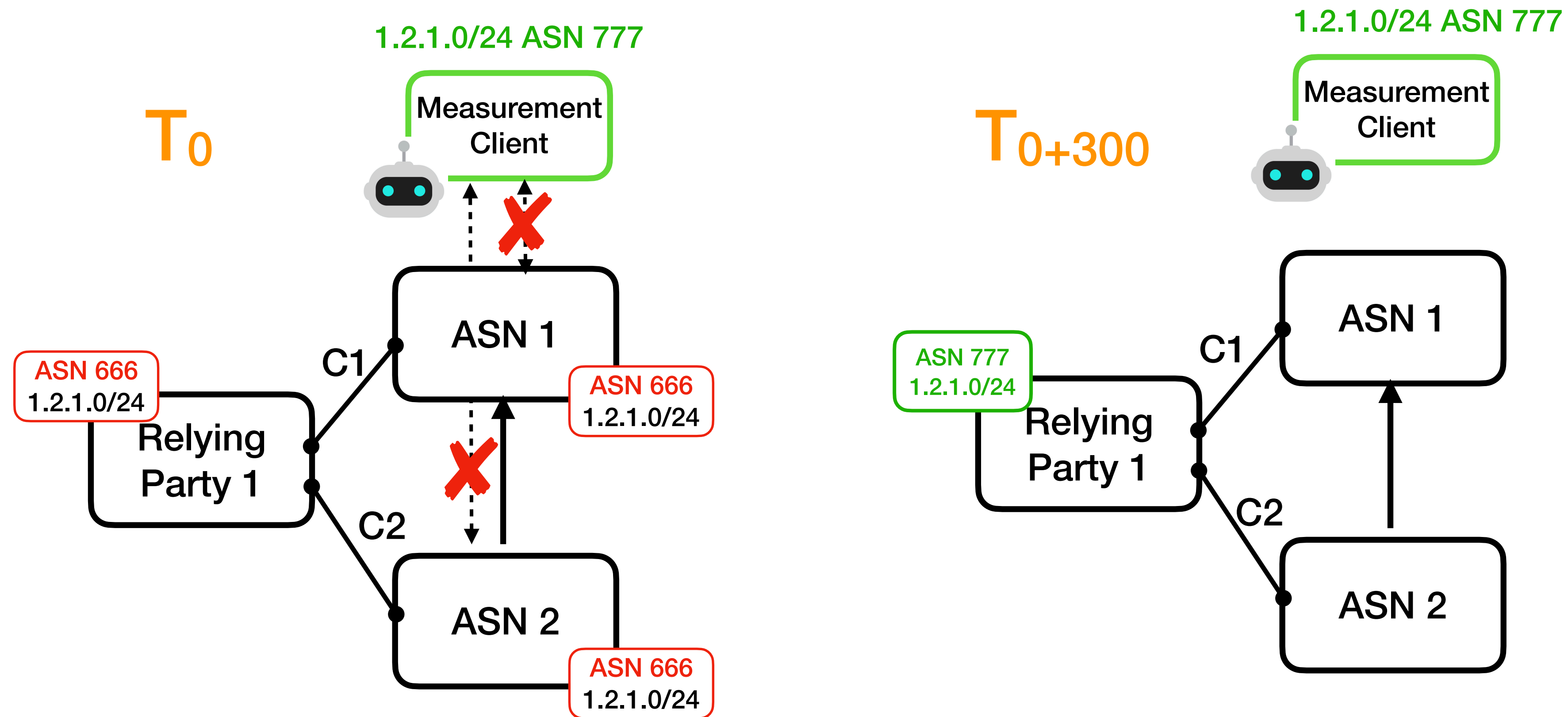
Distinguishing Local vs. Upstream Filtering

(1) Shared Relying Party



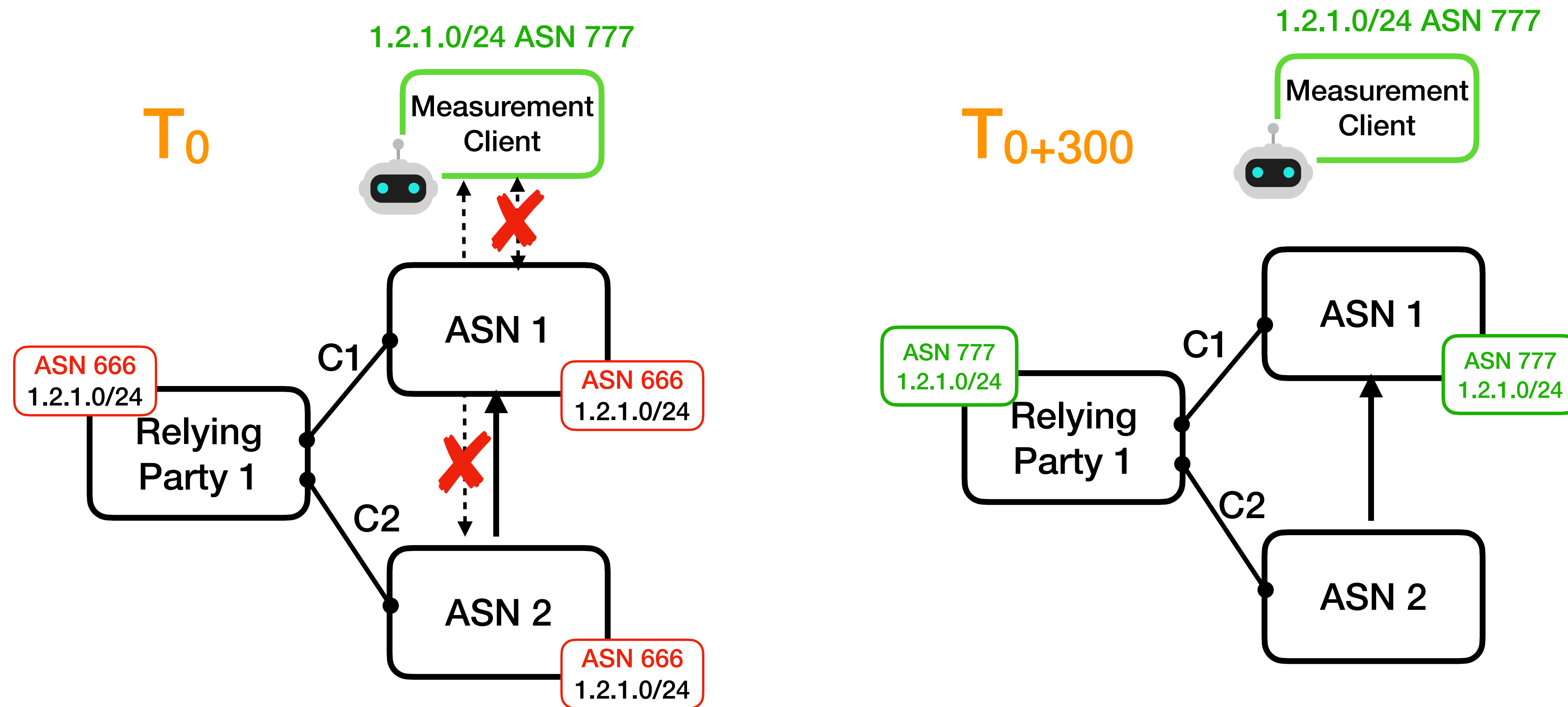
Distinguishing Local vs. Upstream Filtering

(1) Shared Relying Party



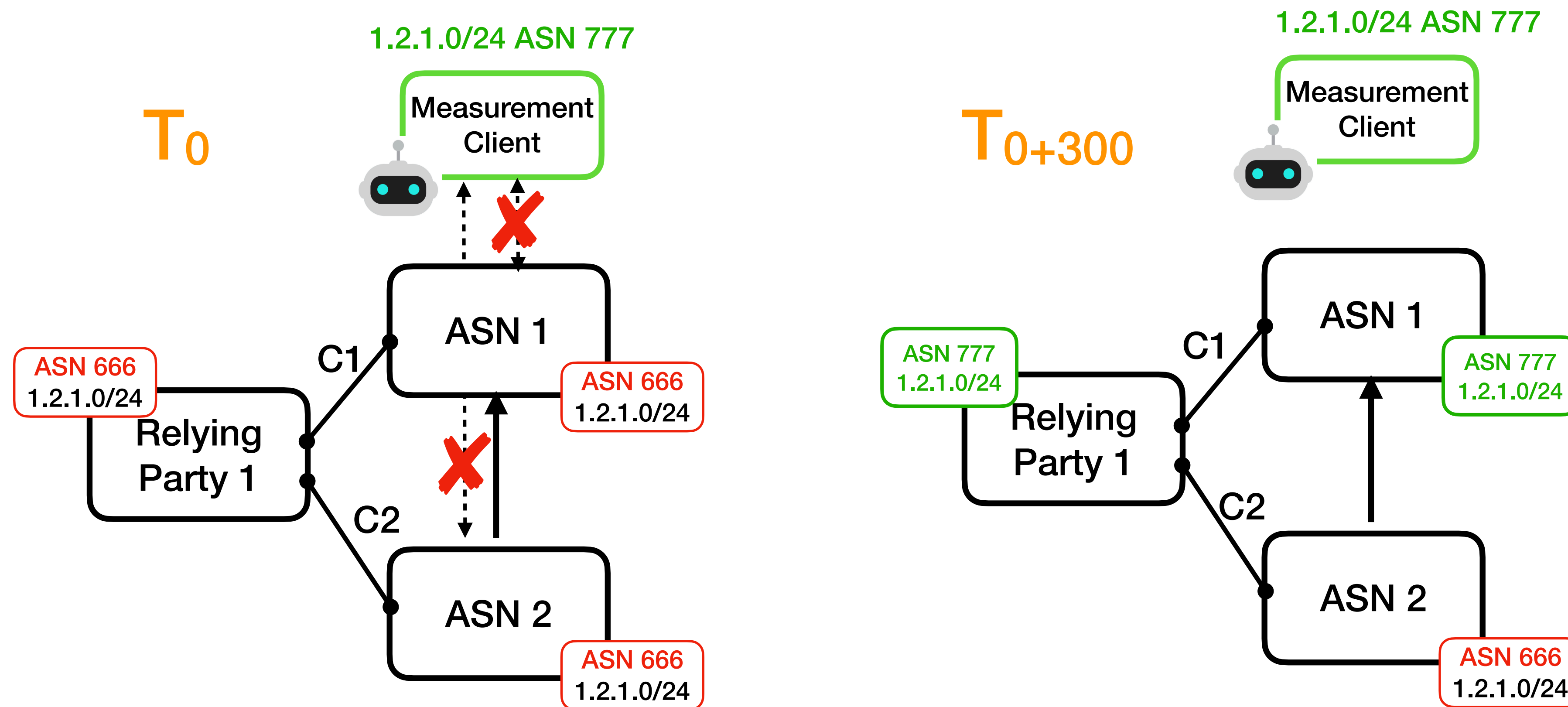
Distinguishing Local vs. Upstream Filtering

(1) Shared Relying Party



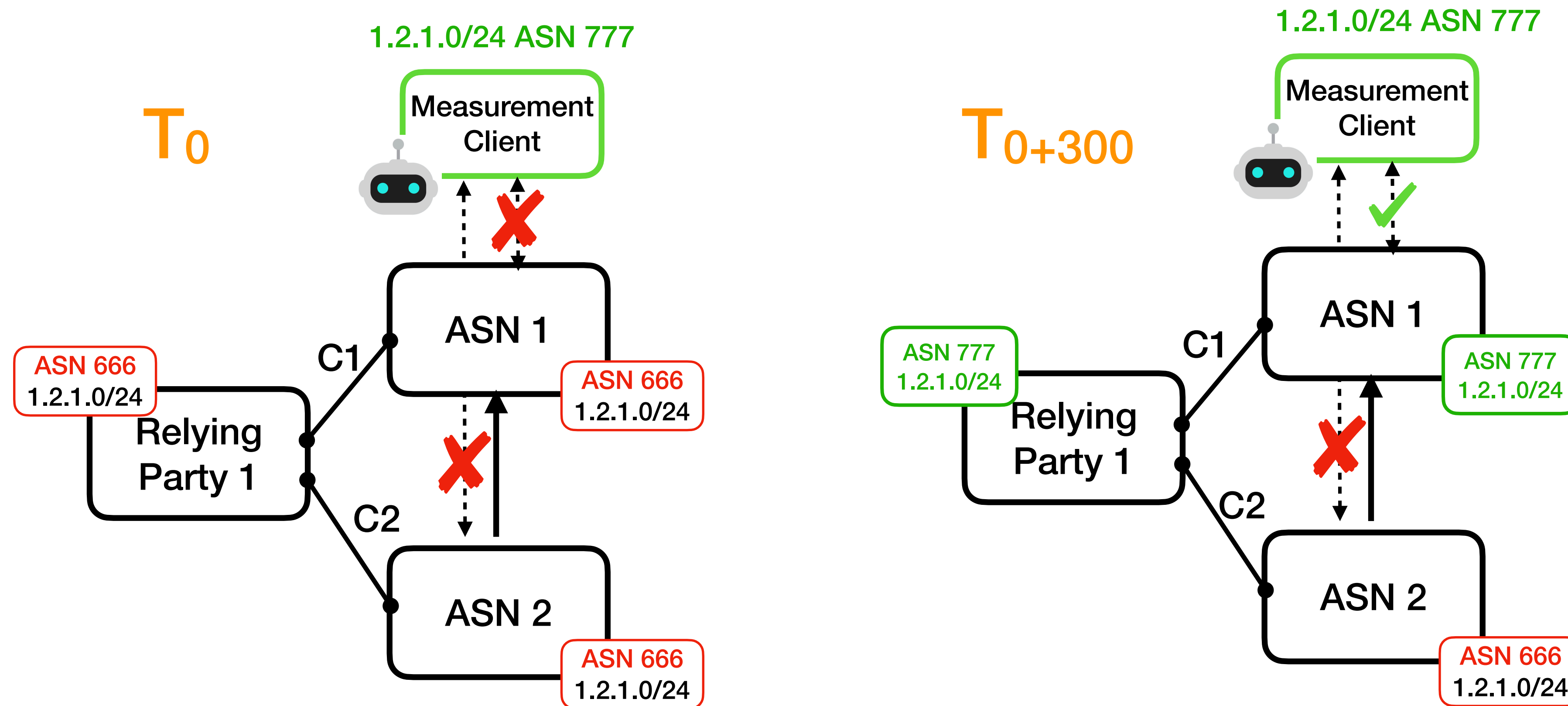
Distinguishing Local vs. Upstream Filtering

(1) Shared Relying Party



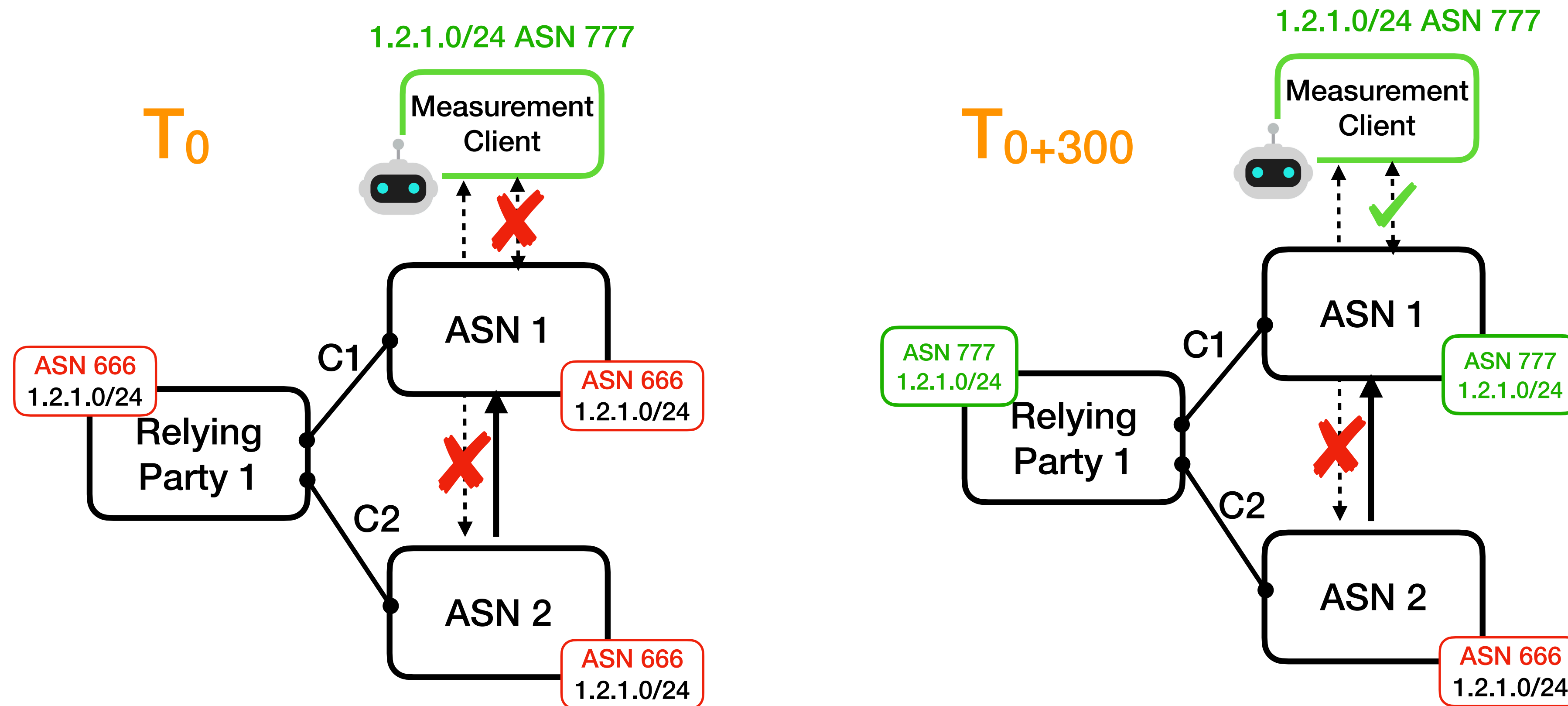
Distinguishing Local vs. Upstream Filtering

(1) Shared Relying Party



Distinguishing Local vs. Upstream Filtering

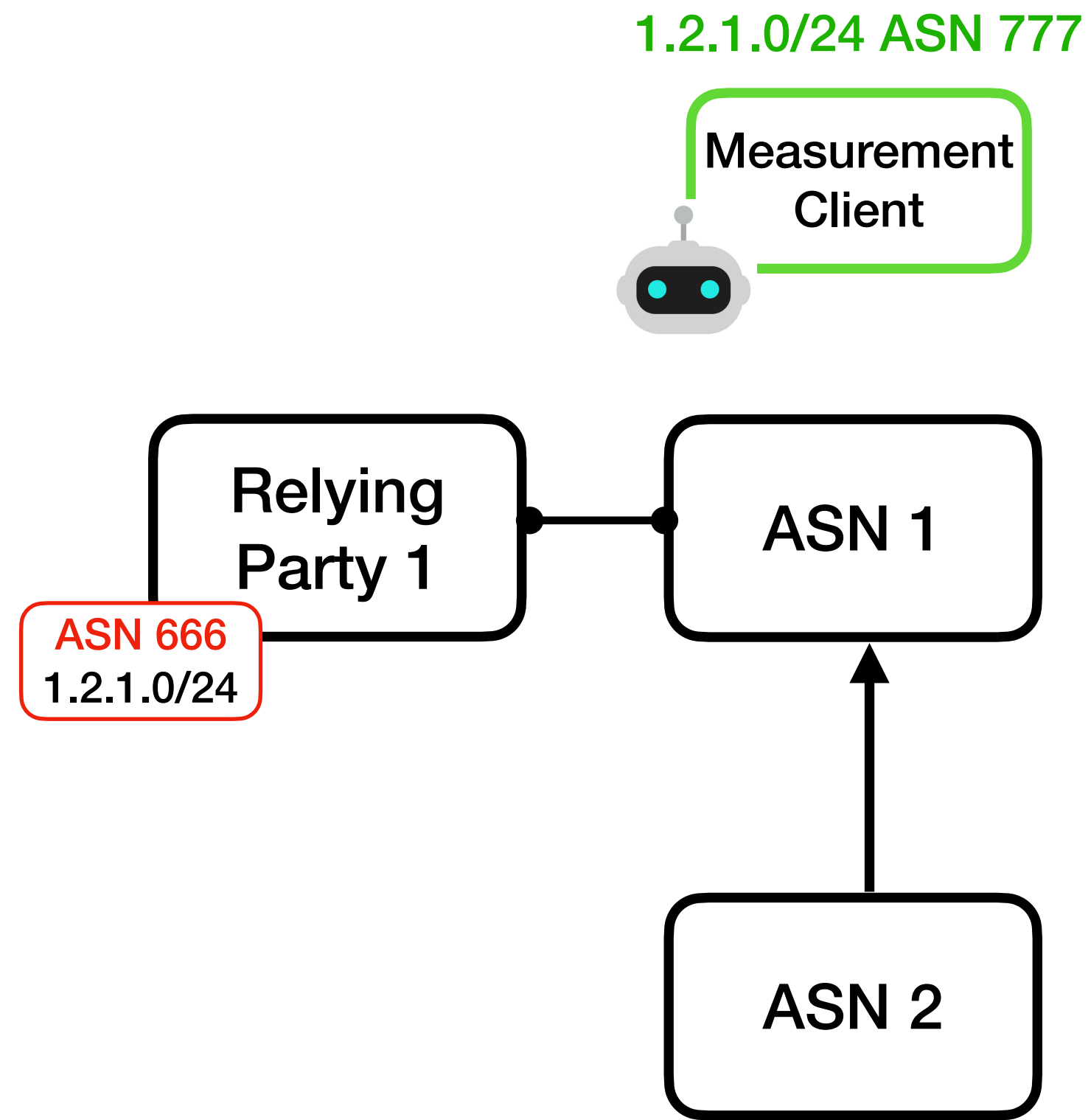
(1) Shared Relying Party



- 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

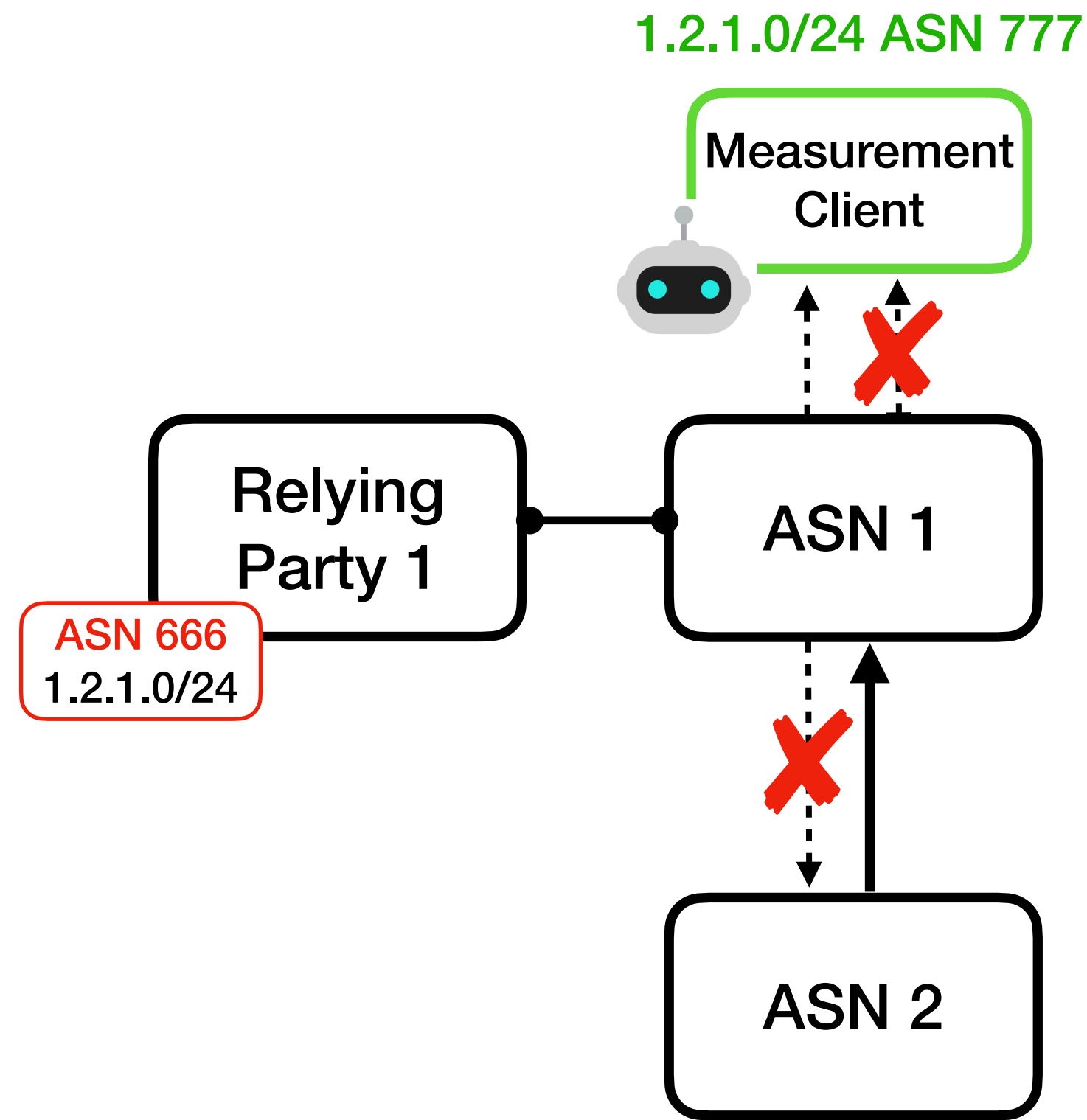
(2) Upstream Filtering



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

Distinguishing Local vs. Upstream Filtering

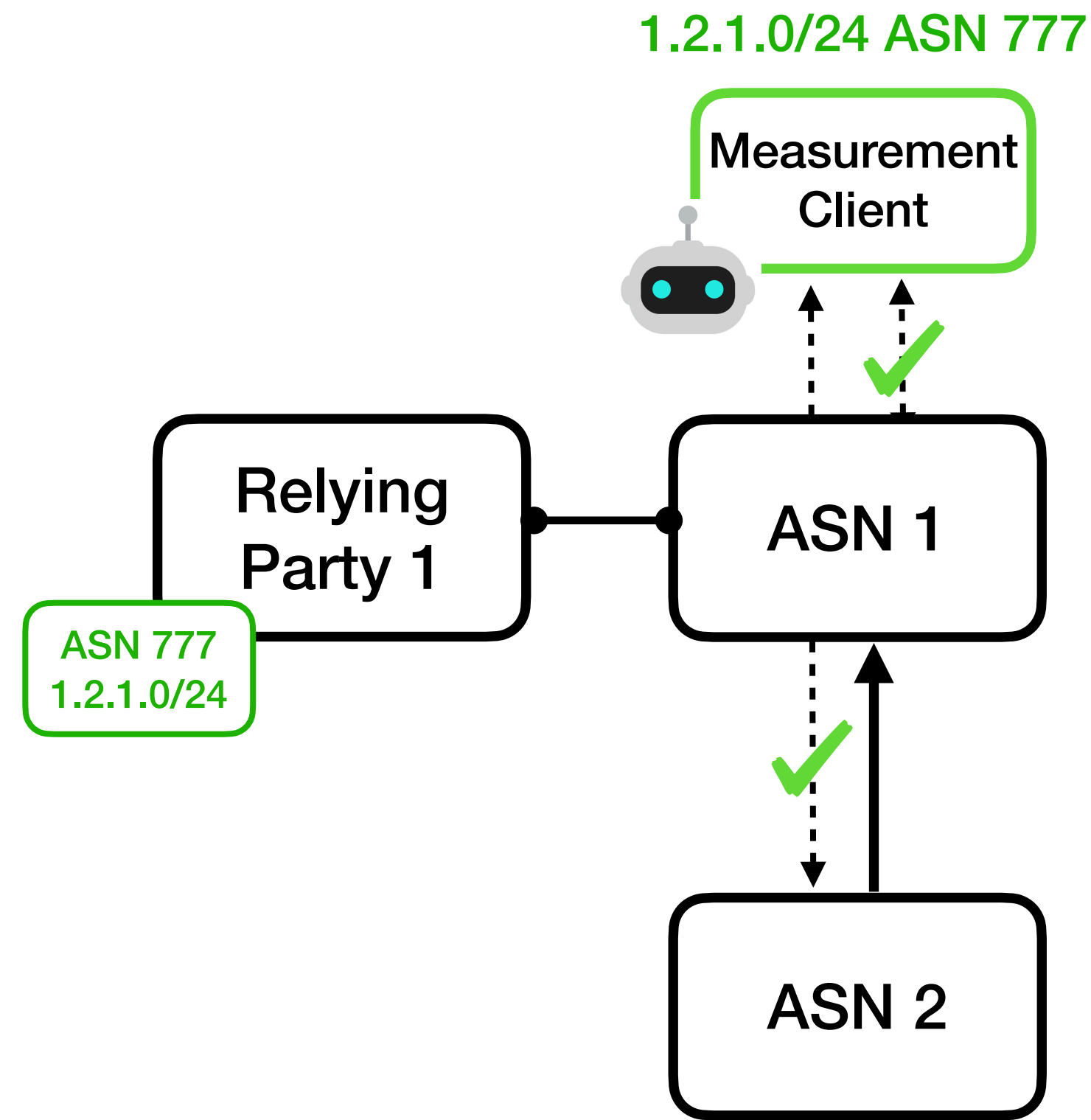
(2) Upstream Filtering



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

Distinguishing Local vs. Upstream Filtering

(2) Upstream Filtering



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

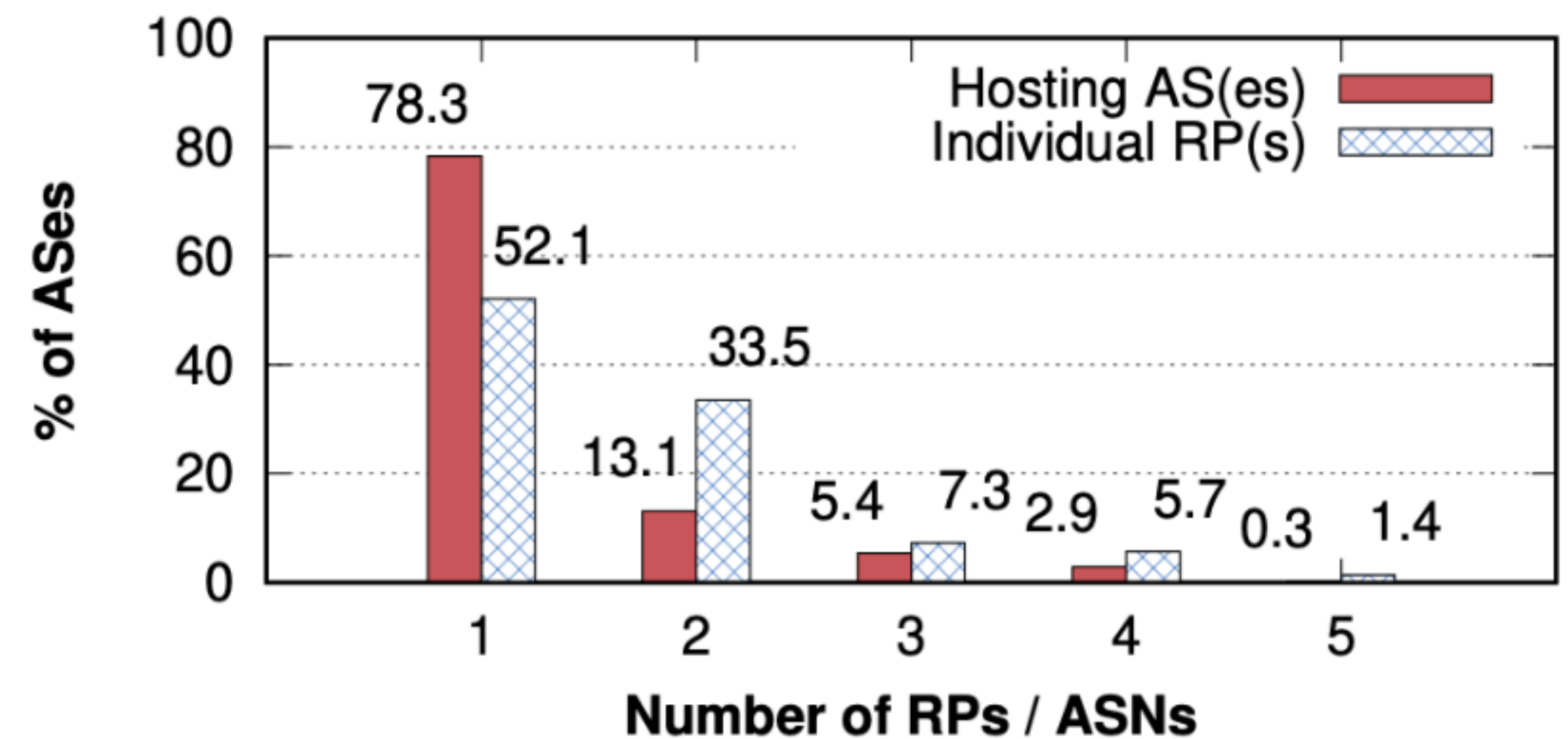
Results

- 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.

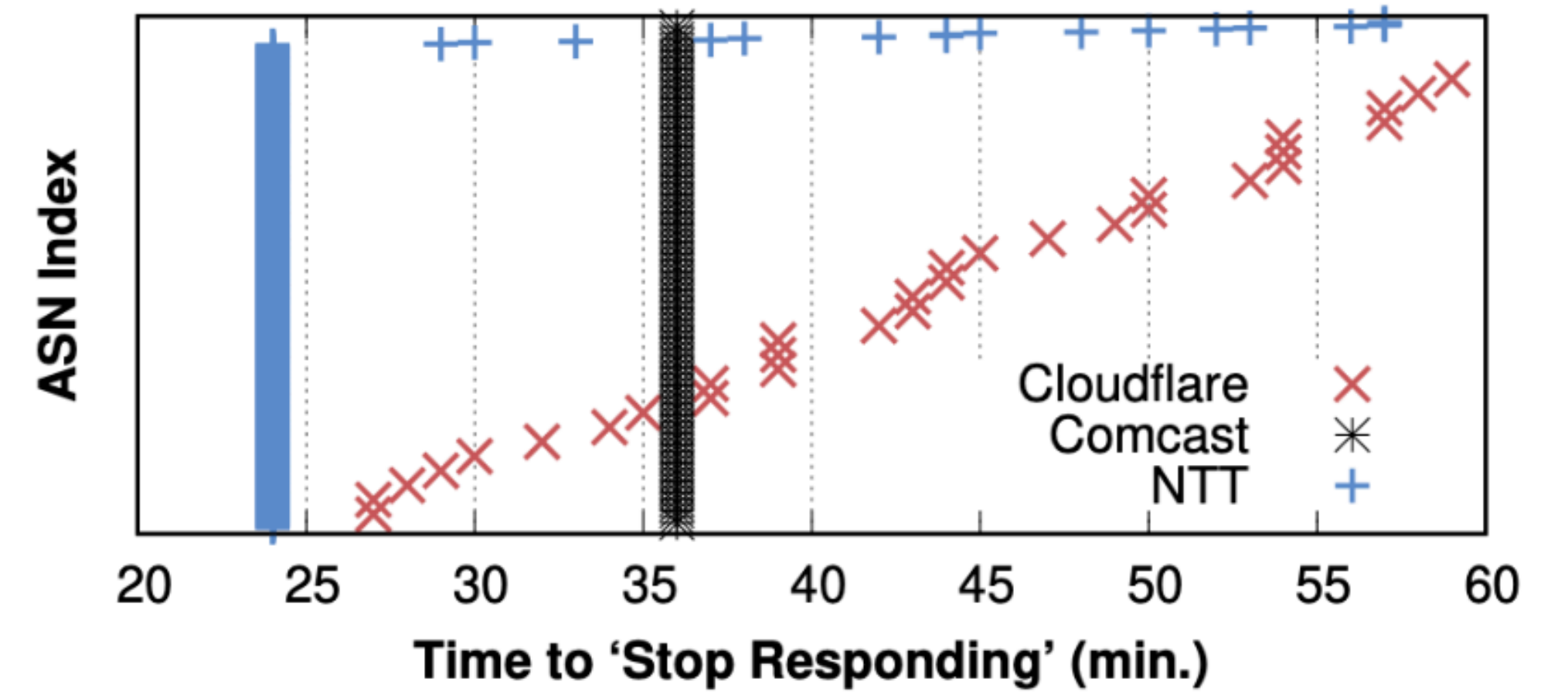
Observation

(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.

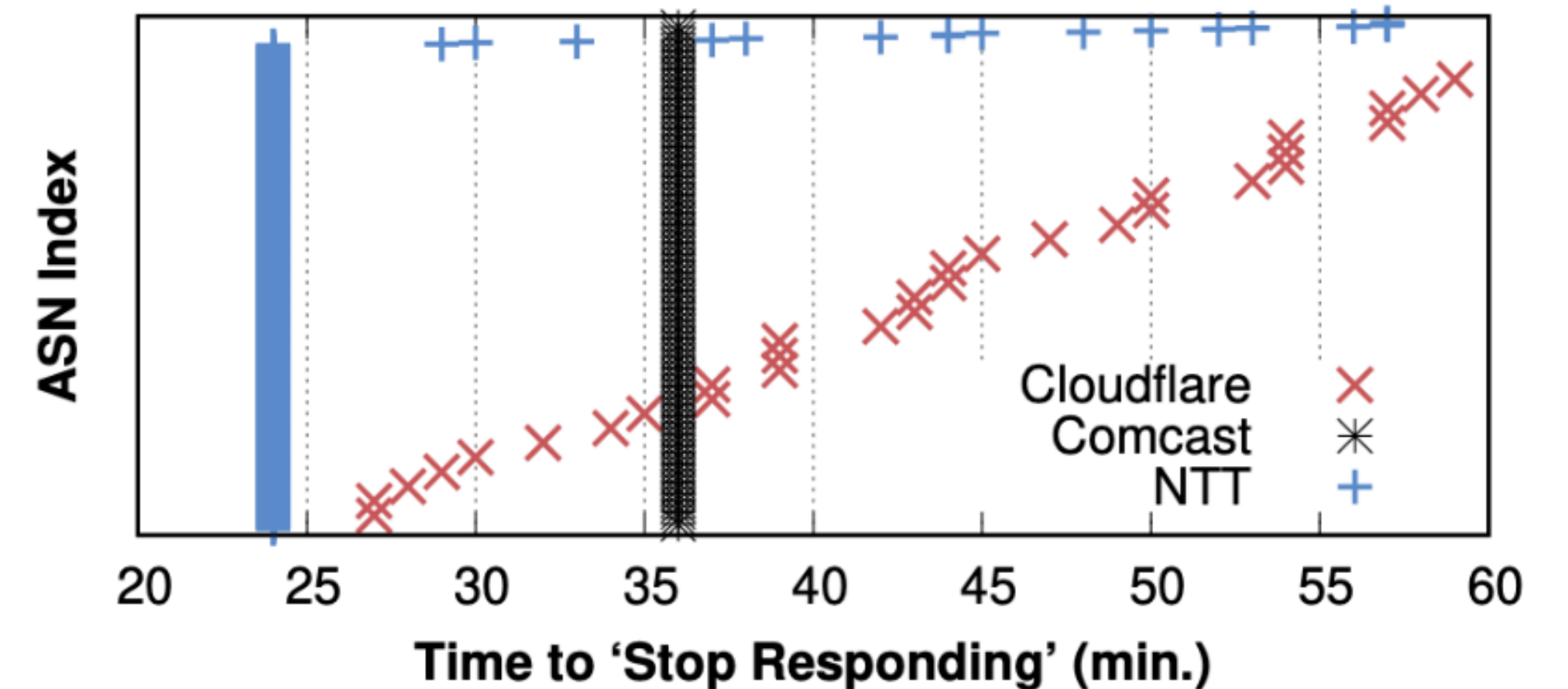


(2) Timing-Based ROV Detection



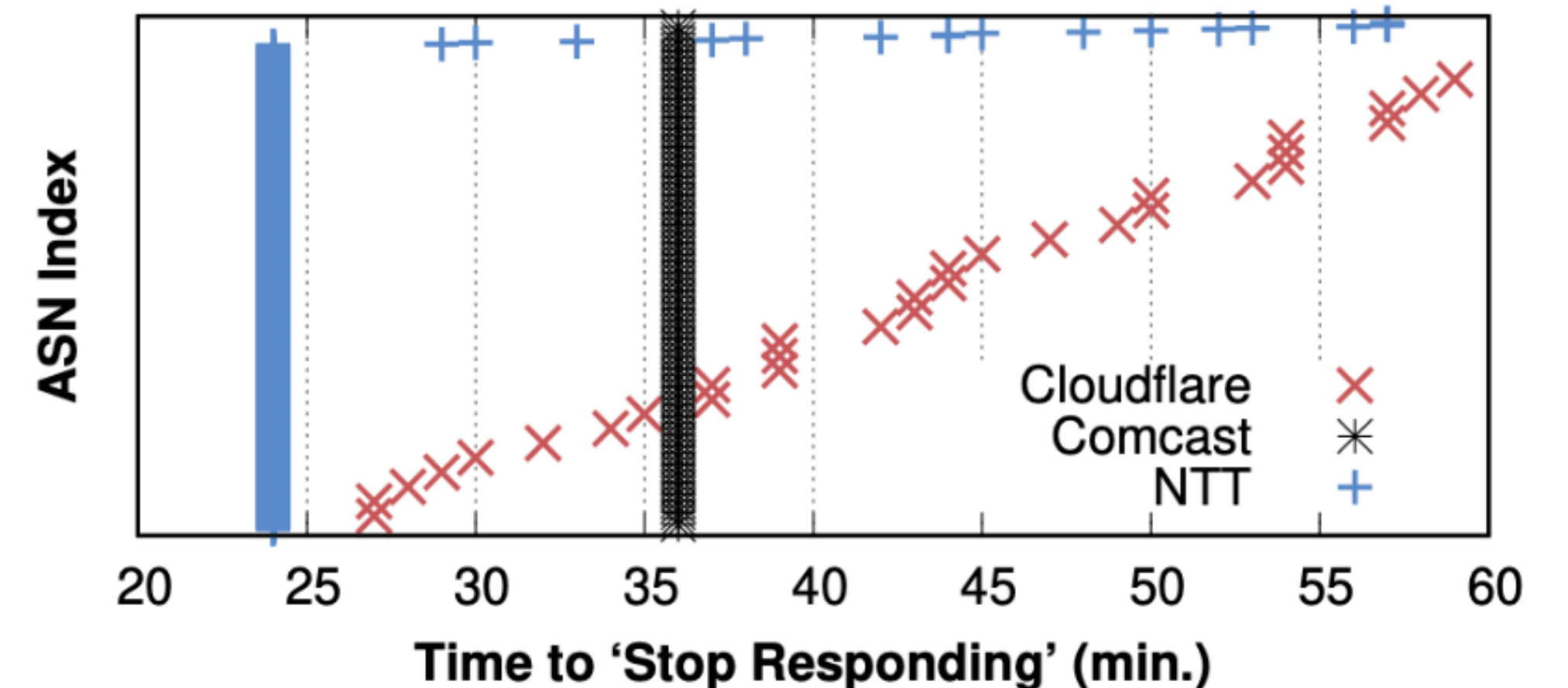
(2) Timing-Based ROV Detection

- 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).



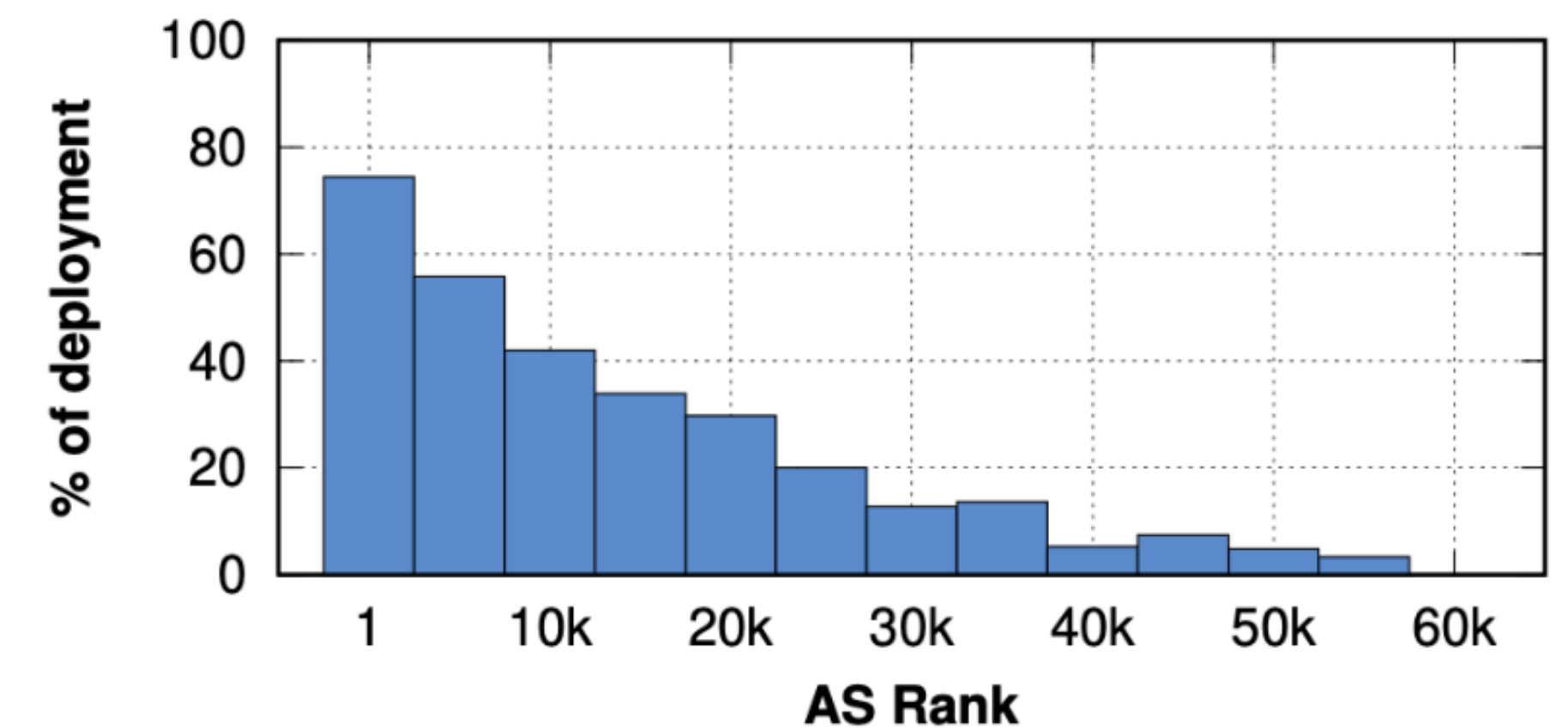
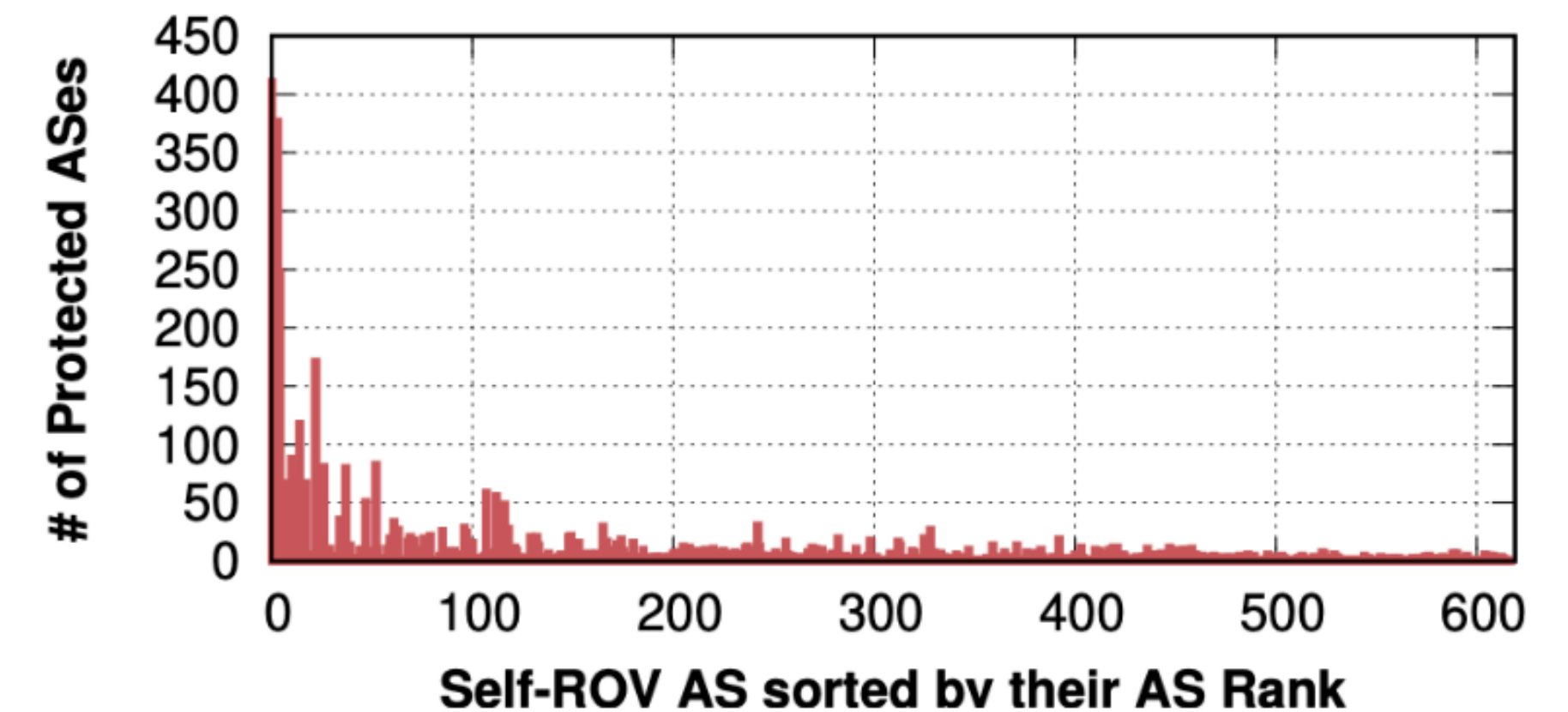
(2) Timing-Based ROV Detection

- 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



Summary

- RScope 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 (expanding it to support ASPA experiments.)
 - The Internet-wide scan
- We will release results at <https://rovista.netsecurelab.org>

Q&A and Thanks

- This work is a joint effort with Weitong Li, Yongzhe Xu (VT), Mingwei Zhang, and Vasileios Giotsas (Cloudflare) —will be appearing at IMC'2026
- This research has been generously supported by NSF and Comcast Innovation Fund.

