Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Freie Universität Berlin

Measuring the Adoption of Route Origin Validation and Filtering

Andreas Reuter (andreas.reuter@fu-berlin.de)

Joint work with Randy Bush, Ethan Katz-Bassett,
Italo Cunha, Thomas C. Schmidt, and Matthias Wählisch

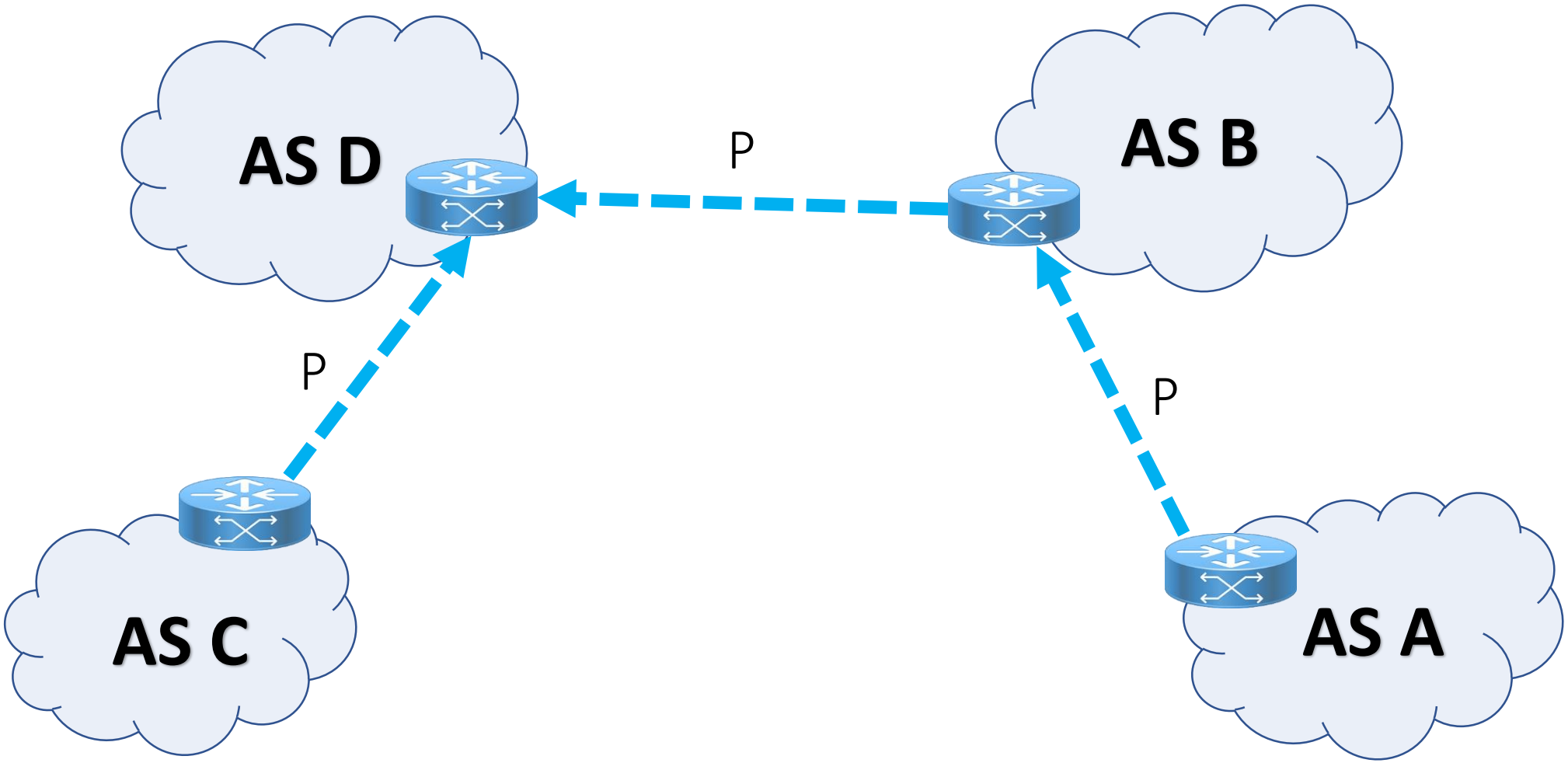
Internet Initiative Japan

UFMG
UNIVERSIDADE FEDERAL
DE MINAS GERAIS

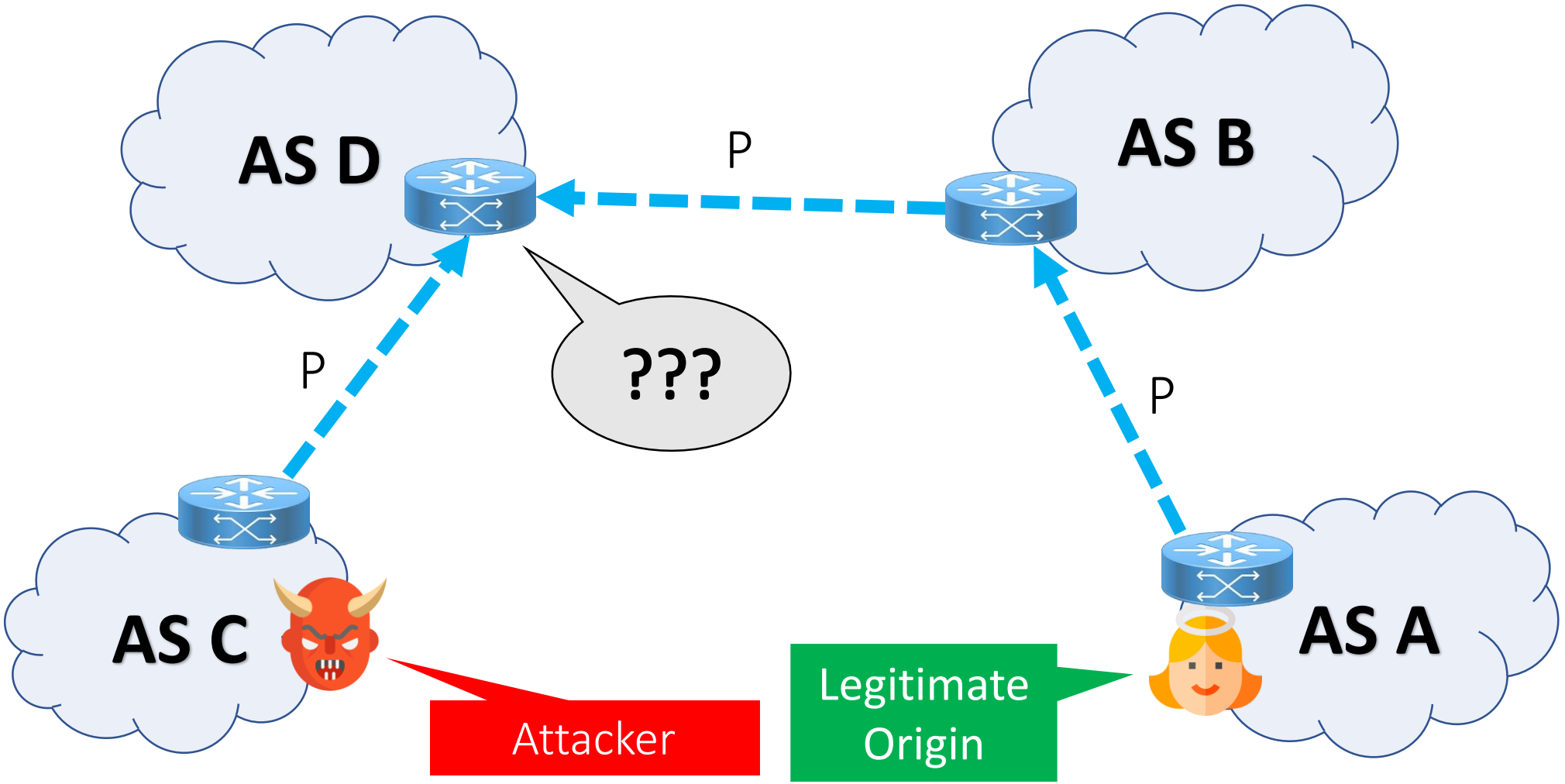
COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

PEERING
The BGP Testbed

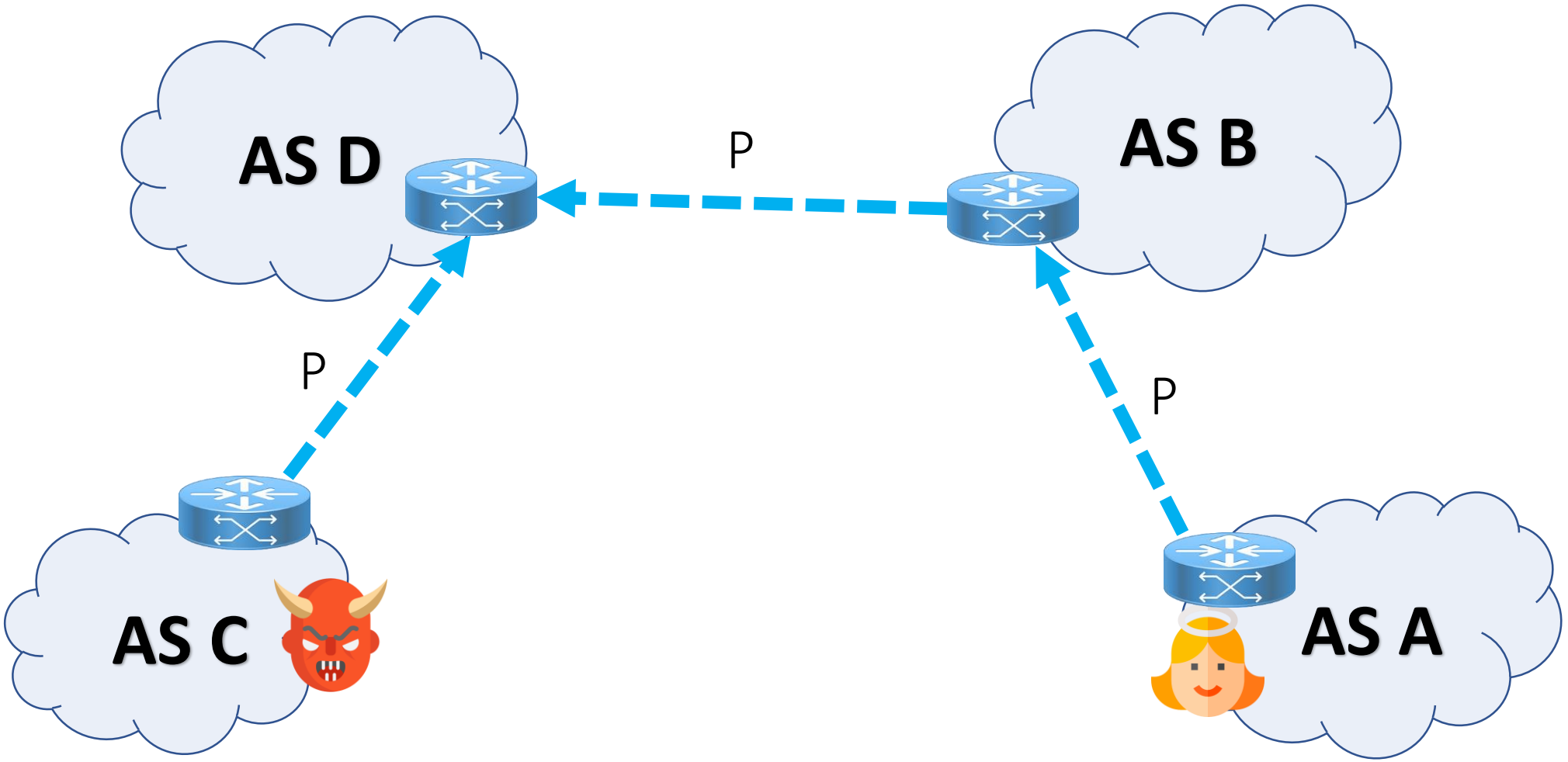
The BGP Problem…



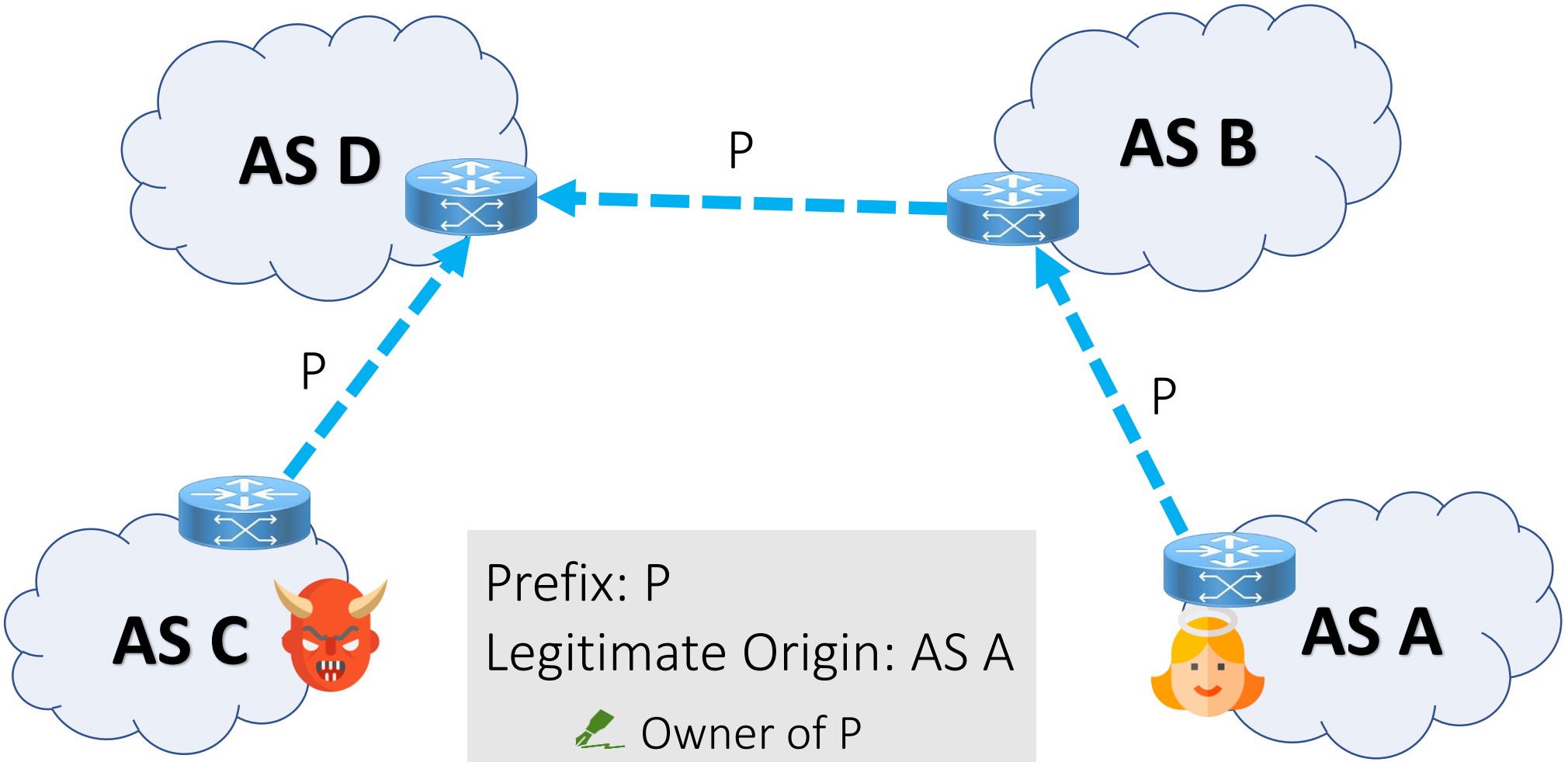
The BGP Problem…



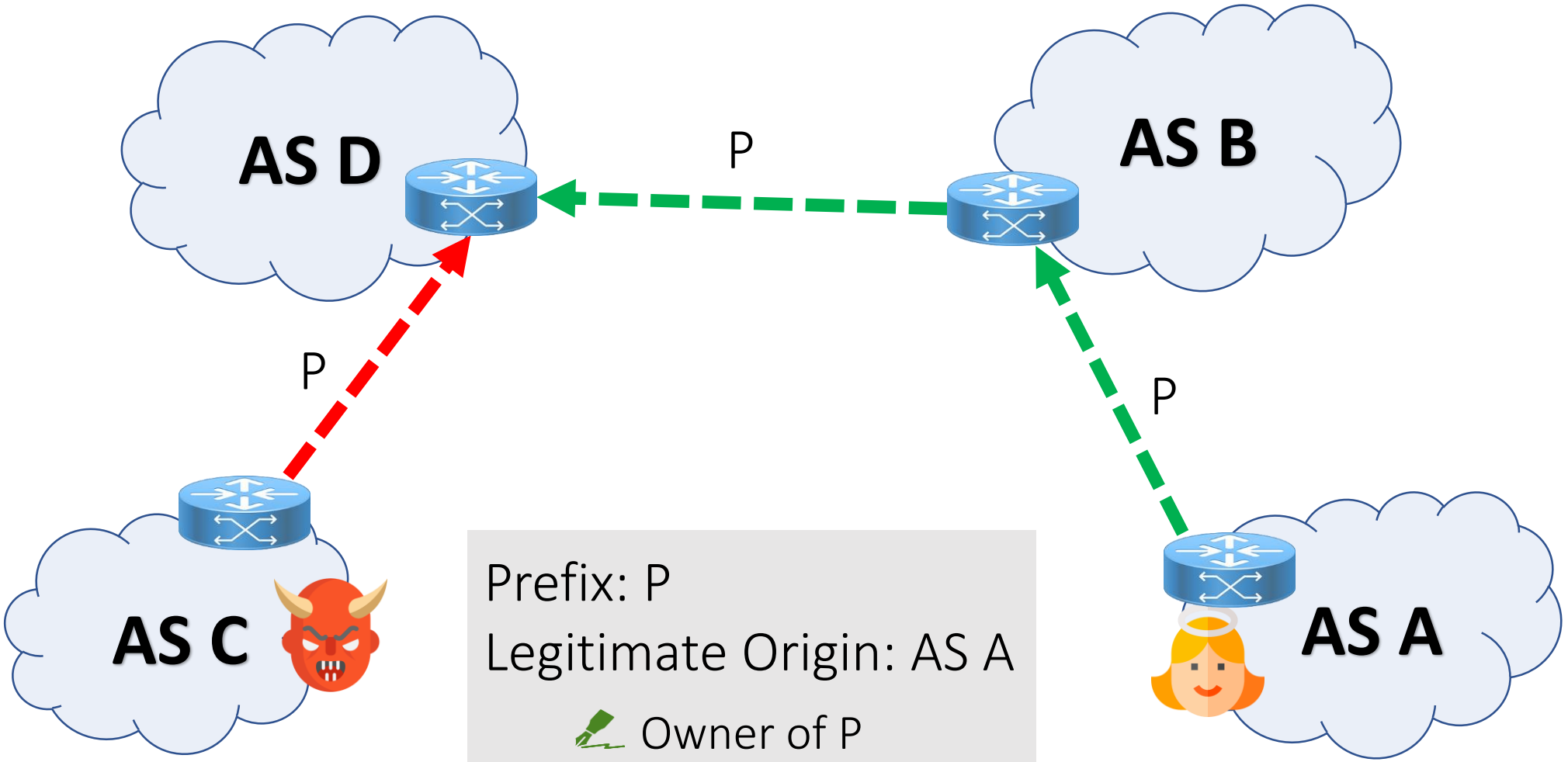
…and the (partial) solution: RPKI



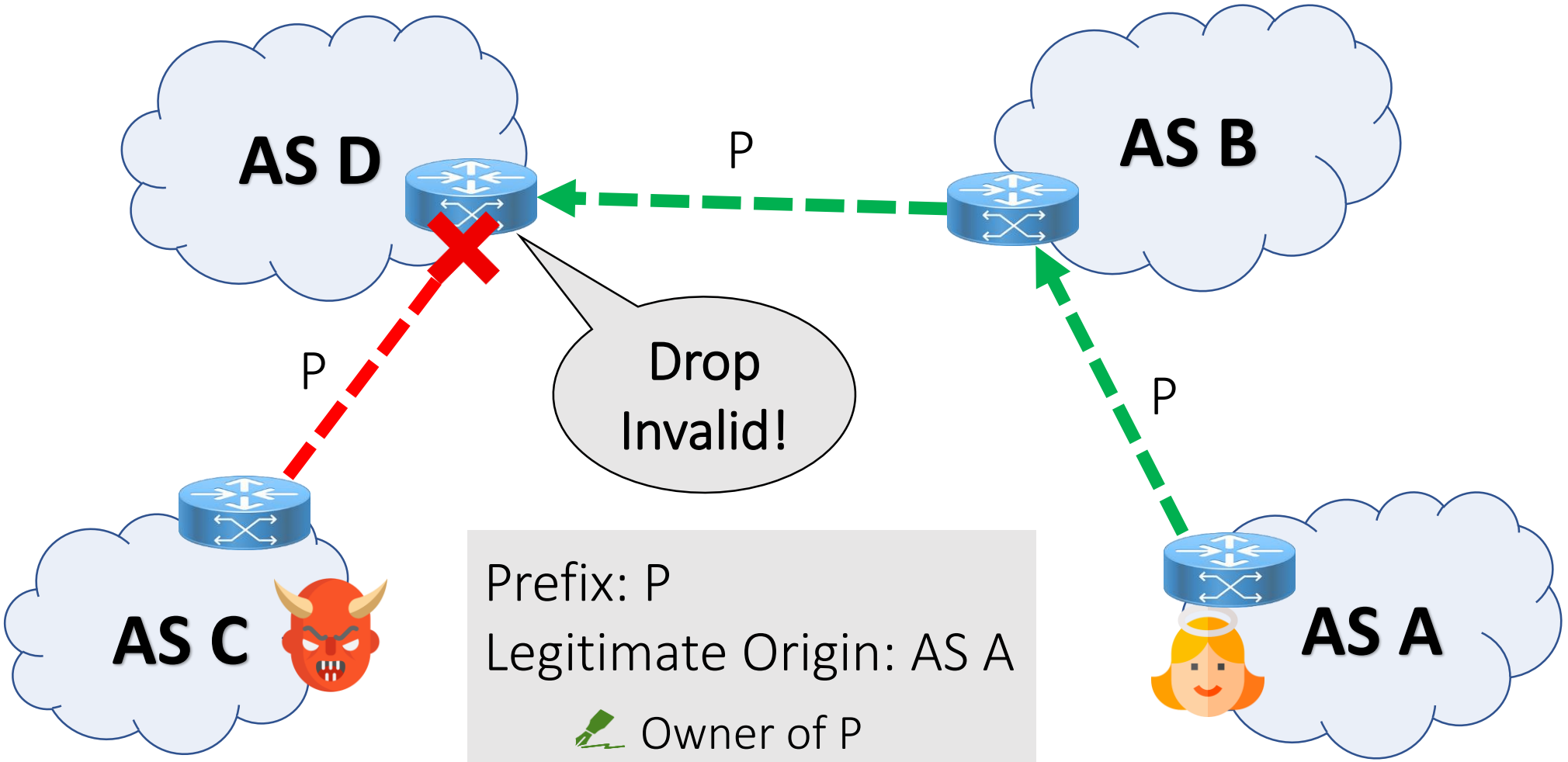
…and the (partial) solution: RPKI



…and the (partial) solution: RPKI



…and the (partial) solution: RPKI



ROA and ROV

Route Origin Authorization (ROA)	Prefix owner authorizes AS to legitimately announce the prefix

ROA and ROV

Route Origin Authorization (ROA)	Prefix owner authorizes AS to legitimately announce the prefix
Route Origin Validation (ROV)	BGP router validates received routes using ROA information

Research Problem

Goal: Are any ASes using ROV-based filtering policies?

Research Problem

Goal: Are any ASes using ROV-based filtering policies?

Assess current state of deployment

Track deployment over time

Create an incentive to deploy

Research Problem

Goal: Are any ASes using ROV-based filtering policies?

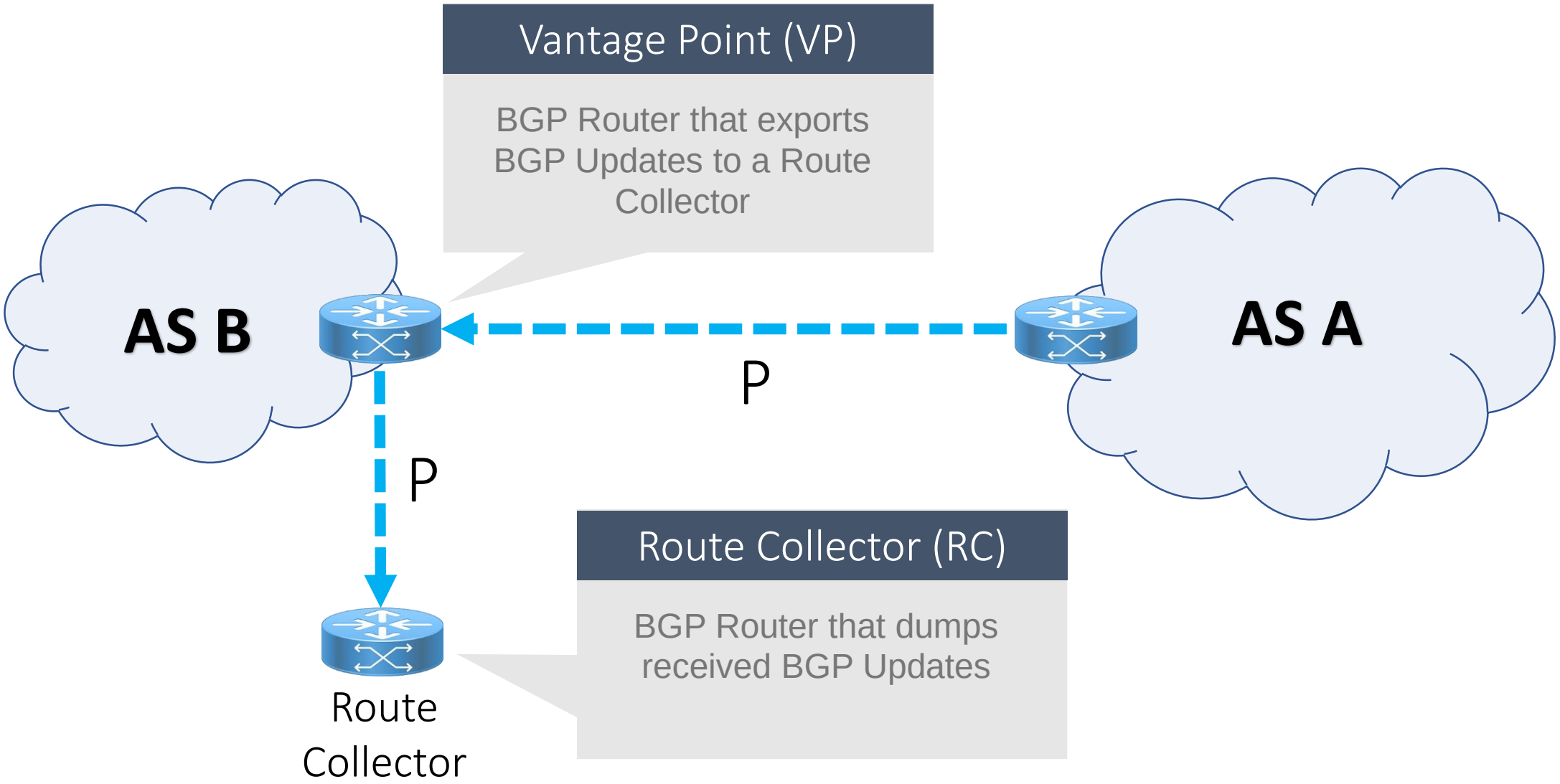
Assess current state of deployment

Track deployment over time

Create an incentive to deploy

Challenge: Private router configurations must be inferred.

Route Collectors & Vantage Points



Measuring ROV: Approaches

Description

Property

Measuring ROV: Approaches

Freie Universität Berlin

	Uncontrolled
Description	Analyzing existing BGP data and ROAs, trying to infer who is filtering
Property	Needs Existing Data Fast

Measuring ROV: Approaches

	Uncontrolled	Controlled
Description	Analyzing existing BGP data and ROAs, trying to infer who is filtering	Actively inject routes and dynamically create ROAs Analyze resulting data to infer who is filtering
Property	Needs Existing Data Fast	Needs own AS & Prefixes Slow

Controlled Experiments

Goal: Find AS that filter invalid routes

Controlled Experiments

Goal: Find AS that filter invalid routes

BGP
Announce prefixes P_A (Anchor) and P_E (Experiment)
✓ Same RIR DB route object ✓ Same prefix length ✓ Announced at the same time ✓ Announced to same peers ✓ Announced from same origin AS

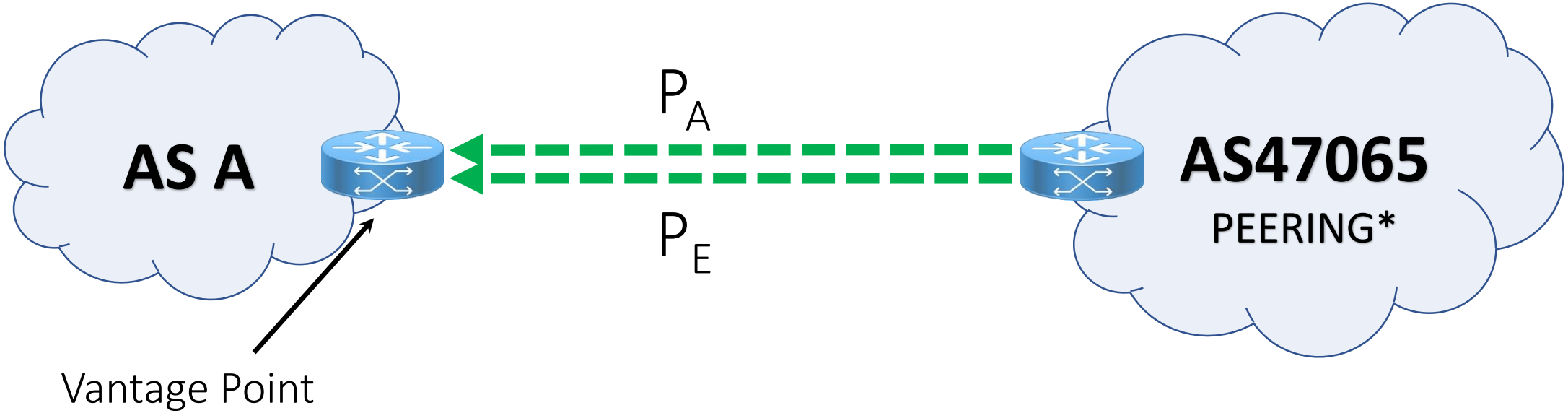
Controlled Experiments

Goal: Find AS that filter invalid routes

BGP	RPKI
Announce prefixes P_A (Anchor) and P_E (Experiment)	Issue ROAs for both prefixes
✓ Same RIR DB route object ✓ Same prefix length ✓ Announced at the same time ✓ Announced to same peers ✓ Announced from same origin AS	P_A announcement is always *valid*. Periodically change ROA for P_E : ➢ Flips announcement from *valid* to *invalid* to *valid* daily.

Controlled Experiments

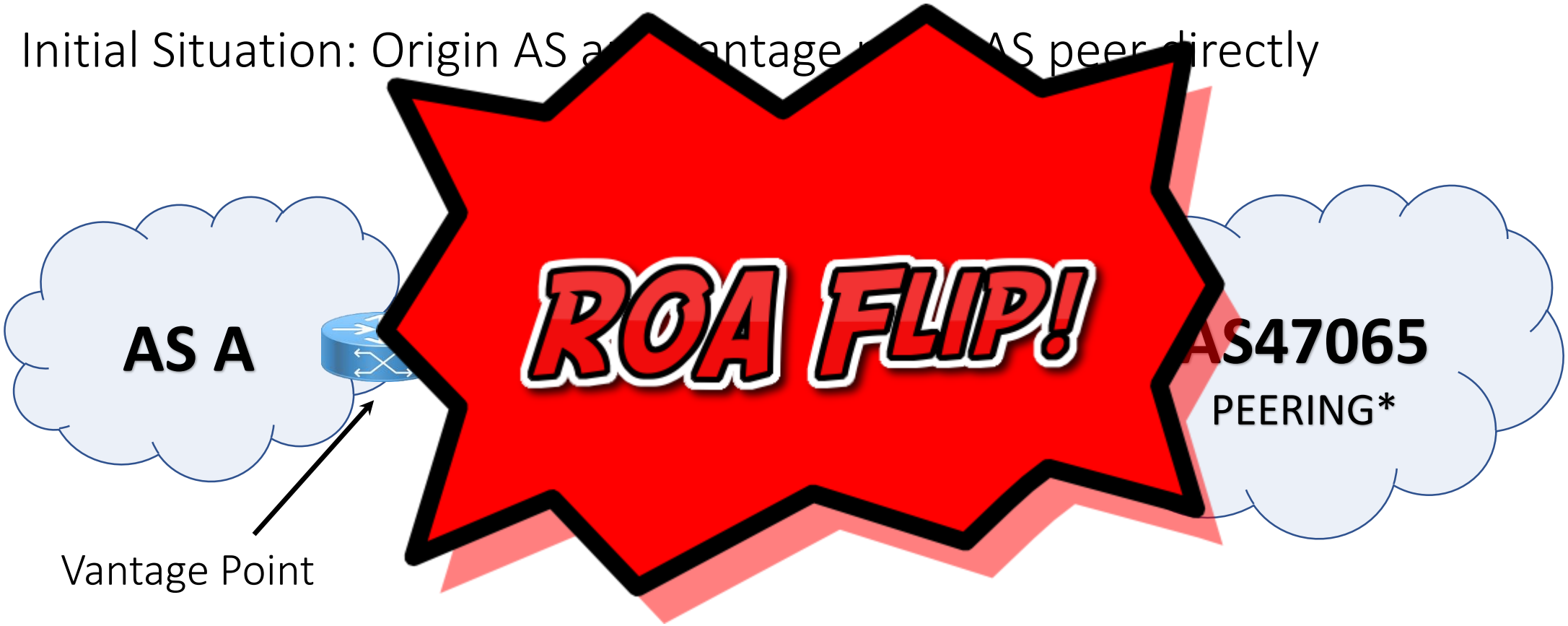
Initial Situation: Origin AS and vantage point AS peer directly



*https://peering.usc.edu/

Controlled Experiments

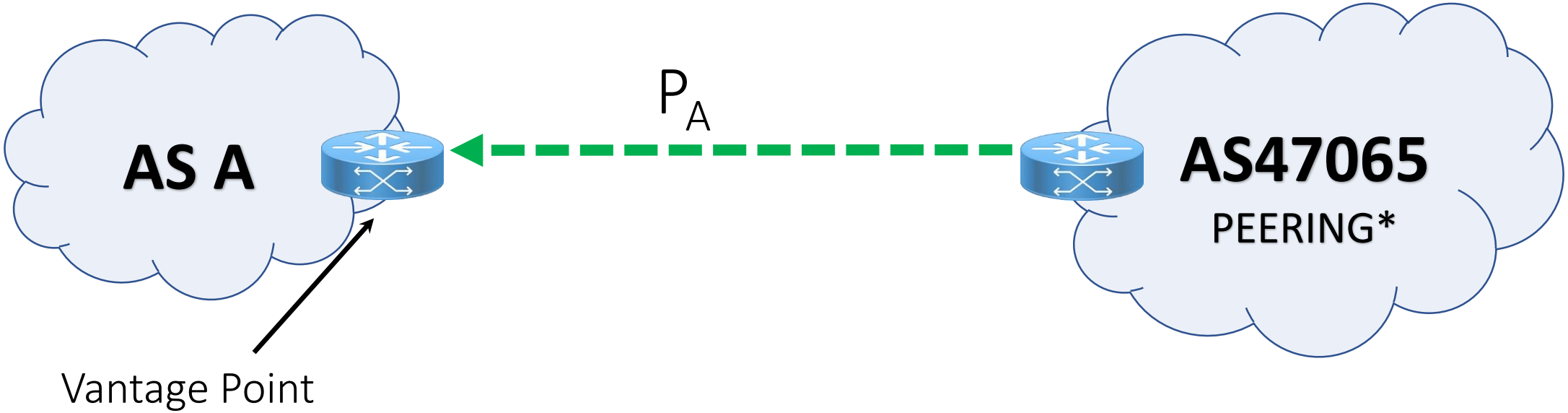
Initial Situation: Origin AS a[illegible]ntage [illegible]AS peer directly



*https://peering.usc.edu/

Controlled Experiments

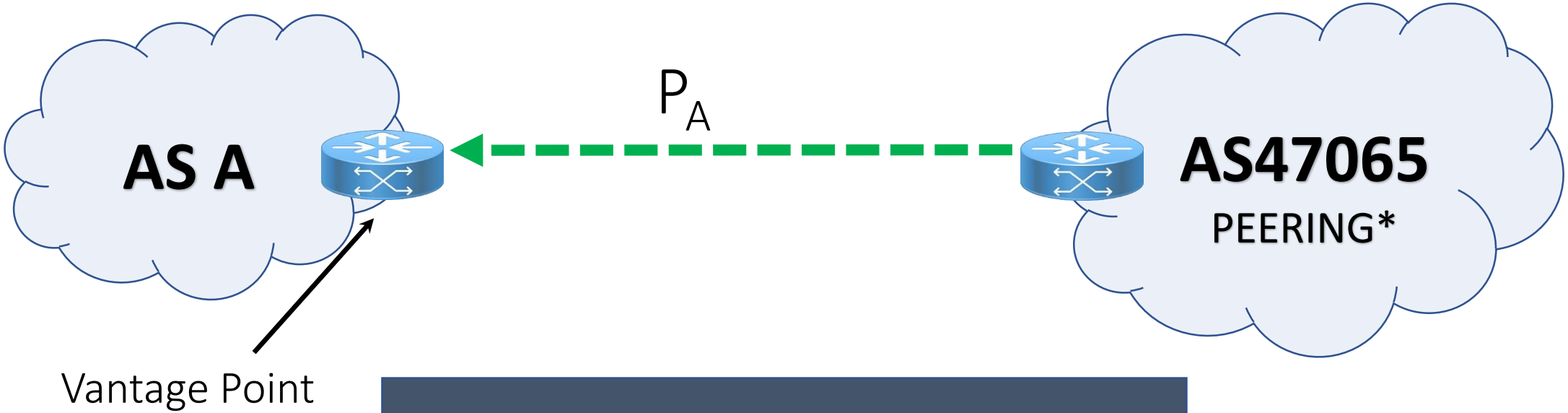
Observation 1: Vantage point exports no route for P_E



*https://peering.usc.edu/

Controlled Experiments

Observation 1: Vantage point exports no route for P_E

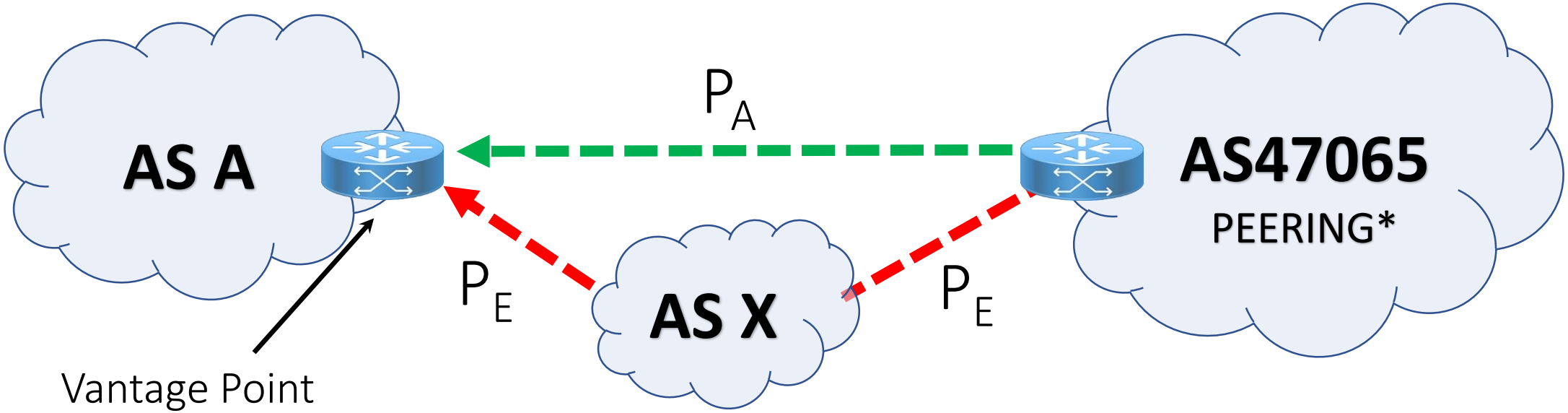


Conclusion: Vantage point is using ROV-based filtering

*https://peering.usc.edu/

Controlled Experiments

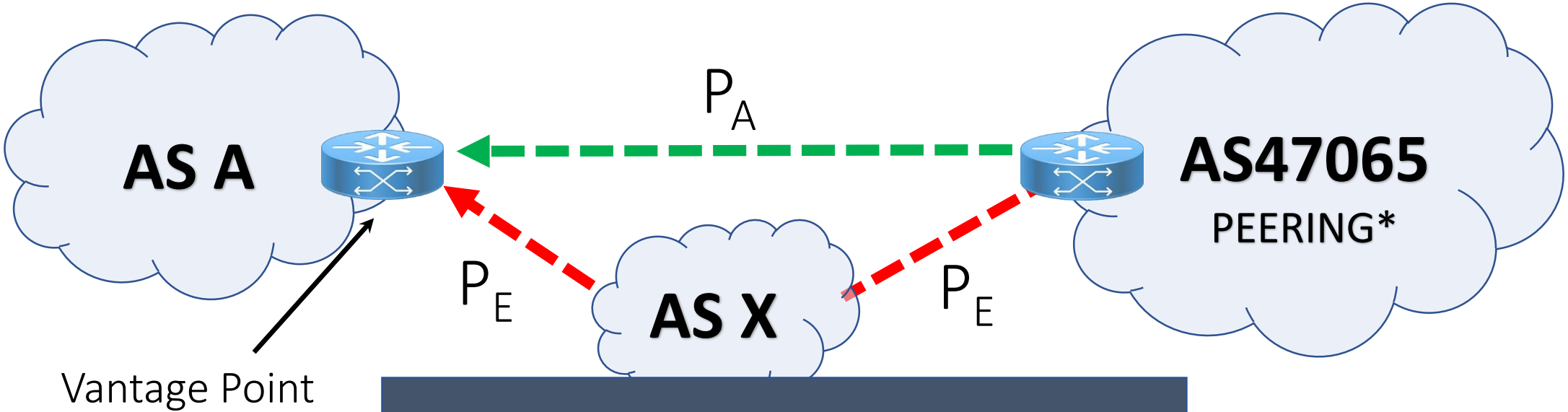
Observation 2: Vantage point exports alternate route for P_E



*https://peering.usc.edu/

Controlled Experiments

Observation 2: Vantage point exports alternate route for P_E

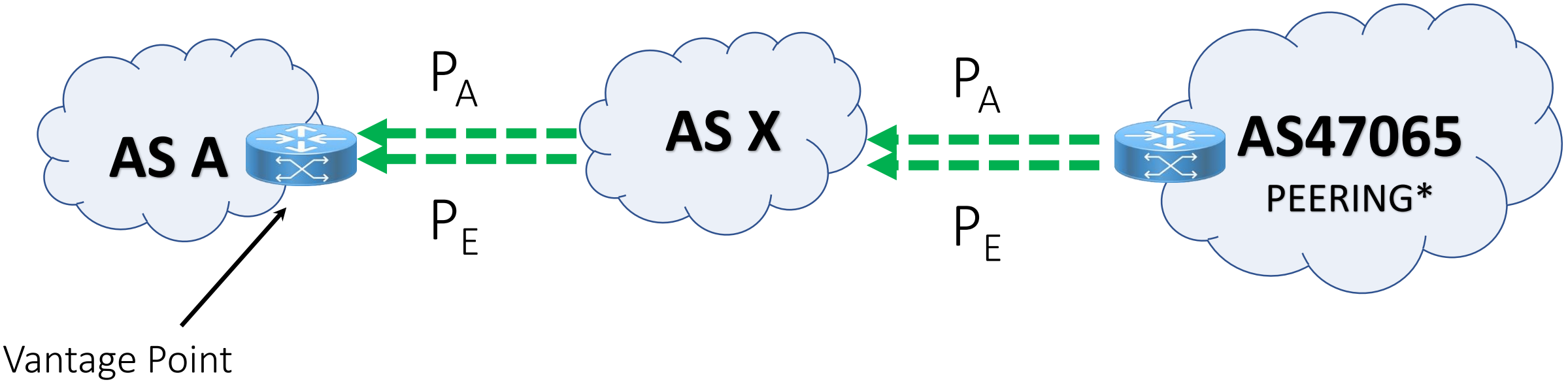


Conclusion: Vantage point is using ROV-based filtering *selectively*.

*https://peering.usc.edu/

Controlled Experiments

Situation: Origin AS and vantage point AS do not peer directly



*https://peering.usc.edu/

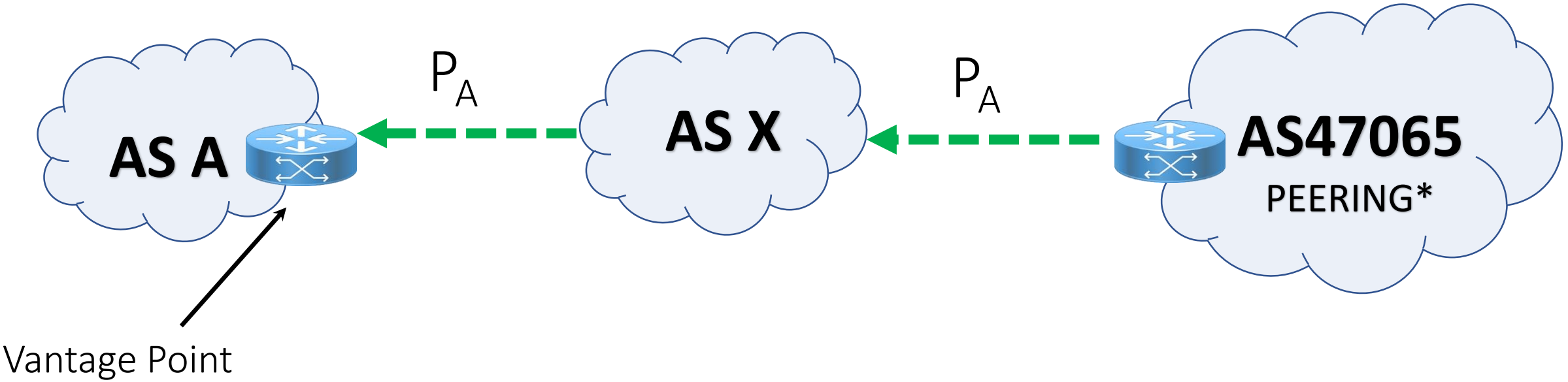
Controlled Experiments

Situation: Origin AS and vantage point AS47065 do not peer directly

*https://peering.usc.edu/

Controlled Experiments

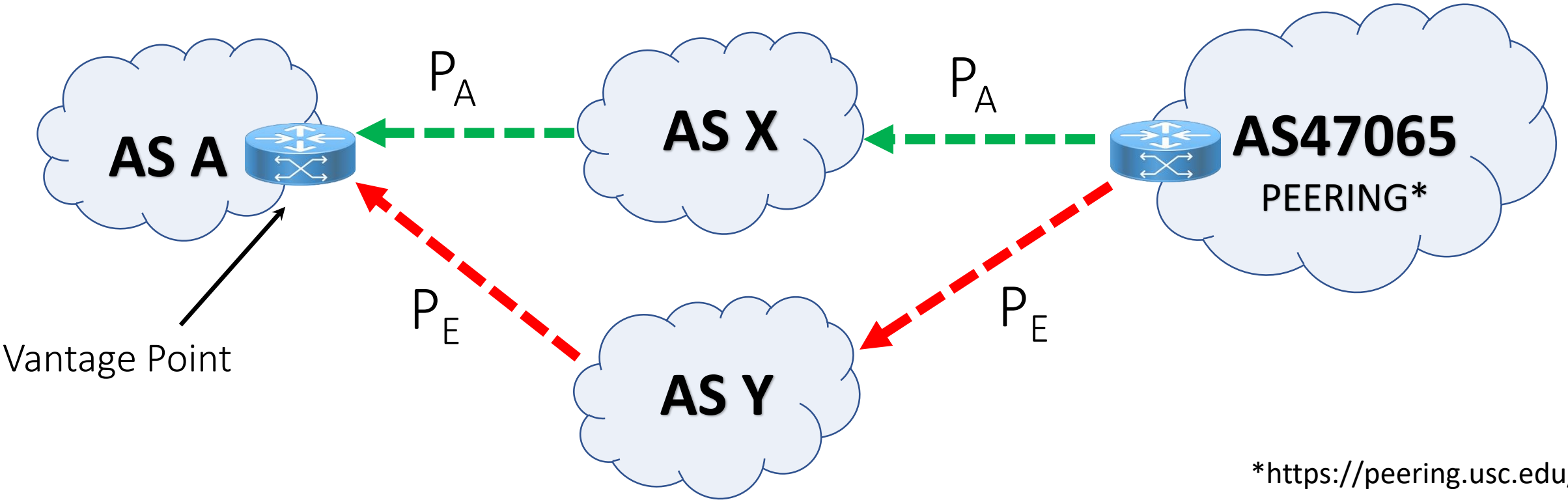
Observation 1: Vantage point exports no route for P_E



*https://peering.usc.edu/

Controlled Experiments

Observation 2: Vantage point exports different route for P_E



*https://peering.usc.edu/

Controlled Experiments

Freie Universität Berlin

Problem

Measuring vantage point AS that is not direct peer introduces ambiguity:

Is the vantage point AS filtering or an intermediate AS?

Controlled Experiments

Freie Universität Berlin

Problem	Solution
Measuring vantage point AS that is not direct peer introduces ambiguity: Is the vantage point AS filtering or an intermediate AS?	Establishing direct peering with vantage point AS *or* Check if intermediate ASes have vantage points

Controlled Experiments Results

Before October 20th 2017:

- Three AS drop invalid routes

October 20th 2017:

- AMS-IX Route Server changes ROV based filtering to ‘opt-out’
- 50+ ASes “drop” invalid routes

Caveat: Technically, using Route Server filtering isn’t “deploying ROV”!

ROV Deployment Monitor

Idea

Give the networking community means to assess state of deployment

➡ Launched rov.rpki.net

ROV Deployment Monitor

https://rov.rpki.net

Show 50 entries Search:

Details	ASN	AS Name	Confidence	Notes	Feedback
	38880	M21-AS-AP Micron21 Datacentre Pty Ltd, AU	1		
	10026	PACNET Pacnet Global Ltd, JP	0.957747		
	42541	FIBERBY, DK	0.957747		
	13237	LAMBDANET-AS European Backbone of AS13237, DE	0.957747		
	3267	RUNNET, RU	0.957747		
	63956	COLO-AS-AP Colocation Australia Pty Ltd, AU	0.957747		
	37100	SEACOM-AS, MU	0.957747		

Implements our measurement methodology.

Table with AS that have deployed ROV.

Updated daily.

ROV Deployment Monitor

https://rov.rpki.net

⛔	10026	PACNET Pacnet Global Ltd, JP	0.957747	🏷	✉

Vantage Point IP	Days Measured	Days Filtering	Confidence	Last Measured	Last Marked	Details
202.147.61.12	71	68	0.957747	2018-05-01	2018-04-30	Details
45.127.172.44	71	68	0.957747	2018-05-01	2018-04-30	Details

Details show vantage points of AS

Data Plane

Idea: Complementary Measurements

Using RIPE Atlas, traceroute towards prefixes P_A and P_E

Data Plane

Idea: Complementary Measurements

Using RIPE Atlas, traceroute towards prefixes P_A and P_E

Successful traceroute to P_A
+
Unsuccessful traceroute to P_E when routes are invalid

Data Plane

Idea: Complementary Measurements

Using RIPE Atlas, traceroute towards prefixes P_A and P_E

Successful traceroute to P_A
+
Unsuccessful traceroute to P_E when routes are invalid

= Some AS on path is using ROV!

Data Plane

Idea: Complementary Measurements

Using RIPE Atlas, traceroute towards prefixes P_A and P_E

Successful traceroute to P_A
+
Unsuccessful traceroute to P_E when routes are invalid

= Some AS on path is using ROV!

Note: False negatives are possible because of default routes!

Conclusion

Freie Universität Berlin

Conclusion

- Controlled experiments are crucial to measuring adoption of ROV-based filtering policies

Conclusion

- Controlled experiments are crucial to measuring adoption of ROV-based filtering policies
- There are ASes that do ROV-based filtering.

  Before Oct. 2017: At least 3 AS drop invalids

  After Oct. 2017: 50+ AS drop invalids via Route Server@AMSIX

Conclusion

- Controlled experiments are crucial to measuring adoption of ROV-based filtering policies
- There are ASes that do ROV-based filtering.

  Before Oct. 2017: At least 3 AS drop invalids

  After Oct. 2017: 50+ AS drop invalids via Route Server@AMSIX
- IXP offering ROV at Route Servers can boost deployment

Conclusion

Please peer with PEERING* and Route Collectors!

Questions?

*https://peering.usc.edu/

ROV Deployment Monitor: rov.rpki.net
More details about methodology: ACM CCR 48(1)

Reference

Andreas Reuter, Randy Bush, Italo Cunha, Ethan Katz-Bassett, Thomas C. Schmidt, Matthias Wählisch, **Towards a Rigorous Methodology for Measuring Adoption of RPKI Route Validation and Filtering**, *ACM SIGCOMM Computer Communication Review,* Vol. **48**, No. 1, pp. 19-27, Jan. 2018.

Towards a Rigorous Methodology for Measuring Adoption of RPKI Route Validation and Filtering

Andreas Reuter
Freie Universität Berlin
andreas.reuter@fu-berlin.de

Randy Bush
IIJ Research Lab / Dragon Research
randy@psg.com

Italo Cunha
Universidade Federal de Minas Gerais
cunha@dcc.ufmg.br

Ethan Katz-Bassett
Columbia University
ethan@ee.columbia.edu

Thomas C. Schmidt
HAW Hamburg
t.schmidt@haw-hamburg.de

Matthias Wählisch
Freie Universität Berlin
m.waehlisch@fu-berlin.de

ABSTRACT

A proposal to improve routing security—Route Origin Authorization (ROA)—has been standardized. A ROA specifies which network is allowed to announce a set of Internet destinations. While some networks now specify ROAs, little is known about whether other networks check routes they receive against these ROAs, a process known as Route Origin Validation (ROV). Which networks blindly accept invalid routes? Which reject them outright? Which de-preference them if alternatives exist?

Recent analysis attempts to use uncontrolled experiments to characterize ROV adoption by comparing valid routes and invalid routes [5]. However, we argue that gaining a solid understanding of ROV adoption is impossible using currently available data sets and techniques. Instead, we devise a verifiable methodology of controlled experiments for measuring ROV. Our measurements suggest that, although some ISPs are not observed using invalid routes in uncontrolled experiments, they are actually using different routes for (non-security) traffic engineering purposes, without performing ROV. We conclude with presenting three AS that do implement ROV as confirmed by the operators.

CCS CONCEPTS

• **Networks** → **Routing protocols**; **Network measurement**; **Security protocols**; *Public Internet*;

KEYWORDS

BGP, RPKI, routing policies, Internet security

1 INTRODUCTION

The Border Gateway Protocol (BGP) [17] is responsible for establishing Internet routes, yet it does not check that routes are valid. An autonomous system (AS) can hijack destinations it does not control by announcing invalid routes to them, either intentionally or unintentionally, as in the well-known accidental announcement of YouTube's address space by Pakistan Telecom [2].

Because this critical aspect of the Internet is vulnerable, there are proposals to improve routing security [7], and one—the RPKI—is standardized and is in early adoption. The Resource Public Key Infrastructure (RPKI) [12] is a specialized PKI to help secure Internet interdomain routing by providing attestation objects for Internet resource holders (*i.e.*, IP prefixes and AS numbers). The RPKI publishes Route Origin Authorization (ROA) objects, each specifying which AS is allowed to announce an IP prefix. Using ROA data, a BGP router can perform RPKI-based origin validation (ROV) verifying whether the AS originating an IP prefix announcement in BGP is authorized to do so [14] and labeling the route as valid or invalid. The validity of a route can be used as part of the router's local BGP policy decisions, *e.g.*, filtering routes that reflect invalid announcements or preferring valid ones. While the RPKI is fairly populated with ROAs and growing [9, 15, 23, 24], adoption of ROV and filtering has been negligible, according to operator gossip. A major reason for this is the lack of economic incentives. Since a significant share of invalid routes are due to misconfiguration [23], adopting ROV and filtering can even have adverse effects such as a loss of connectivity to legitimate network destinations.

A recent paper examined RPKI and ROV adoption from multiple angles, focusing on the slow state of ROV adoption, the security implications of partial adoption, and reasons for slow adoption. The paper also identifies an attack vector that exploits *loose* ROAs to hijack traffic of a RPKI-secured prefix [5]. To capture the current state of limited adoption, the paper included a measurement study that claimed that most large AS had not deployed ROV, but that 9 of the 100 largest AS had. This result was based on observations of existing BGP routes from BGP route collectors, meaning that the experiments were uncontrolled. At a basic level, the approach finds an AS that originates both valid and invalid announcements, then identifies other AS that appear on paths towards the valid prefix but not on paths towards the invalid prefix. It then assumes these AS are performing ROV to filter invalid routes.

In this paper, we contribute a verifiable methodology for measuring ROV after demonstrating that the above approach to identify ROV adoption, based on passive observation of routes in uncontrolled experiments [5], has three major limitations. First, our measurements show that its characterizations of some networks change depending on which set of BGP collectors is used, inferring ROV adoption in some cases when

Freie Universität Berlin

Backup

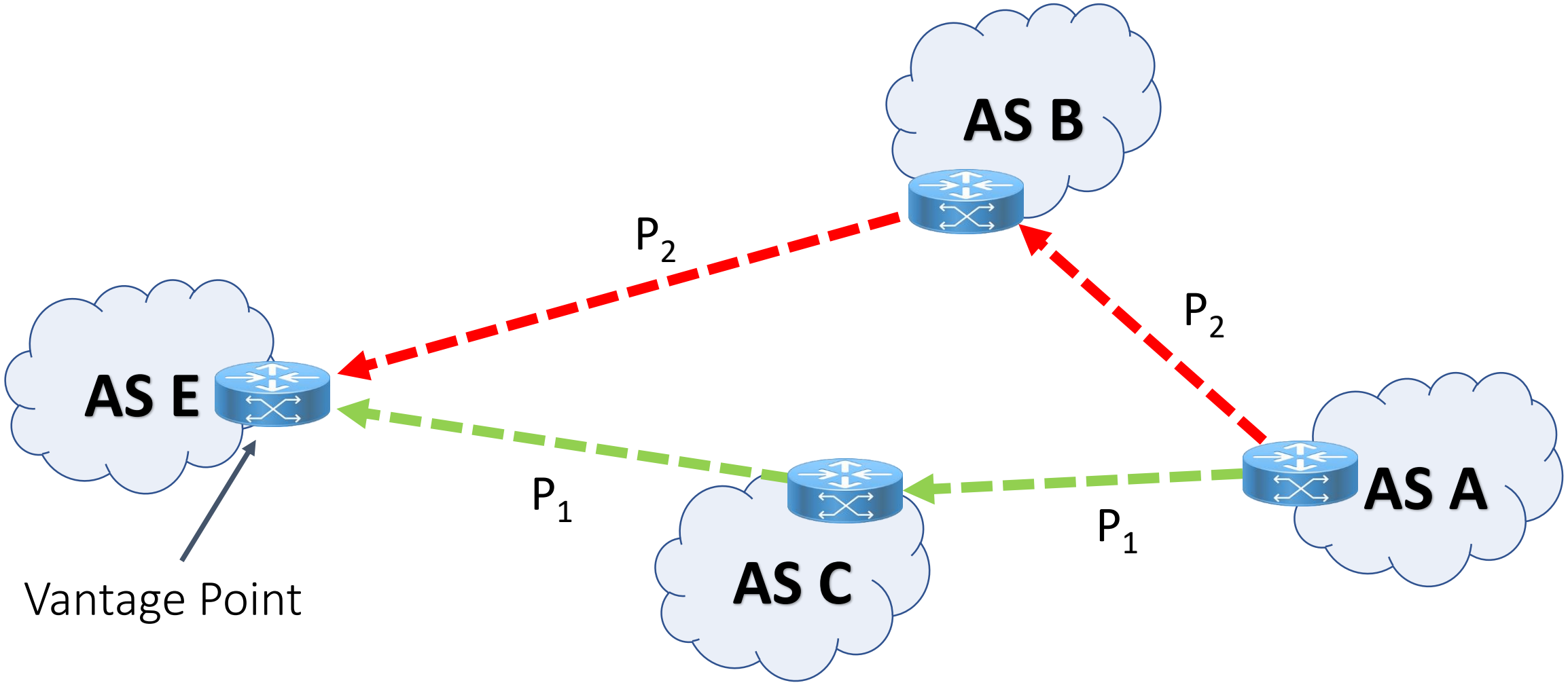
Uncontrolled Experiments

Limited Control	Don’t know origin AS policy Can’t distinguish between ROV-filtering and other filtering
Limited Visibility	Incomplete data can lead to misclassification
Reproducibility	No

Controlled: Advantages

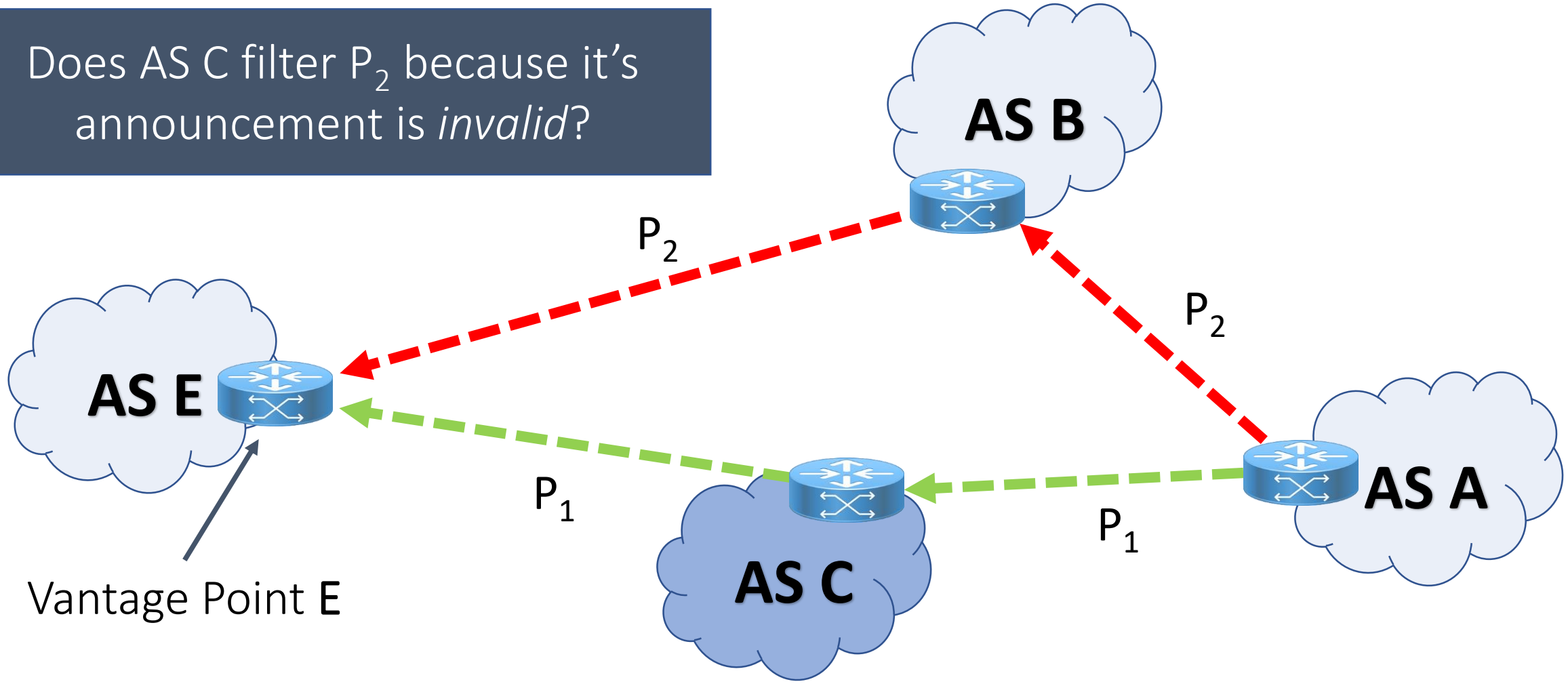
Limited Control	Control origin AS policy, can announce own routes Can distinguish ROV-filtering by changing route RPKI state
Limited Visibility	Less of an issue: Only care about our routes
Reproducibility	Yes

Uncontrolled Experiments

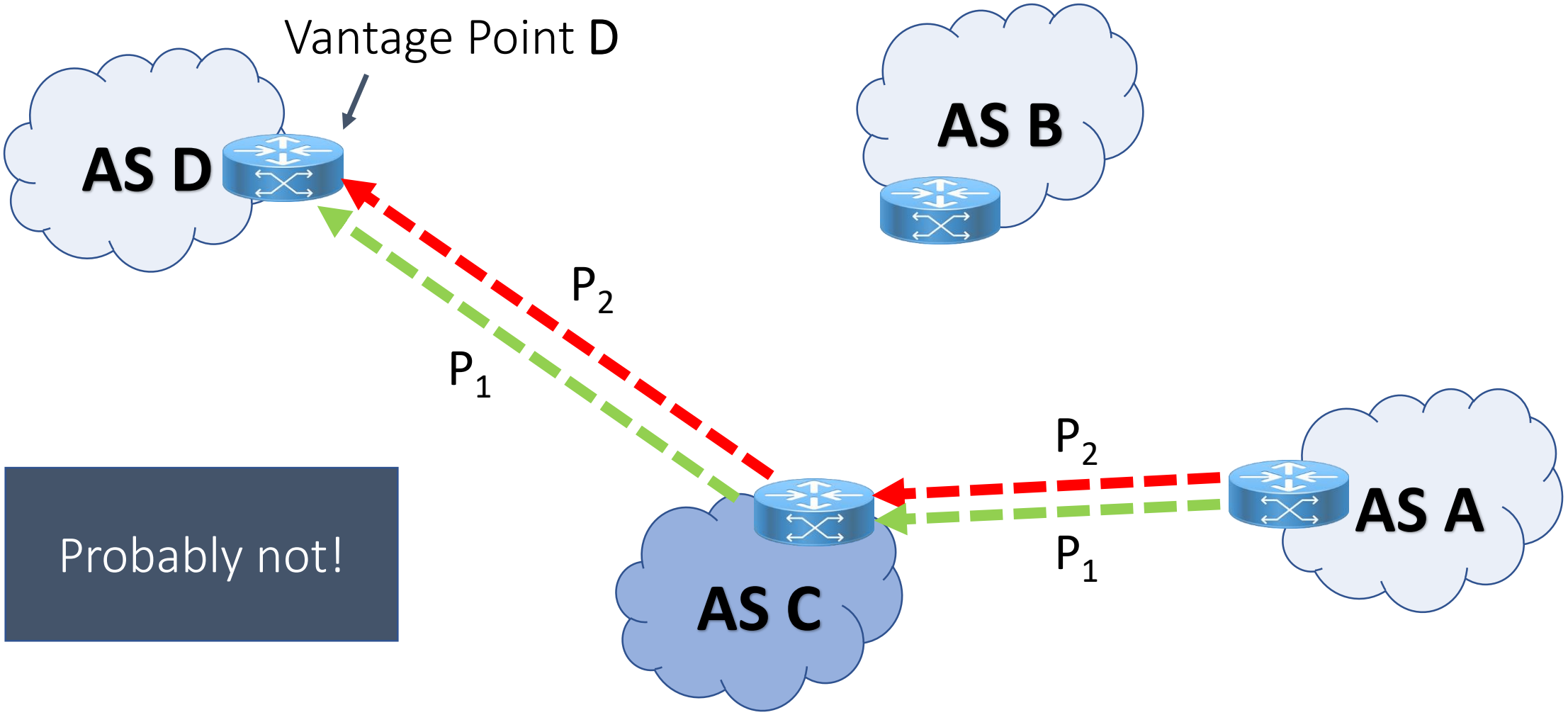


Uncontrolled Experiments

Does AS C filter P_2 because it's announcement is *invalid*?

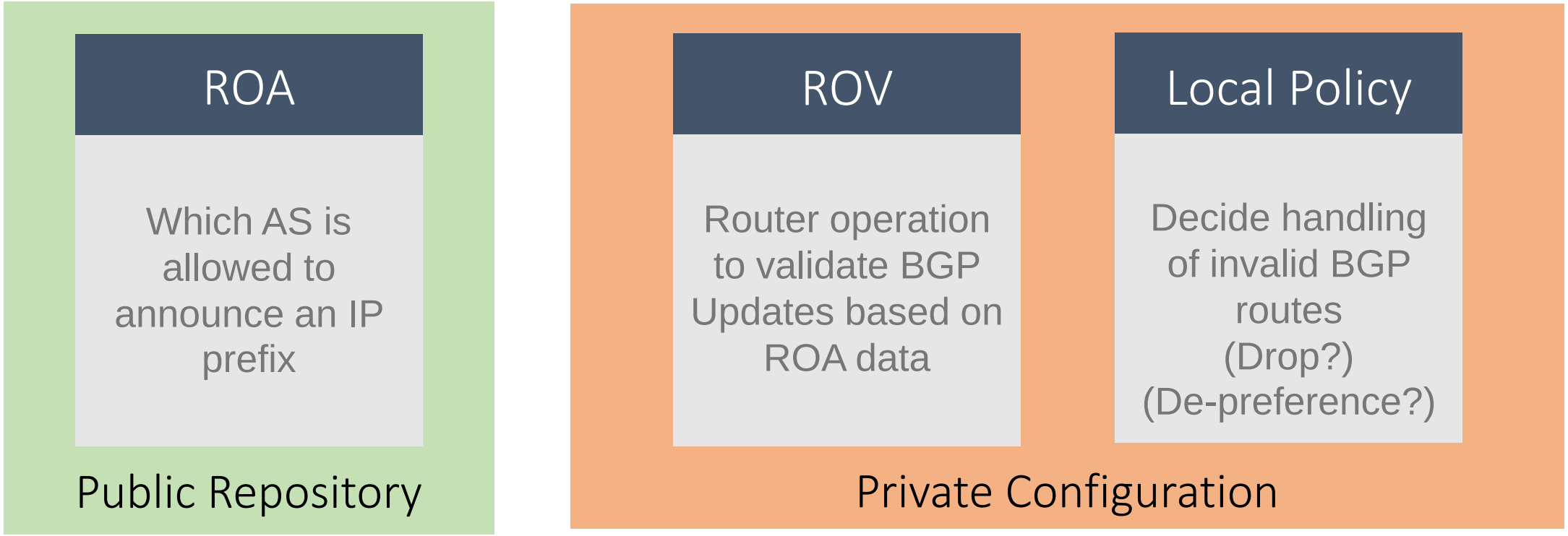


Uncontrolled Experiments



Research Problem

Goal: Measure the adoption of ROV-based filtering policies



Challenge: Private policies must be inferred from measurements