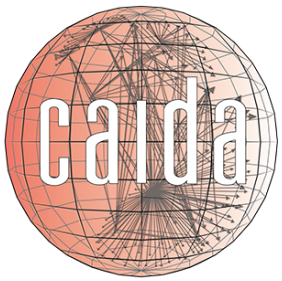
Challenges in Inferring Spoofed Traffic at IXPs

Lucas Müller, Matthew Luckie, Bradley Huffaker,
Kc Claffy, **Marinho Barcellos**

{lfmuller, marinho}@inf.ufrgs.br

Federal University of Rio Grande do Sul (INF/UFRGS)
Center for Applied Internet Data Analysis (CAIDA/UC San Diego)



September 09, 2019

Recent DDoS incidents

Recent DDoS incidents

Recent DDoS incidents

LILY HAY NEWMAN SECURITY 03.01.18 11:01 AM

GITHUB SURVIVED THE BIGGEST DDOS ATTACK EVER RECORDED

CLOUDFLARE BLOG WHAT WE DO SUPPORT COMMUNITY

400Gbps: Winter of Whopping Weekend DDoS Attacks

03 Mar 2016 by Marek Majkowski.

NETSCOUT Arbor Confirms 1.7 Tbps DDoS Attack; The Terabit Attack Era Is Upon Us

Carlos Morales on March 5, 2018.

Security

How many Internet of S**t devices knocked out Dyn? Fewer than you may expect

DNS *really* needs to be fixed if it can be taken out by 100,000 home devices

Rio 2016 Olympics Suffered Sustained 540Gbps DDoS Attacks

Ben Sullivan, August 31, 2016, 5:31 pm

B

Brazil hit by 30 DDoS attacks per hour in 2017

The country is part of a global ranking of the five nations most targeted by cybercriminals, says study.

By Angelica Mari for Brazil Tech | February 21, 2018 -- 14:59 GMT (06:59 PST) | Topic: Security

Recent DDoS incidents

LILY HAY NEWMAN SECURITY 03.01.18 11:01 AM

GITHUB SURVIVED THE BIGGEST DDOS ATTACK EVER RECORDED

CLOUDFLARE BLOG WHAT WE DO SUPPORT COMMUNITY

400Gbps: Winter of Whopping Weekend DDoS Attacks

03 Mar 2016 by Marek Majkowski.

NETSCOUT Arbor Confirms 1.7 Tbps DDoS Attack; The Terabit Attack Era Is Upon Us

Carlos Morales on March 5, 2018.

Security

How many Internet of S**t devices knocked out Dyn? Fewer than you may expect

DNS *really* needs to be fixed if it can be taken out by 100,000 home devices

Rio 2016 Olympics Suffered Sustained 540Gbps DDoS Attacks

Ben Sullivan, August 31, 2016, 5:31 pm

Brazil hit by 30 DDoS attacks per hour in 2017

The country is part of a global ranking of the five nations most targeted by cybercriminals, says study.

By Angelica Mari for Brazil Tech | February 21, 2018 -- 14:59 GMT

US service provider survives the biggest recorded DDoS in history

Nearly 100,000 memcached servers are imperiling the stability of the Internet.

DAN GOODIN - 3/5/2018, 1:24 PM

Recent DDoS incidents

LILY HAY NEWMAN SECURITY 03.01.18 11:01 AM

GITHUB SURVIVED THE BIGGEST DDOS ATTACK EVER RECORDED

CLOUDFLARE BLOG WHAT WE DO SUPPORT COMMUNITY

400Gbps: Winter of Whopping W

03

CLOUDFLARE BLOG WHAT WE DO SUPPORT COMMUNITY

The real cause of large DDoS - IP Spoofing

06 Mar 2018 by Marek Majkowski.

Security

How ma knocked expect

DNS *really* by 100,000

Brazil hit by 30 DDoS attacks per hour in 2017

The country is part of a global ranking of the five nations most targeted by cybercriminals, says study.

By Angelica Mari for Brazil Tech | February 21, 2018 -- 14:59 GMT

irms The pon Us

ympics stained DoS Attacks

Ben Sullivan, August 31, 2016, 5:31 pm

US service provider survives the biggest recorded DDoS in history

Nearly 100,000 memcached servers are imperiling the stability of the Internet.

DAN GOODIN - 3/5/2018, 1:24 PM

IP Spoofing is an old problem

- 1998 — Network Ingress Filtering (RPF) - RFC2267
- 2000 — BCP38 - RFC2827
- 2004 — BCP84 for multi-homed — RFC3704
- 2005 — Spoofer (Berverly, Bauer)
- 2009 — IETF SAVI wg (until 2015)
- 2014 — MANRS Project, Anti-spoofing
- 2015 — CAIDA Spoofer Project

two decades reliably providing the basis for DDoS attacks…

IP spoofing
made possible because of
lack of filtering

Source **A**ddress **V**alidation

Our investigation

design and develop a methodology to identify spoofed traffic crossing an IXP and infer lack of SAV

we imagine it as part of a suite of
cybersecurity services or compliance practices of modern IXPs
in line with efforts to improve Internet security

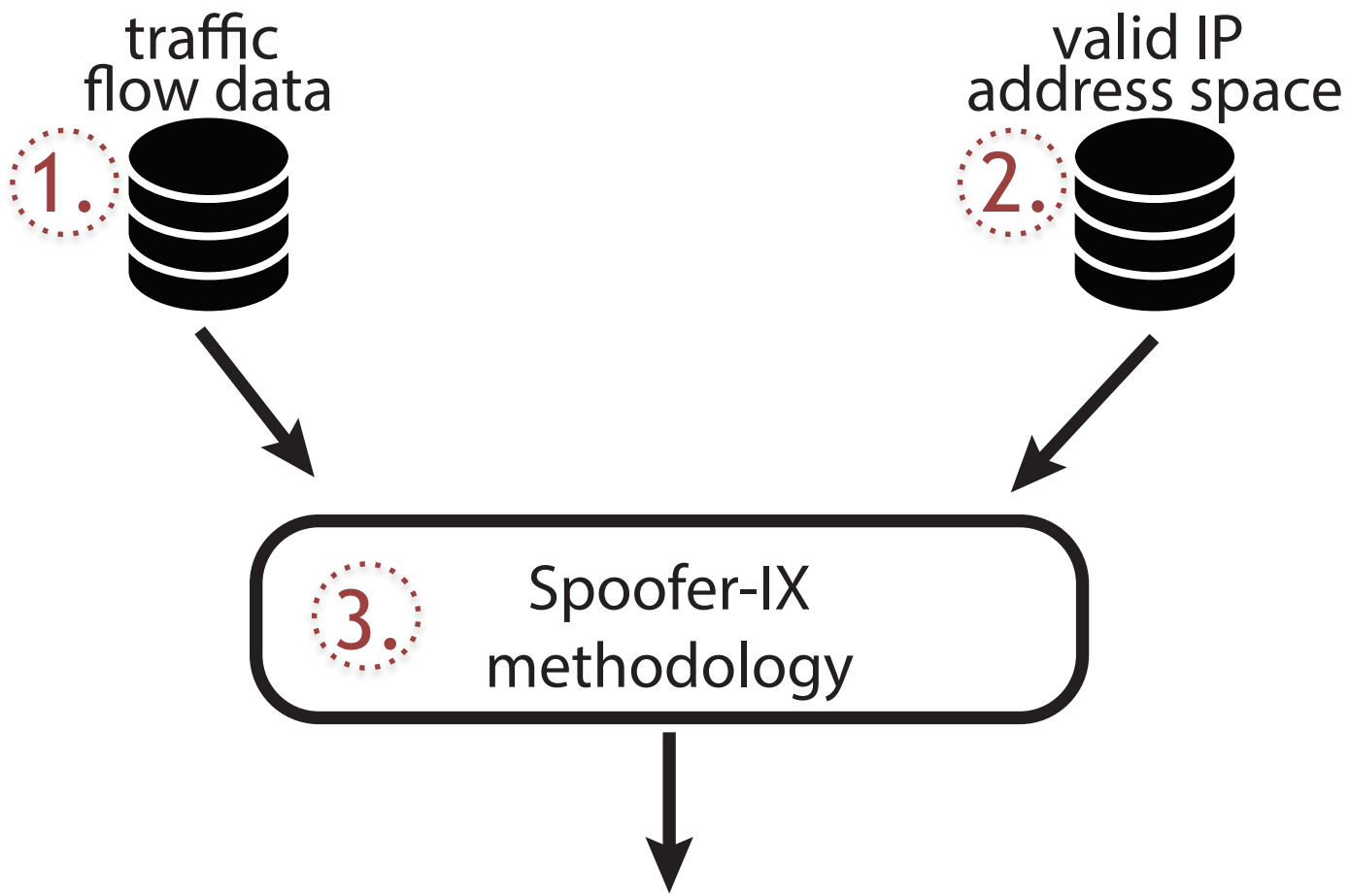
Three contributions

1. **Analysis of Challenges**
   provide a detailed analysis of methodological challenges for inferring spoofed packets at IXPs

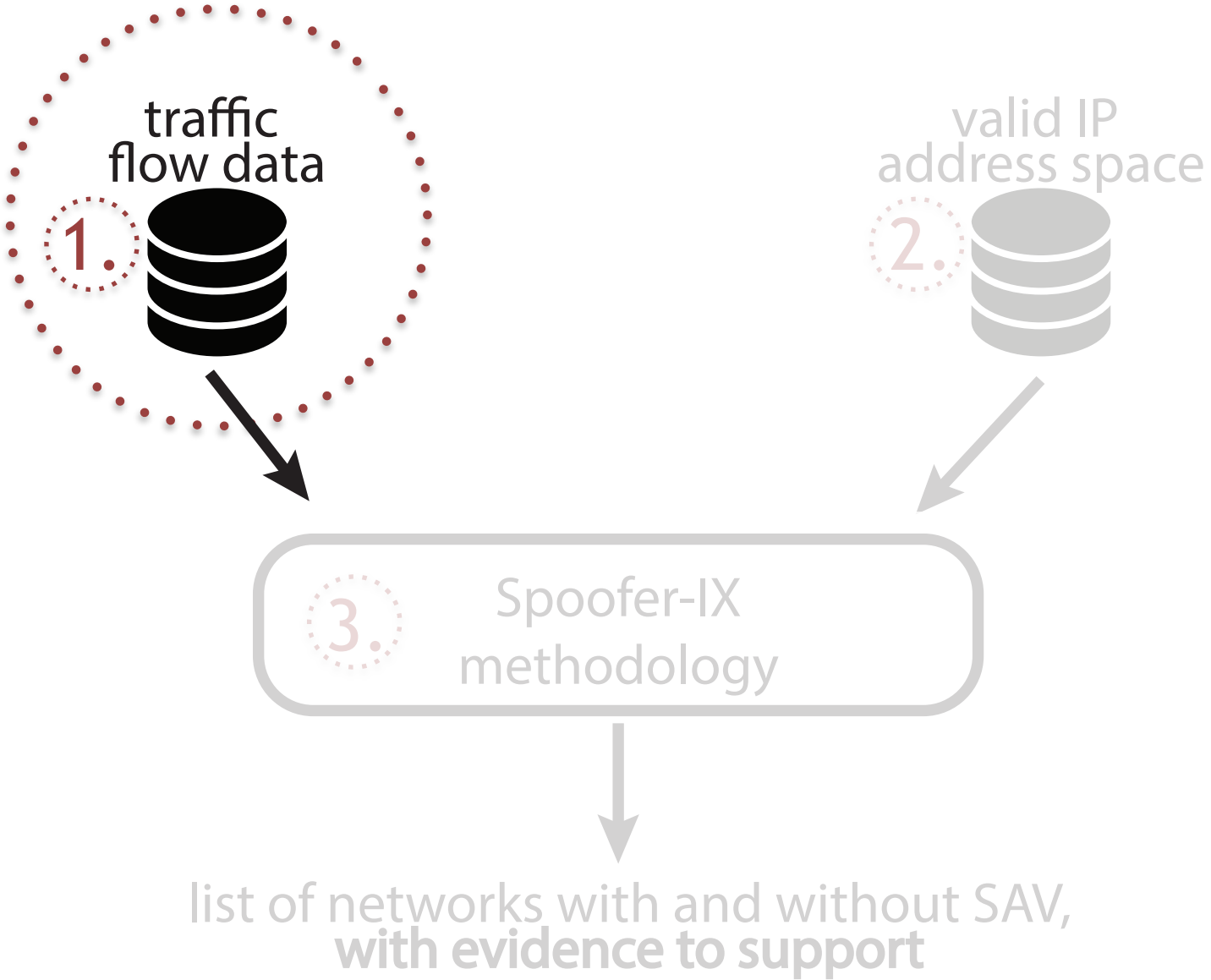
2. **Methodology**
   design and implement **Spoofer-IX**, a novel methodology to accurately detect the transmission of spoofed traffic (which implies lack of source address validation) by AS members of IXPs

3. **Observations**
   apply our method to traffic and topology data from one of the largest IXPs in Brazil, with more than 200 member ASes using the IXP switching fabric

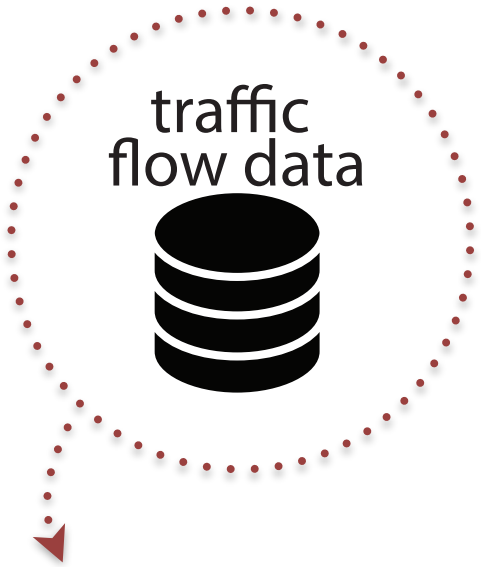
Bird's eye view of Spoofer-IX



Spoofer-IX inputs: traffic flow data



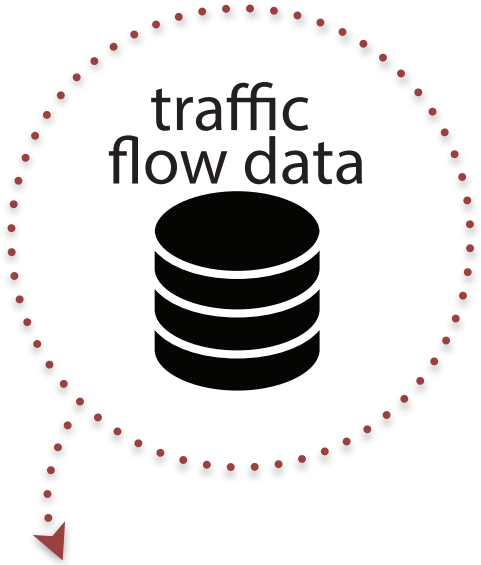
Spoofer-IX inputs: traffic flow data



To avoid sparse data points and to increase the visibility into the spoofing problem

IXP as an observatory

Spoofer-IX inputs: traffic flow data

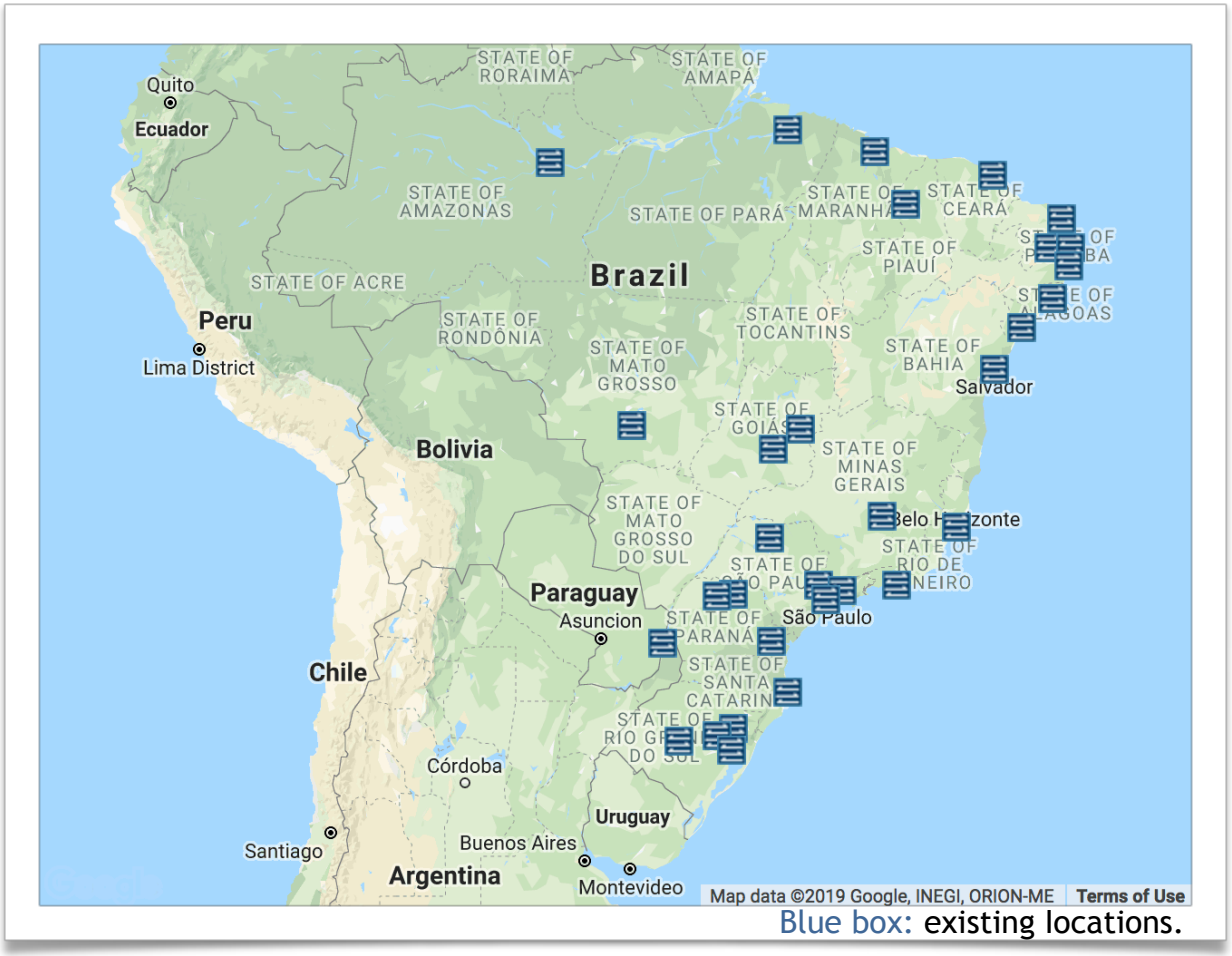


To avoid sparse data points and to increase the visibility into the spoofing problem

IXP as an observatory

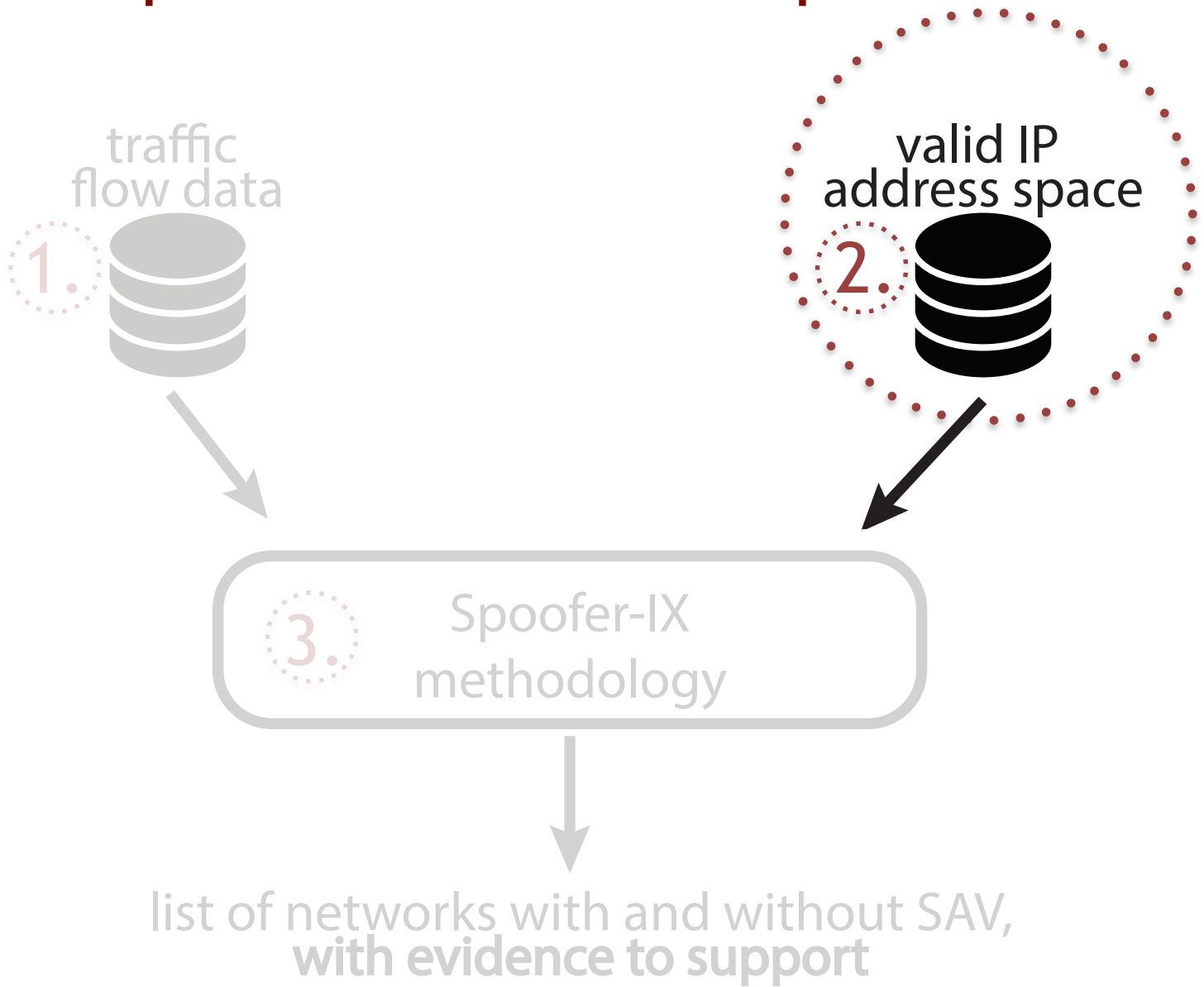
Brazilian IX.br ecosystem

- **31 IXPs** unevenly distributed in 27 states
- total of **~2500 member ASes**
- **6.28 Tbps** max traffic peak

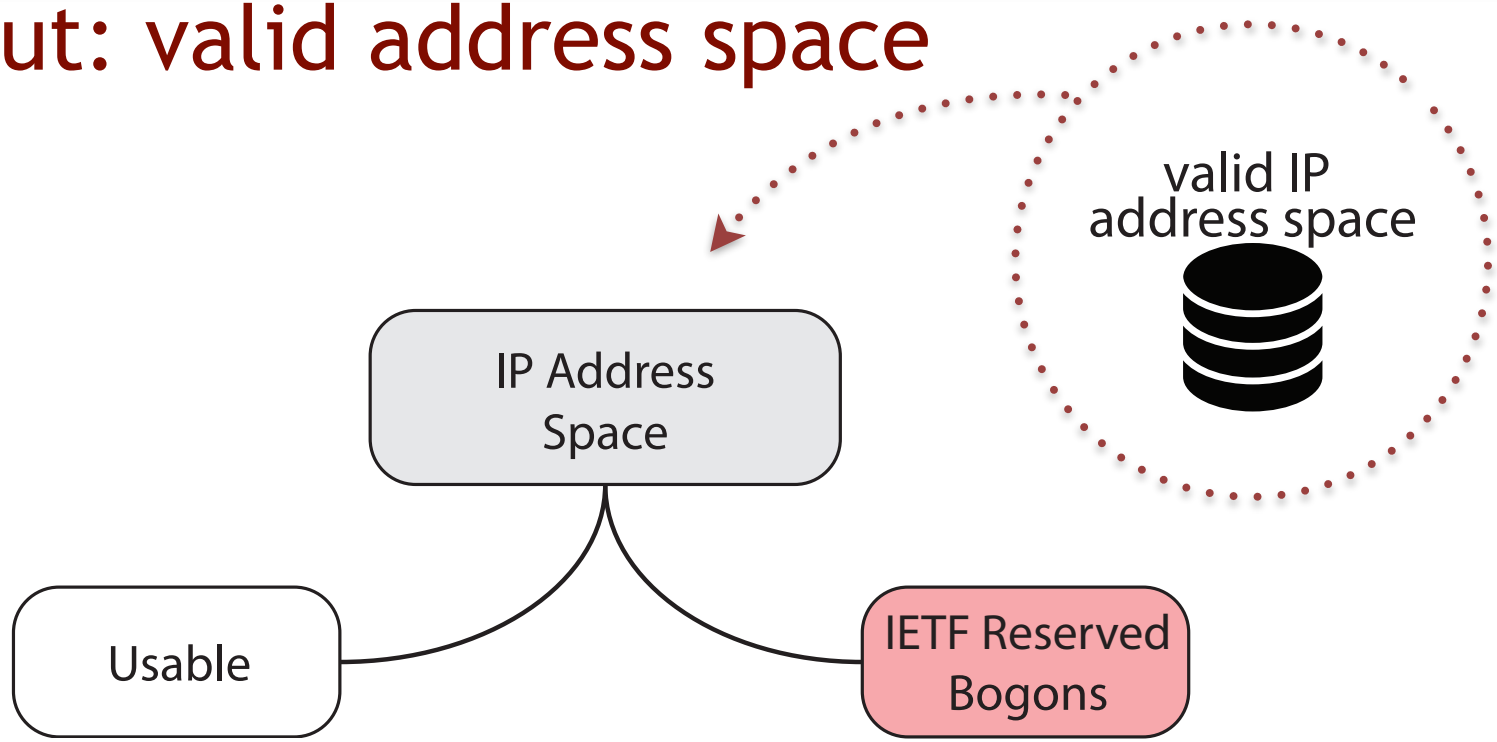


Blue box: existing locations.

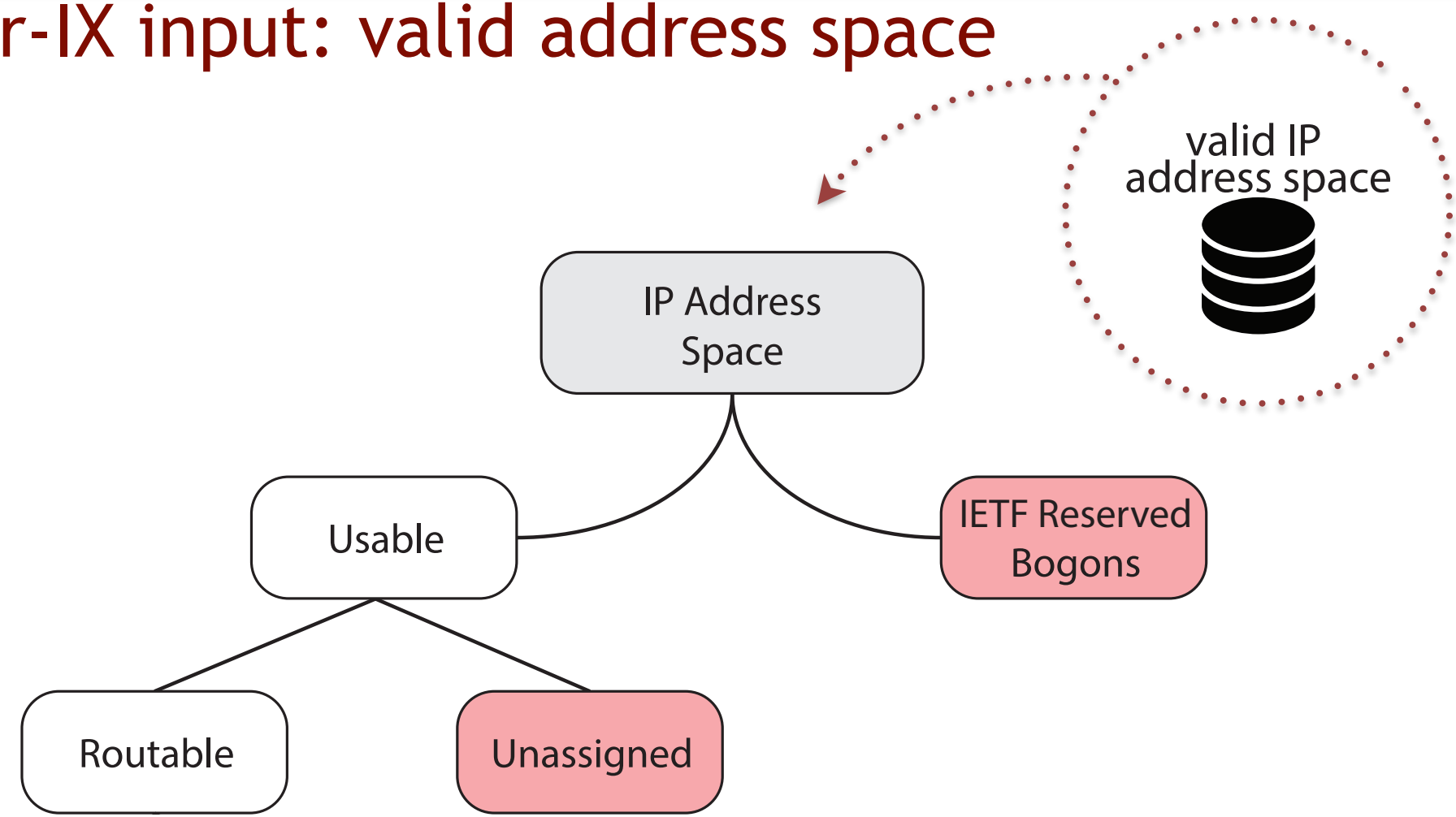
Spoofer-IX input: valid address space



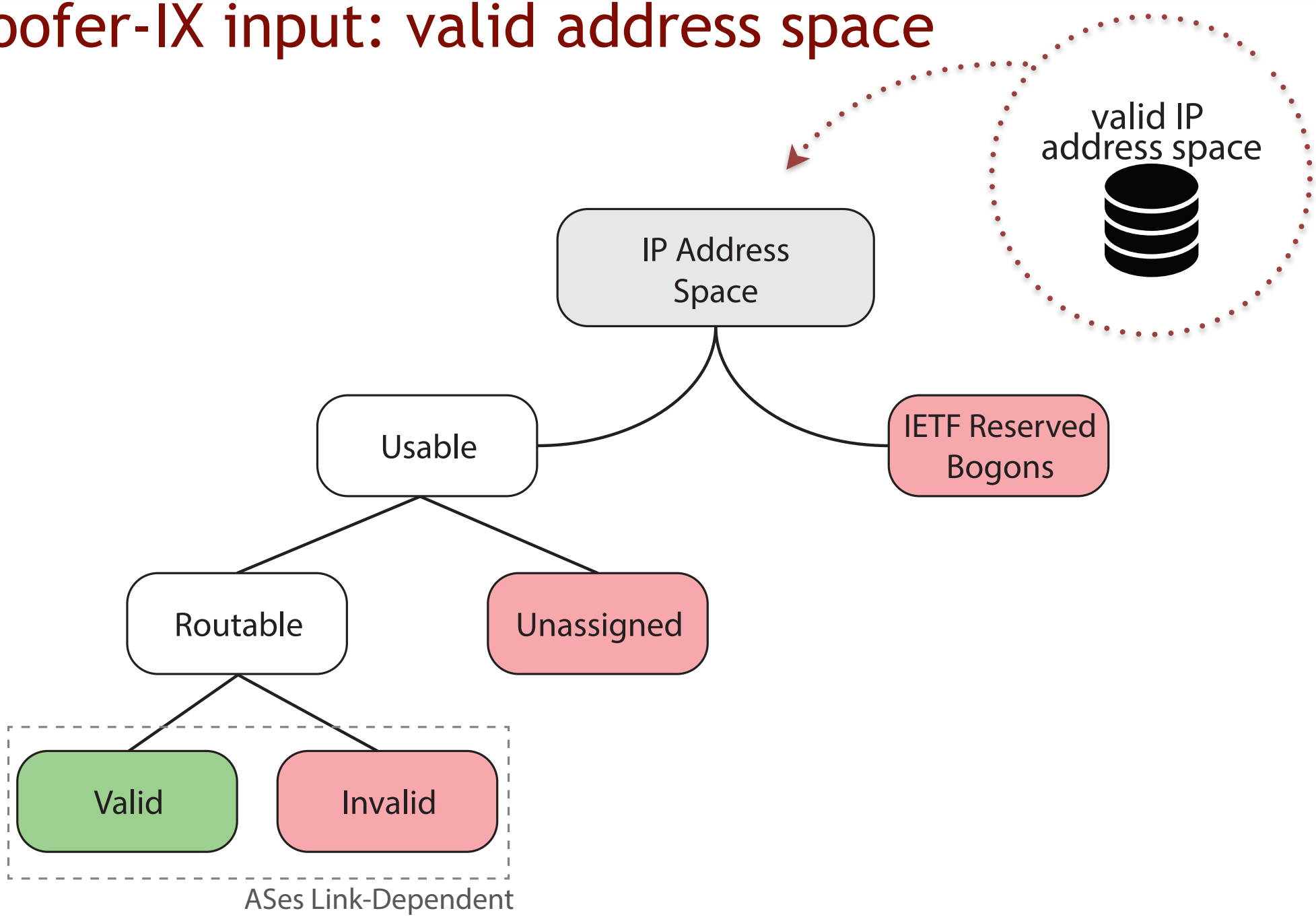
Spoofer-IX input: valid address space



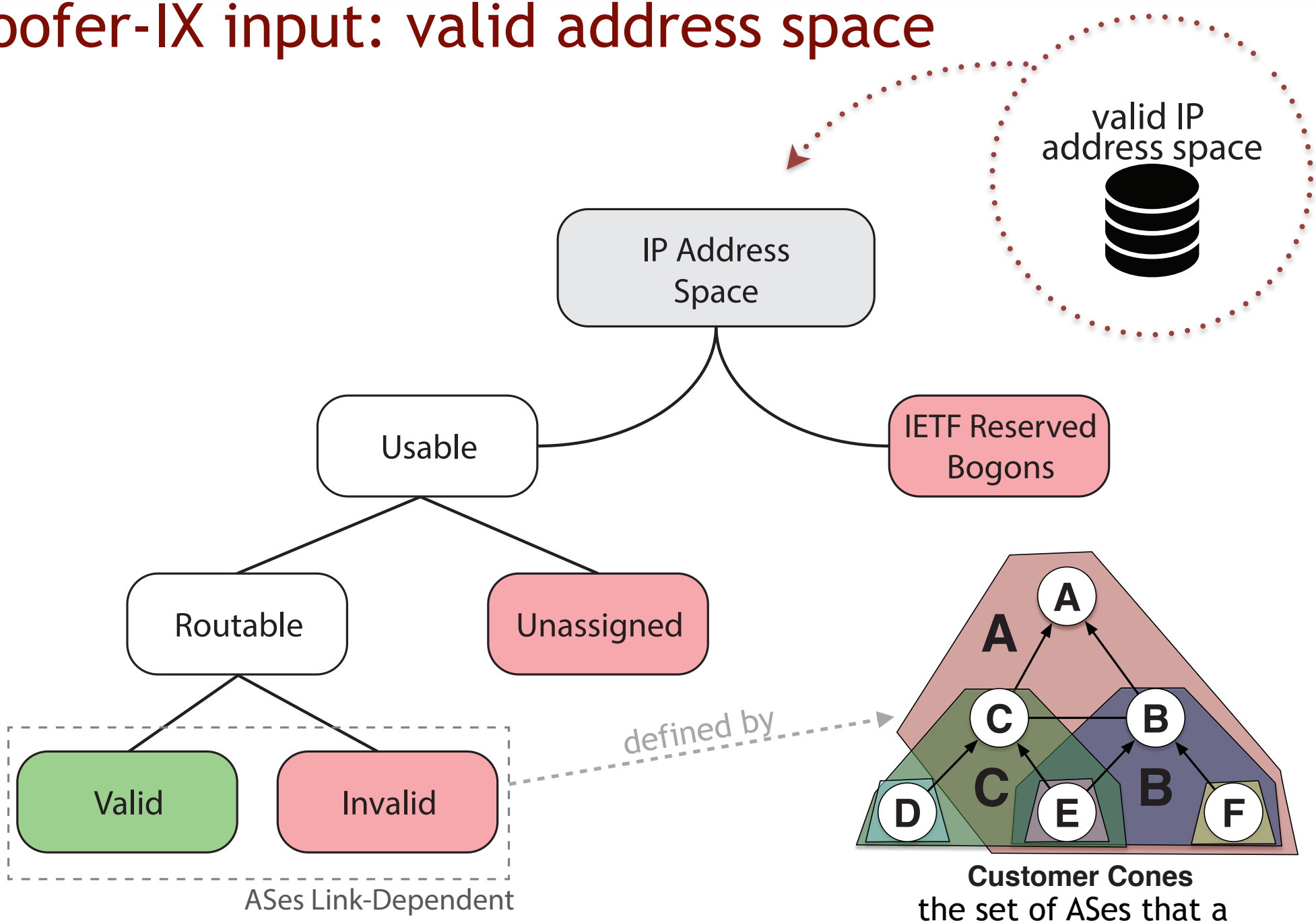
Spoofer-IX input: valid address space



Spoofer-IX input: valid address space

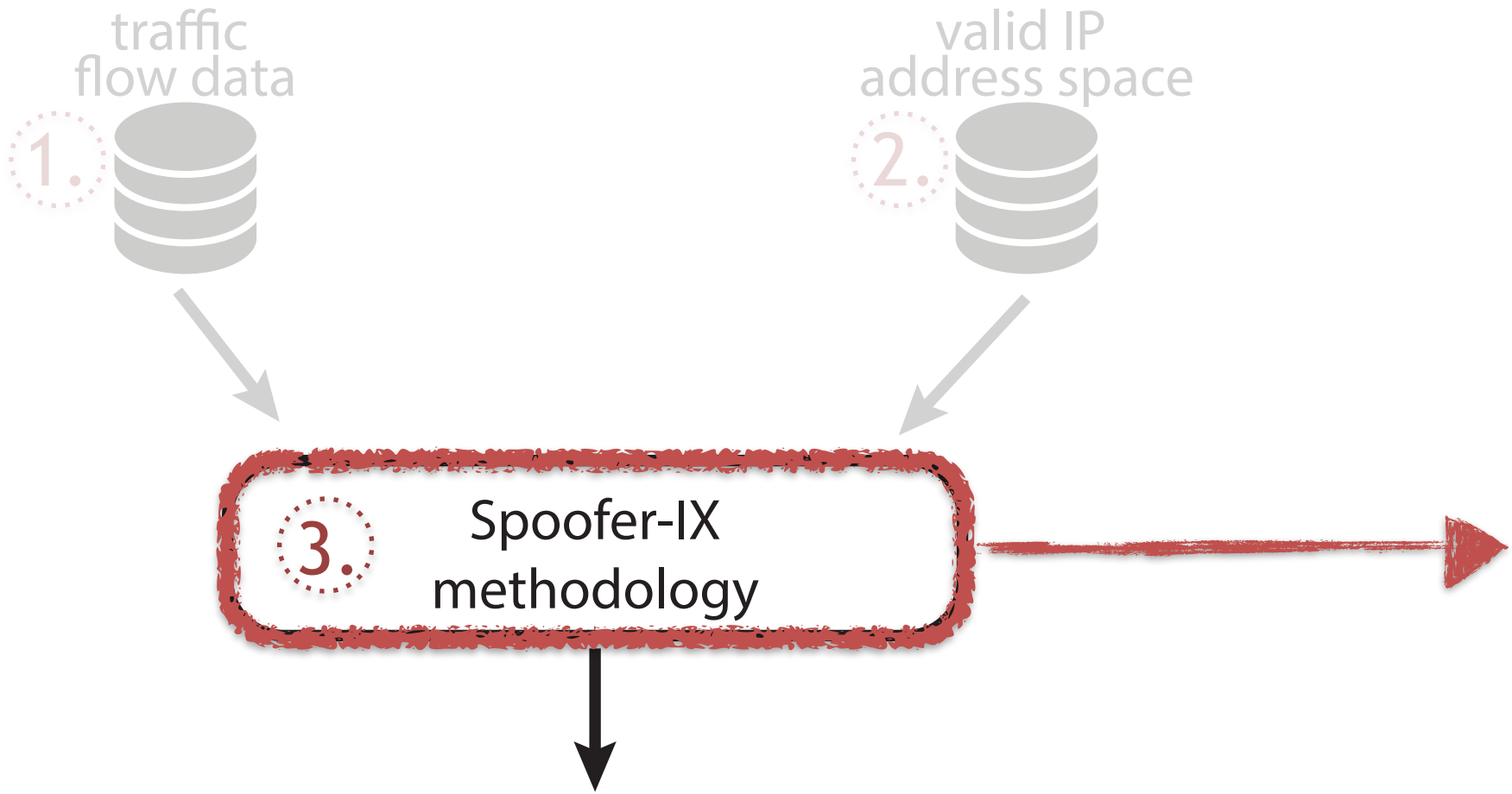


Spoofer-IX input: valid address space

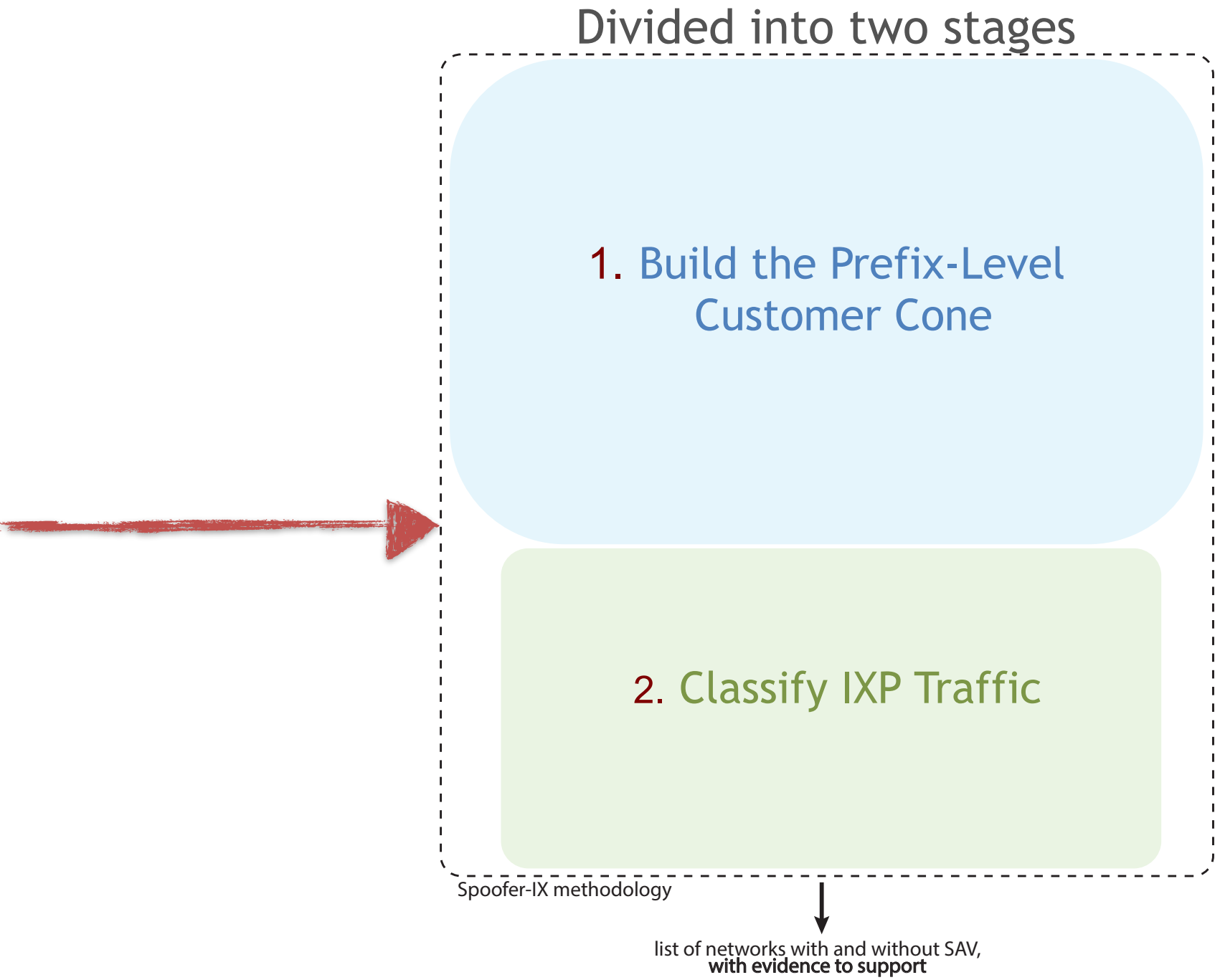


(DIMITROPOULOS et al., 2007; LUCKIE et al., 2013)

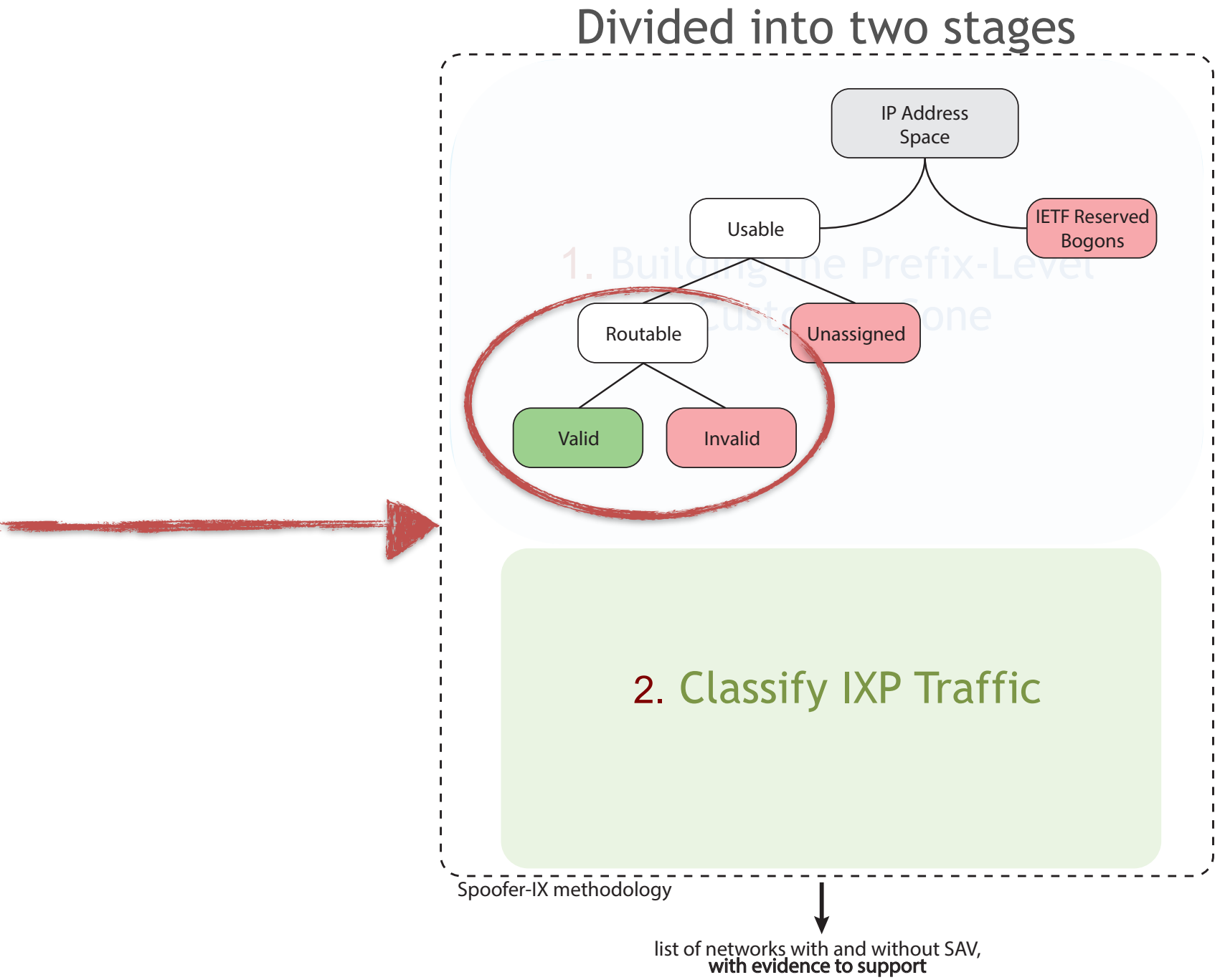
Bird's eye view of Spoofer-IX



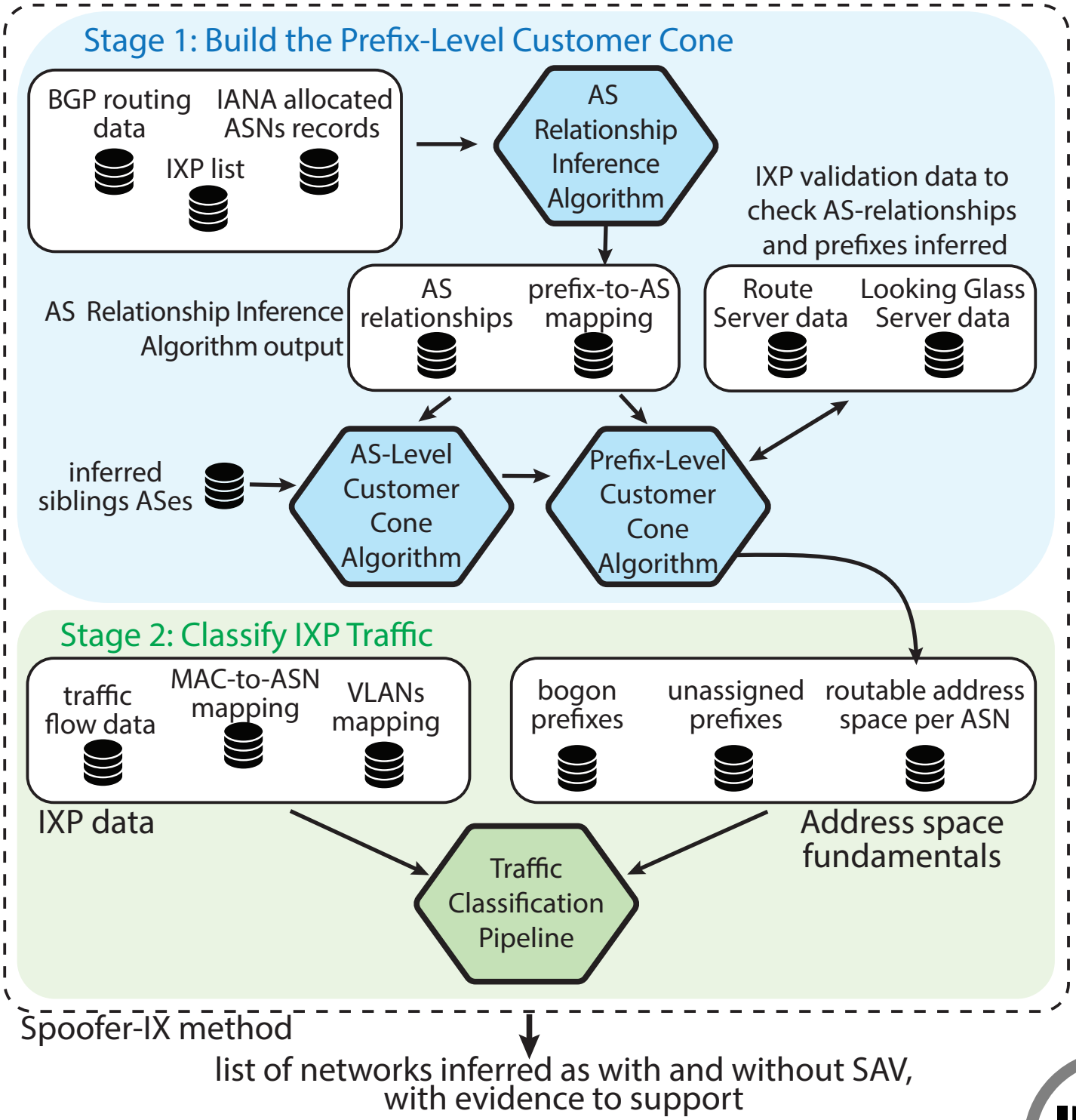
Spoofer-IX Overview



Spoofer-IX Overview



Spoofer-IX Overview



Major Datasets used by Spoofer-IX

IXP-BR: traffic, topology and routing data

Team Cymru: Bogons and Unassigned addresses

Routeviews, RIPE RIS: public BGP Data

CAIDA ITDK: router IP interfaces addresses

Comparing Spoofer-IX with prior work

Few efforts have tried to empirically measure SAV compliance for networks attached to the global Internet

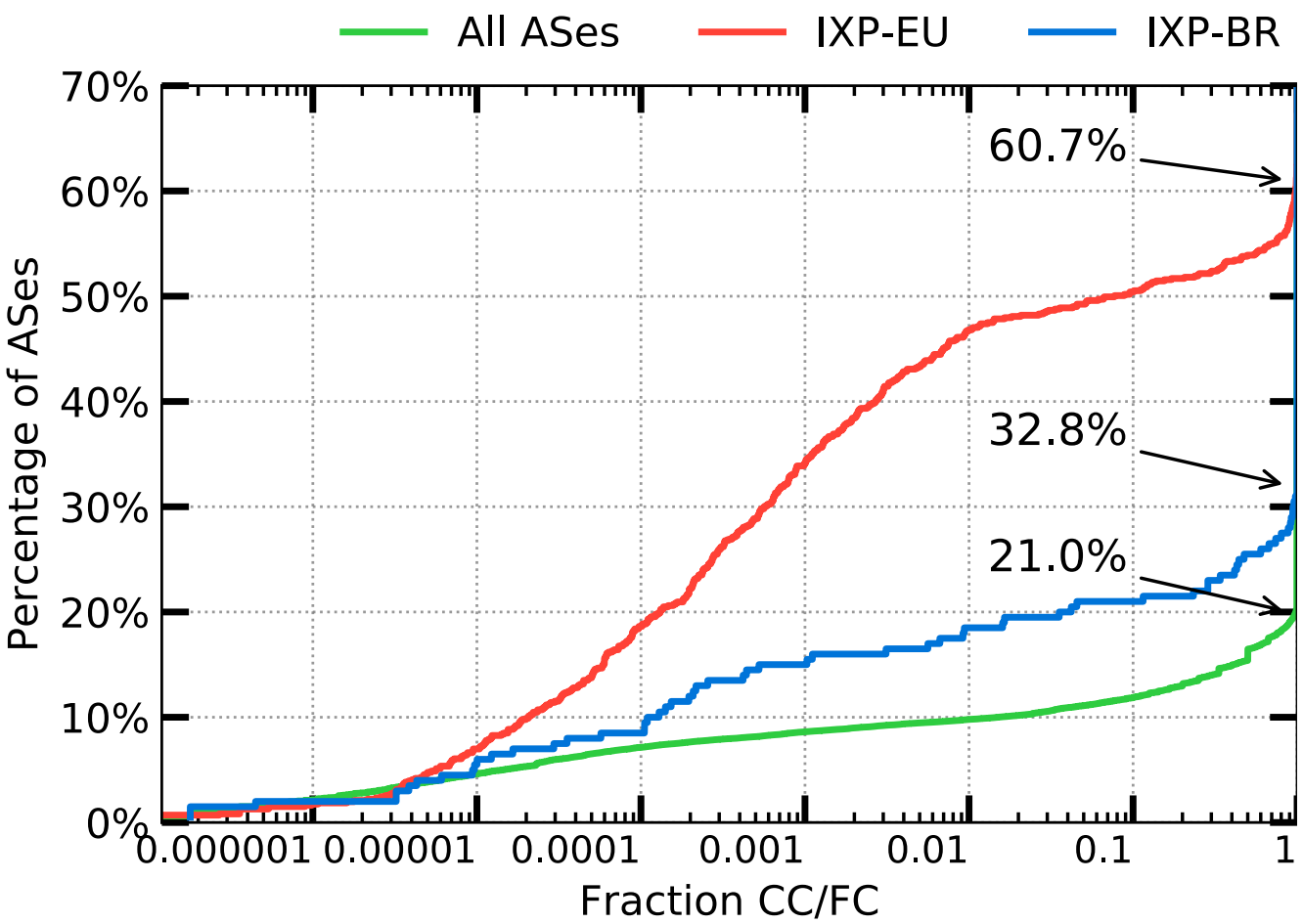
1. Under-explored in the context of IXP
2. There is no validation of previous results
3. No official publicly-shared code to enable research reproducibility

- Lichtblau et al. offers a limited approach
  - Uses a "**Full Cone**" that assumes all BGP paths configurations and announcements are valid
  - Assumes all relationships are equal, i.e., all ASes share all prefixes they can reach with all peers, customers or providers
  - Assumes that all traffic can be validated using the same logical rules

Lichtblau et al. Detection, Classification, and Analysis of Inter-domain Traffic with Spoofed Source IP Addresses. In: ACM IMC, 2017.

Cone Affected by Design Choices

How the two methods behave in terms of the cone sizes (in address space)?



Customer Cone/Full Cone

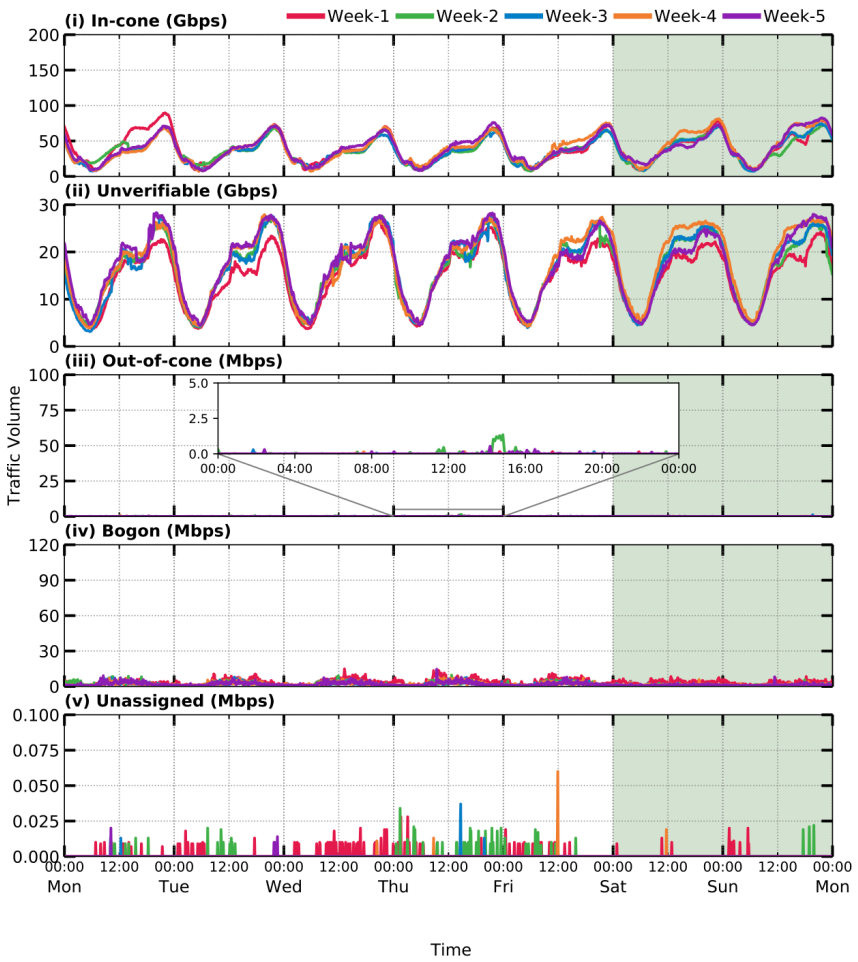
(May 2019)

79% of ASes in the Internet had the same list of prefixes (All ASes) BUT

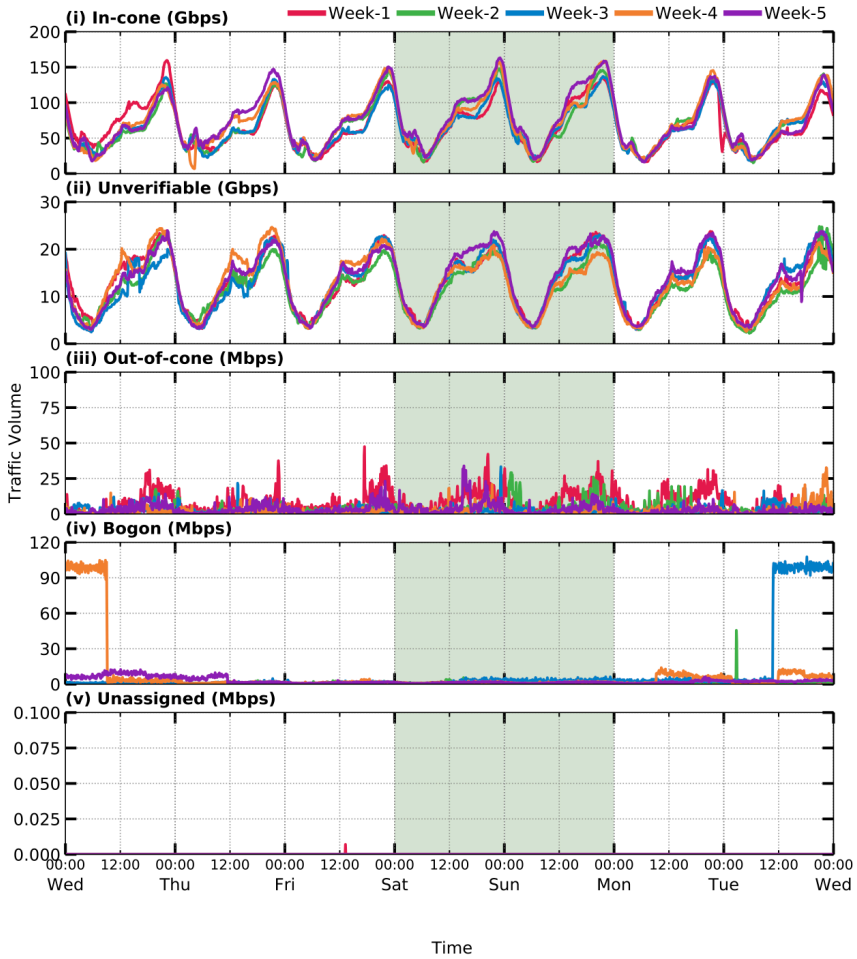
60.7% of the IXP-EU members had a larger list, out of which **40% had a list 100x larger in the FC than the CC**

Traffic Classification 2017 vs 2019

May 1 — Jun 5, 2017



May 1 — Jun 5, 2019



5 weeks in 2017, 5 weeks 2 years later

In-cone, *Unverifiable*, *Out-of-cone*, *Bogon*, *Unassigned*

Unlike prior work, in all 10 weeks we found almost **no Out-of-cone traffic** in 2019 not more than 40Mbps for an IXP with a peak of 200Gbps

Take aways

- It's much **harder** than imagined to identify spoofing
- Requires understanding of underlying IXPs infrastructures and subtleties in the Customer Cone construction
- Developed method for inferring lack of SAV from IXP-aggregated traffic data
- Analyzed and checked method longitudinally from an IXP in Brazil
- *Complement it with data from the Telescope?*

Thanks!

{lfmuller, marinho}@inf.ufrgs.br

INSTITUTO DE INFORMÁTICA UFRGS