Challenges in Inferring Spoofed Traffic at IXPs

Lucas Müller
UFRGS/CAIDA

Matthew Luckie
University of Waikato

Bradley Huffaker
CAIDA/UC San Diego

Kc Claffy
CAIDA/UC San Diego

Marinho Barcellos
UFRGS/University of Waikato

ACM CoNEXT 2019 — Orlando, Florida, U.S.A.
December 9-12, 2019

UFRGS UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

KO TE TANGATA

caida

UC San Diego

Broader visibility of networks that
do not filter spoofed packets

Consequences:
spoofed denial-of-service (DoS) attacks

Consequences:
spoofed denial-of-service (DoS) attacks

LILY HAY NEWMAN SECURITY 03.01.18 11:01 AM

GITHUB SURVIVED THE BIGGEST DDOS ATTACK EVER RECORDED

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.

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

Consequences:
spoofed denial-of-service (DoS) attacks

LILY HAY NEWMAN SECURITY 03.01.18 11:01 AM

GITHUB SURVIVED THE BIGGEST DDOS ATTACK EVER RECORDED

Bezos DDoS'd: Amazon Web Services' DNS systems knackered by hours-long cyber-attack

Distributed assault hampering connectivity for websites, apps, customers are

By Chris Williams, Editor in Chief 22 Oct 2019 a

400Gbps: Winter of Whopping Weekend DDoS Attacks

03 Mar 2016 by Marek Majkowski.

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

By Richard Chirgwin 27 Oct 2016 at 01:30 14 SHARE ▼

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

Carlos Morales on March 5, 2018.

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 t

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

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

Consequences: spoofed denial-of-service (DoS) attacks

LILY HAY NEWMAN SECURITY 03.01.18 11:01 AM

GITHUB SURVIVED THE BIGGEST DDOS ATTACK EVER RECORDED

Bezos DDoS'd: Amazon Web Services' DNS systems knackered by hours-long cyber-attack

Distributed assault hampering connectivity for websites, apps, customers are

400Gbps: Winter of Whopping Weekend DDoS Attacks

03 Mar 2016 by Marek Majkowski.

Security

How many Internet of knocked out Dyn? Few expect

DNS *really* needs to be fixed i by 100,000 home devices

By Richard Chirgwin 27 Oct 2016 at 01:30

NETSCOUT Arbor Confirms The on Us

16 Olympics ed Sustained ps DDoS ks

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

CLOUDFLARE BLOG WHAT WE DO SUPPORT COMMUNITY

The real cause of large DDoS - IP Spoofing

06 Mar 2018 by Marek Majkowski.

Brazil hit by 30 DDoS attacks per hour in 2017

The country is part of a global ranking of the five nations most t

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

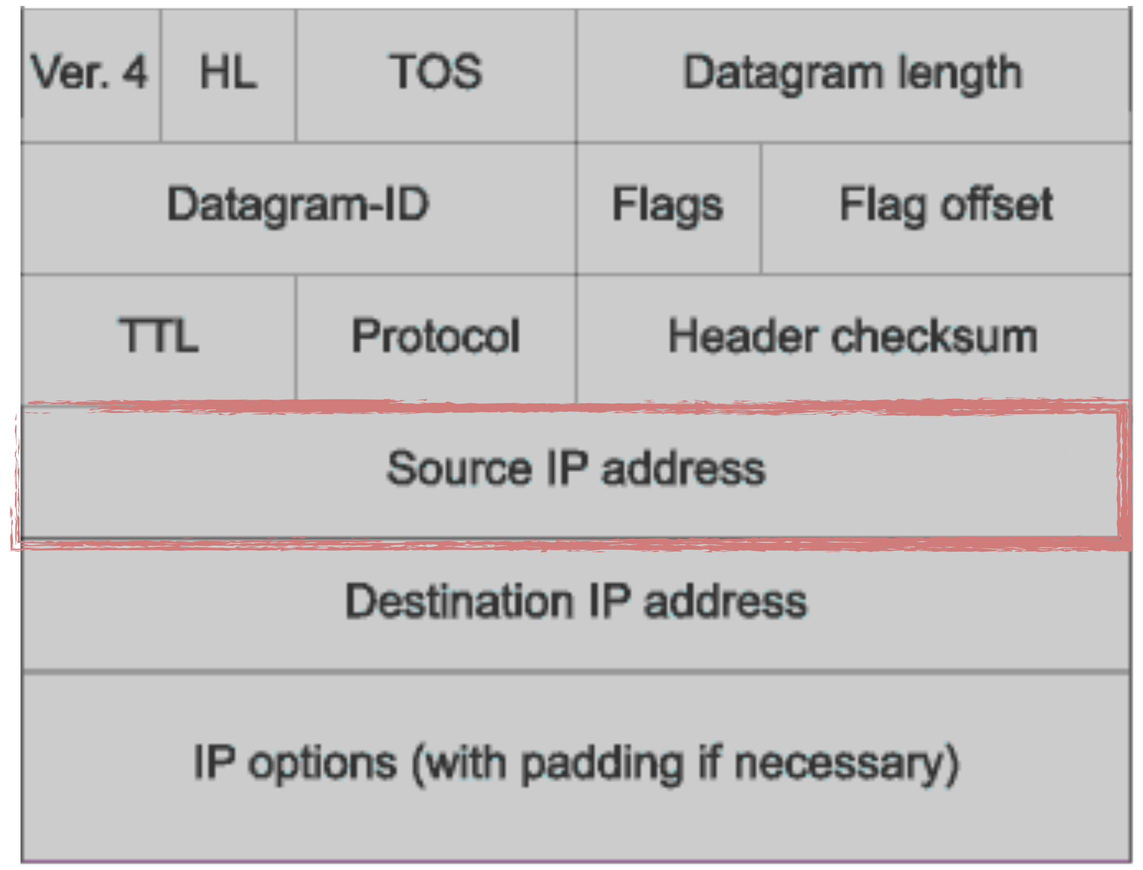
US service provider survives the biggest recorded DDoS in history

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

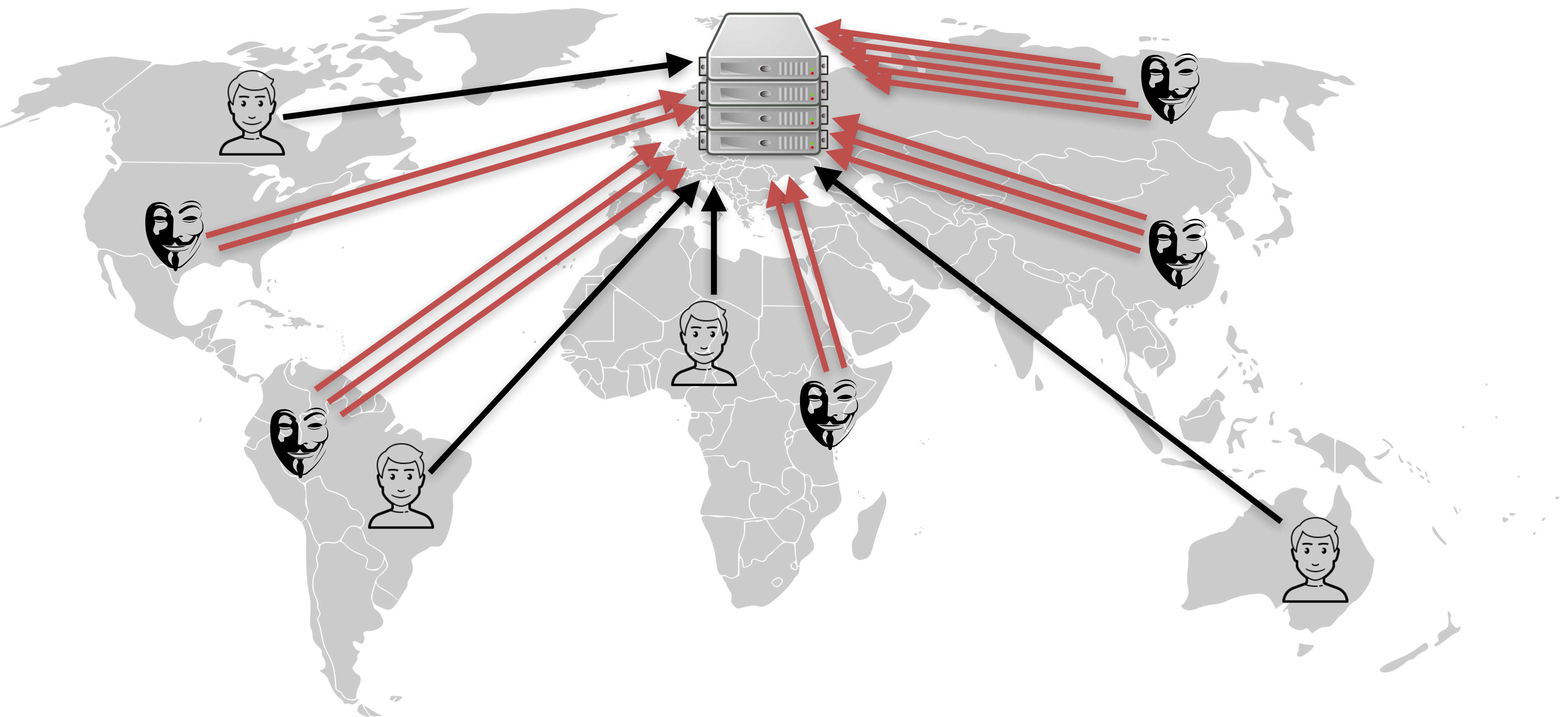
DAN GOODIN - 3/5/2018, 1:24 PM

IP Spoofing

Architectural limitation that provides an attacker with the ability to send packets using spoofed source IP addresses

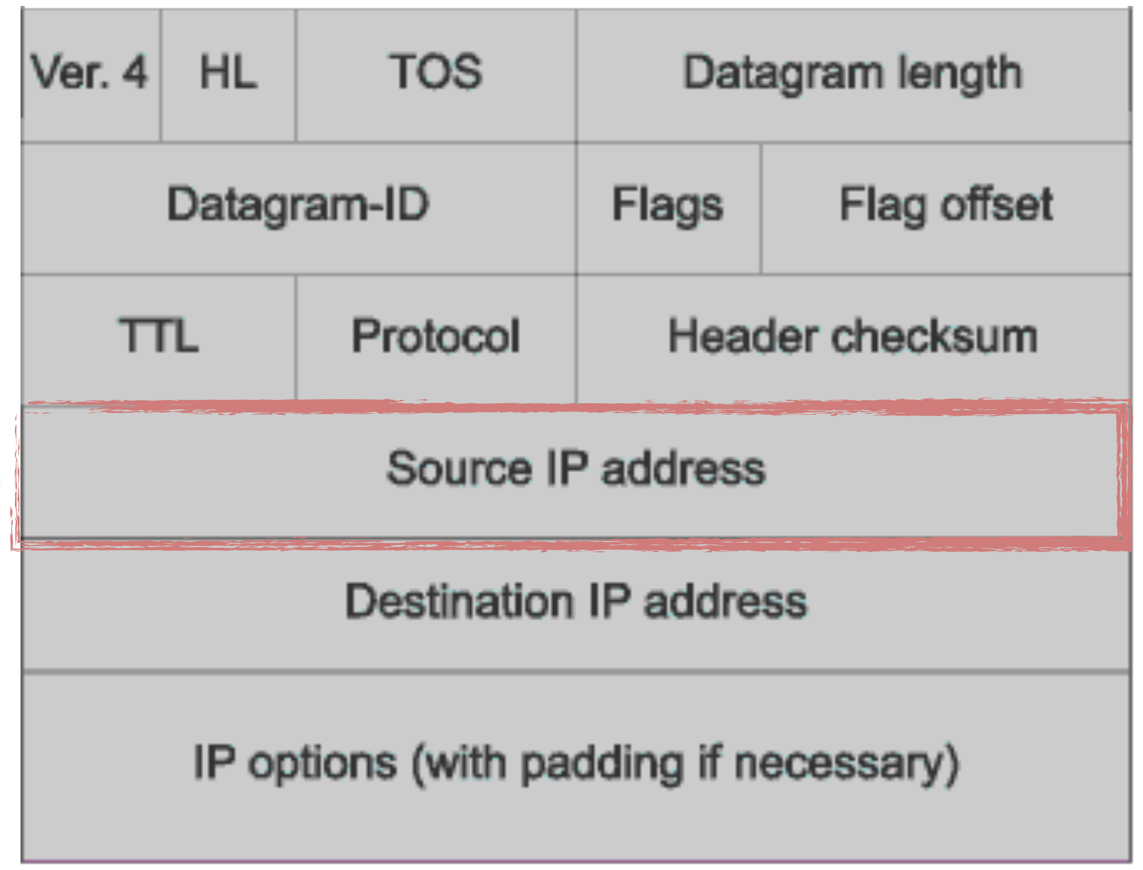


IPv4 header

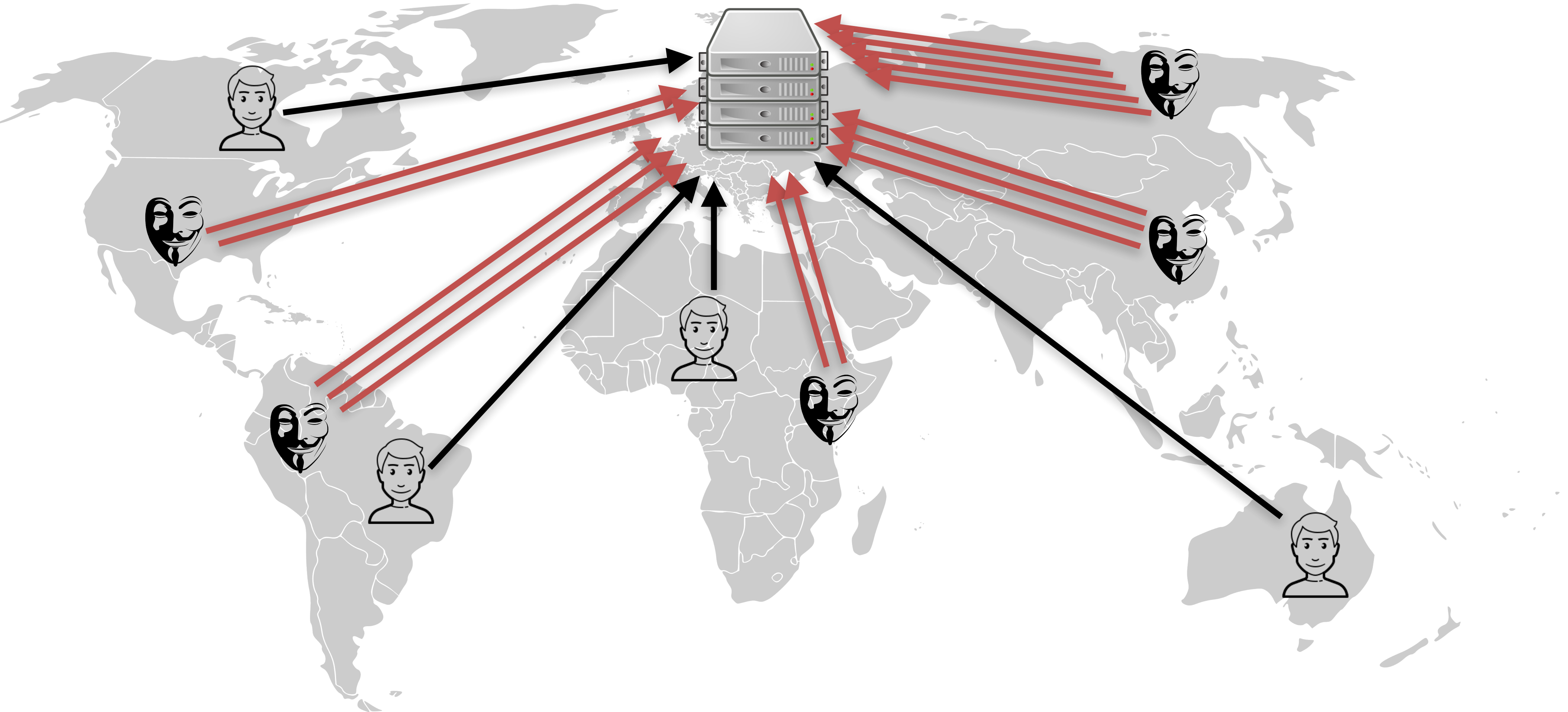


IP Spoofing

Architectural limitation that provides an attacker with the ability to send packets using spoofed source IP addresses



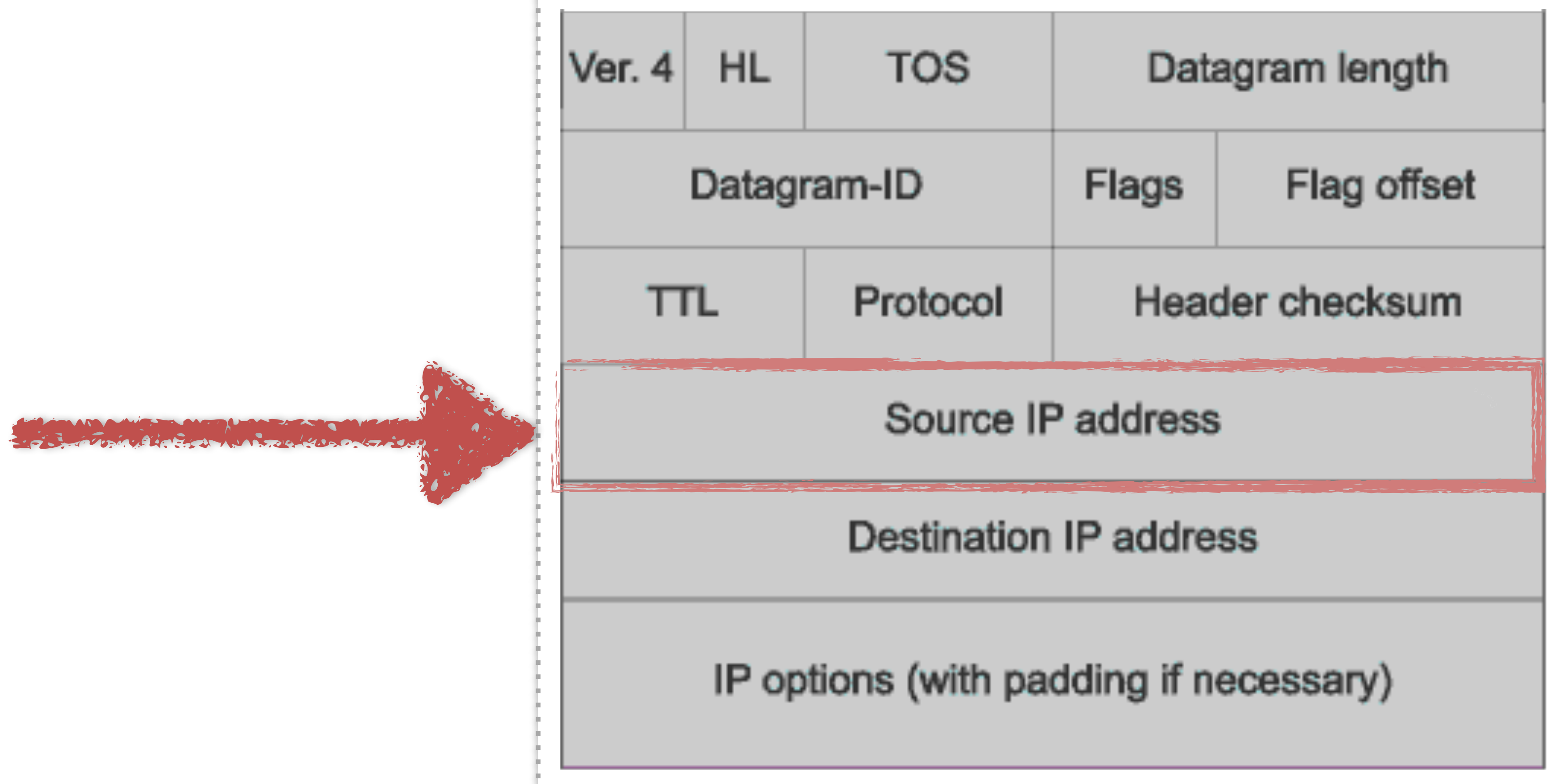
IPv4 header



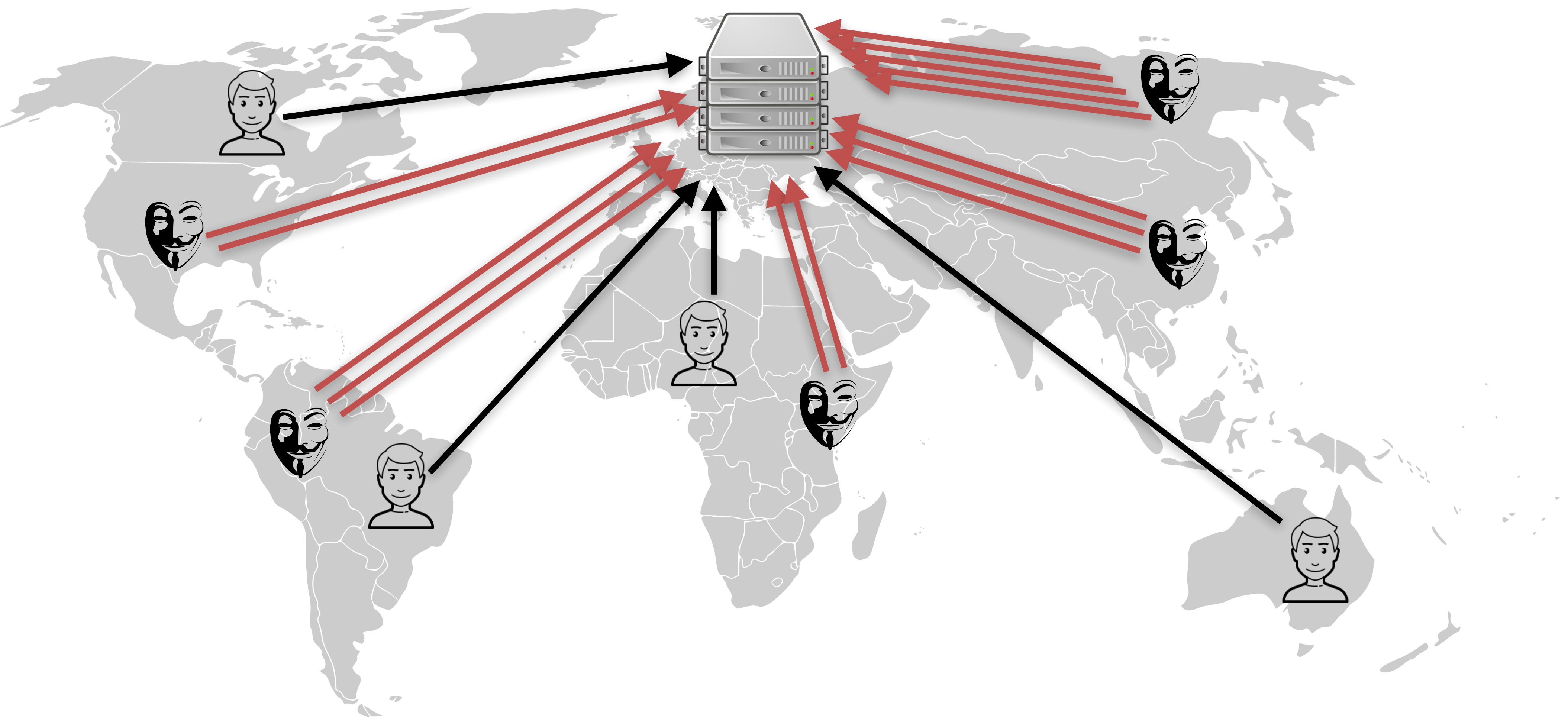
IETF introduced Best Current Practices (BCPs) recommending that networks block these packets – i.e., implement **Source Address Validation (SAV)**

IP Spoofing

Architectural limitation that provides an attacker with the ability to send packets using spoofed source IP addresses



IPv4 header



IETF introduced Best Current Practices (BCPs) recommending that networks block these packets – i.e., implement **Source Address Validation (SAV)**

- Compliance with these filtering practices has misaligned incentives
- Deploying SAV is primarily for the benefit of other networks

Remediation and Policy Interventions

Remediation and Policy Interventions

We need to identify networks lacking SAV deployment, but doing this is challenging at Internet scale

Remediation and Policy Interventions

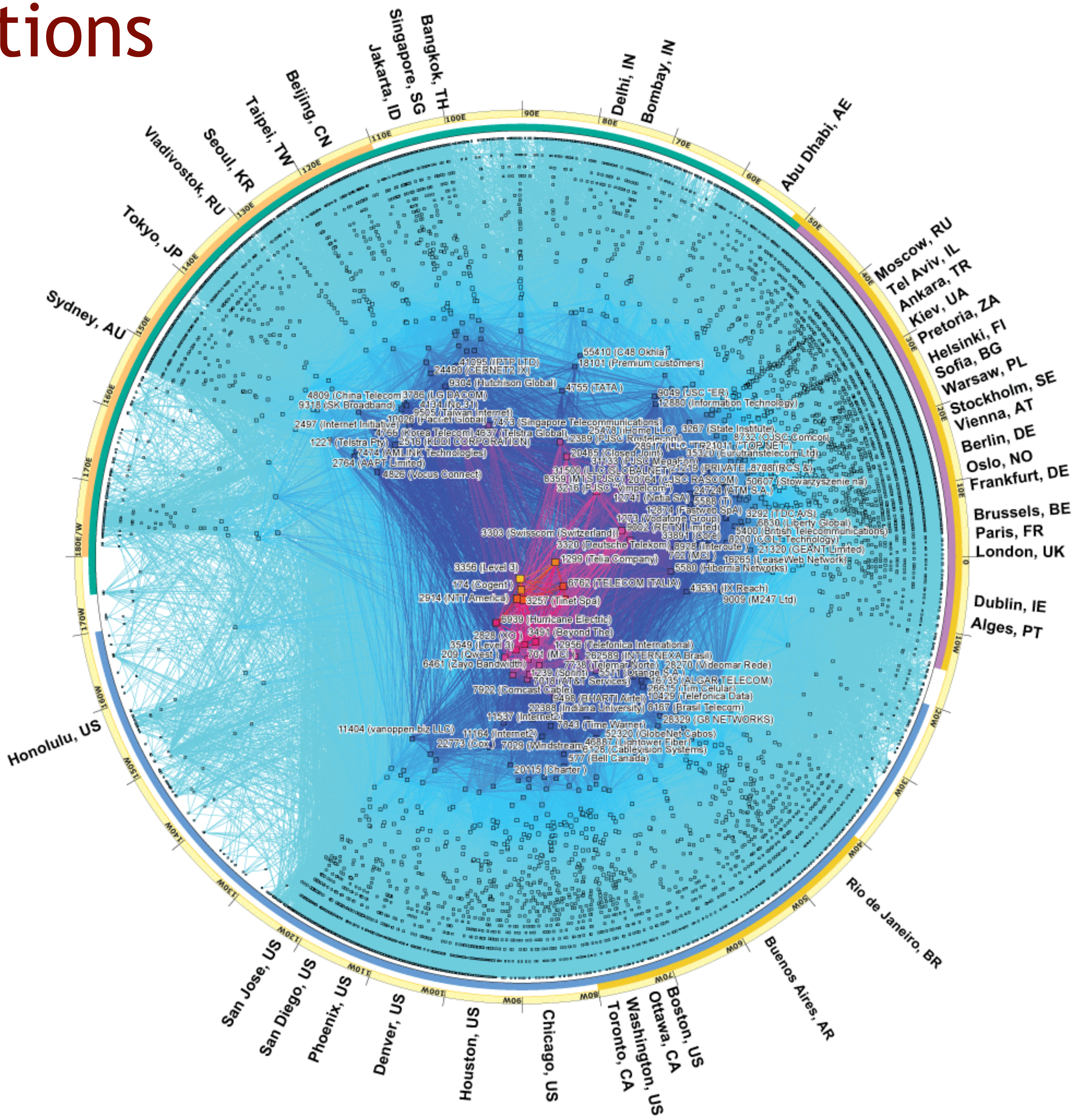
We need to identify networks lacking SAV deployment, but doing this is challenging at Internet scale

- Definitive method requires an active probing vantage point in each network being tested

Remediation and Policy Interventions

We need to identify networks lacking SAV deployment, but doing this is challenging at Internet scale

- Definitive method requires an active probing vantage point in each network being tested
- ~65K independently routed networks

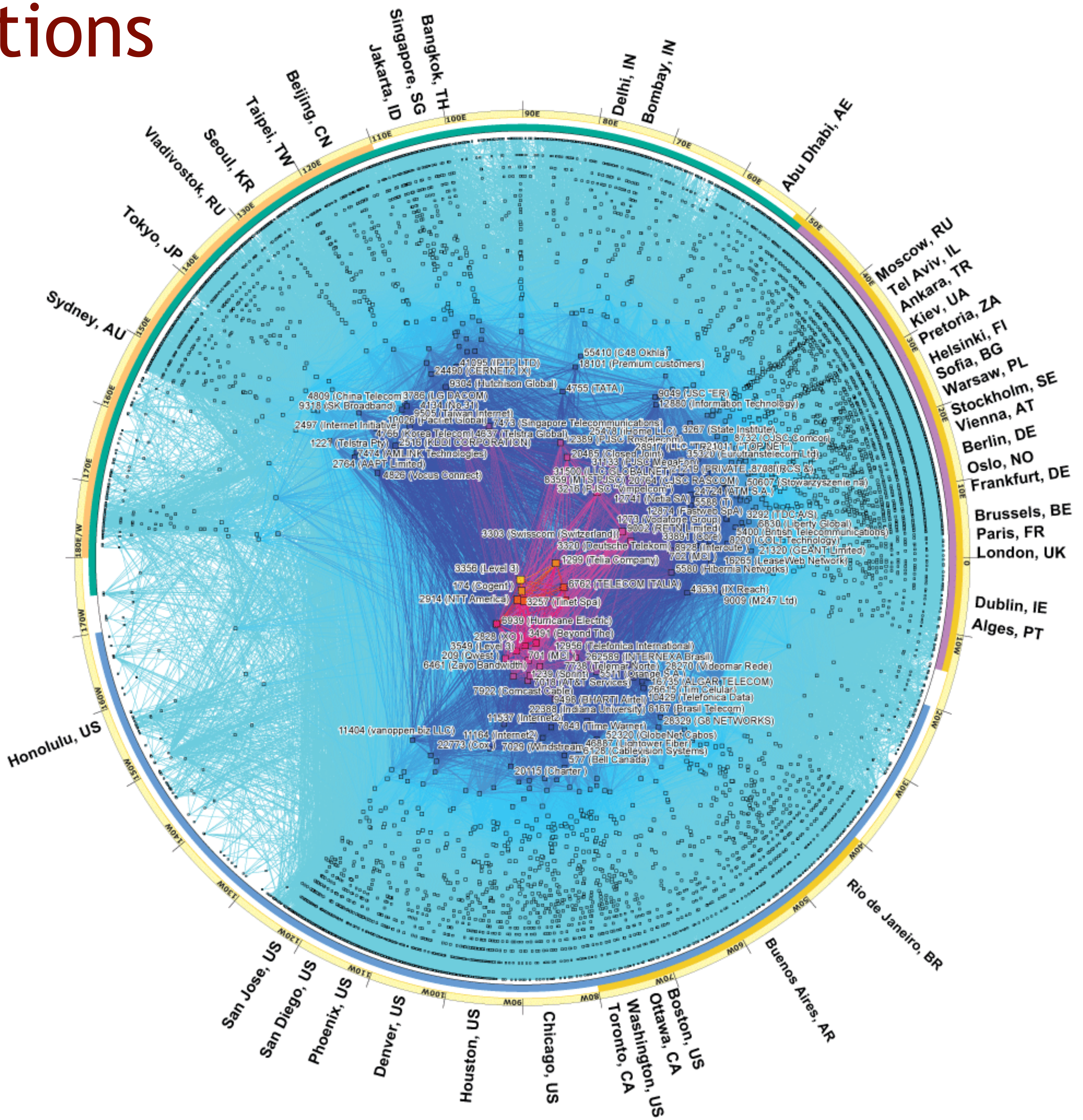


CAIDA's 2017 visualization of IPv4 Internet topology at the Autonomous System (AS) level

Remediation and Policy Interventions

We need to identify networks lacking SAV deployment, but doing this is challenging at Internet scale

- Definitive method requires an active probing vantage point in each network being tested
- ~65K independently routed networks
- Limited feasibility for a comprehensive assessment of Internet spoofing



CAIDA's 2017 visualization of IPv4 Internet topology at the Autonomous System (AS) level

Remediation and Policy Interventions

We need to identify networks lacking SAV deployment, but doing this is challenging at Internet scale

- Definitive method requires an active probing vantage point in each network being tested
- ~65K independently routed networks
- Limited feasibility for a comprehensive assessment of Internet spoofing

700+ Internet Exchange Points (IXP)

[PeeringDB, 2019]

Broader visibility may lie in the capability to infer lack of SAV compliance from aggregated Internet traffic data

our goal

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

nic.br

Núcleo de Informação e Coordenação do Ponto BR

versão 2018-08-21-15-08

Programa por uma Internet mais Segura

Ações no IX.br

Introdução

O IX.br está presente em 31 localidades no Brasil, por meio da
Troca de Tráfego Internet (PTTs), sendo parte integrante da i
Brasil, onde Sistemas Autônomos (ASs) podem trocar tr
próximas.

Dois tipos de serviços são oferecidos aos participantes da troc
de Tráfego Multilateral (ATM), chamado em inglês de *Multil*
(ii) a **Troca de Tráfego Bilateral**, em inglês *Bilateral Peering*
do ATM trocam tráfego entre si: como regra geral, cada AS tr
na Troca de Tráfego Bilateral apenas dois ASs participam, uti
camada 2 exclusivo (uma VLAN bilateral).

O Acordo de Troca de Tráfego Multilateral (ATM), na
compartilhada para a troca de tráfego IPv4 (ATMv4) e outra
Cada PTT possui dois ou mais *route servers*, que também sã
Tráfego Multilateral (ATM) para centralizar o recebimento
participantes da troca de tráfego, permitindo que, com uma úni
localidade seja carregada e mantida. O estabelecimento de se
condição necessária para participar do ATM. A maior parte d
da troca de tráfego multilateral, mas nem todos. Mesmo pa
podem estar presentes nas VLANs do ATMv4 ou ATMv6, pa
fins.

Existem casos em que o participante está presente na VLAN
sessão BGP com o *route server*, mas fecha sessões BGP di
participantes com os quais deseja trocar tráfego, usando os
acordos bilaterais de troca de tráfego podem se utilizar tanto
ATMv6), como de VLANs específicas (VLANs bilaterais).

Desta forma, neste cenário, temos em cada PTT do IX.br:

- um **ambiente privado**, formado pelos Acordos Bila
através VLANs, sejam VLANs bilaterais ou as VLANs d
- um **ambiente compartilhado** formado pelos participan
e/ou ATMv6 e com sessões BGP com os route servers.

https://www.manrs.org/ixps/

MANRS

MANRS IXP Programme

You are here: Home / MANRS IXP Programme

MANRS is an important step toward a globally robust and secure routing infrastructure

The MANRS Actions were initially designed for network operators, but Internet Exchange Points (IXPs) should also play an active role in protecting the Internet. IXPs represent active communities with common operational objectives and already contribute to a more resilient and secure Internet infrastructure.

MANRS can help IXPs build safe neighborhoods, leveraging the MANRS security baseline. It also demonstrates an IXP's commitment to security and sustainability of the Internet ecosystem, and dedication to providing high quality services.

IXPs are important partners in the MANRS community

cyberstability.org

GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE

ABOUT RESEARCH COMMISSIONERS NEWS NORMS CONTACT

GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE

Cyberstability Update –

https://cybertechaccord.org

TECH ACCORD

The Cybersecurity Tech Accord is a public commitment among more than 60 global companies to protect and empower civilians online and to improve the security, stability and resilience of cyberspace.

Cybersecurity Tech Accord

Watch later Share

THAT'S WHY MORE THAN 60 COMPA HAVE JOINED TO TAKE

YouTube

NOVEMBER 12, 2018

The Cybersecurity Tech Accord endorses the Paris Call; strengthening our commitment to ensuring trust and stability in cyberspace

The Cybersecurity Tech Accord is pleased to endorse the Paris Call for Trust and Security in Cyberspace as an early supporter. The Paris Call was announced today by French President Emmanuel Macron at the opening of the 13th Internet Governance

Contributions

Contributions

1. Challenges

Provide detailed analysis of methodological challenges for inferring spoofed packets at IXPs

Contributions

1. Challenges

Provide detailed analysis of methodological challenges for inferring spoofed packets at IXPs

2. Methodology

Developed a methodology to classify flows, navigating through all challenges identified

Contributions

1. Challenges

Provide detailed analysis of methodological challenges for inferring spoofed packets at IXPs

2. Methodology

Developed a methodology to classify flows, navigating through all challenges identified

3. Observations and Lessons

Used our methodology and compare it with the state-of-the-art[1] at an IXP in Brazil, reporting our findings

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

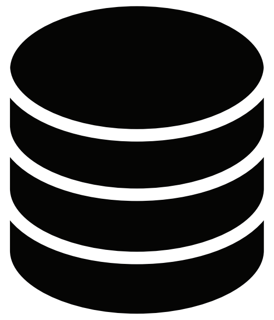
Bird’s Eye View

Bird's Eye View

IXP traffic flow data and
topology information

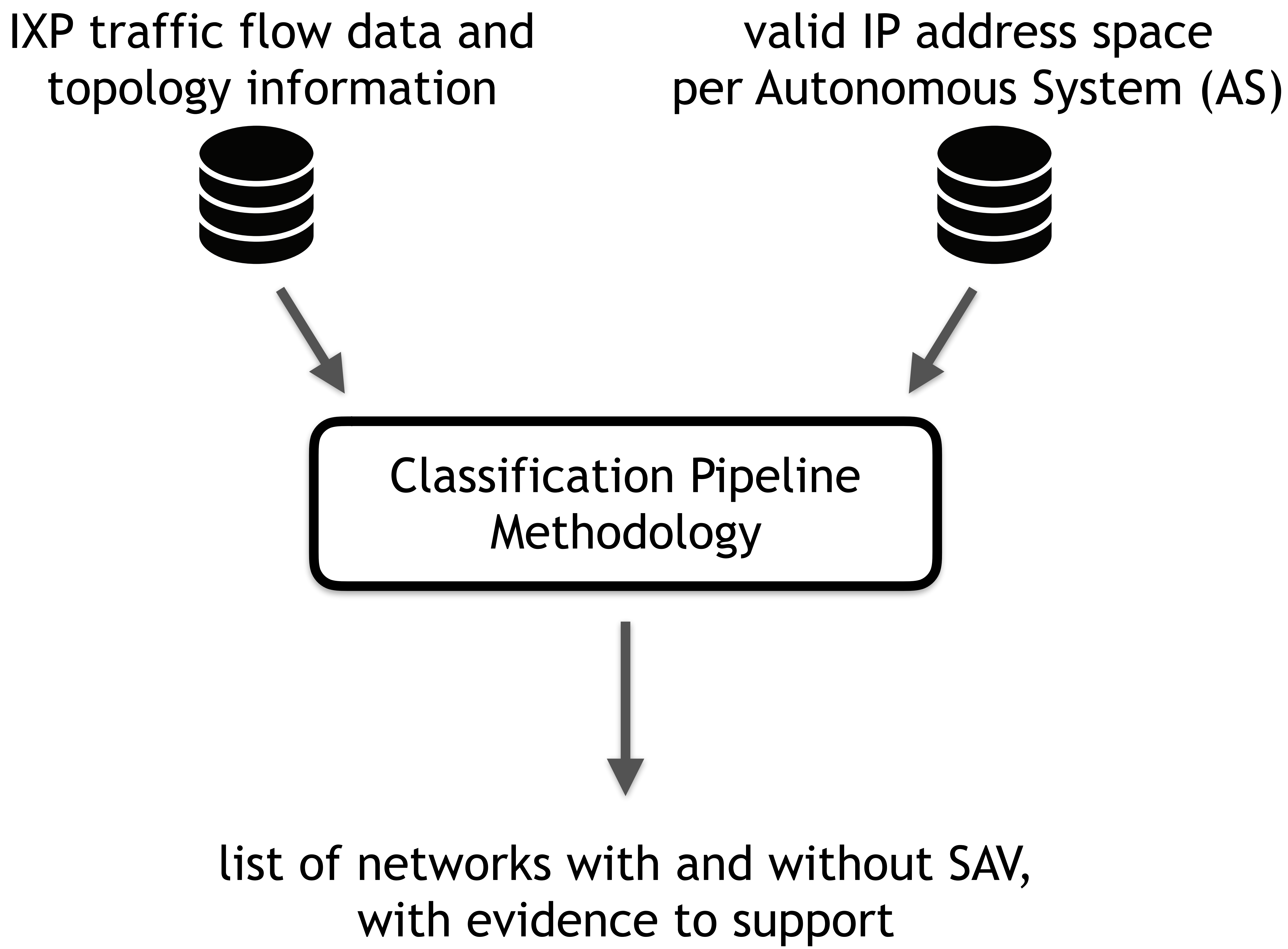
Bird's Eye View

IXP traffic flow data and
topology information

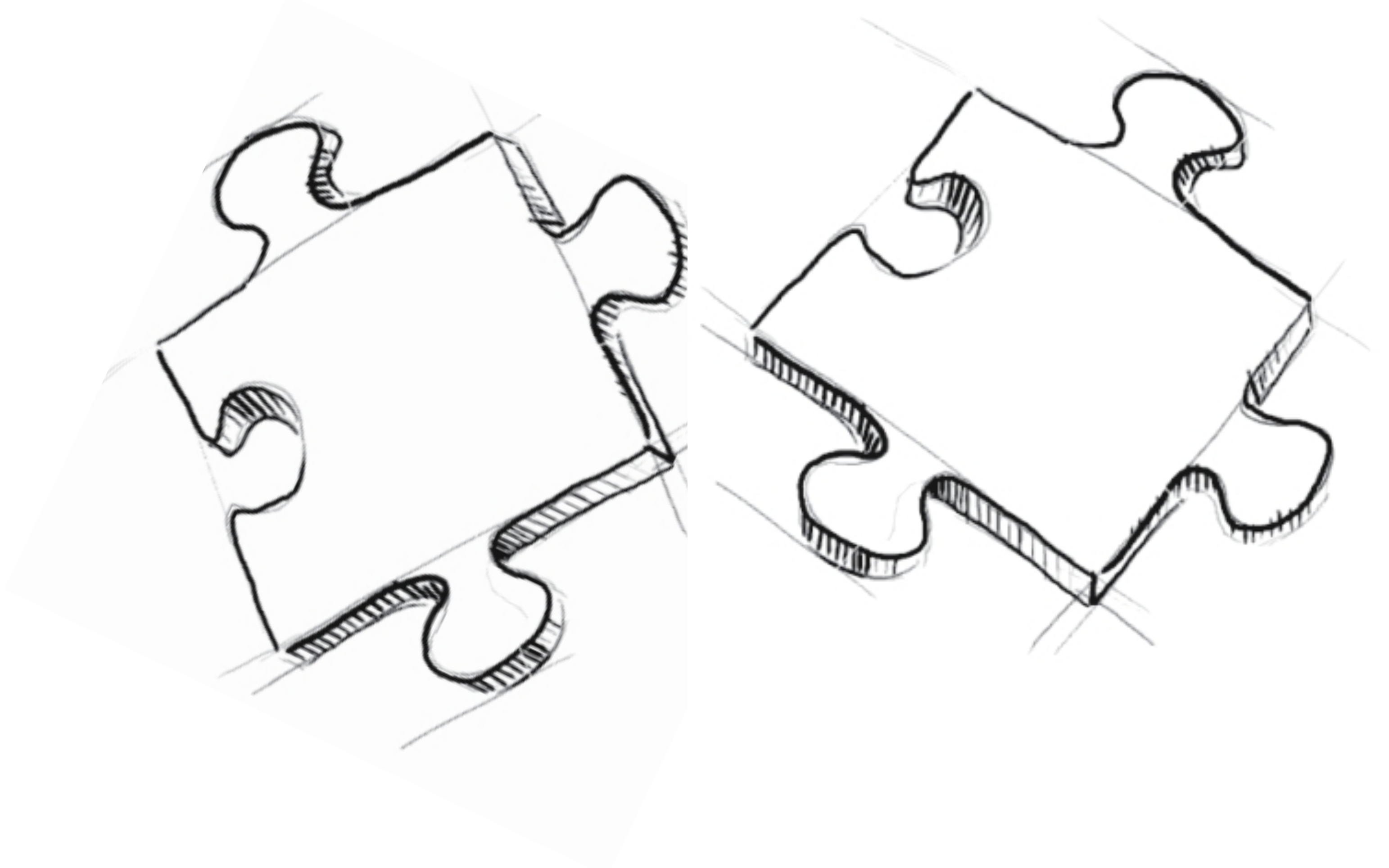


valid IP address space
per Autonomous System (AS)

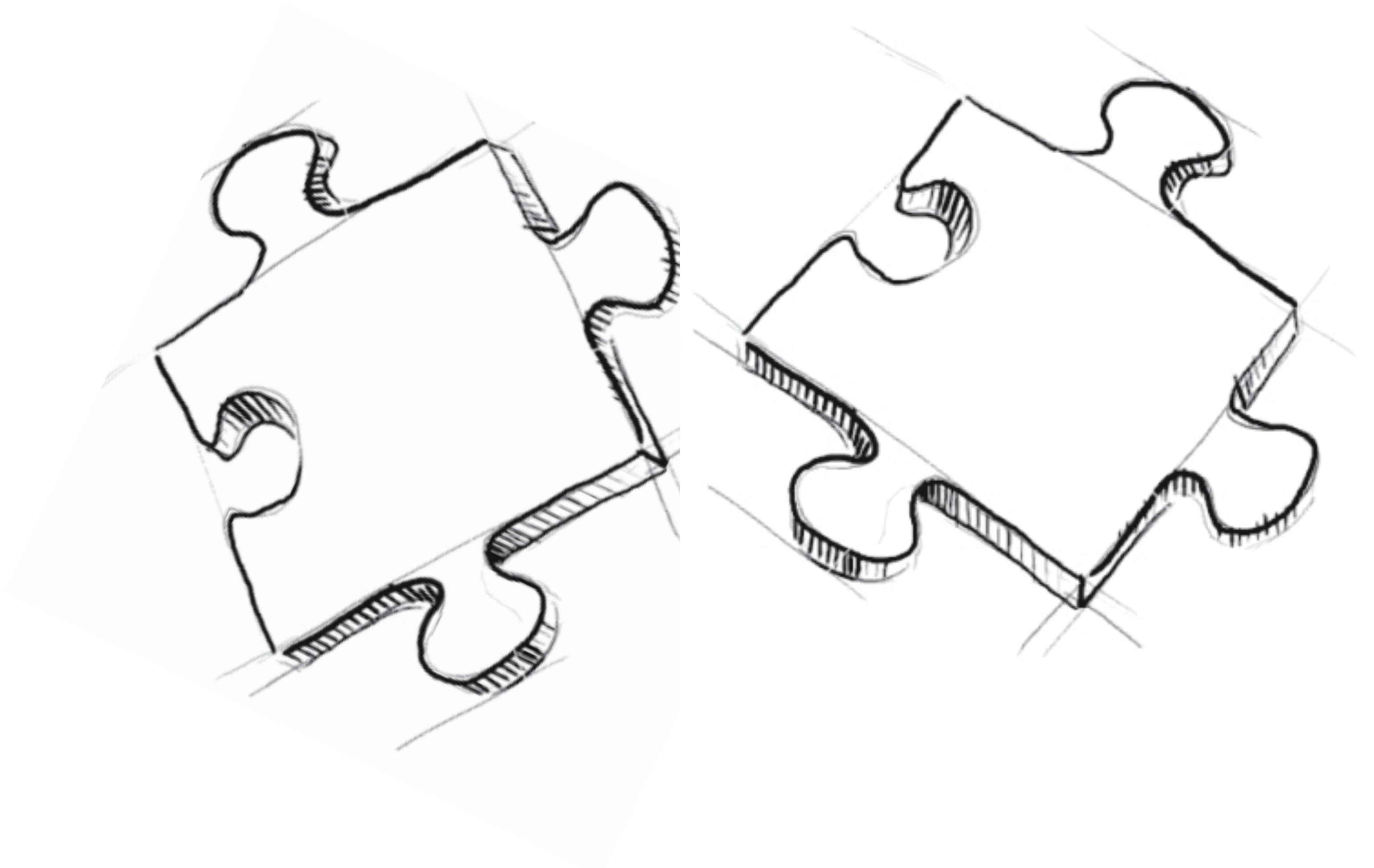
Bird’s Eye View



Challenges: Pieces of the Puzzle

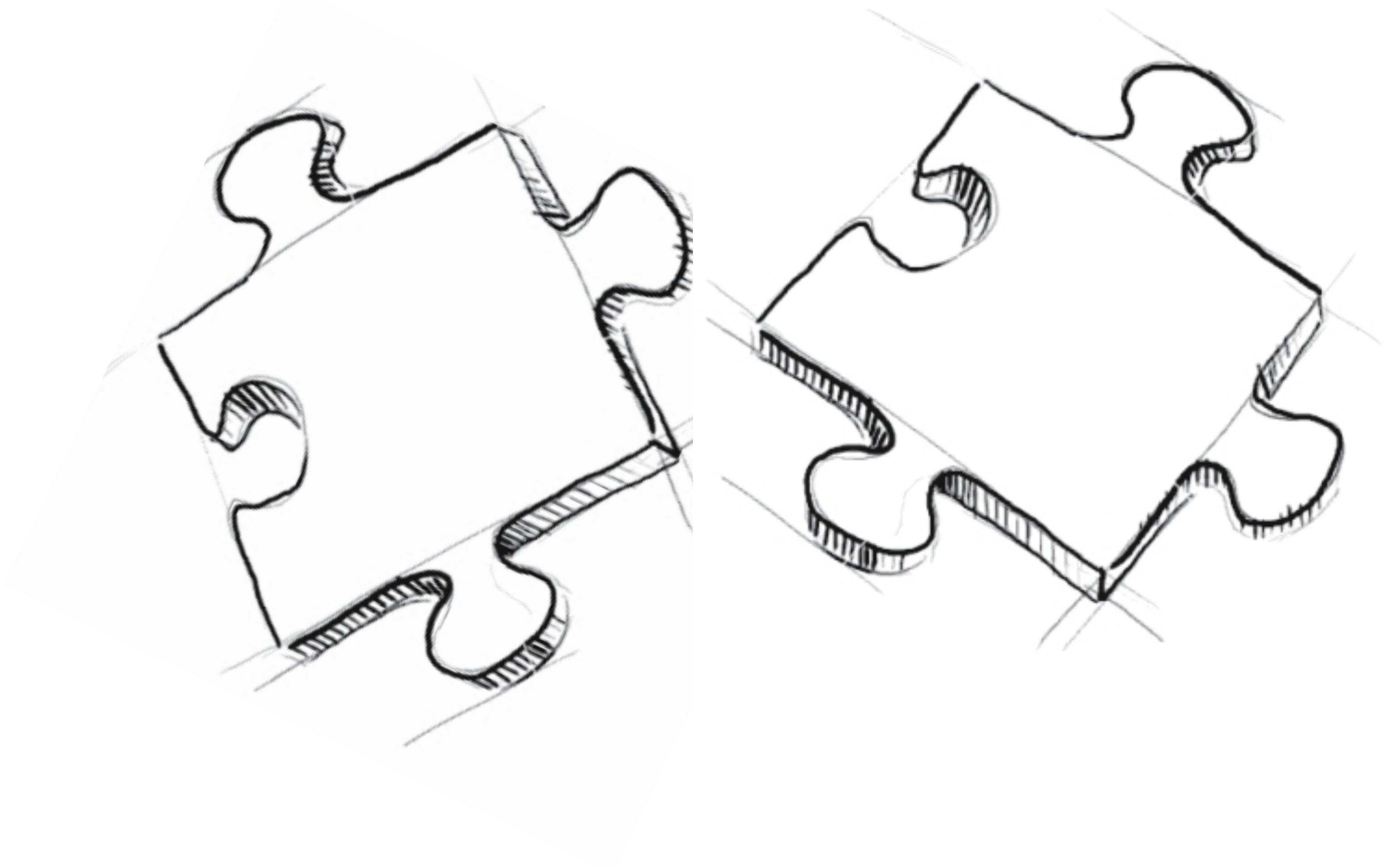


Challenges: Pieces of the Puzzle



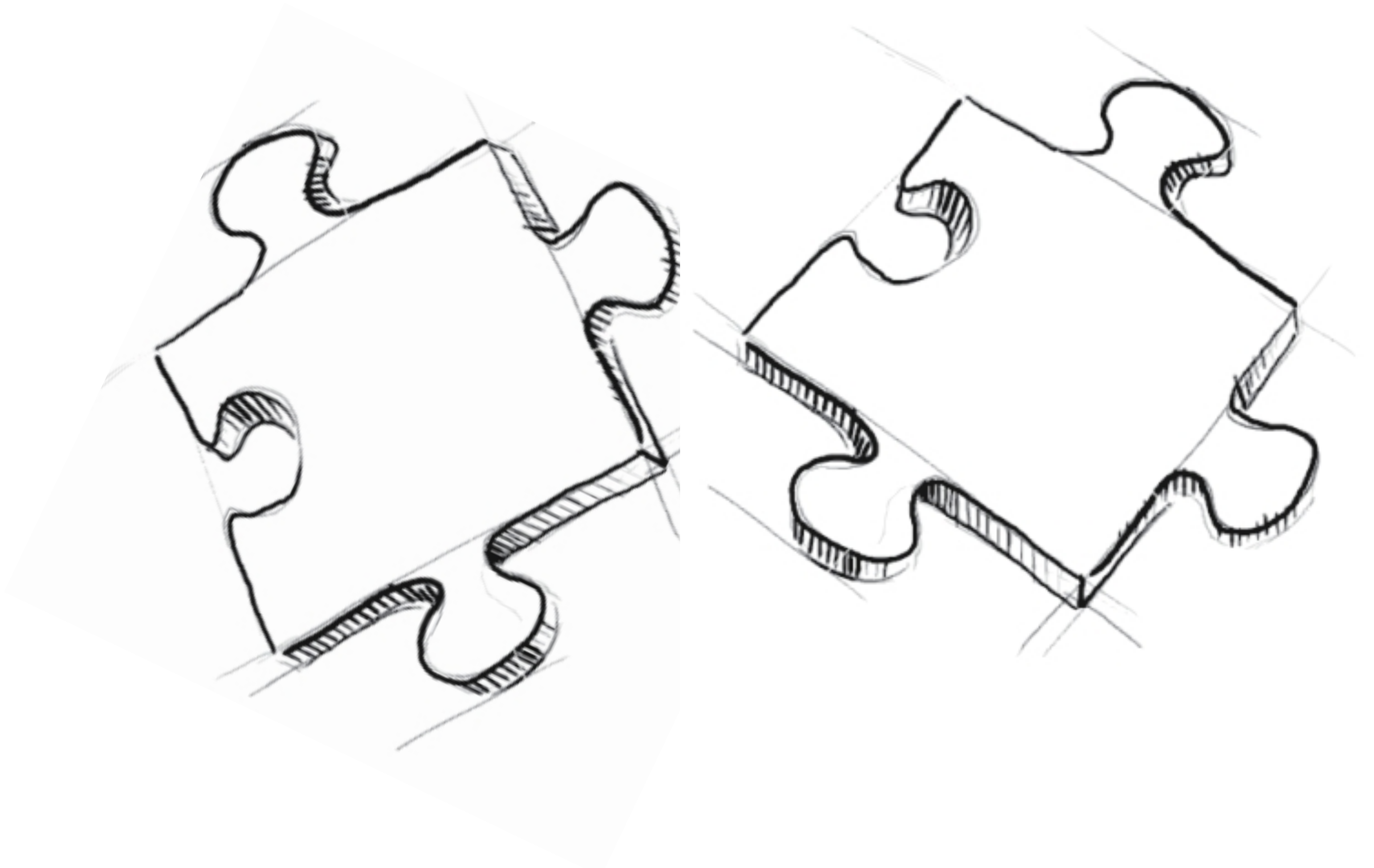
1. Identify Valid Source Address Space

Challenges: Pieces of the Puzzle



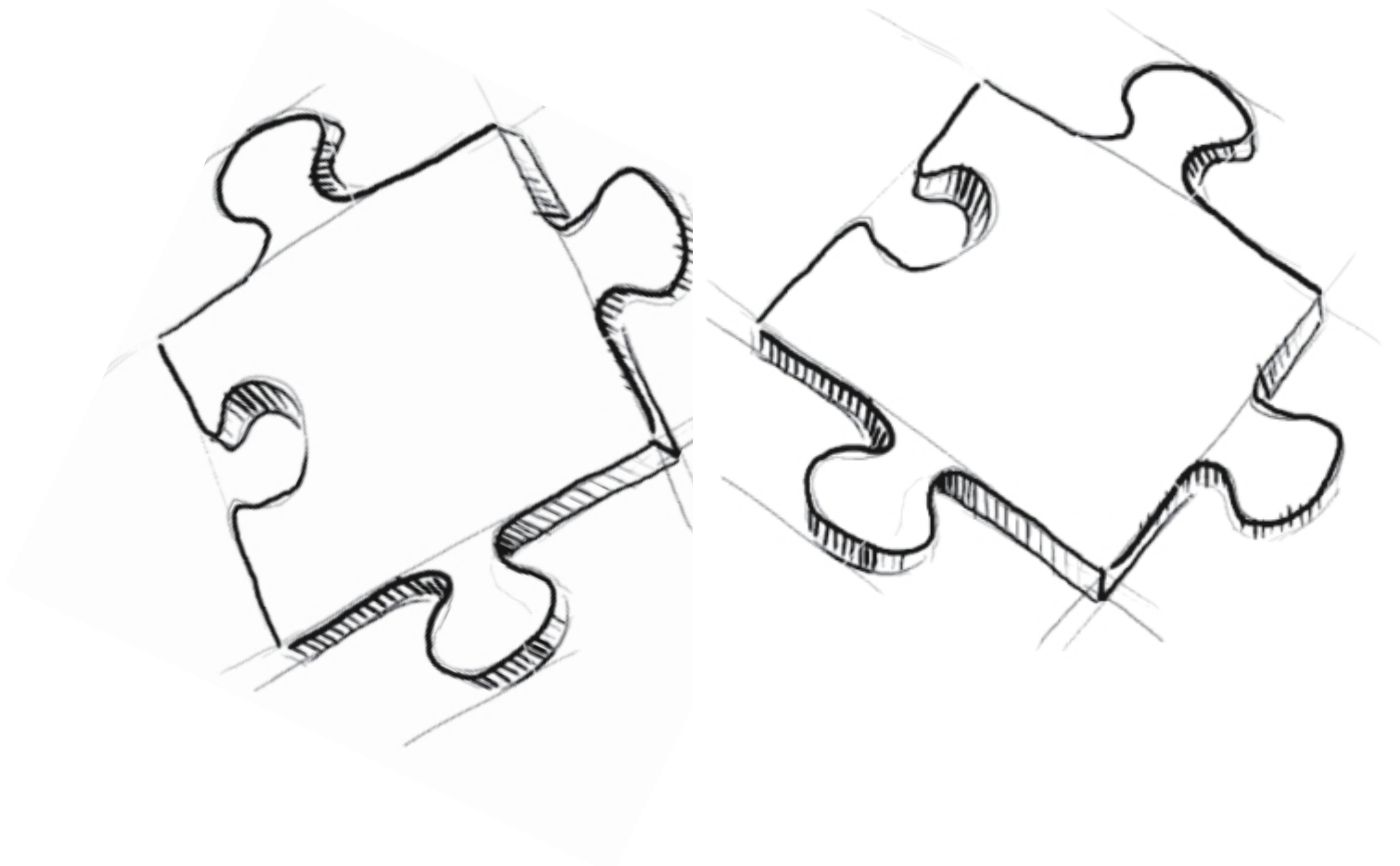
1. **Identify Valid Source Address Space**
   - there is no global registry that contains ground truth

Challenges: Pieces of the Puzzle



1. **Identify Valid Source Address Space**
   - there is no global registry that contains ground truth
   - need to infer the set of valid source addresses

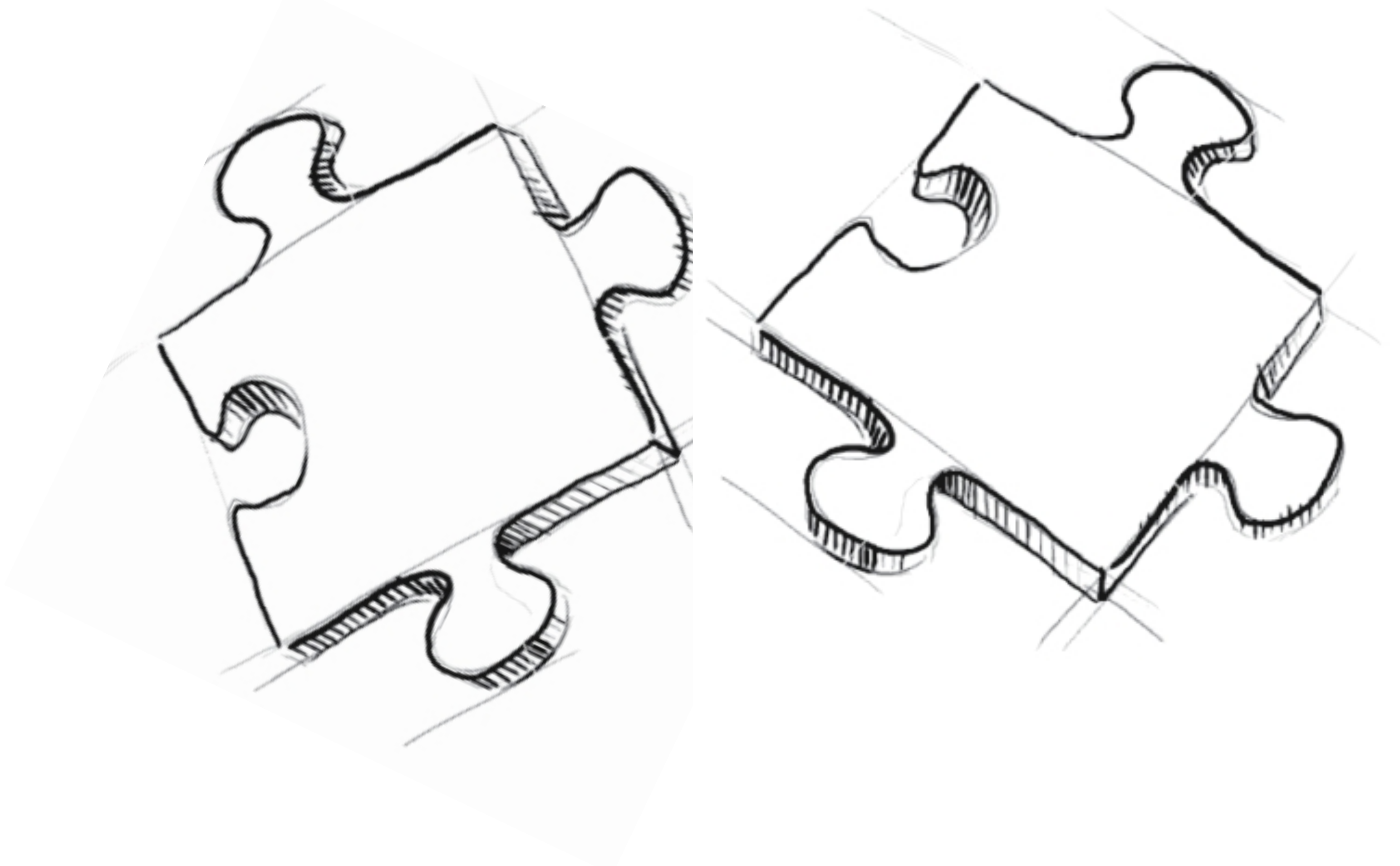
Challenges: Pieces of the Puzzle



1. Identify Valid Source Address Space
   - there is no global registry that contains ground truth
   - need to infer the set of valid source addresses

2. Tackle IXP Topology and Traffic Visibility Properties

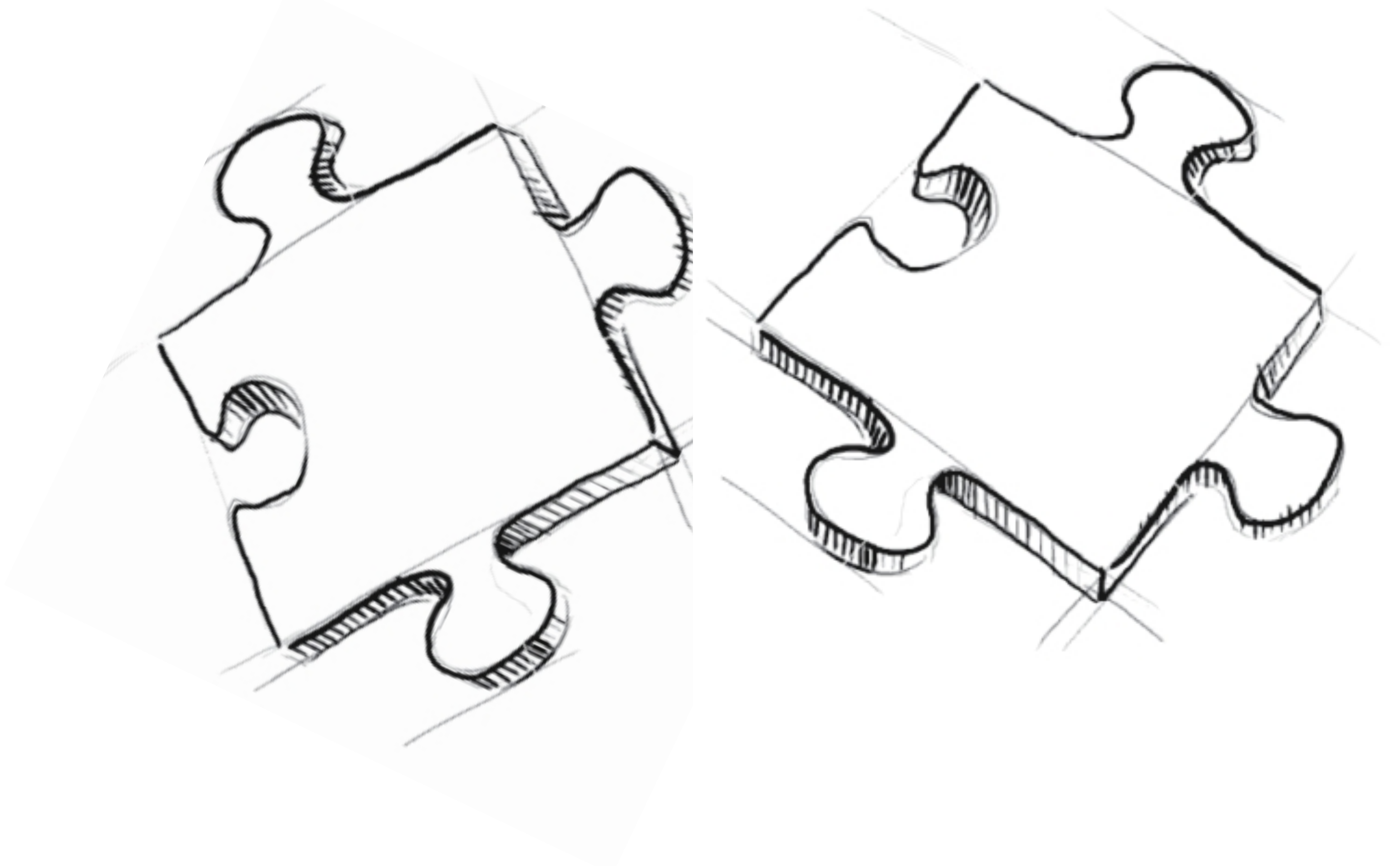
Challenges: Pieces of the Puzzle



1. Identify Valid Source Address Space
   - there is no global registry that contains ground truth
   - need to infer the set of valid source addresses

2. Tackle IXP Topology and Traffic Visibility Properties
   - understand modern IXP interconnection practices

Challenges: Pieces of the Puzzle



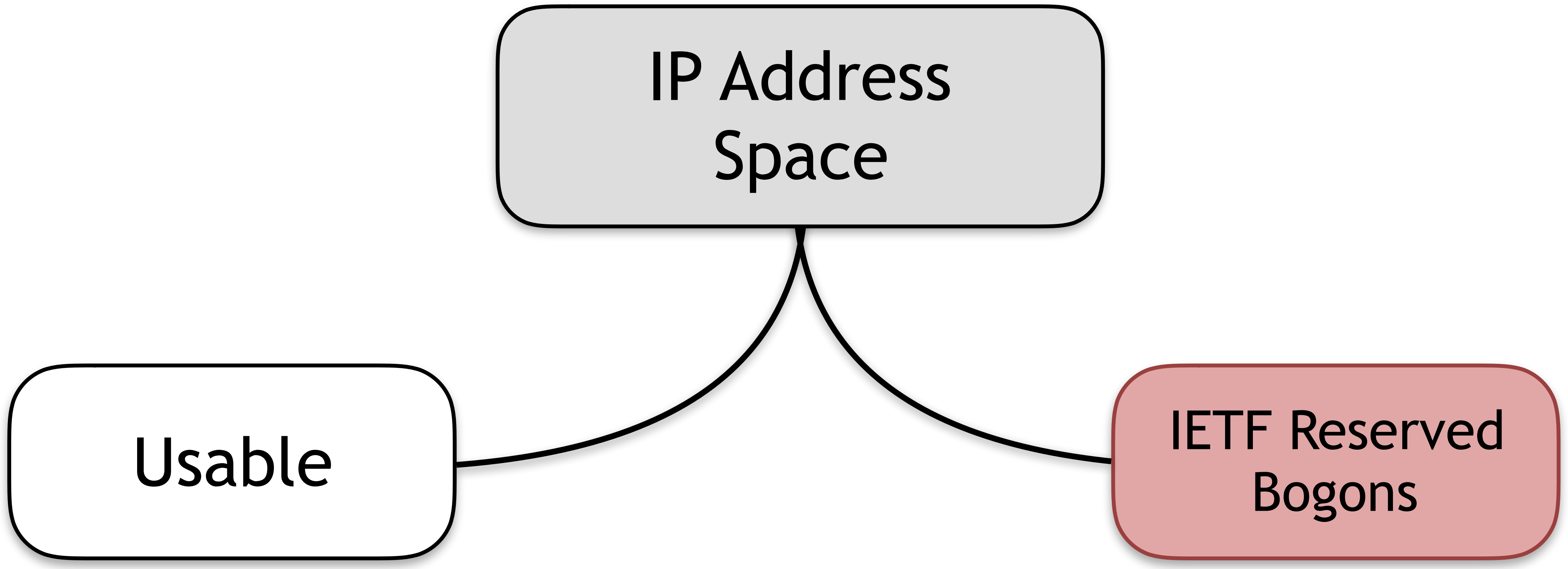
1. Identify Valid Source Address Space
   - there is no global registry that contains ground truth
   - need to infer the set of valid source addresses

2. Tackle IXP Topology and Traffic Visibility Properties
   - understand modern IXP interconnection practices
   - implications on visibility of both topology and traffic

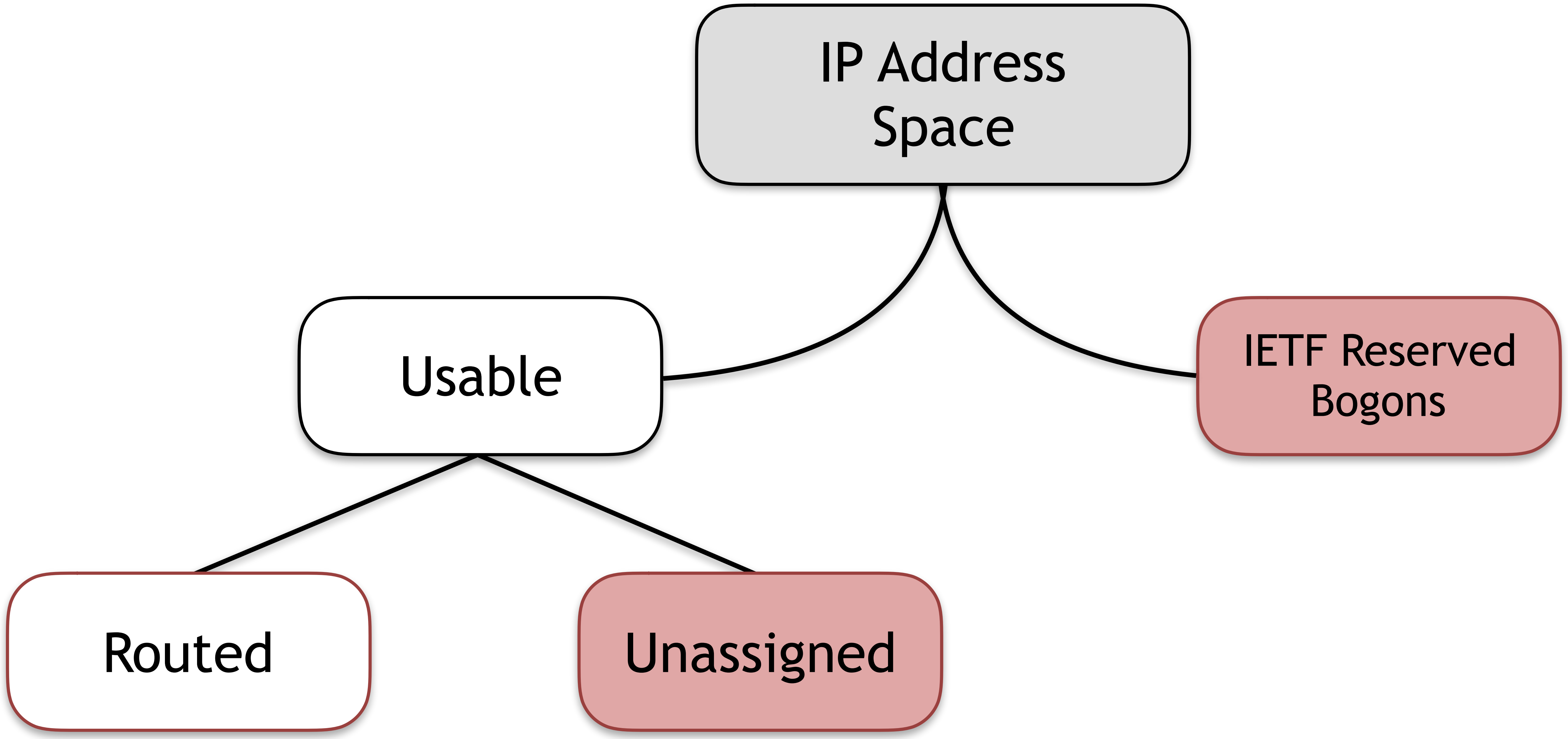
1. Identify Valid Source Address Space

IP Address Space

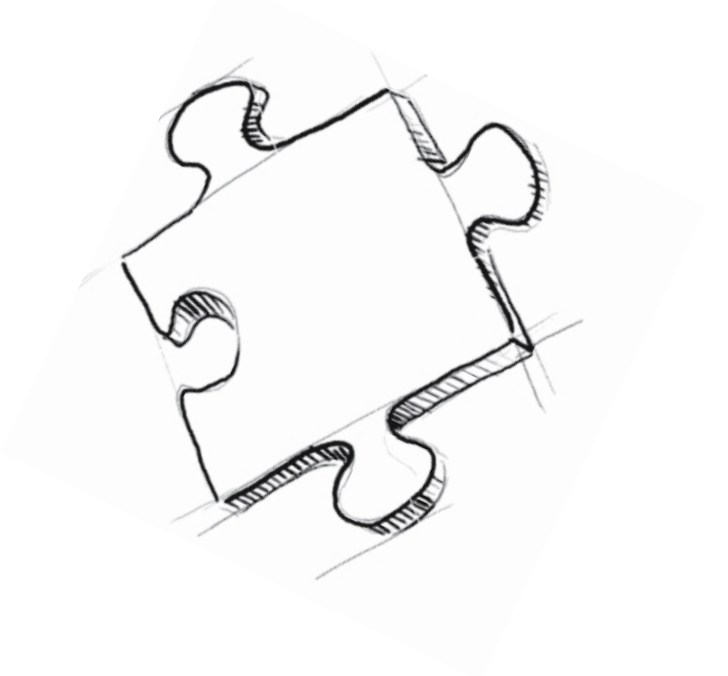
1. Identify Valid Source Address Space

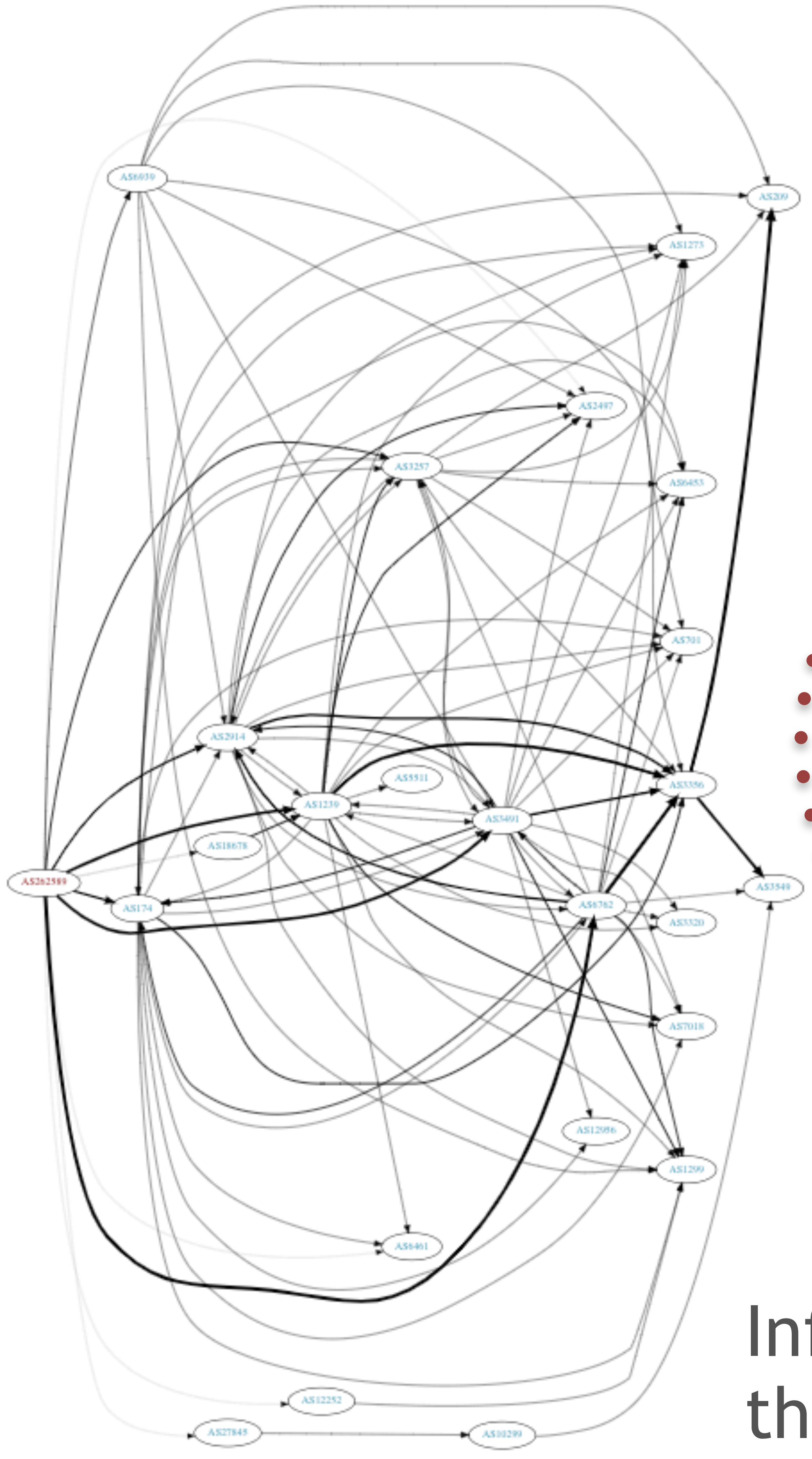


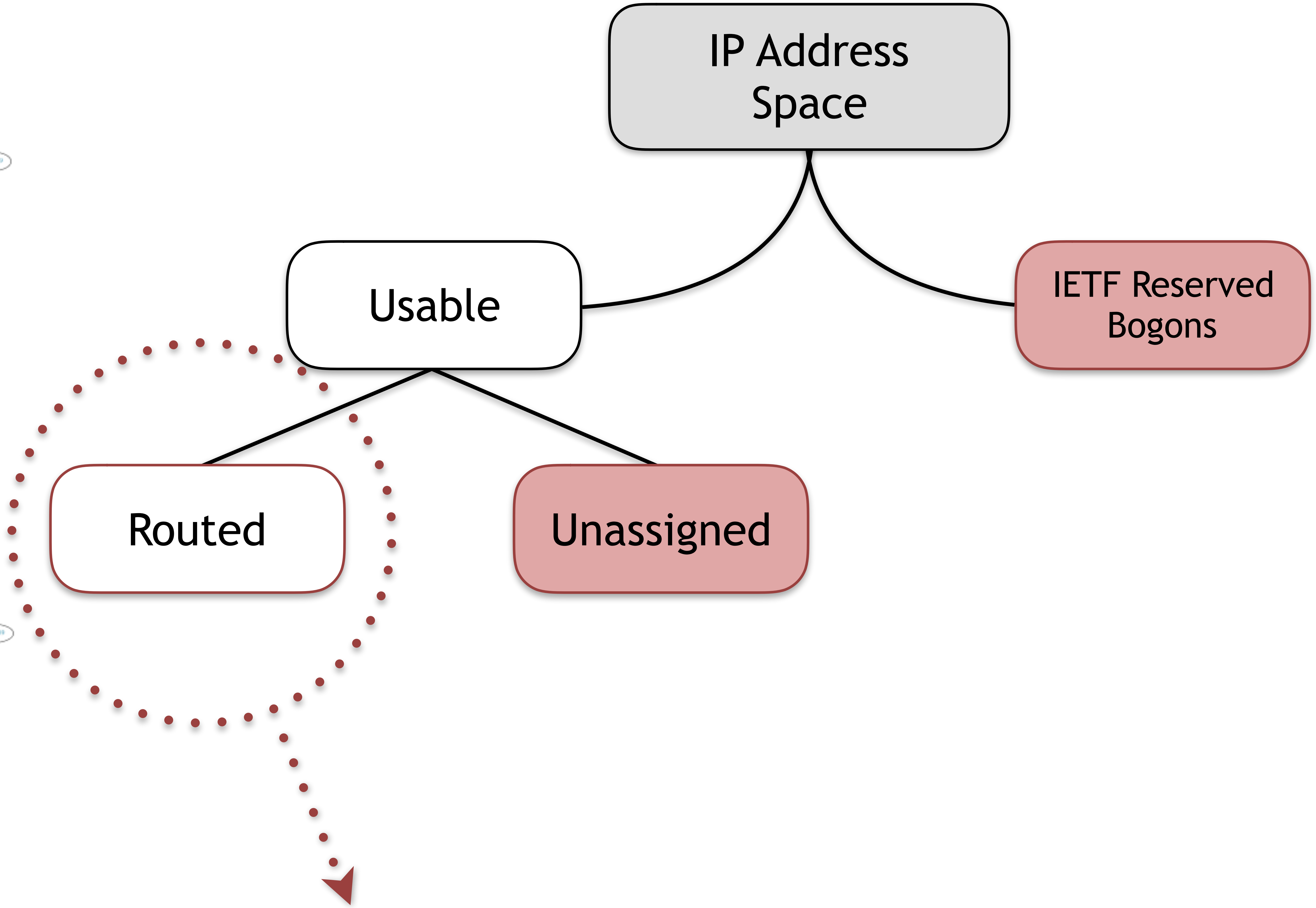
1. Identify Valid Source Address Space



1. Identify Valid Source Address Space

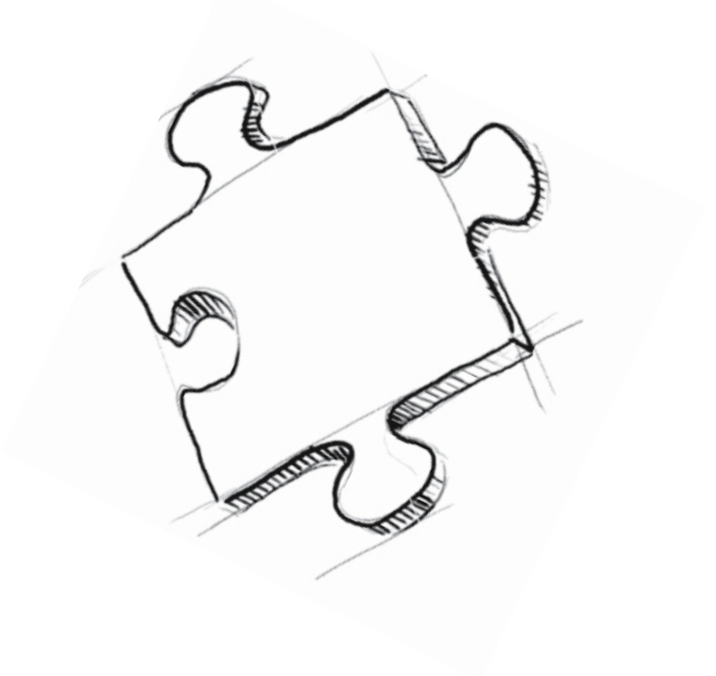


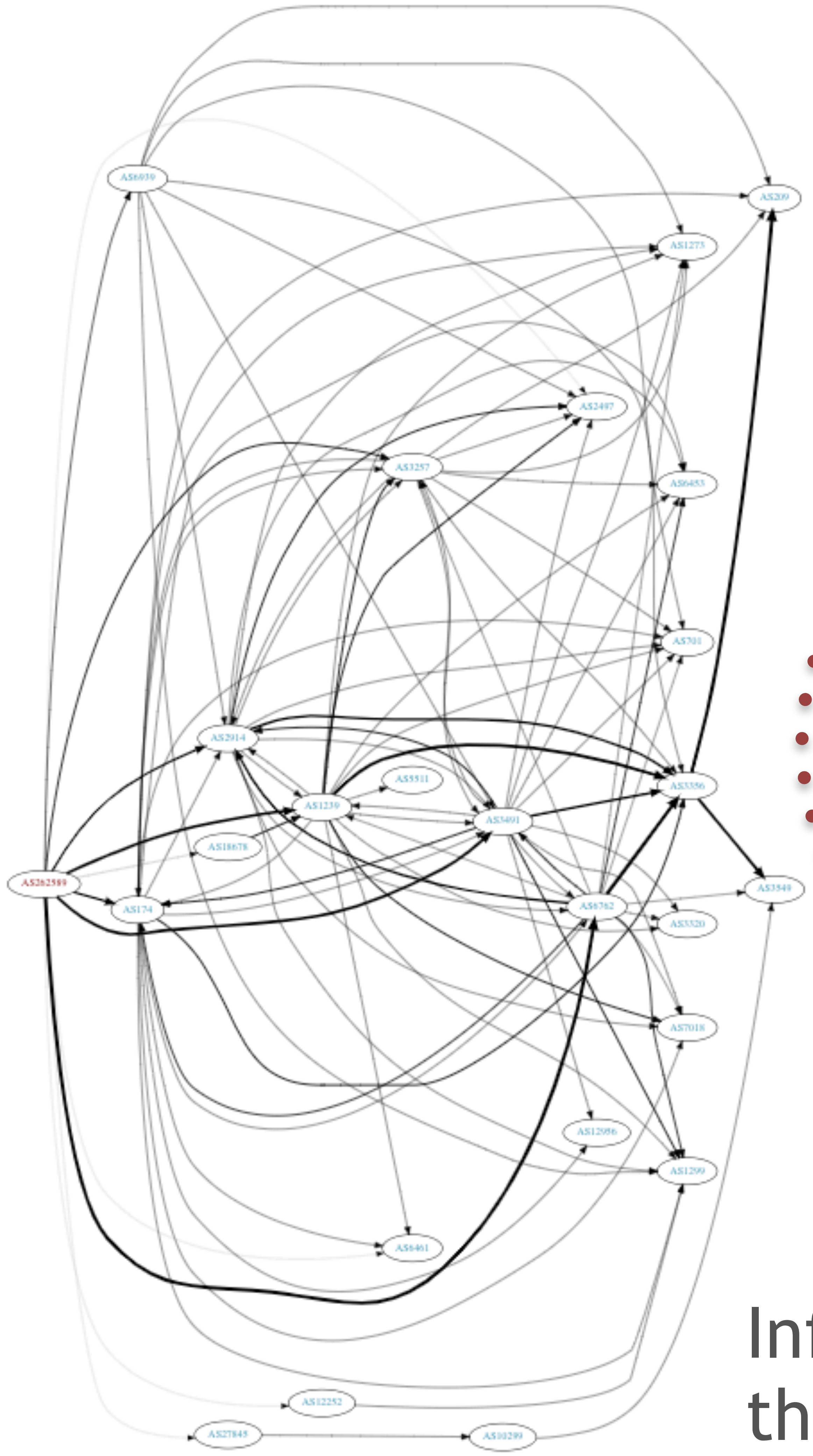


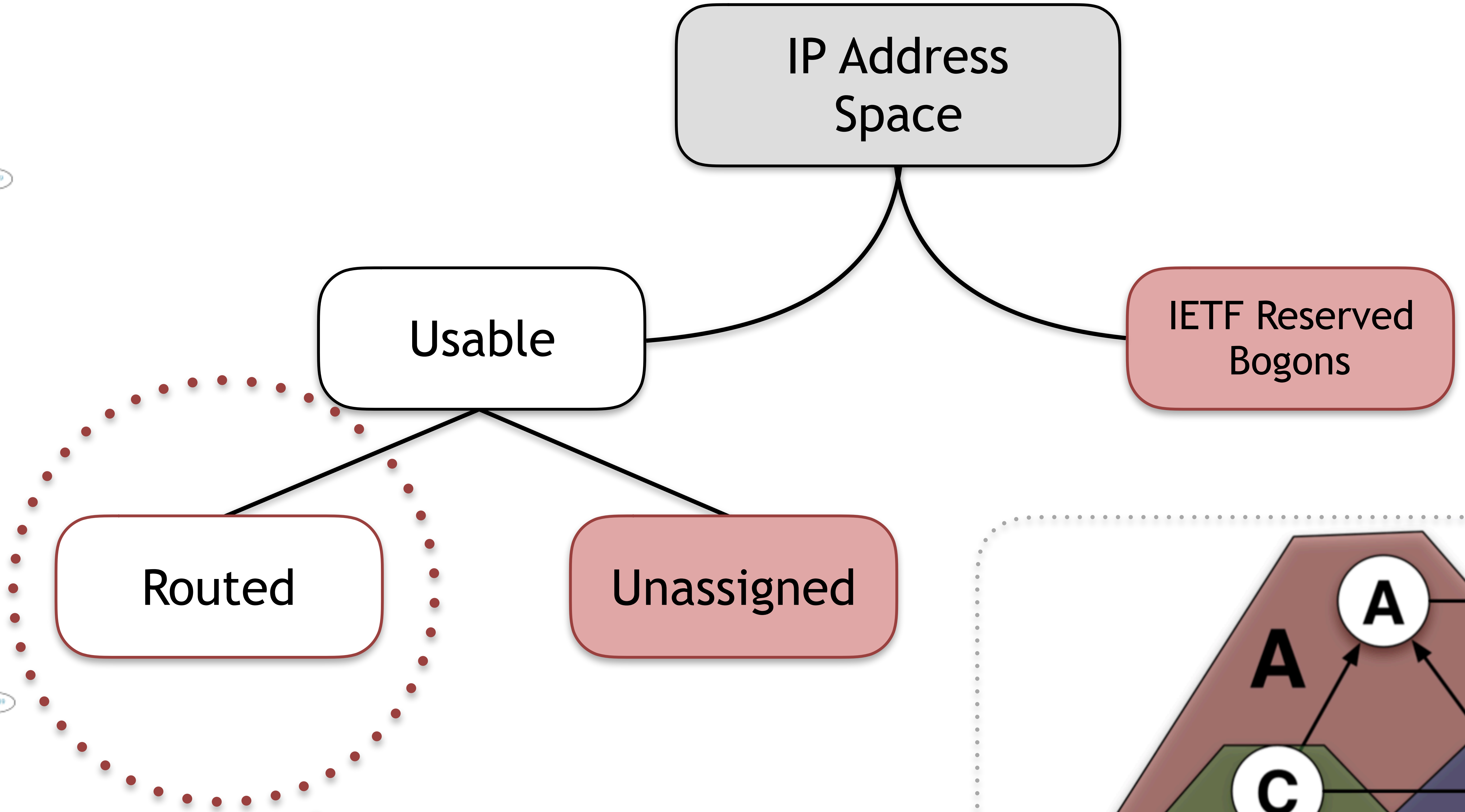


Inferred based on BGP data and the links established by each AS

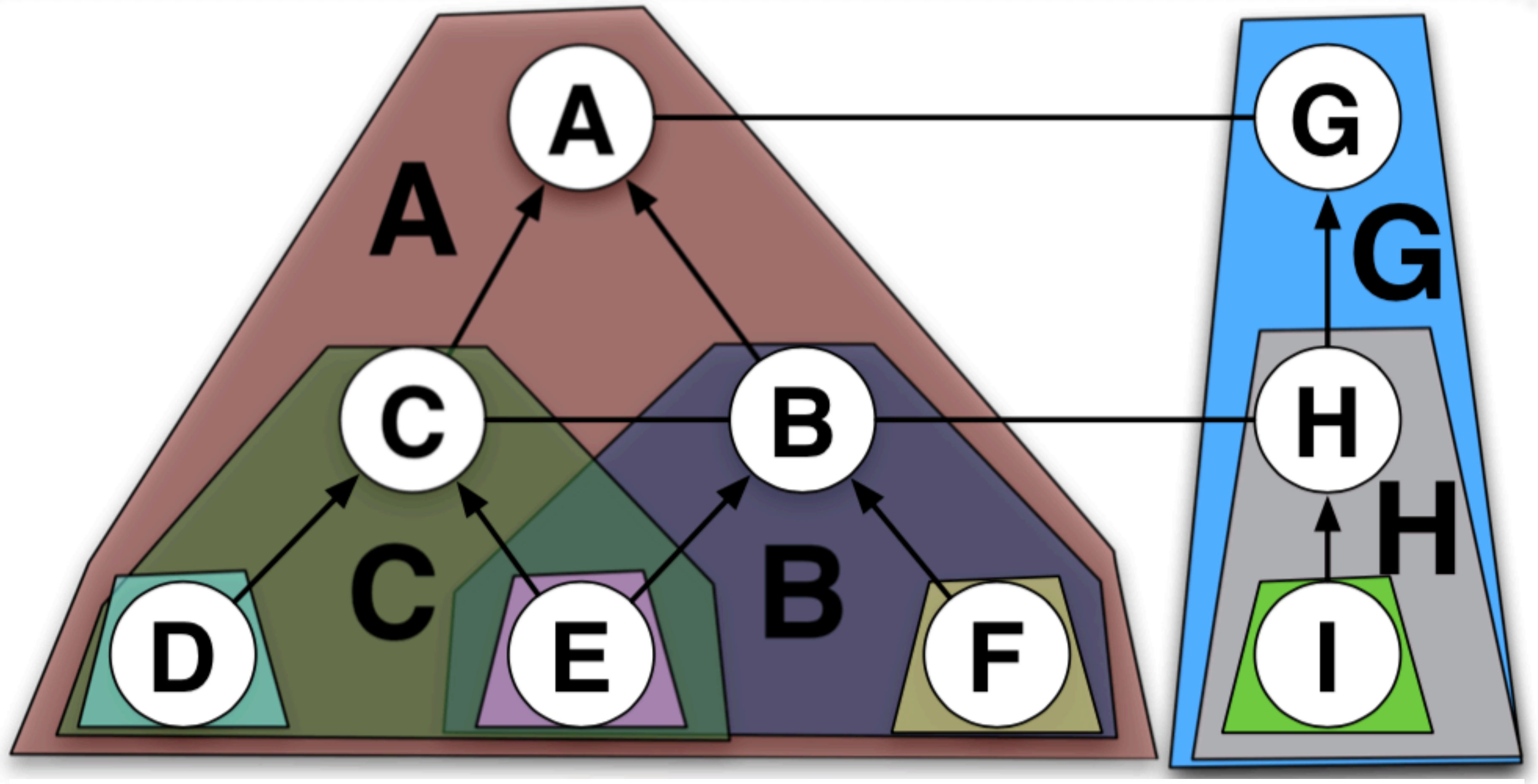
1. Identify Valid Source Address Space







Inferred based on BGP data and the links established by each AS



Customer Cones

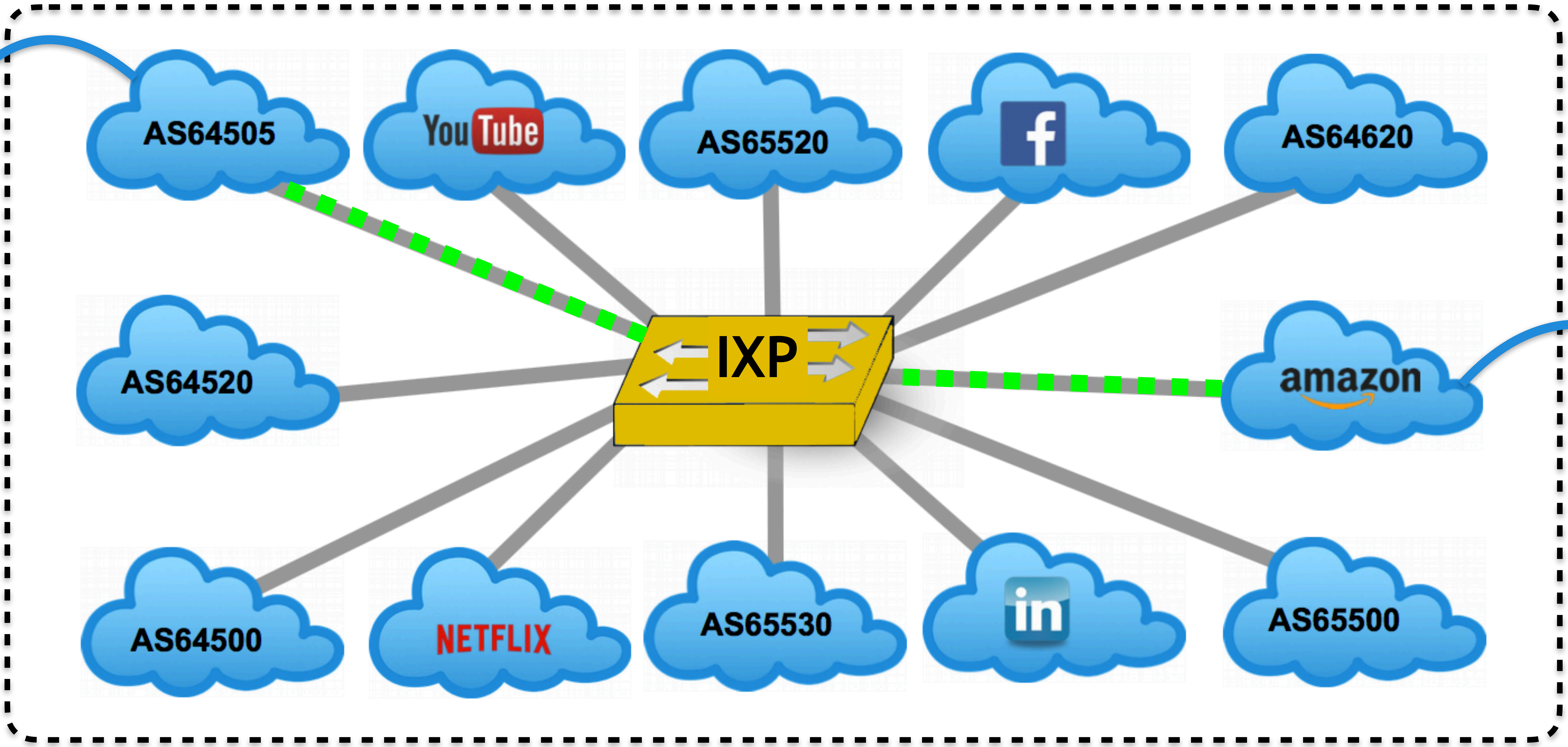
Define the set of ASes a given AS can reach through its customers

2. Tackle IXP Topology and Traffic Visibility Properties

Focus on understanding operational complexities of the vantage point

AS64505
Prefix-level
Customer Cone

168.228.252.0/22
200.17.80.0/20
200.132.59.0/24
200.236.32.0/19
200.19.0.0/21
200.238.0.0/18
…



13.32.136.2/23
52.216.180/24
75.2.82.0/24
161.38.206.0/23
216.137.62.0/24
…

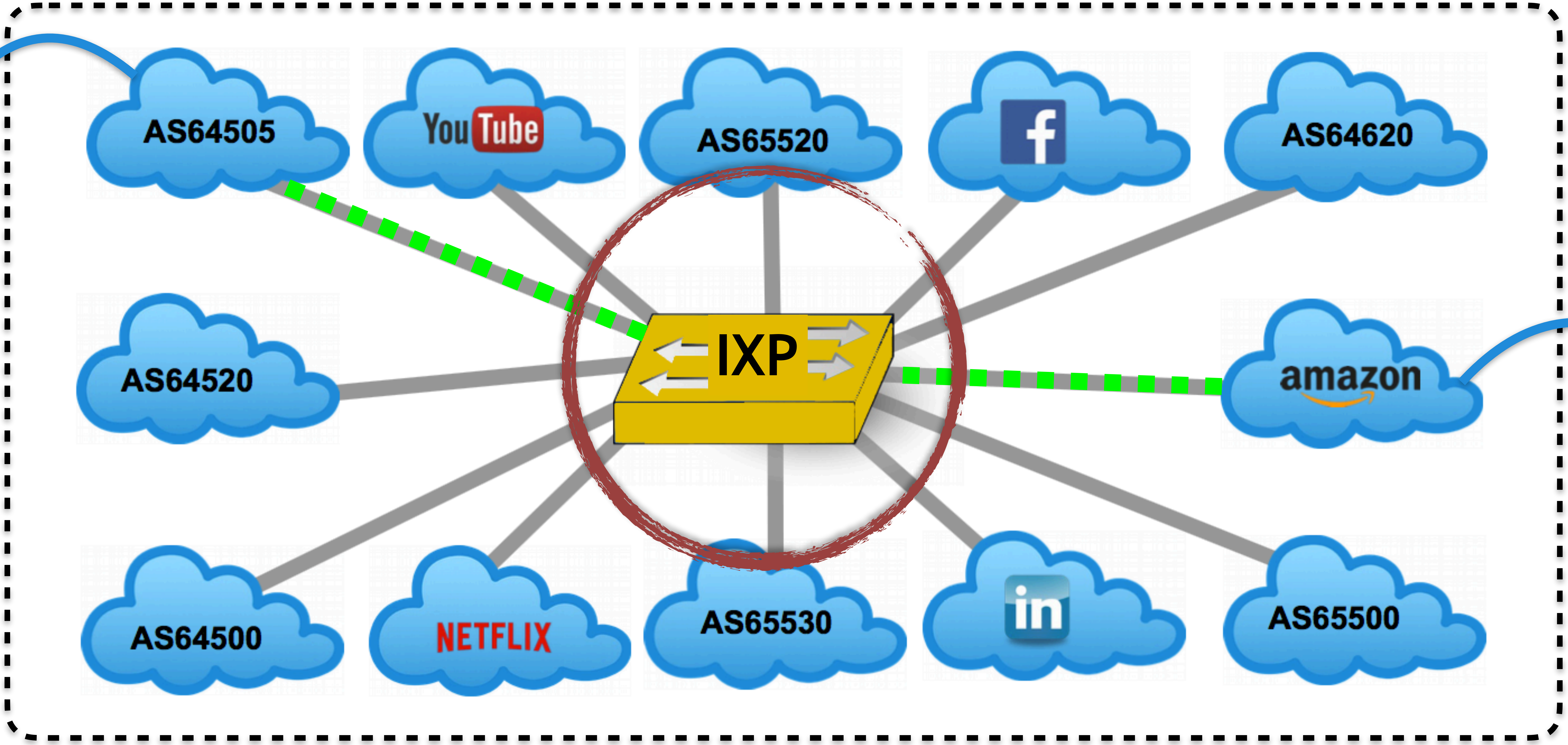
Amazon’s AS
Prefix-level
Customer Cone

2. Tackle IXP Topology and Traffic Visibility Properties

Focus on understanding operational complexities of the vantage point

AS64505
Prefix-level
Customer Cone

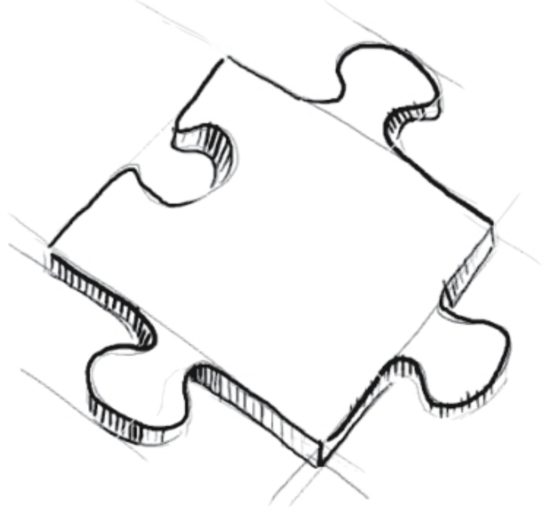
168.228.252.0/22
200.17.80.0/20
200.132.59.0/24
200.236.32.0/19
200.19.0.0/21
200.238.0.0/18
…

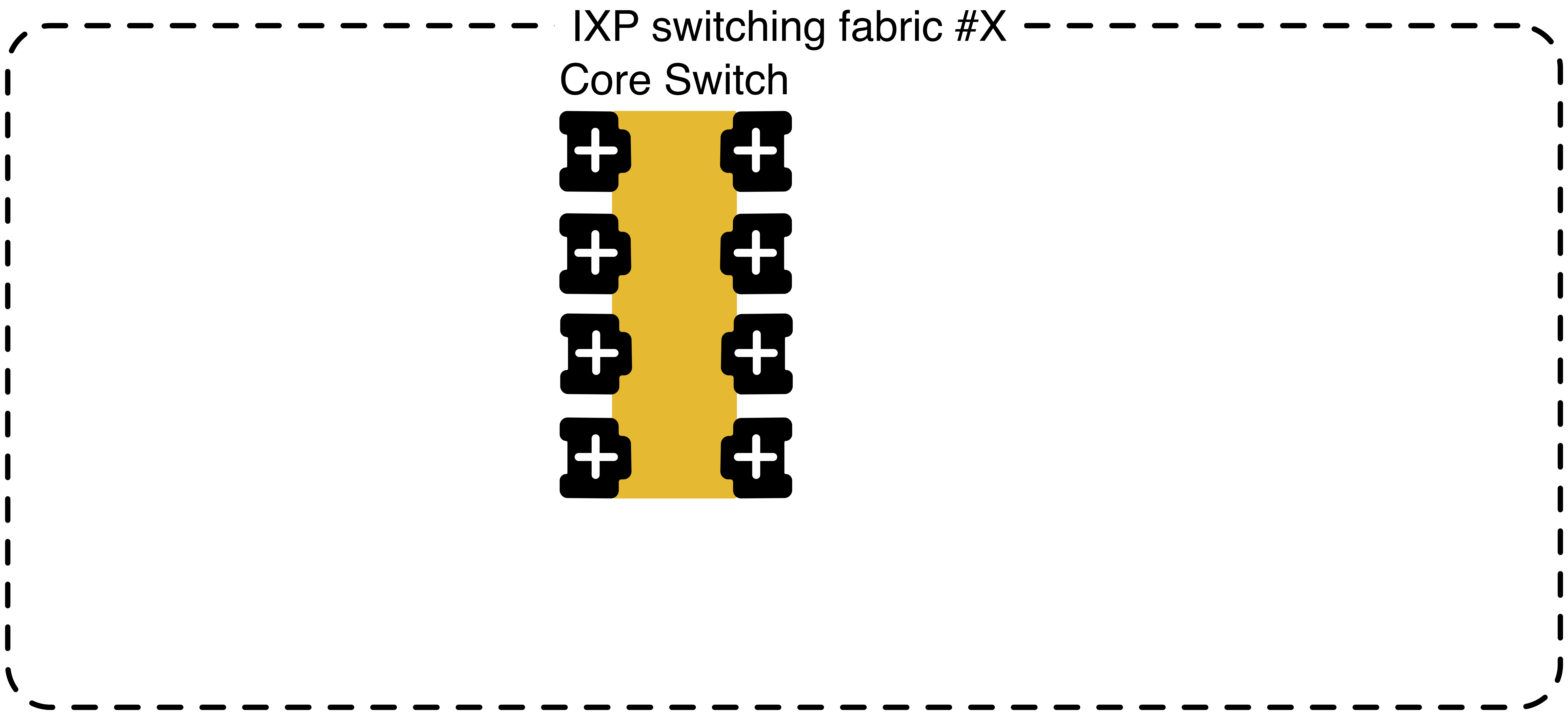


13.32.136.2/23
52.216.180/24
75.2.82.0/24
161.38.206.0/23
216.137.62.0/24
…

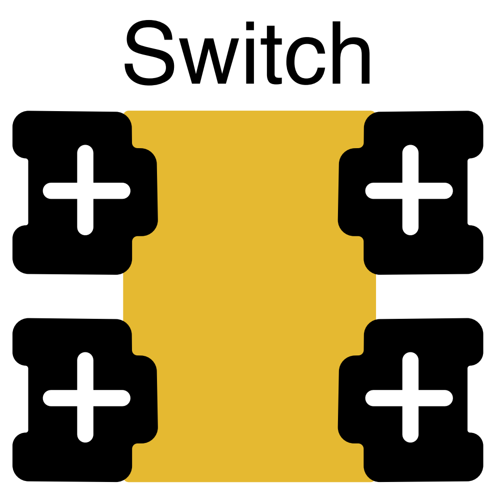
Amazon's AS
Prefix-level
Customer Cone

2. Tackle IXP Topology and Traffic Visibility Properties

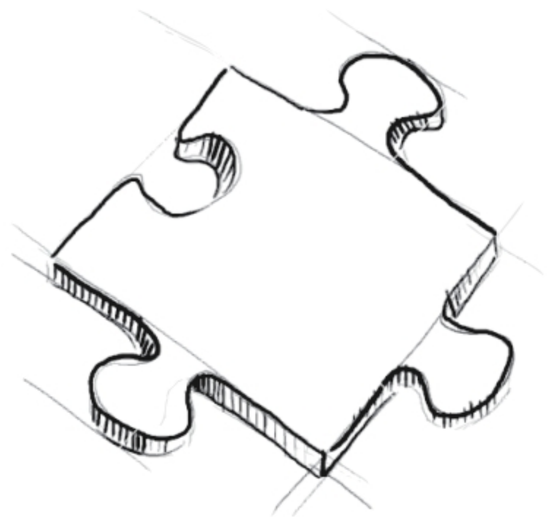


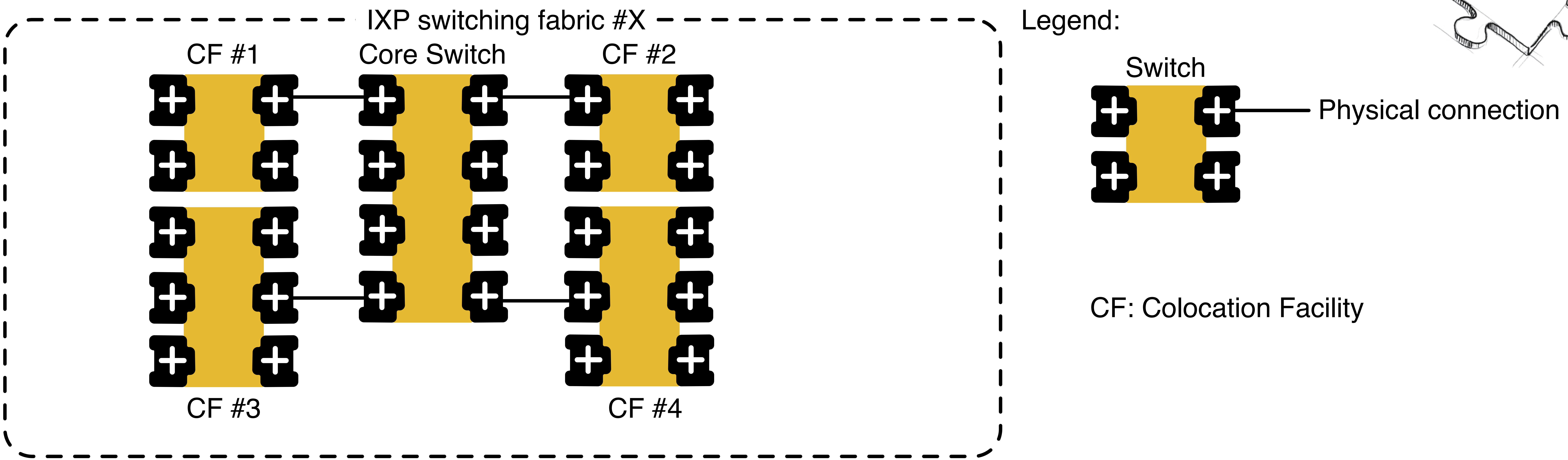


Legend:

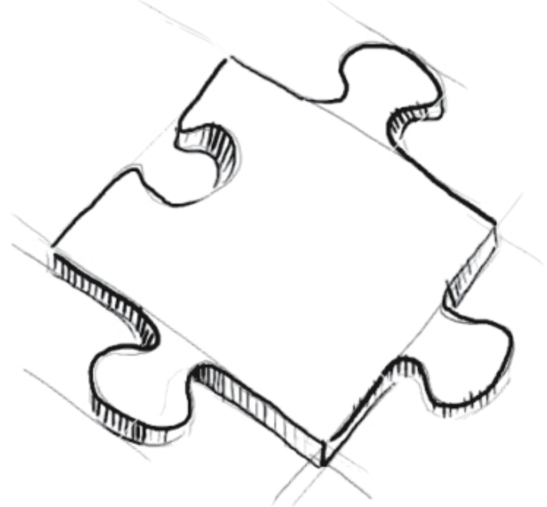


2. Tackle IXP Topology and Traffic Visibility Properties

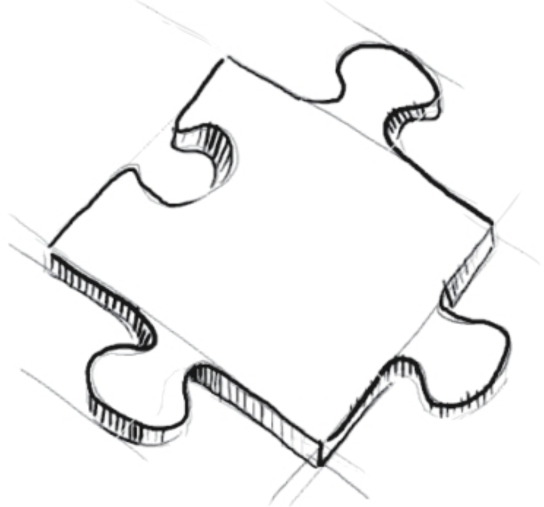




2. Tackle IXP Topology and Traffic Visibility Properties

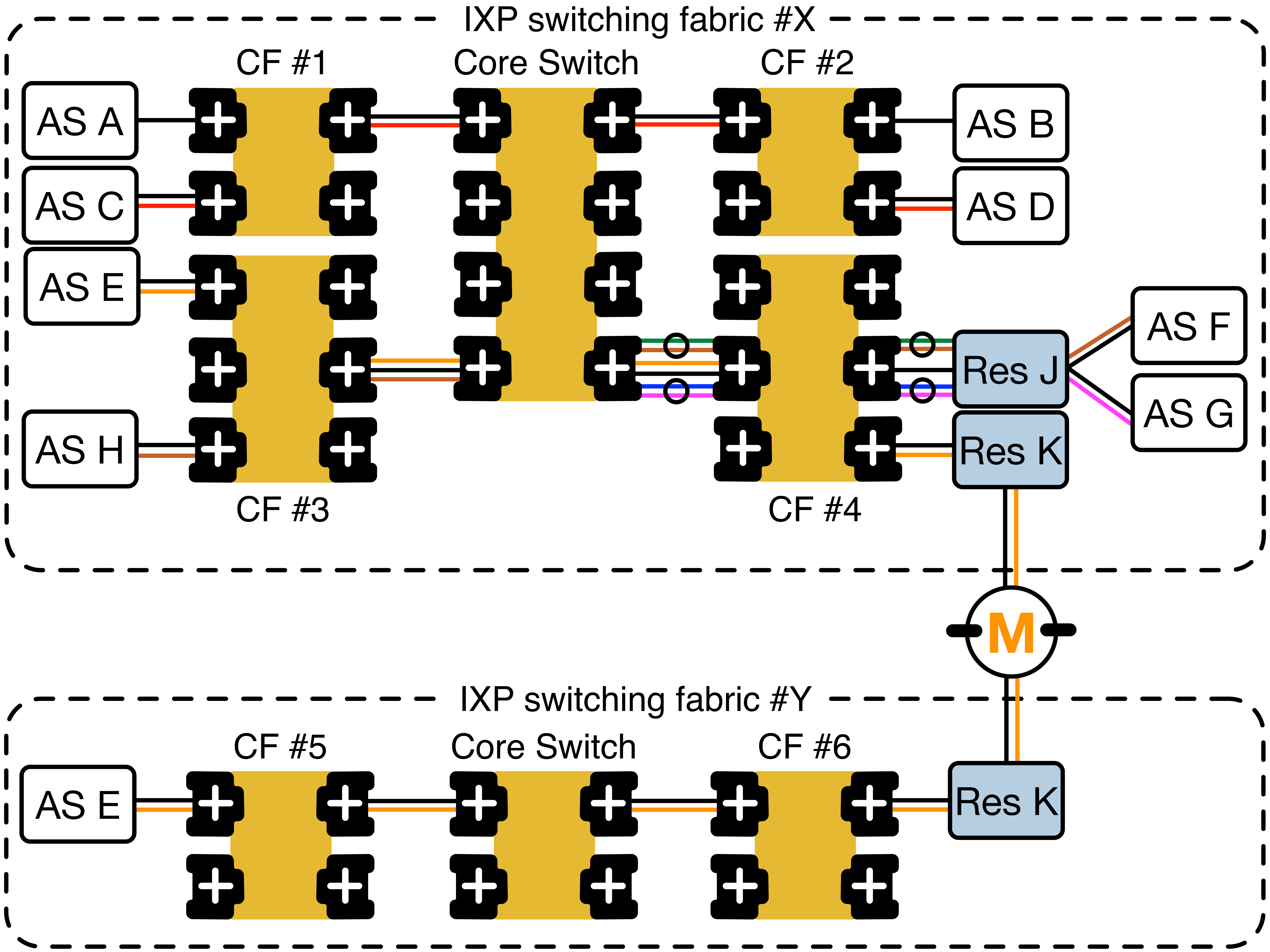


2. Tackle IXP Topology and Traffic Visibility Properties

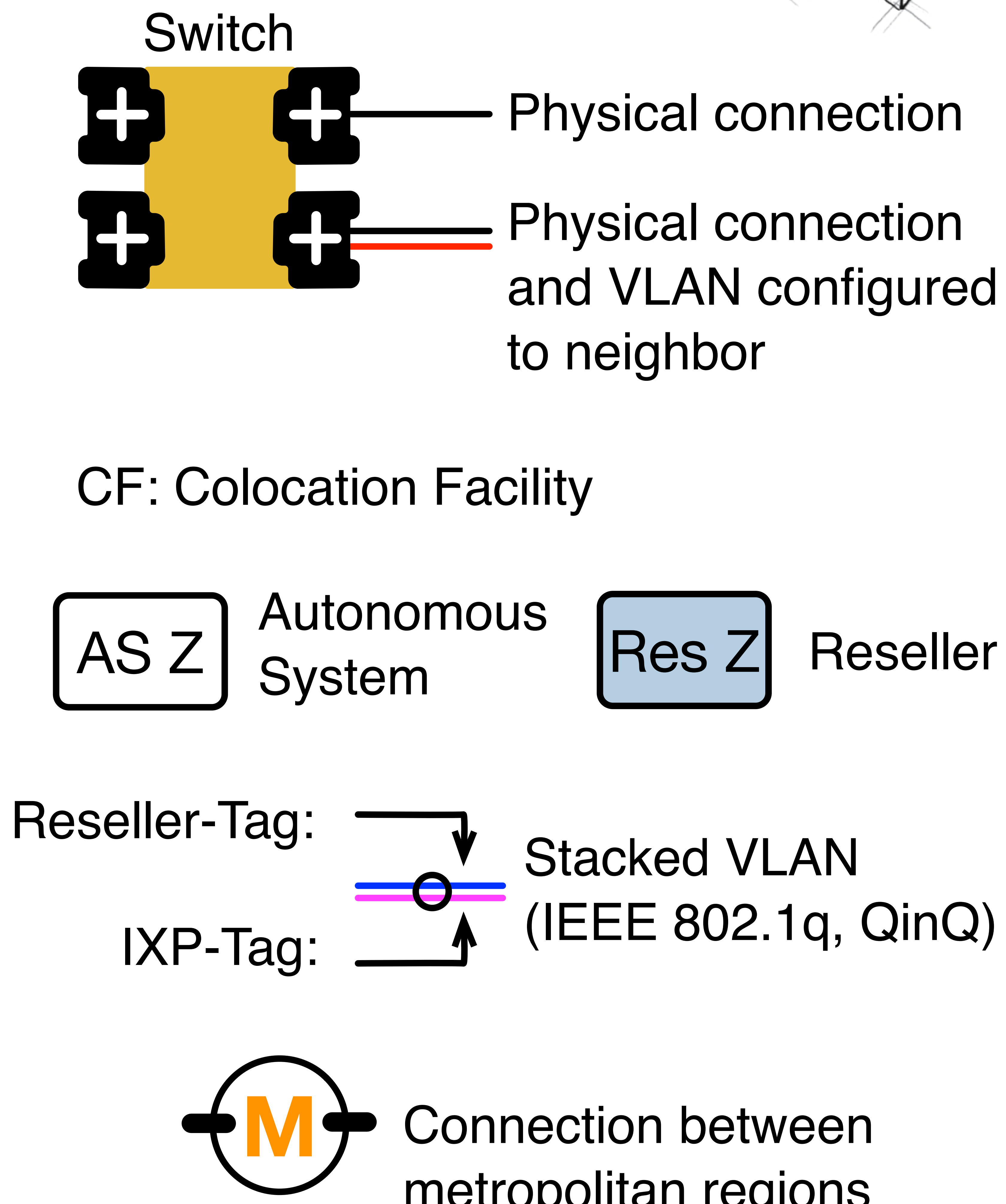


2. Tackle IXP Topology and Traffic Visibility Properties

2. Tackle IXP Topology and Traffic Visibility Properties

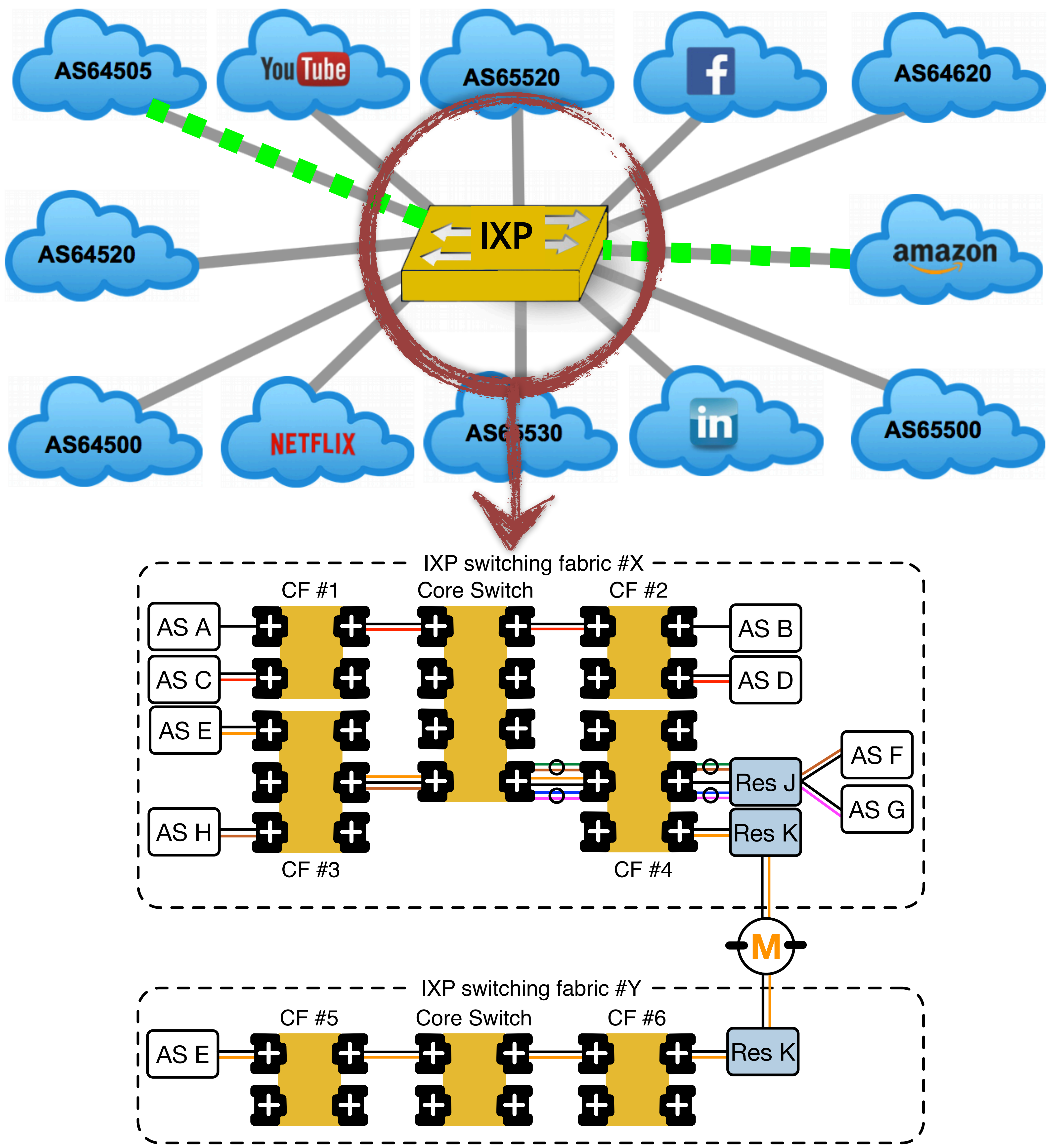


Legend:

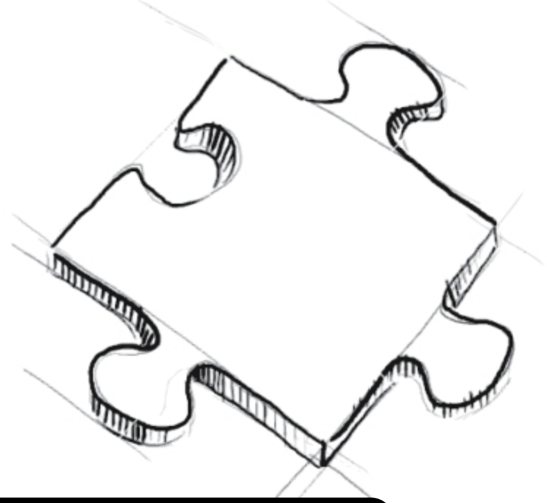


2. Tackle IXP Topology and Traffic Visibility Properties

- In practice IXPs, CFs and resellers offer complex services
- Interconnection practices occur below and are thus not visible to the IP layer or in the BGP Protocol
- **Must take them into account during the traffic classification processing**



2. Tackle IXP Topology and Traffic Visibility Properties

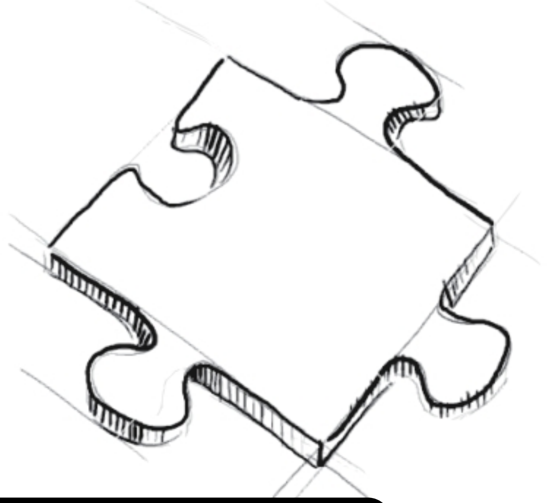


(1) **c2p**: customer-to-provider	(2) **p2p**: peer-to-peer
(3) **p2c**: provider-to-customer	(4) **s2s**: sibling-to-sibling

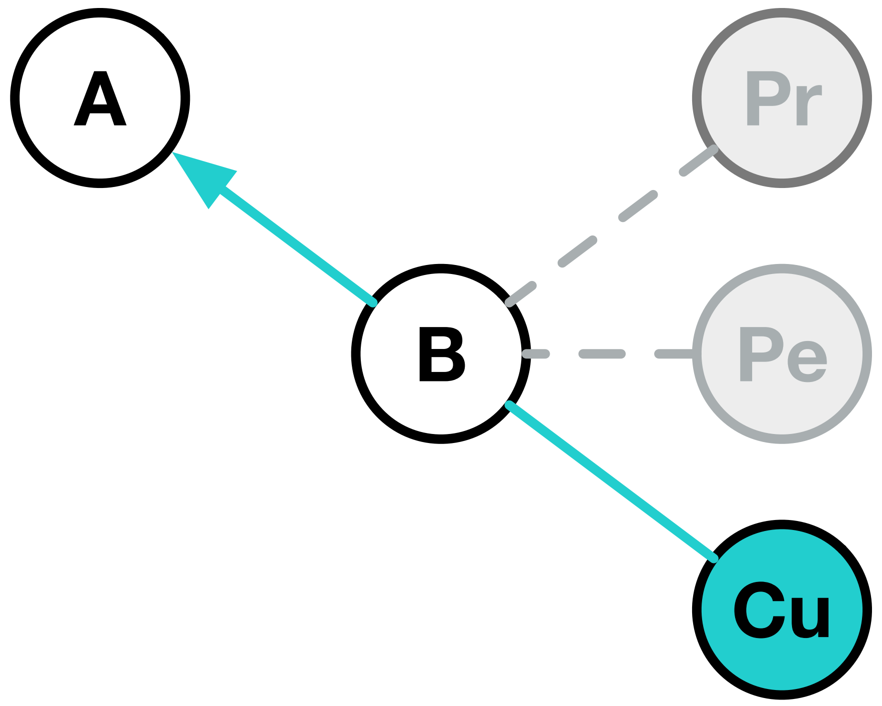
Legend

Pr: Provider
Pe: Peer
Cu: Customer

2. Tackle IXP Topology and Traffic Visibility Properties



(1) **c2p**: customer-to-provider



customer B to **provider** A

(2) **p2p**: peer-to-peer

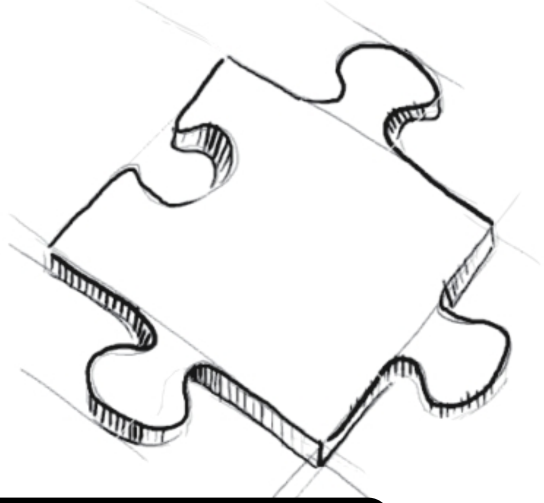
(3) **p2c**: provider-to-customer

(4) **s2s**: sibling-to-sibling

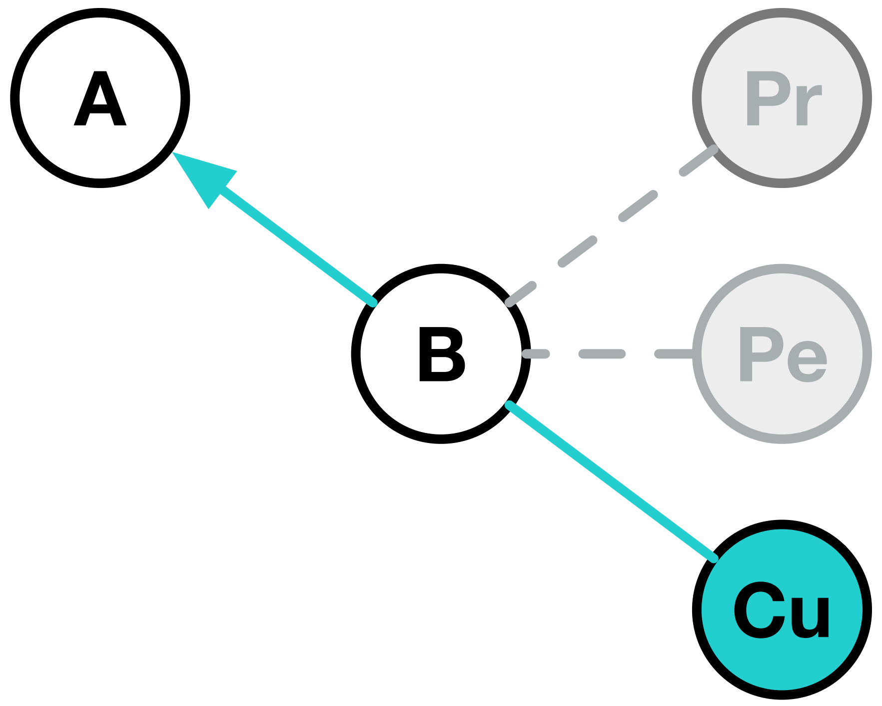
Legend

Pr: Provider
Pe: Peer
Cu: Customer

2. Tackle IXP Topology and Traffic Visibility Properties

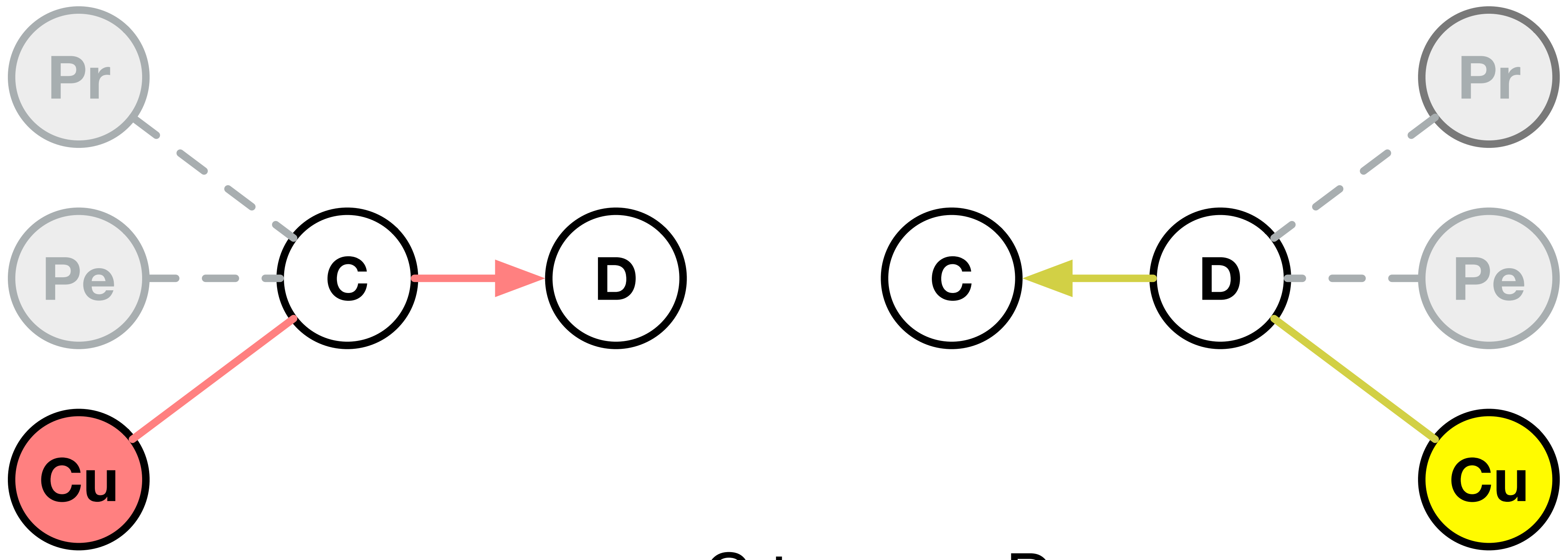


(1) **c2p**: customer-to-provider



customer B to **provider** A

(2) **p2p**: peer-to-peer



peer C to **peer** D

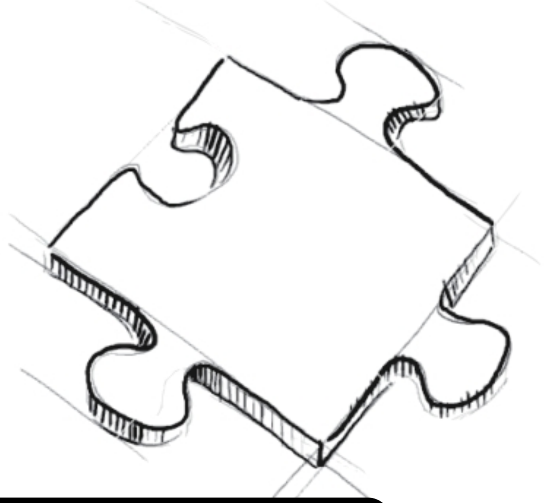
Legend

Pr: Provider
Pe: Peer
Cu: Customer

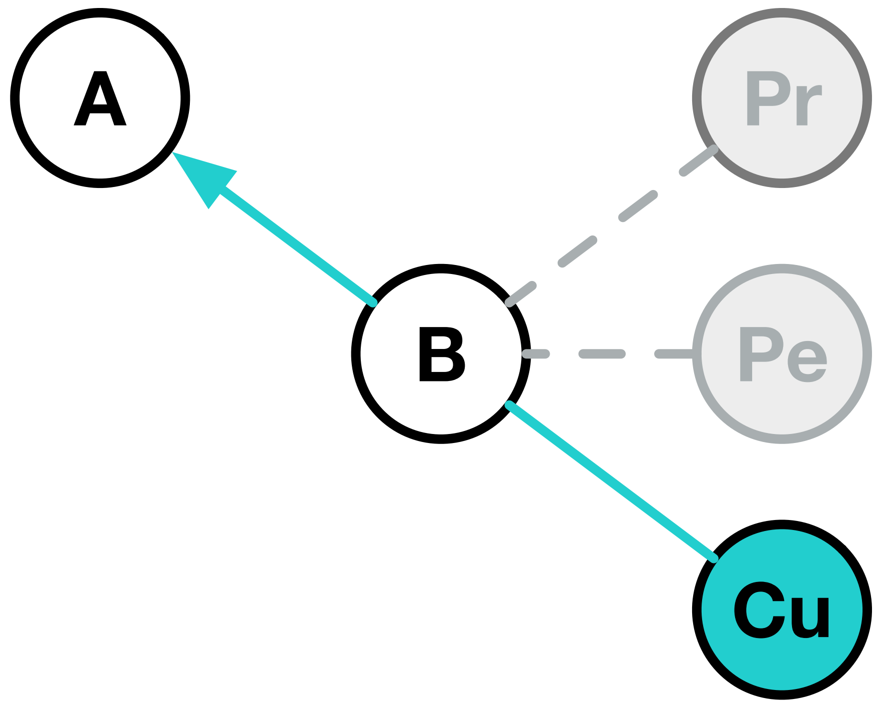
(3) **p2c**: provider-to-customer

(4) **s2s**: sibling-to-sibling

2. Tackle IXP Topology and Traffic Visibility Properties

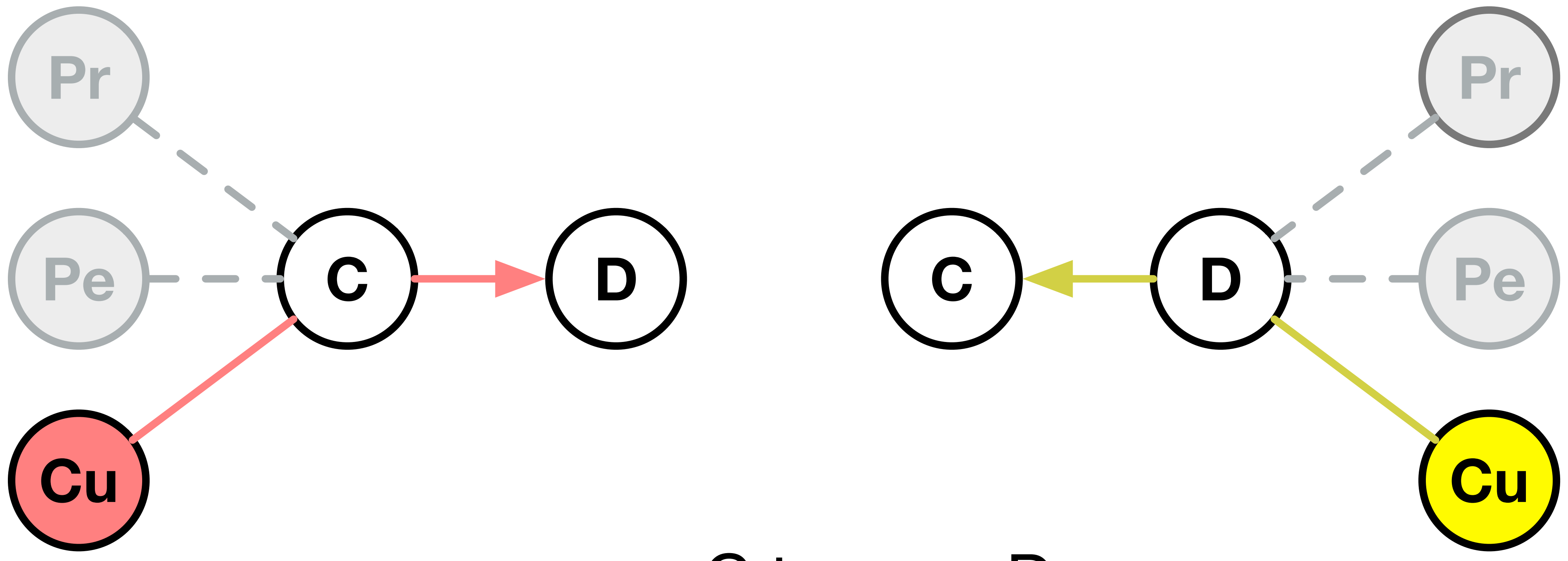


(1) **c2p**: customer-to-provider



customer B to **provider** A

(2) **p2p**: peer-to-peer



peer C to **peer** D

Transits only traffic from its customer cone

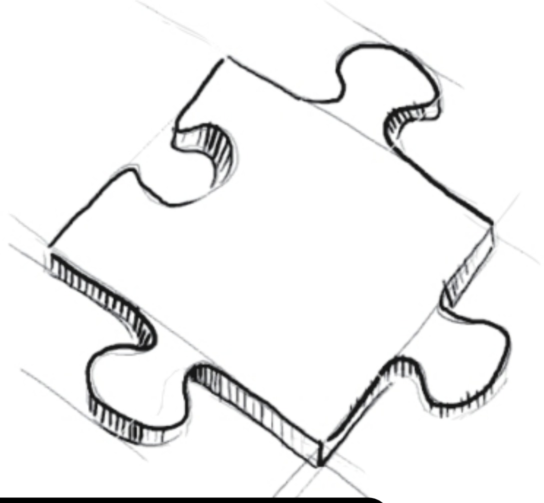
(3) **p2c**: provider-to-customer

(4) **s2s**: sibling-to-sibling

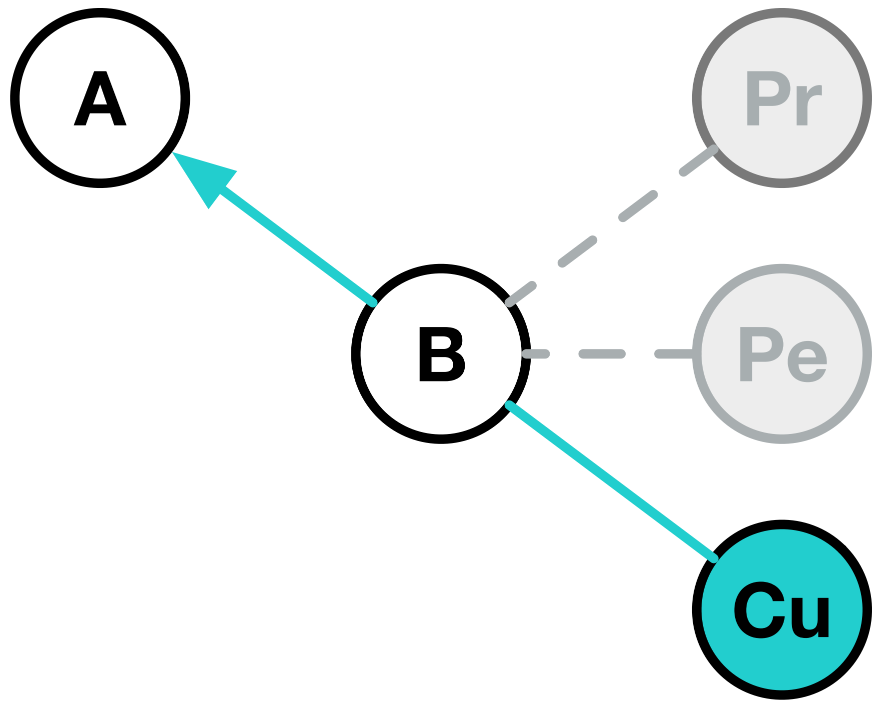
Legend

Pr: Provider
Pe: Peer
Cu: Customer

2. Tackle IXP Topology and Traffic Visibility Properties

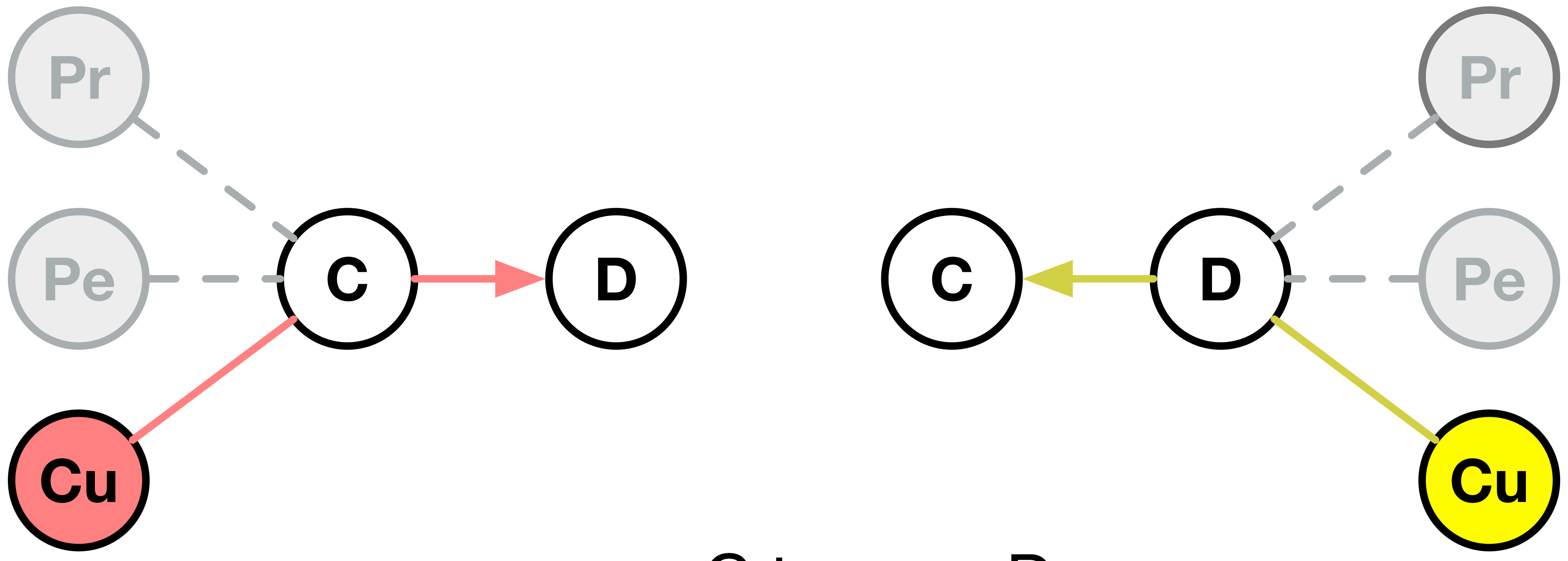


(1) **c2p**: customer-to-provider



customer B to **provider** A

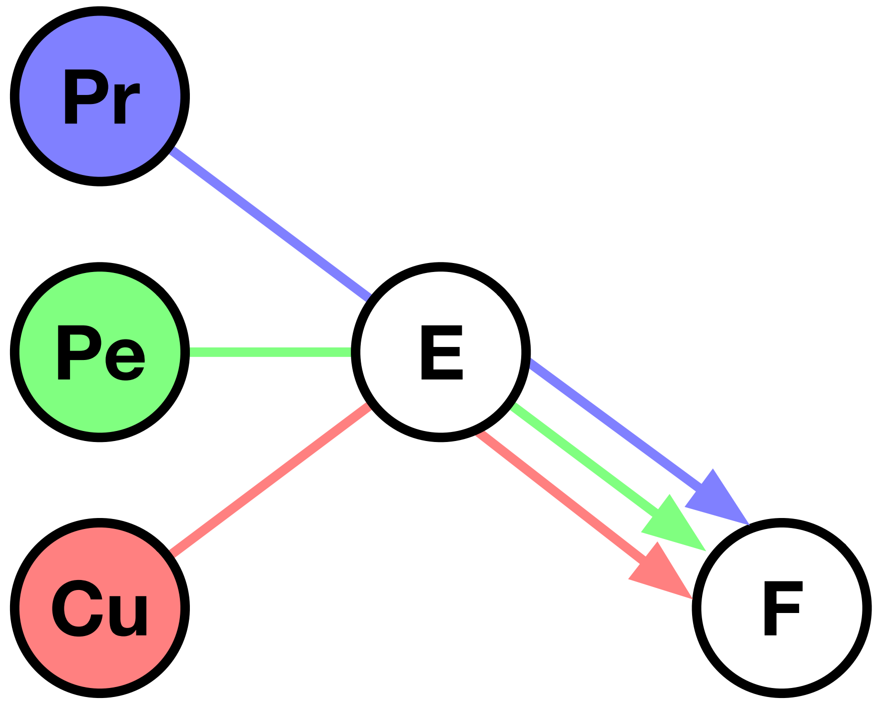
(2) **p2p**: peer-to-peer



peer C to **peer** D

Transits only traffic from its customer cone

(3) **p2c**: provider-to-customer



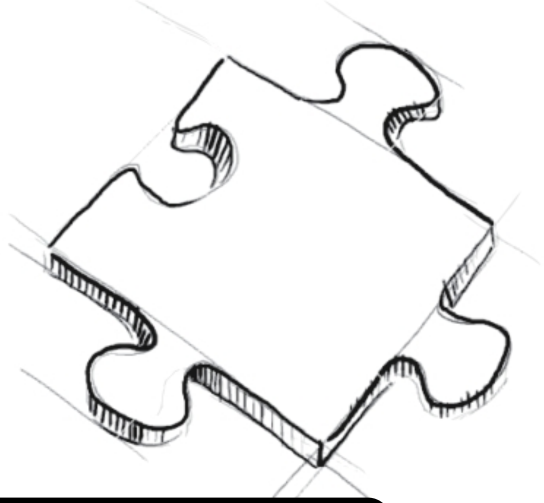
provider E to **customer** F

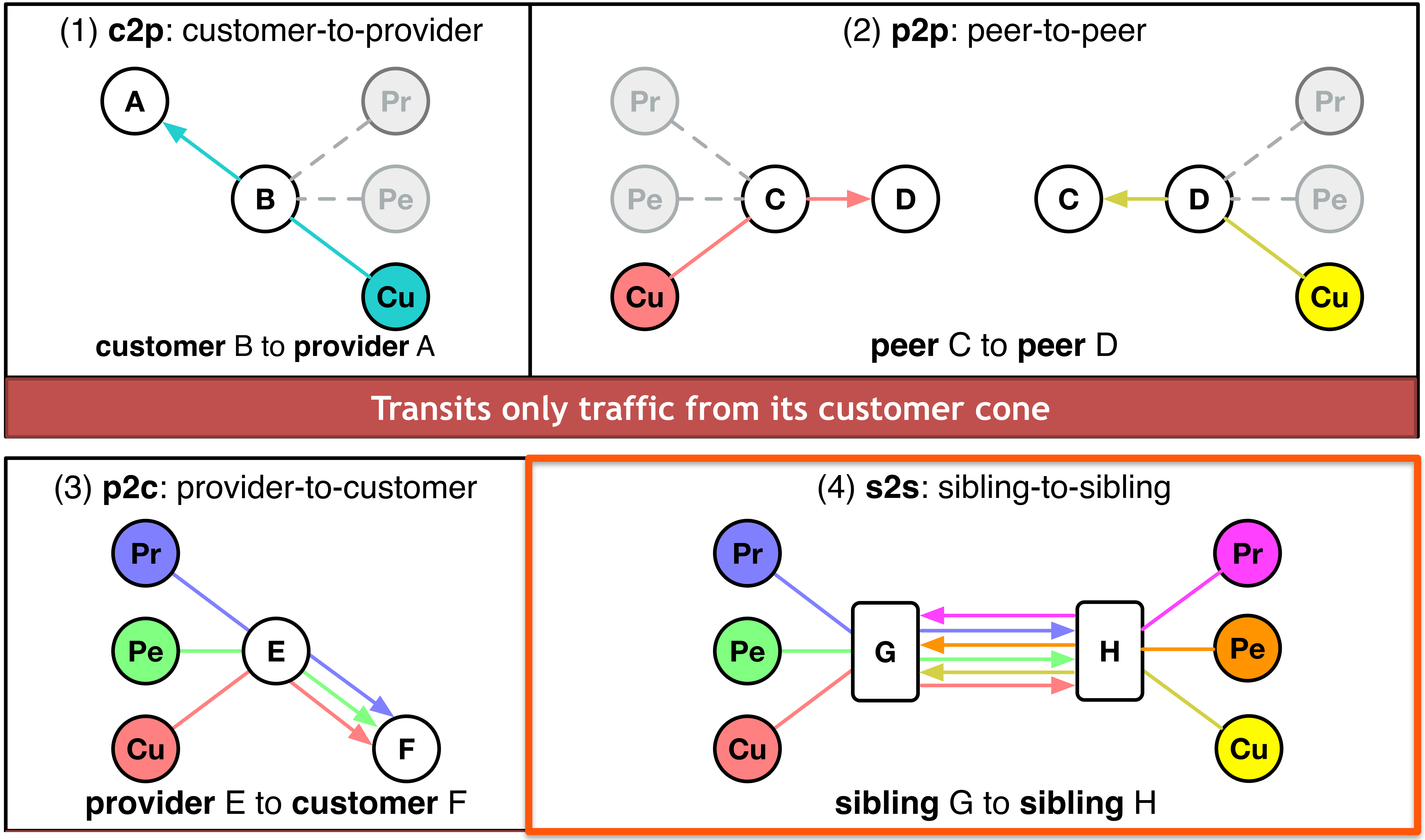
(4) **s2s**: sibling-to-sibling

Legend

Pr: Provider
Pe: Peer
Cu: Customer

2. Tackle IXP Topology and Traffic Visibility Properties

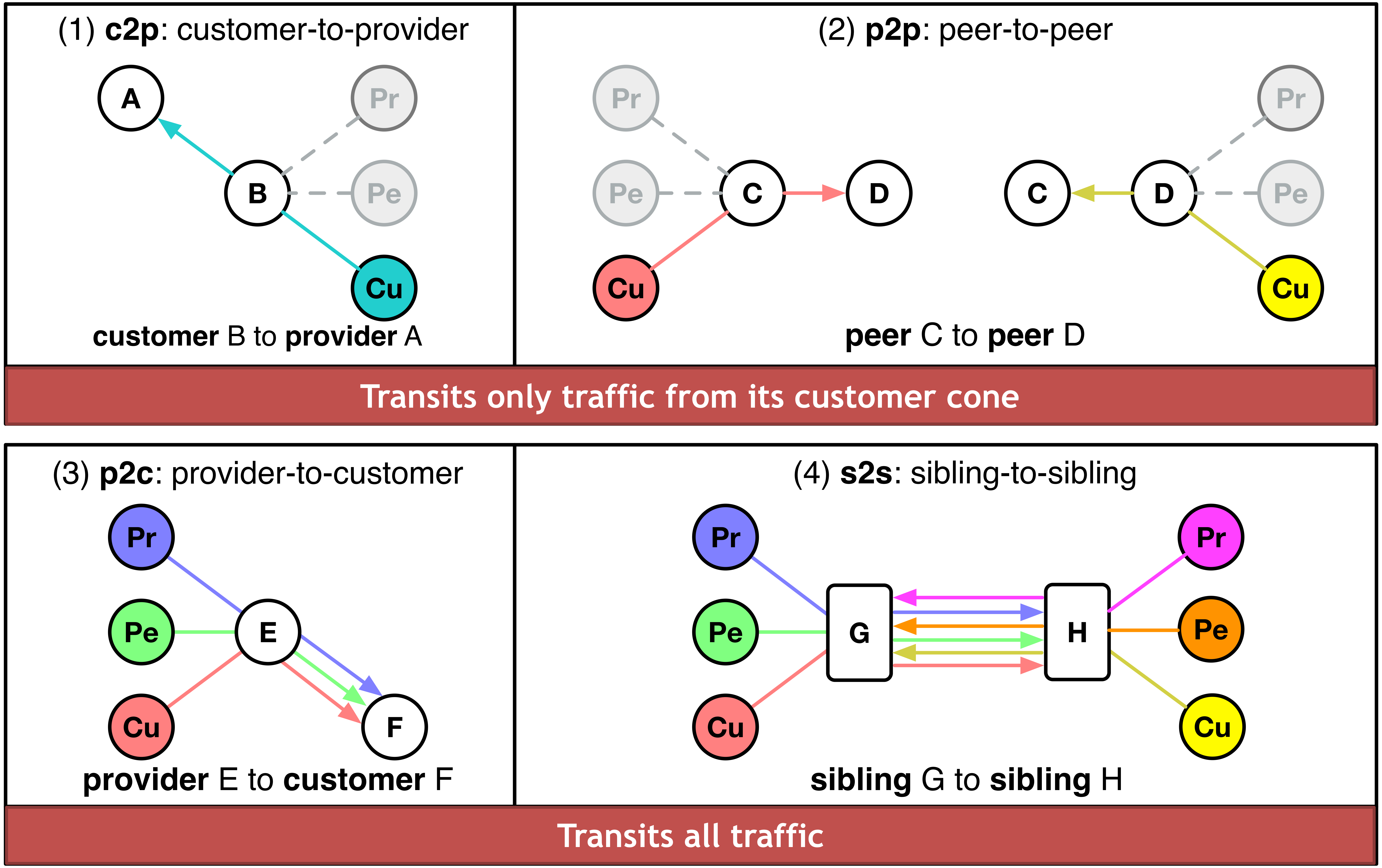




Legend

Pr: Provider
Pe: Peer
Cu: Customer

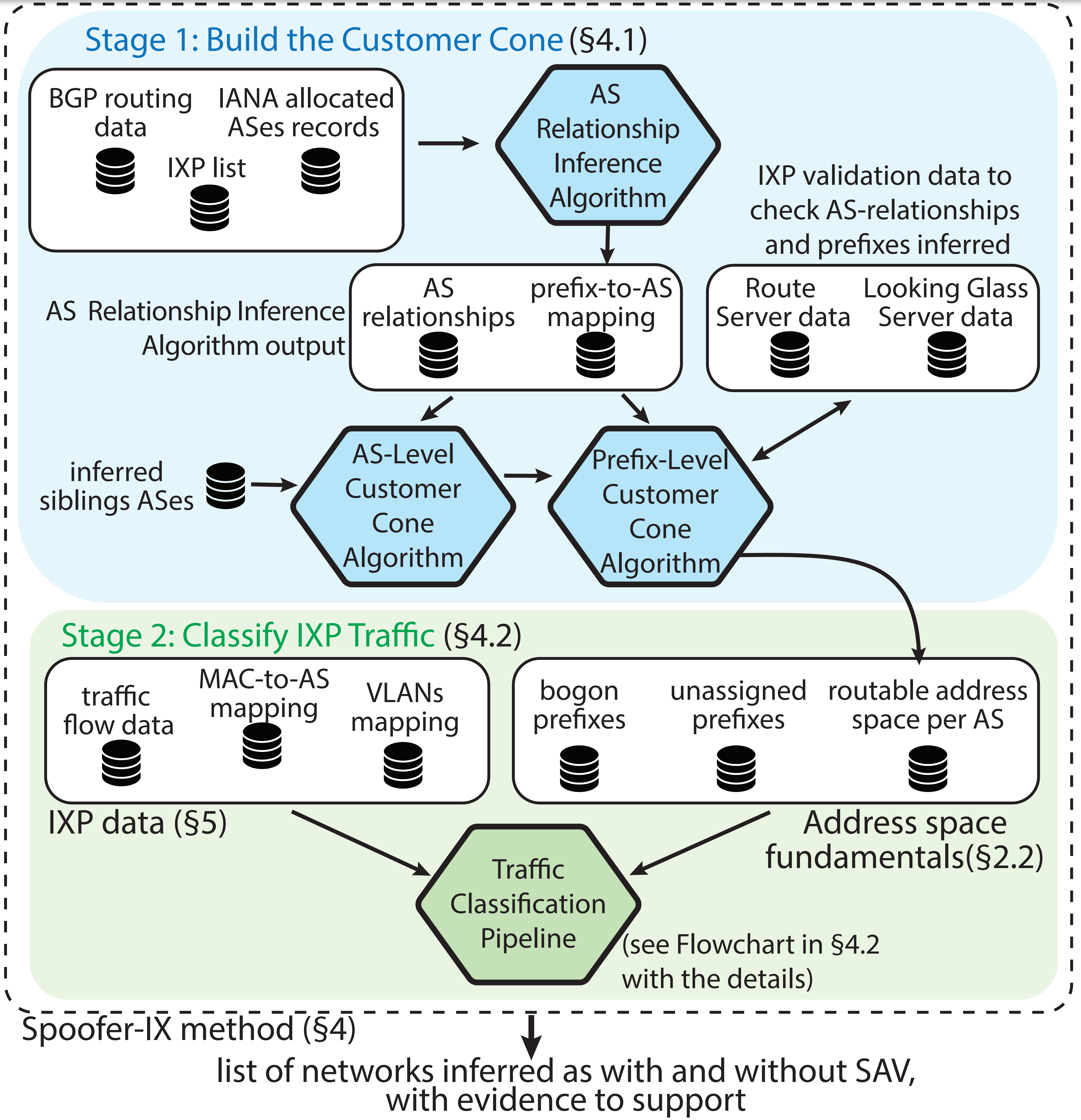
2. Tackle IXP Topology and Traffic Visibility Properties



Legend

Pr: Provider
Pe: Peer
Cu: Customer

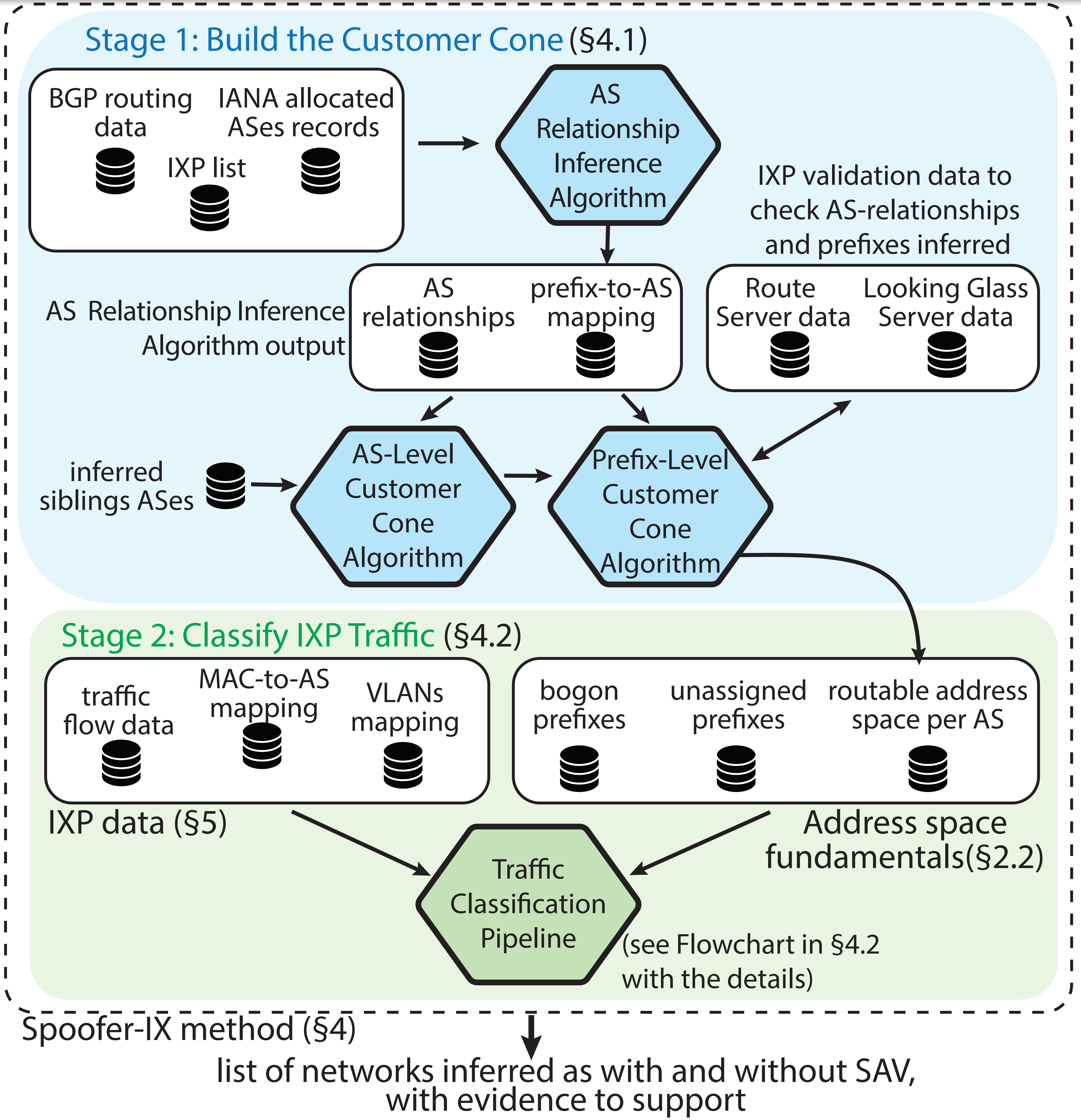
Spoofer-IX Inference Method: Putting the Pieces Together



See paper for details

Spoofer-IX Inference Method: Putting the Pieces Together

Divided into two stages

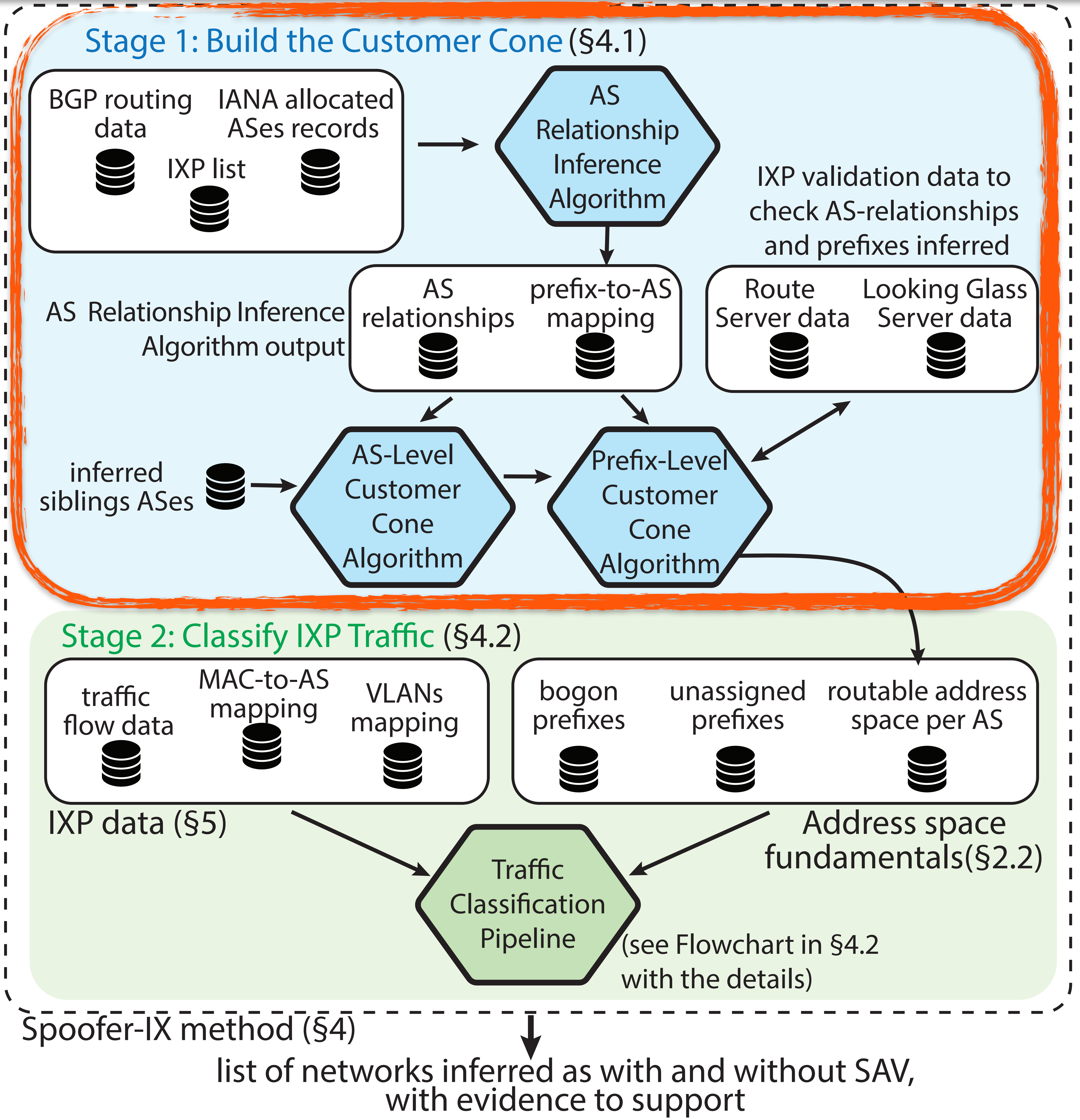


See paper for details

Spoofer-IX Inference Method: Putting the Pieces Together

Divided into two stages

- Stage 1: build the Customer Cone



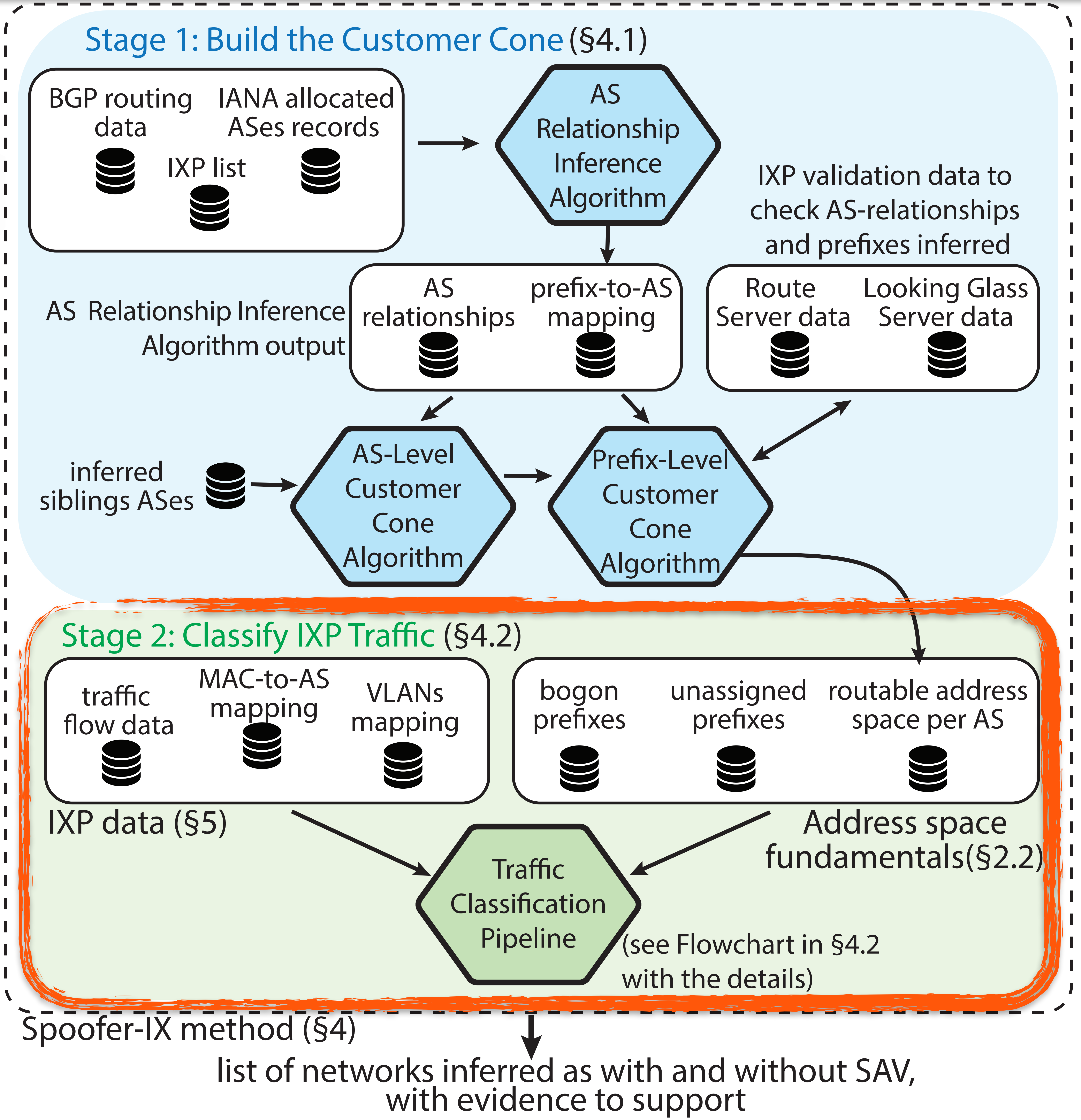
See paper for details

Spoofer-IX Inference Method: Putting the Pieces Together

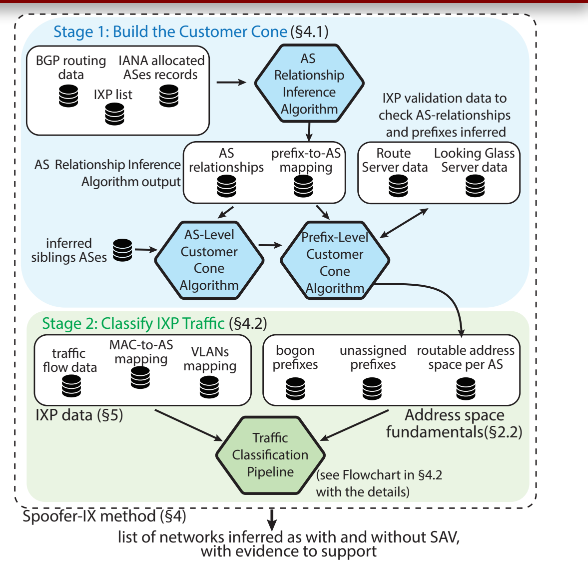
Divided into two stages

- Stage 1: build the Customer Cone
- Stage 2: classify IXP traffic

See paper for details



Stage 1: Build the Customer Cone



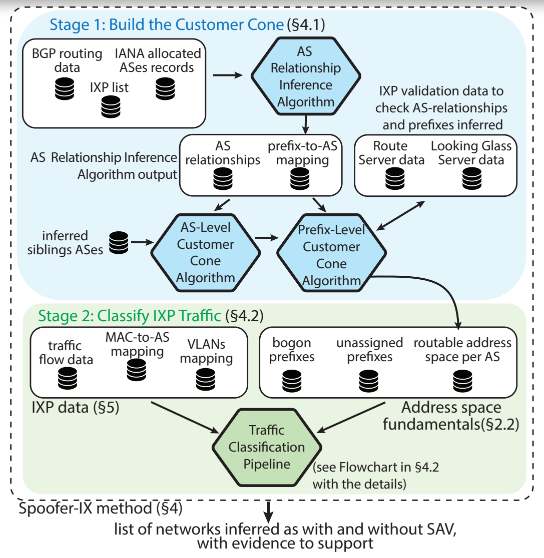
Subtleties in Cone Construction

Full Cone
(state-of-the-art [1])

Customer Cone
(Prefix-level Customer Cone)

Brief overview in this talk
See paper for full details

Stage 1: Build the Customer Cone



Subtleties in Cone Construction

Full Cone
(state-of-the-art [1])

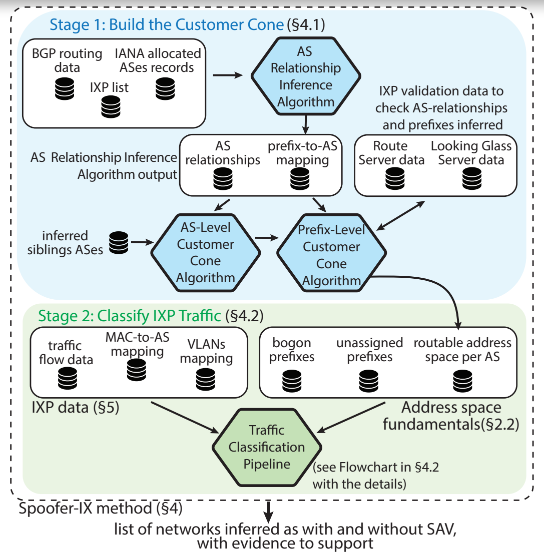
Do not distinguish types of AS-relationships

Customer Cone
(Prefix-level Customer Cone)

Takes into account the semantics of AS-relationships [2]

Brief overview in this talk
See paper for full details

Stage 1: Build the Customer Cone



Subtleties in Cone Construction

Full Cone
(state-of-the-art [1])

Do not distinguish types of AS-relationships

- More permissive
- Aims to minimize false positives
- Acknowledge that intentionally sacrifices specificity, i.e., inflating the address space considered legitimate
- Limited input BGP data sanitization

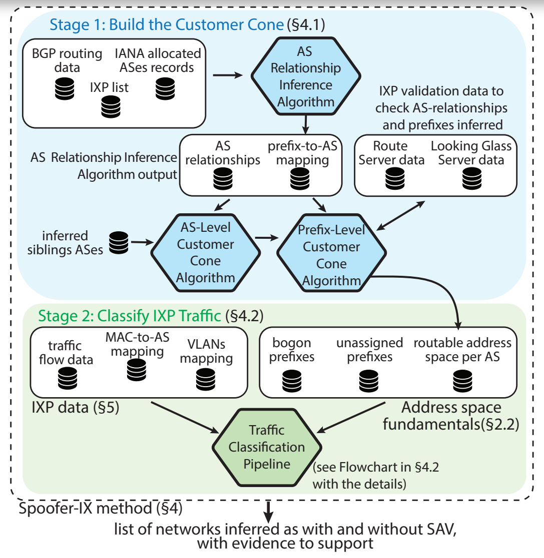
[1] Lichtblau et al. Detection, Classification, and Analysis of Inter-domain Traffic with Spoofed Source IP Addresses. In: ACM IMC, 2017.

Customer Cone
(Prefix-level Customer Cone)

Takes into account the semantics of AS-relationships [2]

Brief overview in this talk
See paper for full details

Stage 1: Build the Customer Cone



Subtleties in Cone Construction

Full Cone
(state-of-the-art [1])

Do not distinguish types of AS-relationships

- More permissive
- Aims to minimize false positives
- Acknowledge that intentionally sacrifices specificity, i.e., inflating the address space considered legitimate
- Limited input BGP data sanitization

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

Customer Cone
(Prefix-level Customer Cone)

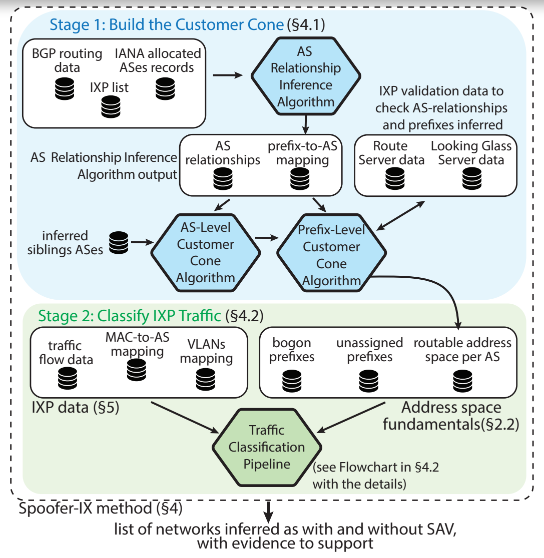
Takes into account the semantics of AS-relationships [2]

- More restrictive
- Aims to be accurate
- Rigorous AS-Path (BGP) sanitization
- Accounts for hybrid relationships and accommodates traffic engineering practices

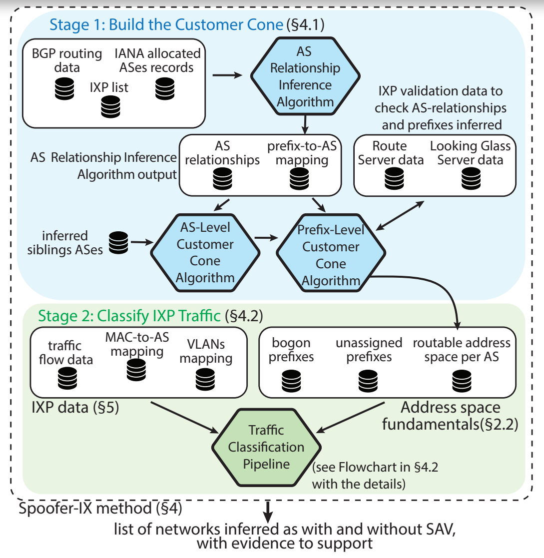
[2] Luckie et al. AS Relationships, Customer Cones, and Validation. In: ACM IMC, 2013.

Brief overview in this talk
See paper for full details

Stage 2: Classify IXP Traffic



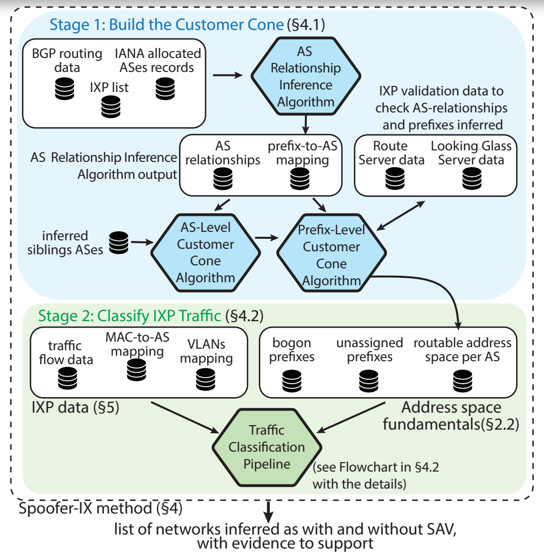
Stage 2: Classify IXP Traffic



Phase 1: filter Bogon and Unassigned addresses

this phase is independent of any routing semantics

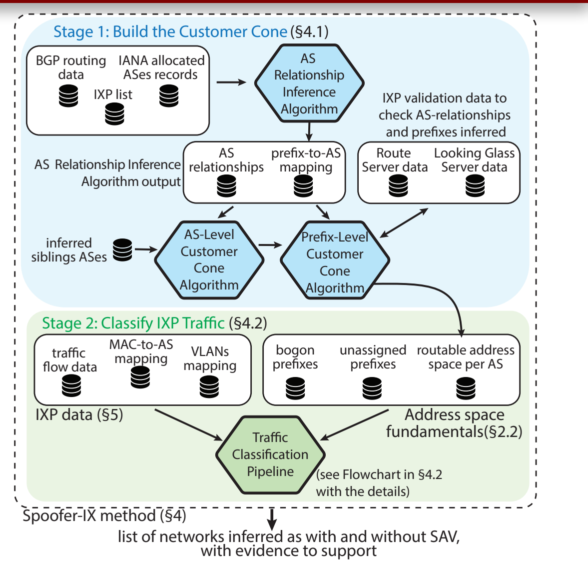
Stage 2: Classify IXP Traffic



Phase 2: filter Unverifiable packets

packets that are not suitable to inference of spoofing using the inferred cones or due to IXP topology and traffic visibility impediments

Stage 2: Classify IXP Traffic

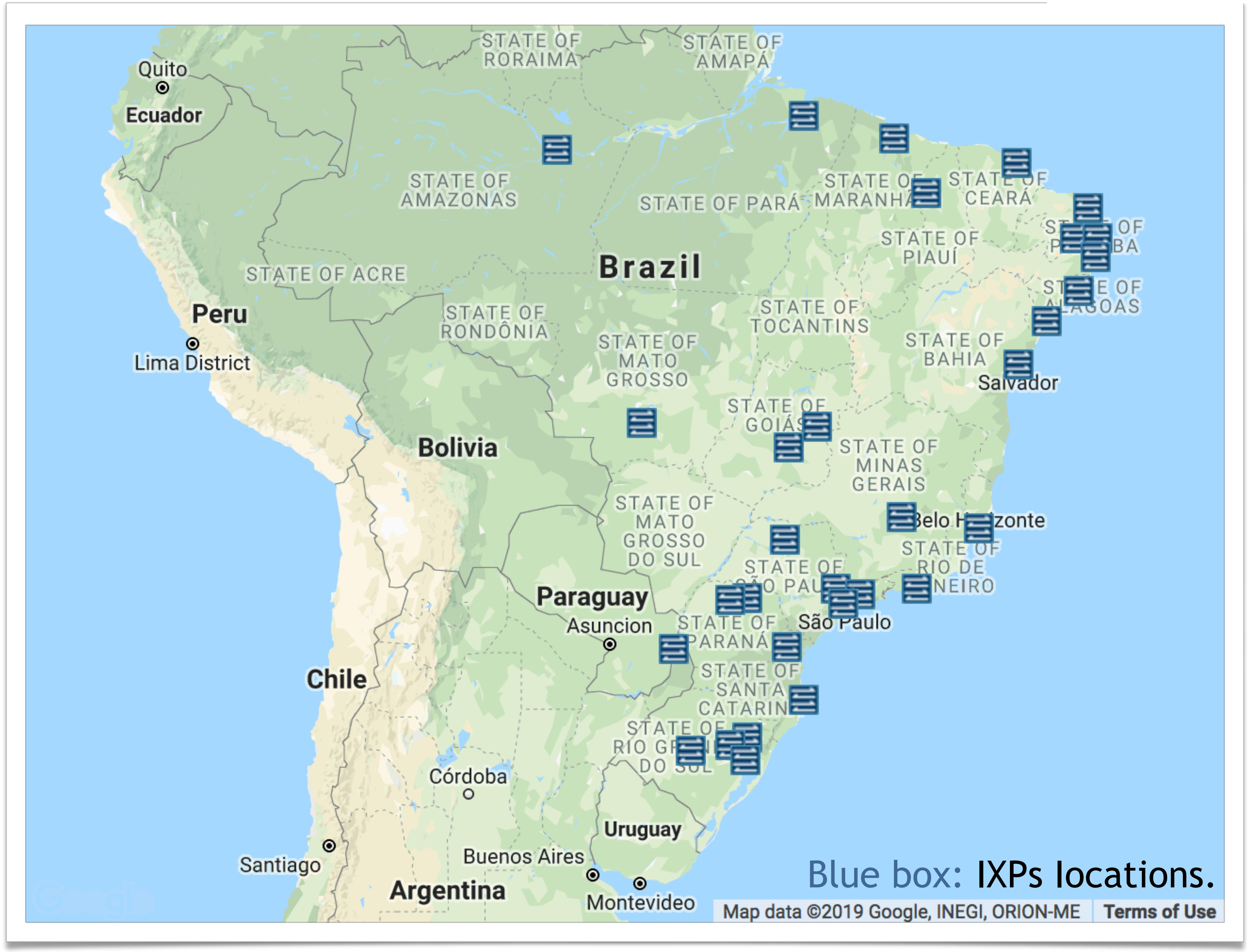


Phase 3: classify Packets with Customer Cone

packets whose source IP belongs to the sending AS’s customer cone address space are classified as *in-cone*. Otherwise, we classify the packet as *out-of-cone*

Longitudinal Study

- Study realized at the third largest IXP at the Brazilian IX.br ecosystem
- Transports up to 200 Gbps of traffic among 200+ members
- Two uninterrupted sFlow datasets:
  - April 1 to May 6, 2017 (5 weeks)
  - May 1 to June 5, 2019 (5 weeks)
  - sampling rate 1/4096
- Compare our method with Full Cone (state-of-the-art) [1]



Brazilian IX.br ecosystem
[IX.br, 2019]

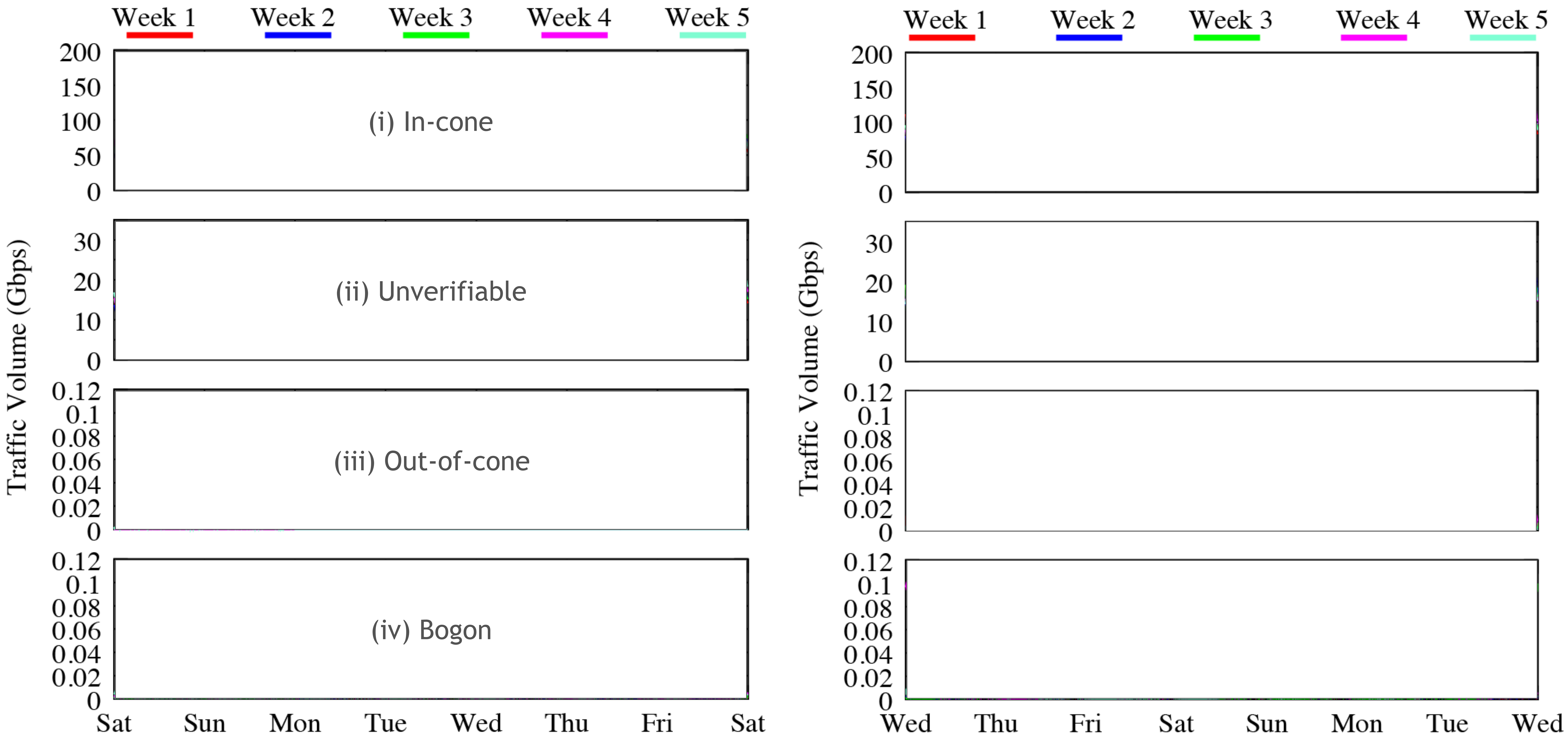
[1] Lichtblau et al. Detection, Classification, and Analysis of Inter-domain Traffic with Spoofed Source IP Addresses. In: ACM IMC, 2017.

What Have We Found ?

- No strong evidence of pervasive presence of spoofed traffic for the different observation periods in 2017 and 2019
- Found an upper bound volume of out-of-cone traffic to be more than an order of magnitude less than the state-of-the-art method
- Our method reveals inaccuracies in methods that are agnostic to AS-relationship semantics

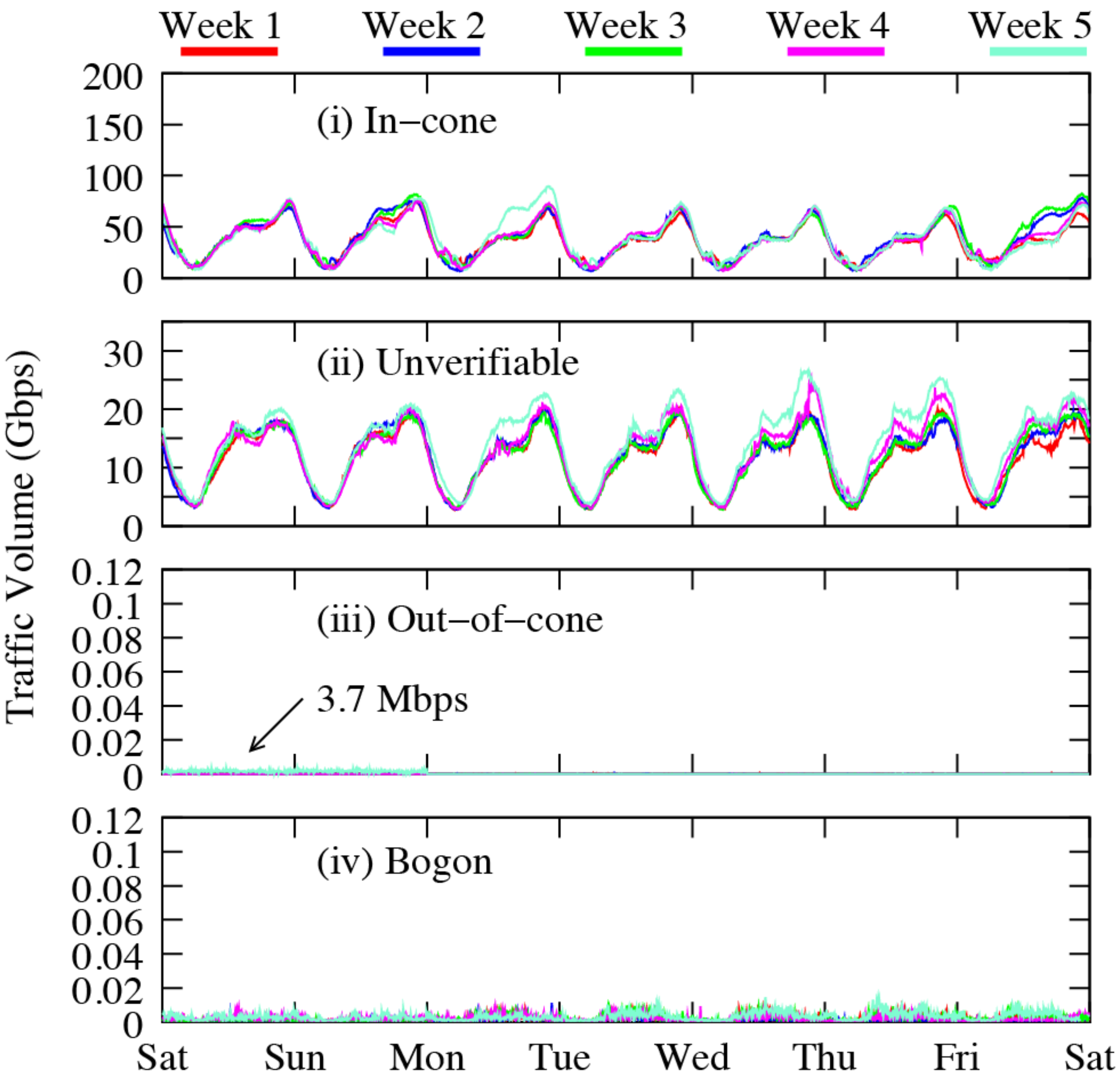
Brief overview
See paper for details

Longitudinal Traffic Classification

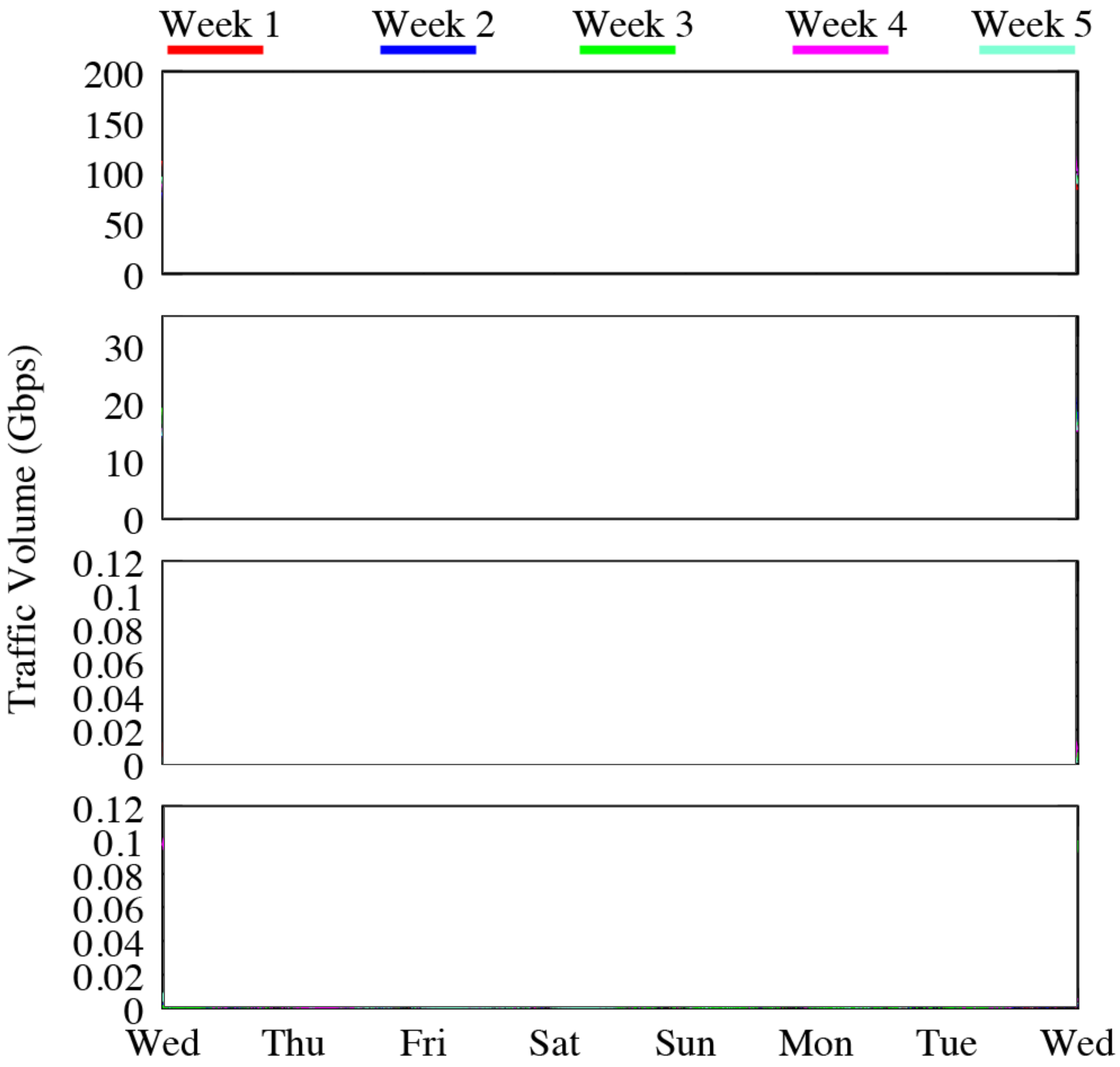


Apr 1 - May 6, 2017 May 1 - Jun 5, 2019

Longitudinal Traffic Classification

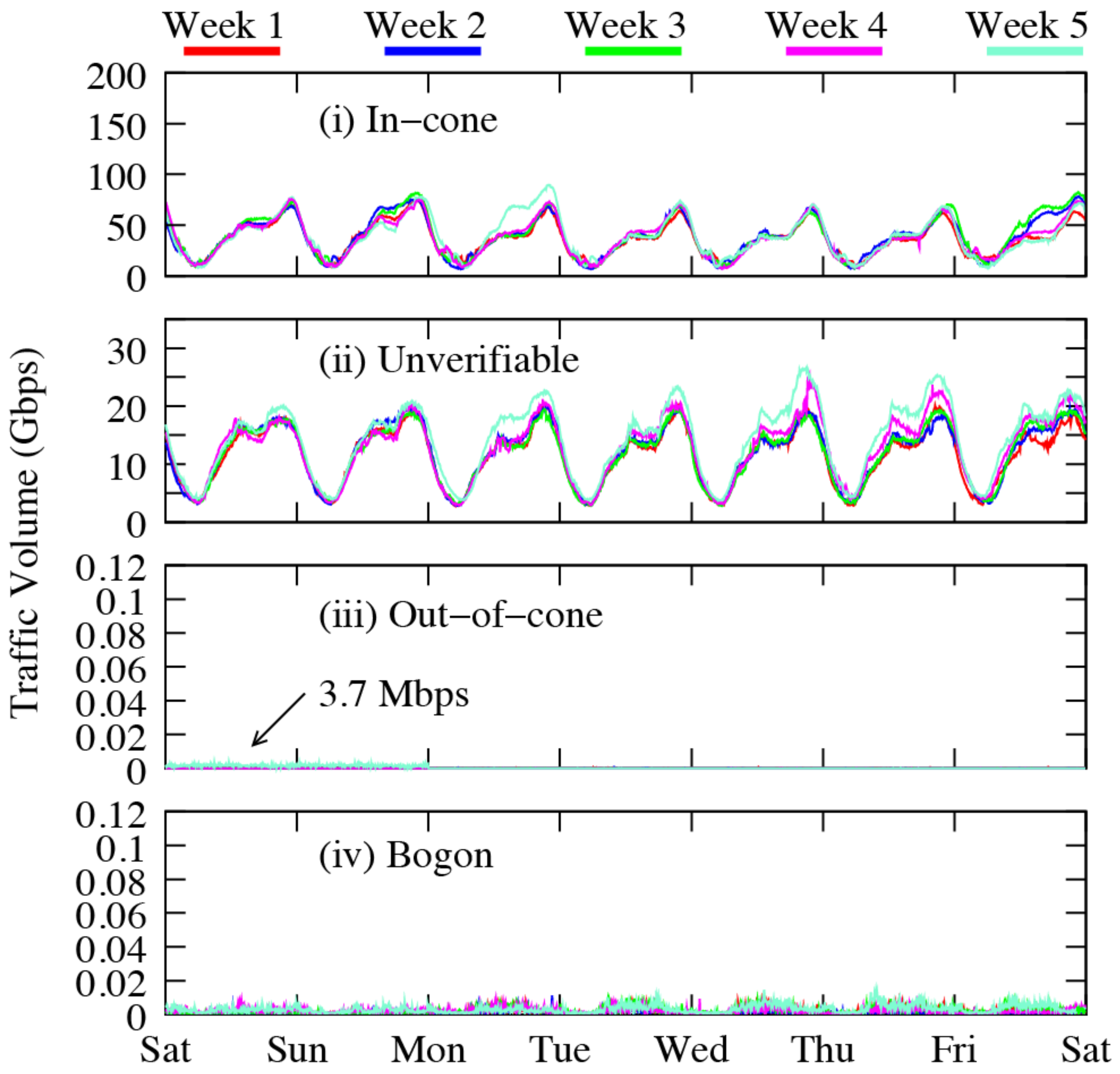


Apr 1 - May 6, 2017

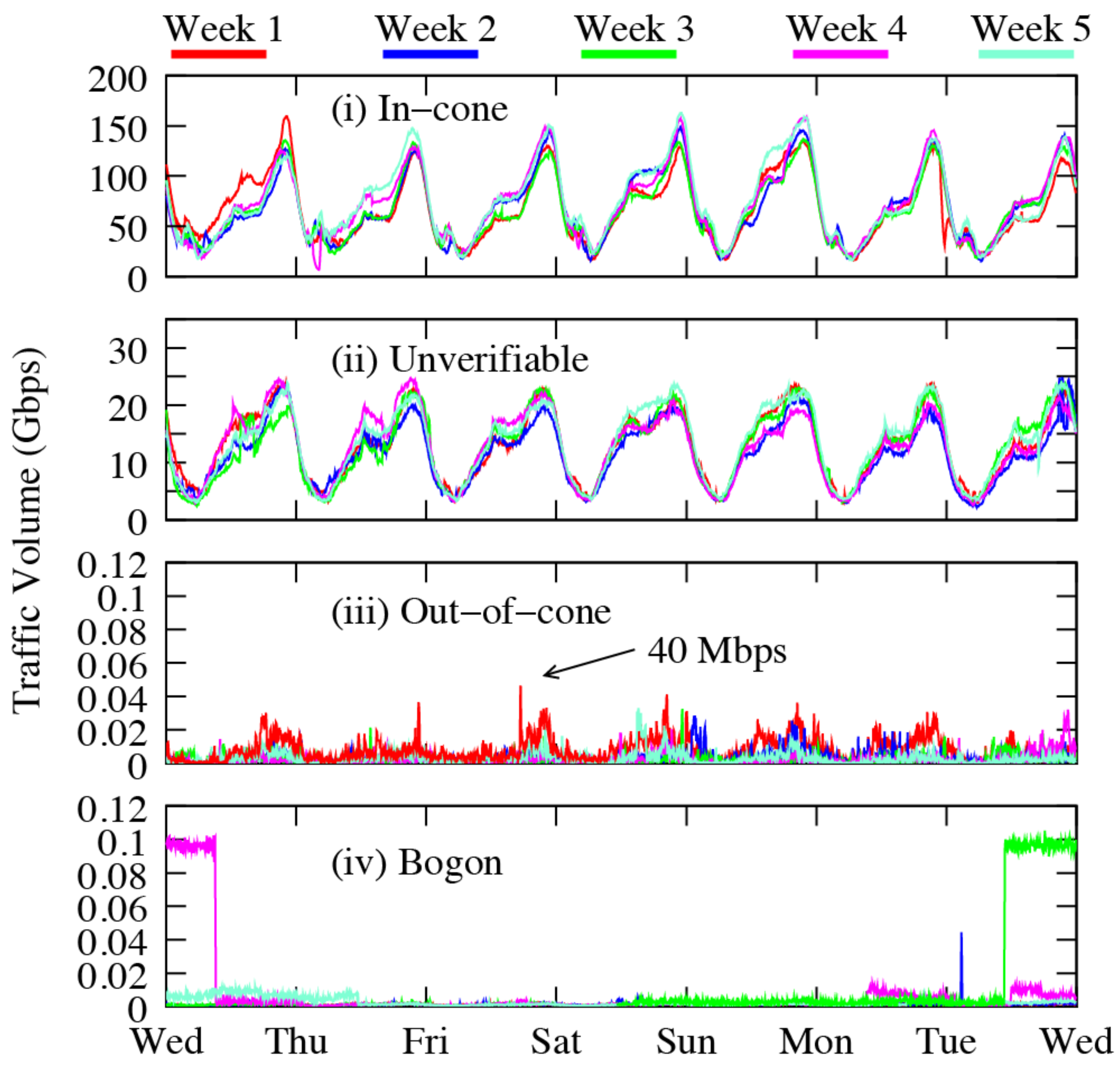


May 1 - Jun 5, 2019

Longitudinal Traffic Classification

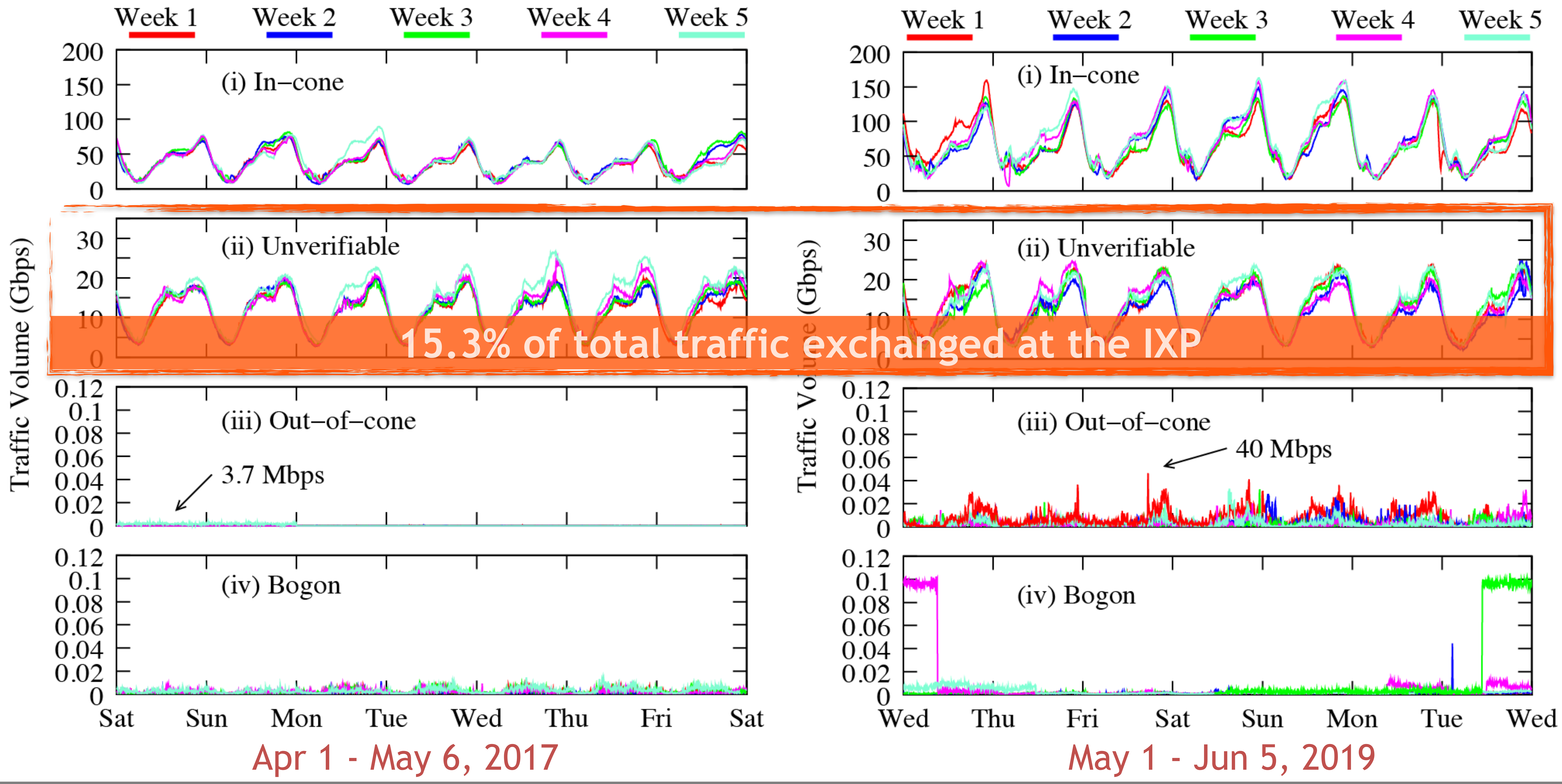


Apr 1 - May 6, 2017

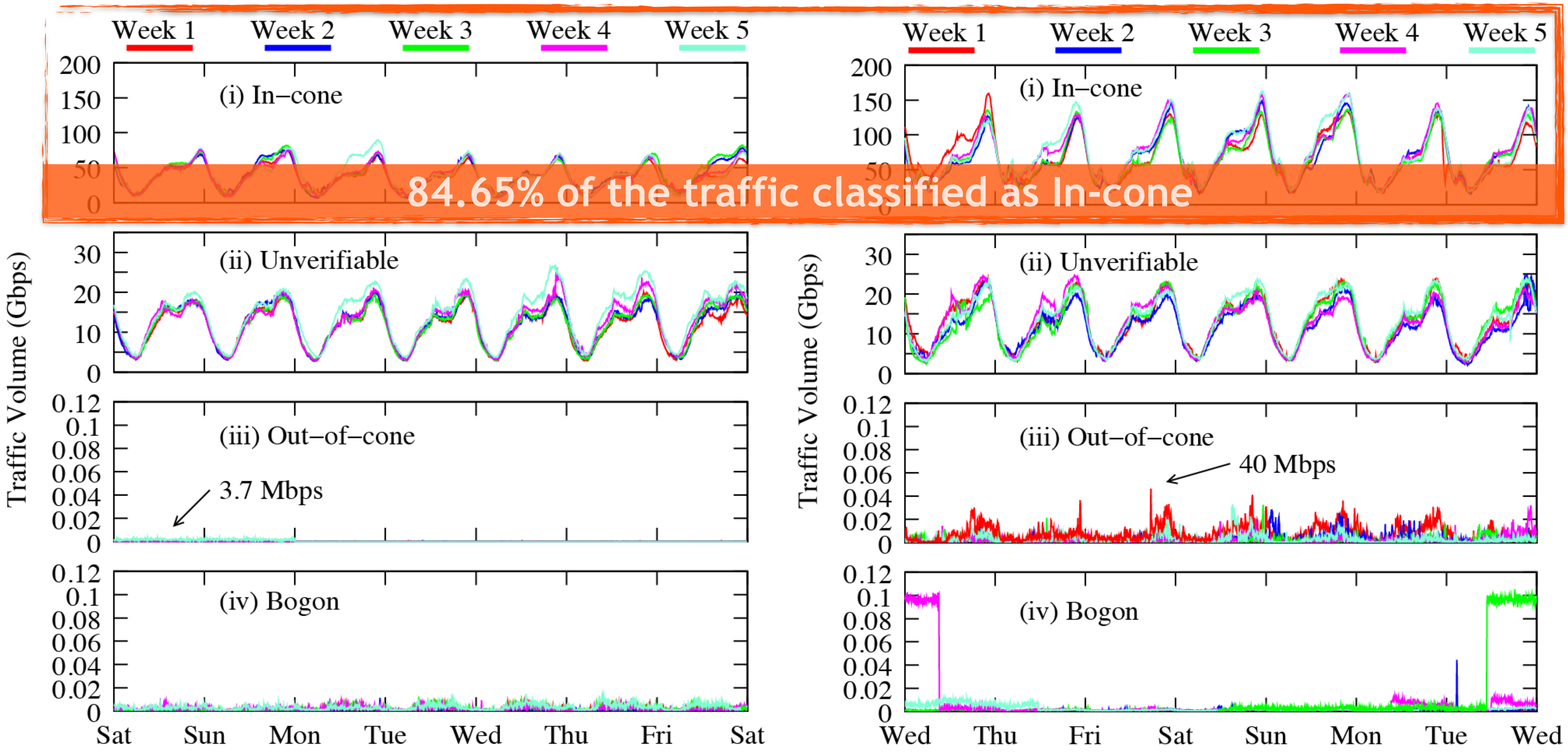


May 1 - Jun 5, 2019

Longitudinal Traffic Classification



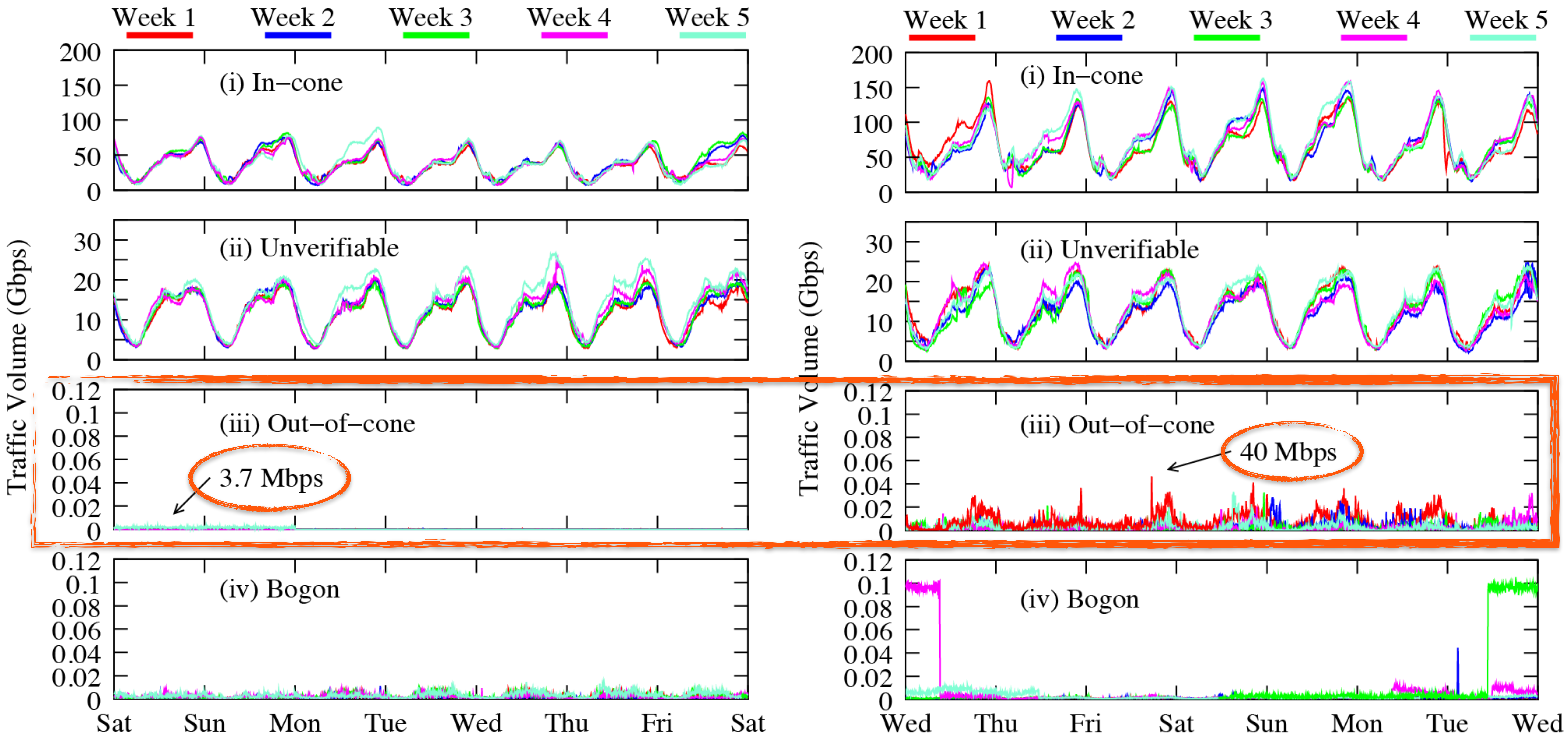
Longitudinal Traffic Classification



Apr 1 - May 6, 2017

May 1 - Jun 5, 2019

Longitudinal Traffic Classification

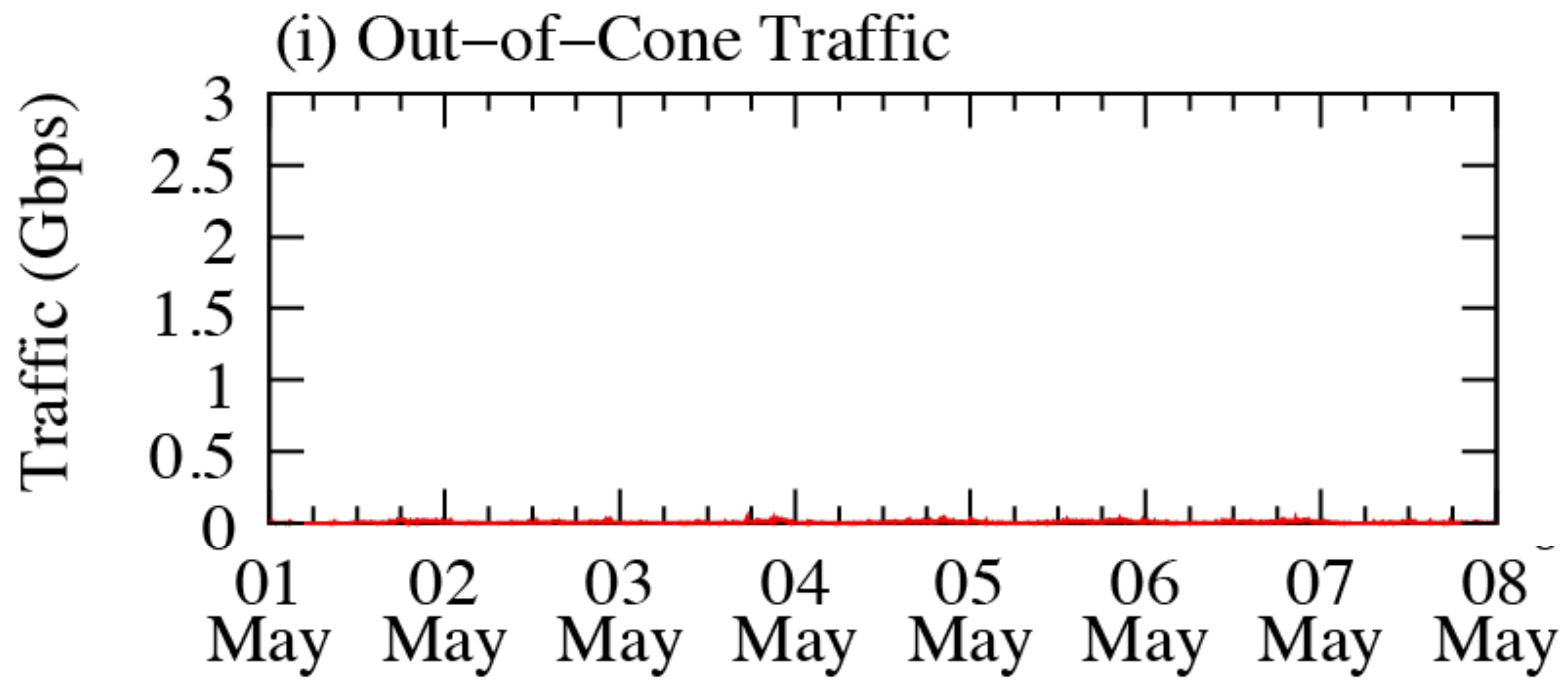


Apr 1 - May 6, 2017

May 1 - Jun 5, 2019

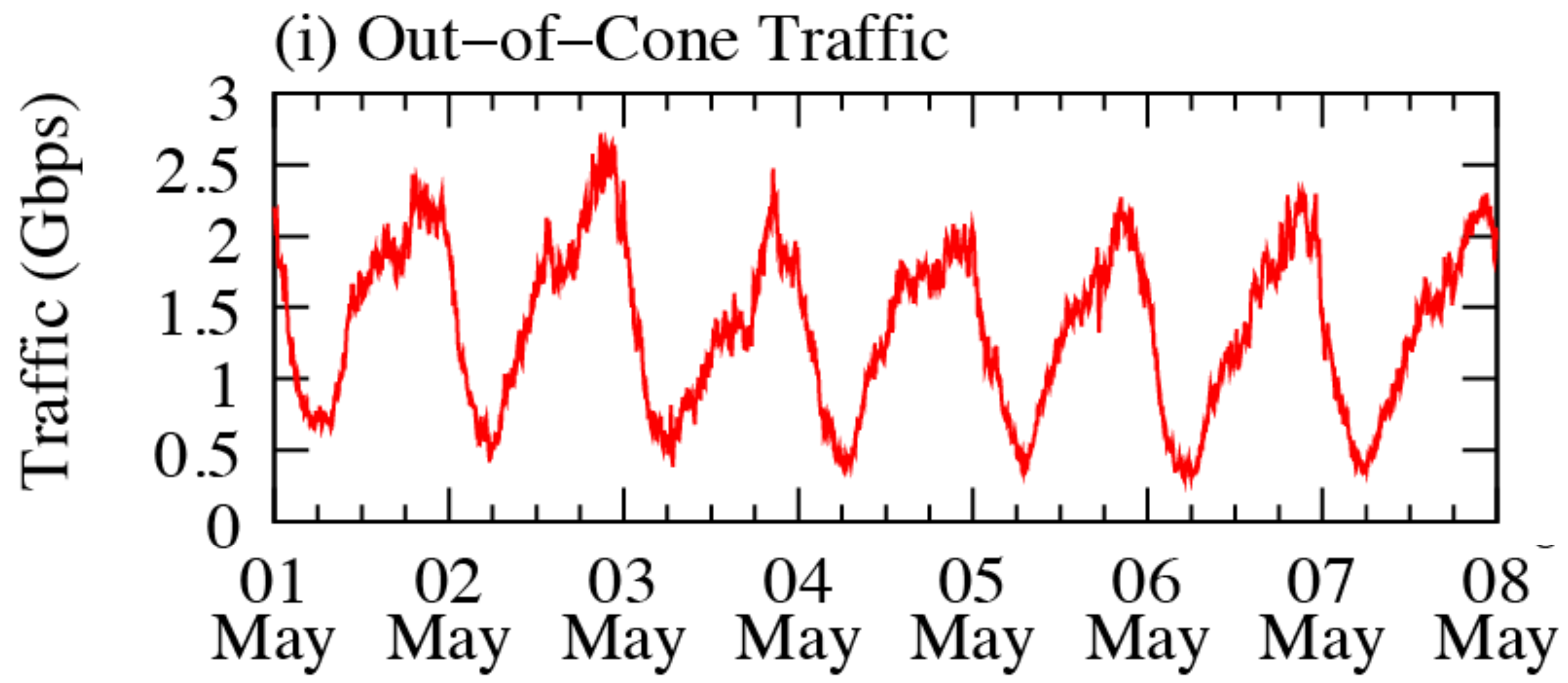
Comparison of Out-of-cone Traffic Inferred by Each Method

(a) Spoofer-IX



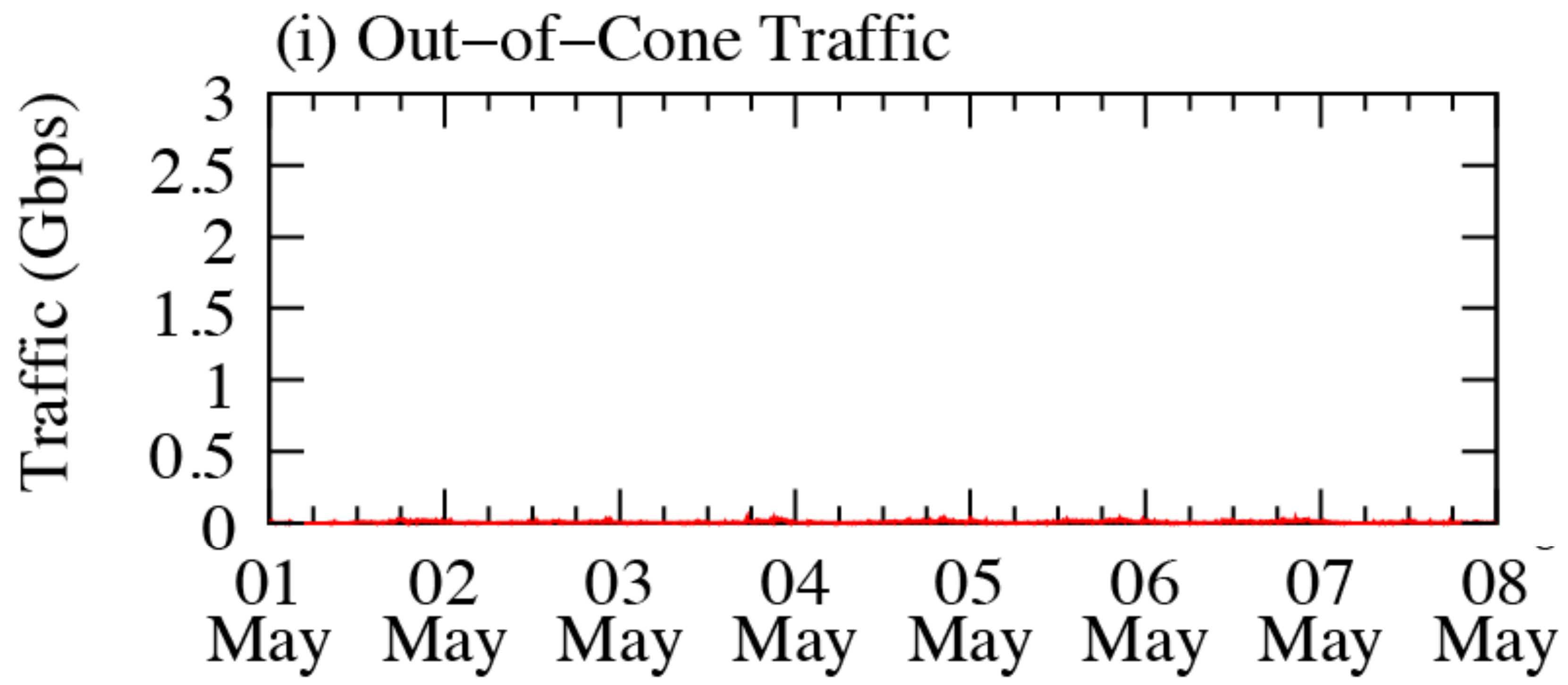
Traffic

(b) State-of-the-art

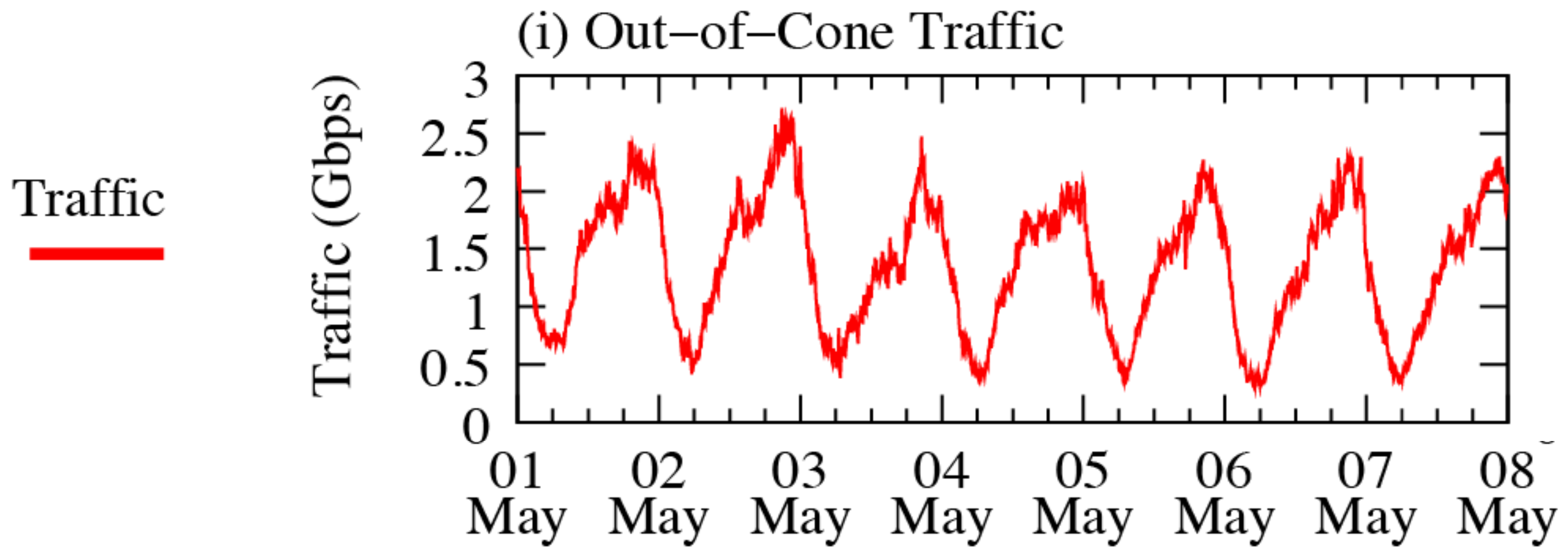


Comparison of Out-of-cone Traffic Inferred by Each Method

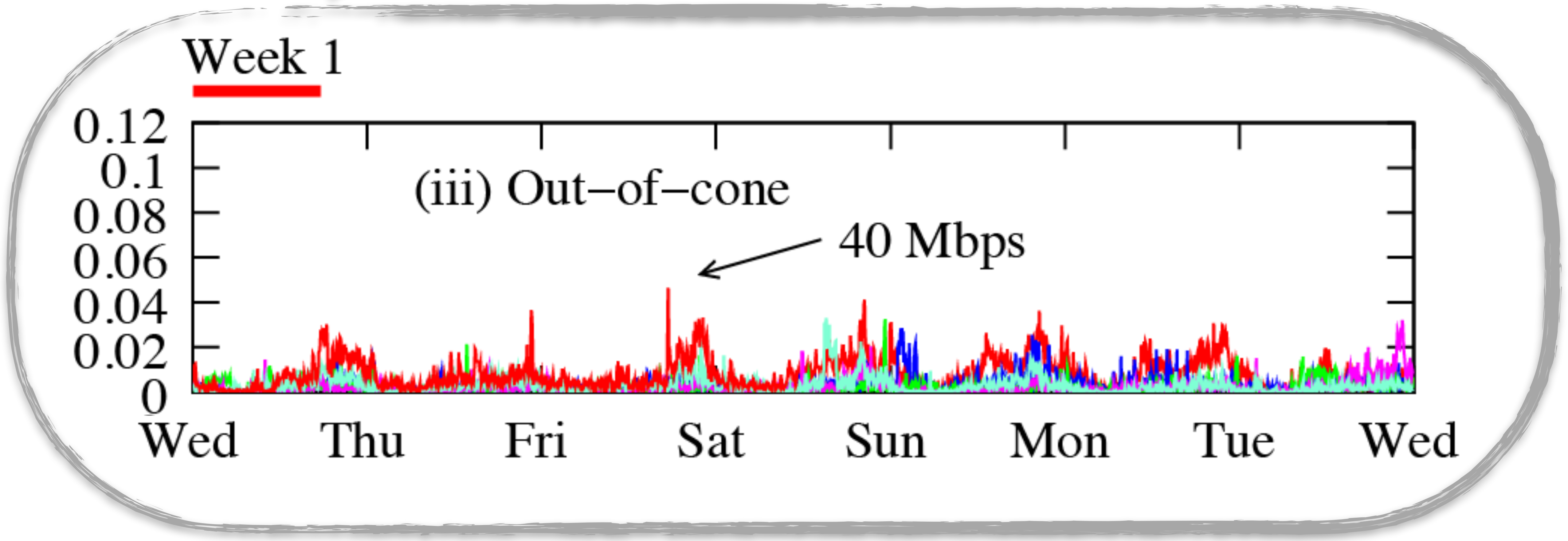
(a) Spoofer-IX



(b) State-of-the-art

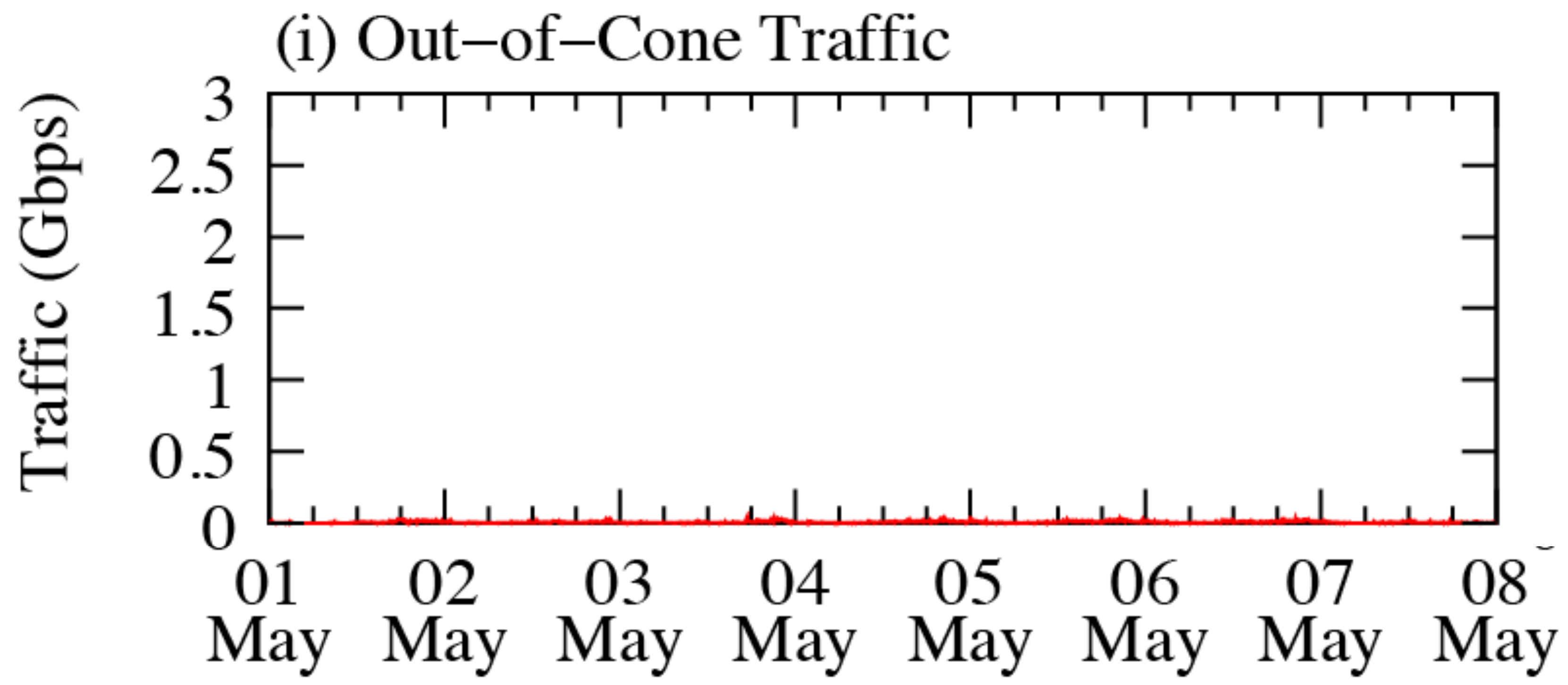


Spoofer-IX inferred a peak of 40 Mbps

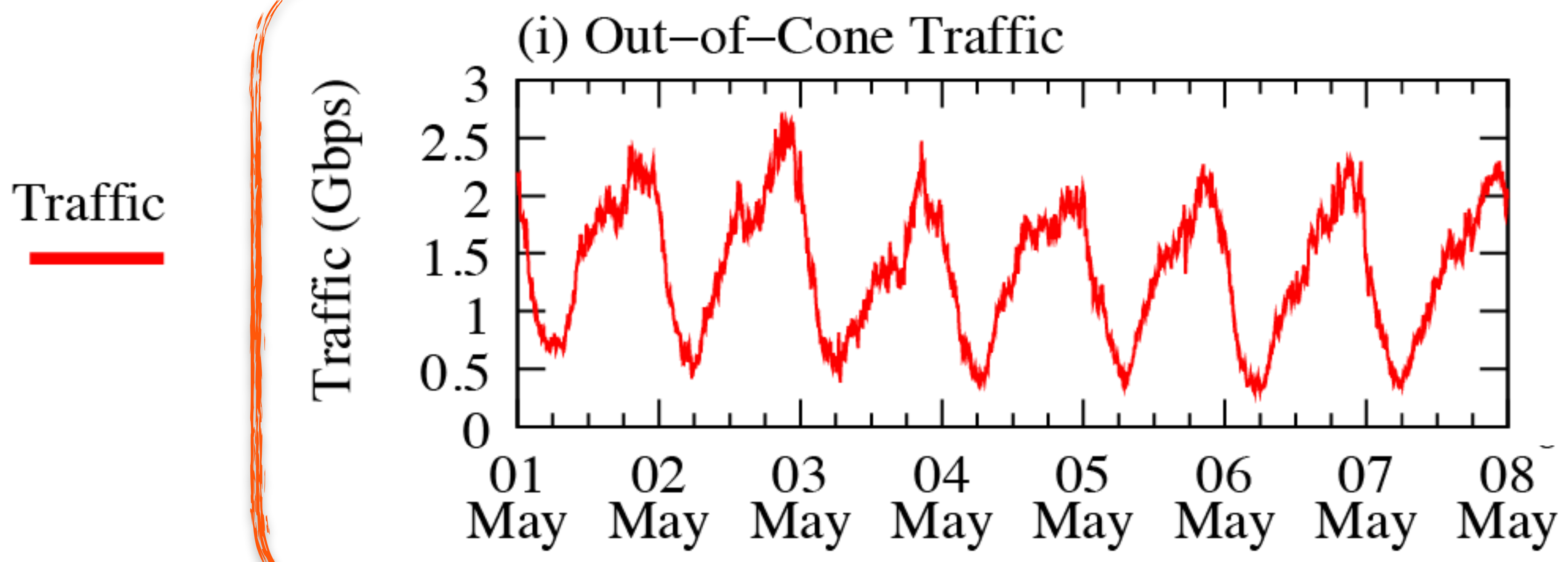


Comparison of Out-of-cone Traffic Inferred by Each Method

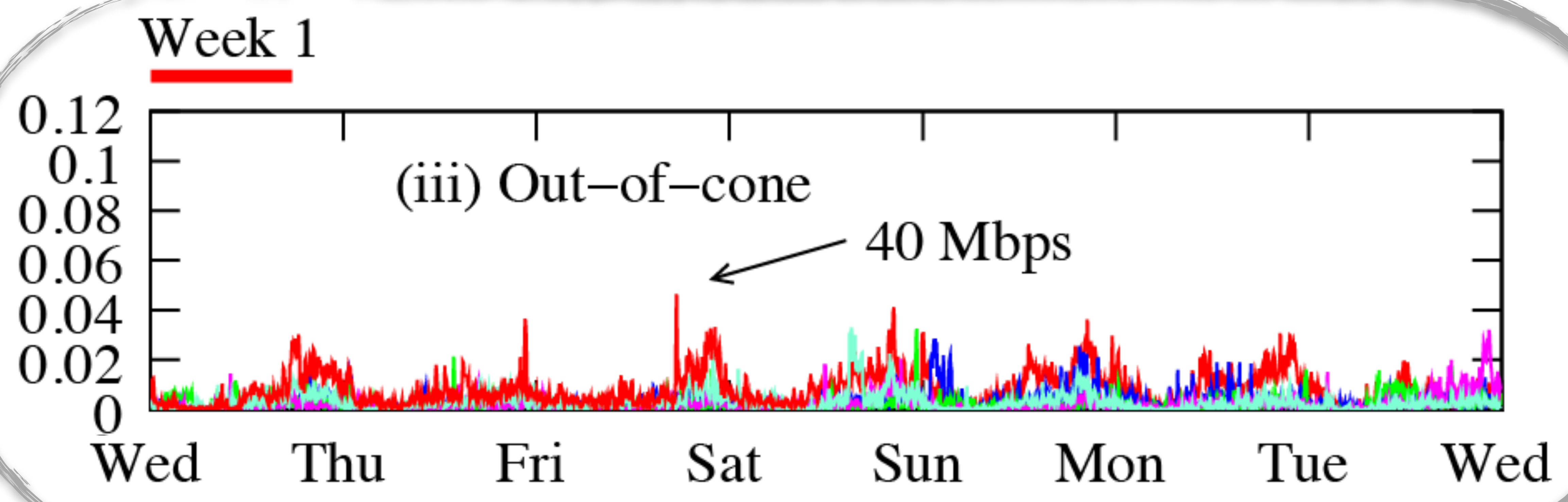
(a) Spoofer-IX



(b) State-of-the-art



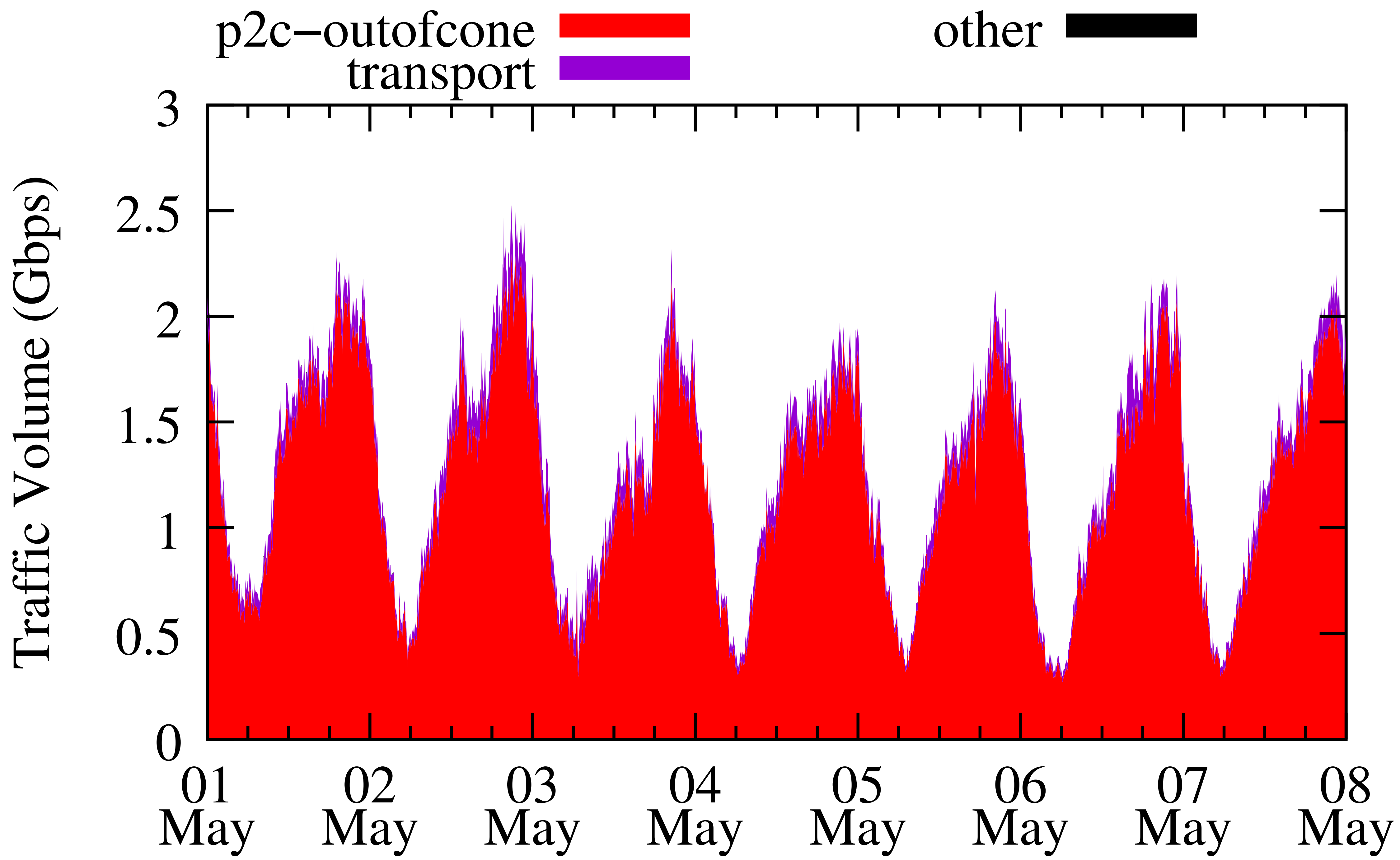
Spoofer-IX inferred a peak of 40 Mbps



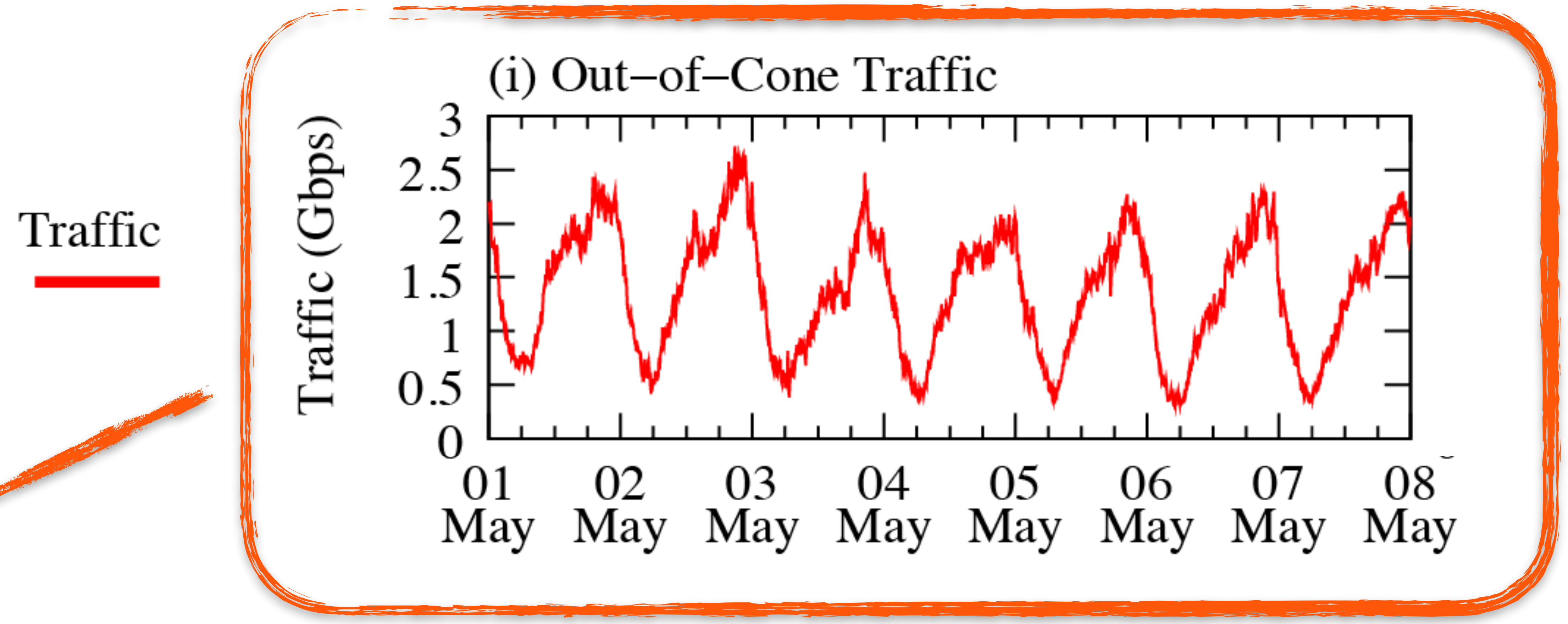
Full Cone method inferred a peak of 2.5 Gbps

Comparison of Out-of-cone Traffic Inferred by Each Method

Unverifiable traffic

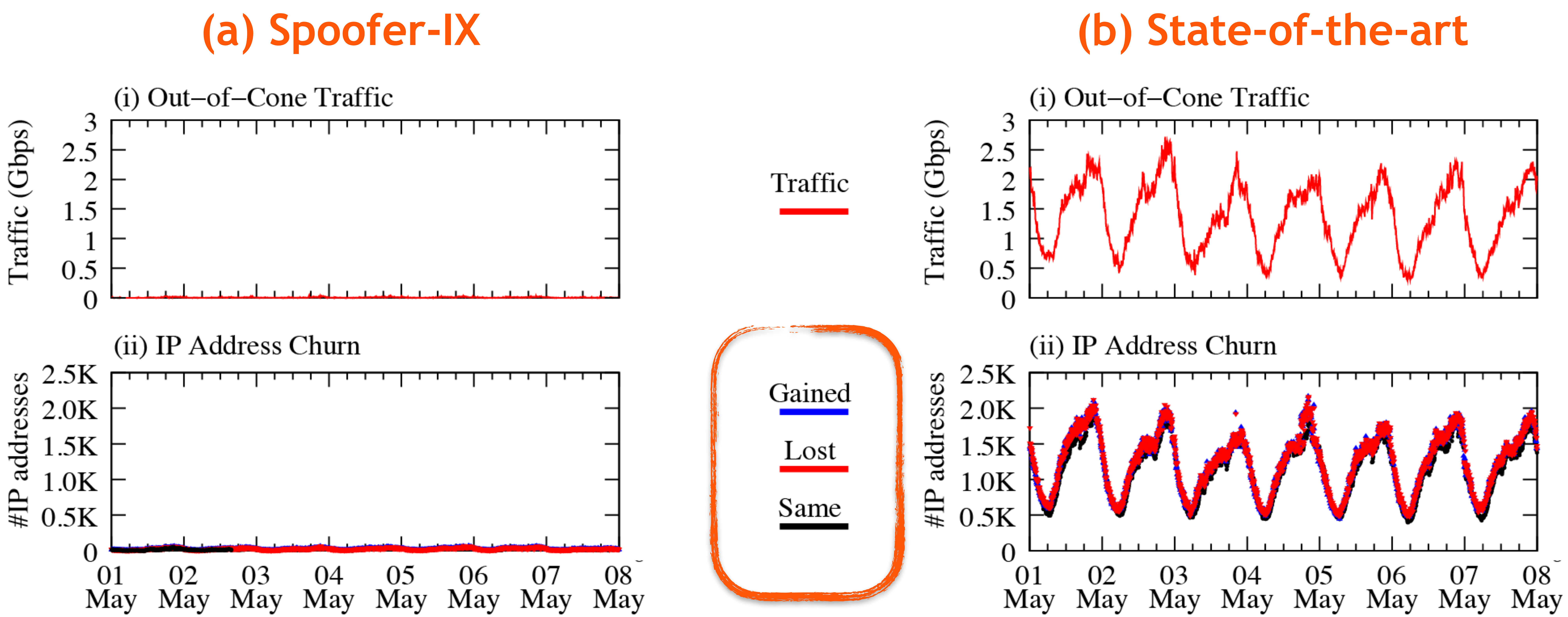


(b) State-of-the-art



92.6% was sent from a provider to a customer across the exchange —
where no cone of valid addresses applies

Comparison of Out-of-cone Traffic Inferred by Each Method

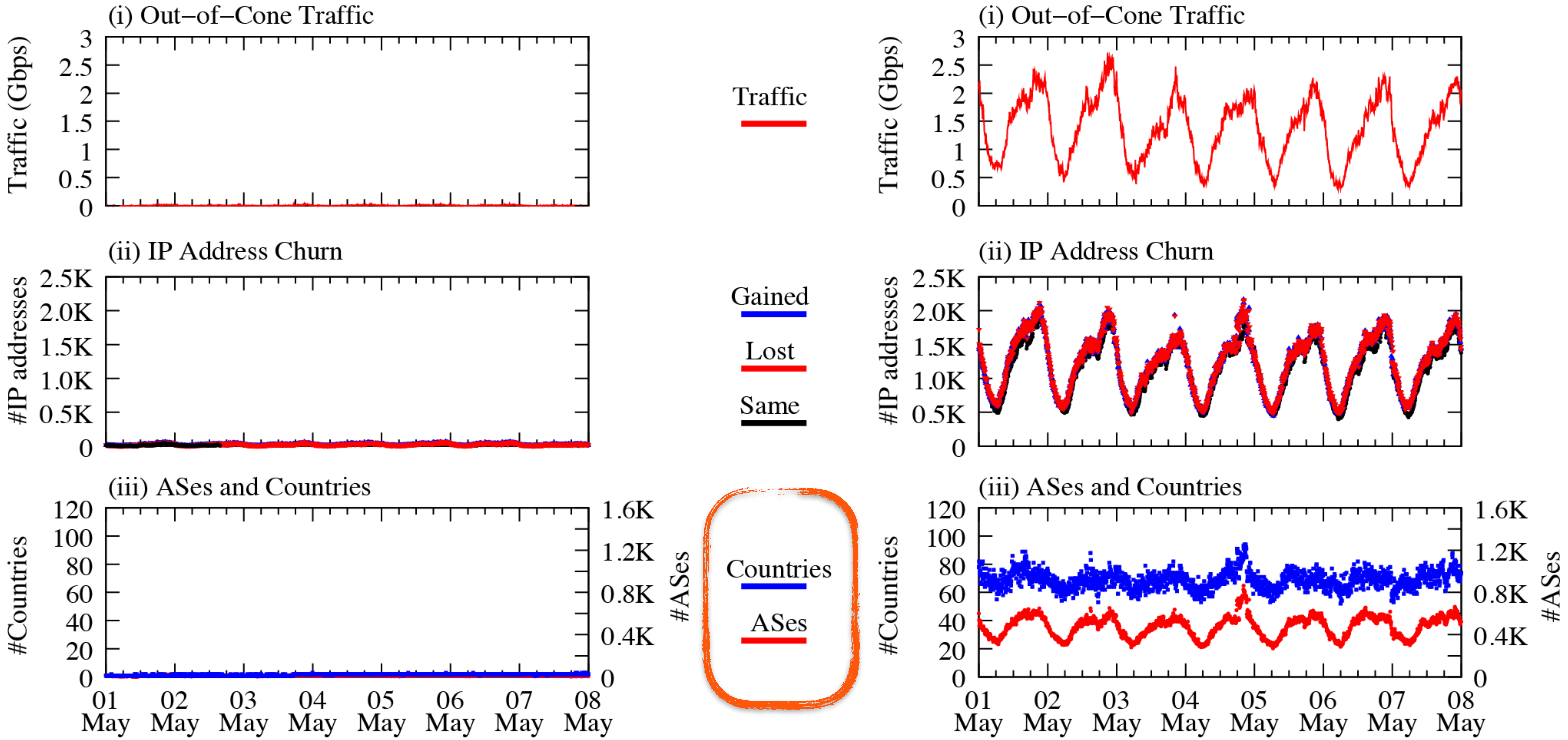


activity and churn in active IP addresses

Comparison of Out-of-cone Traffic Inferred by Each Method

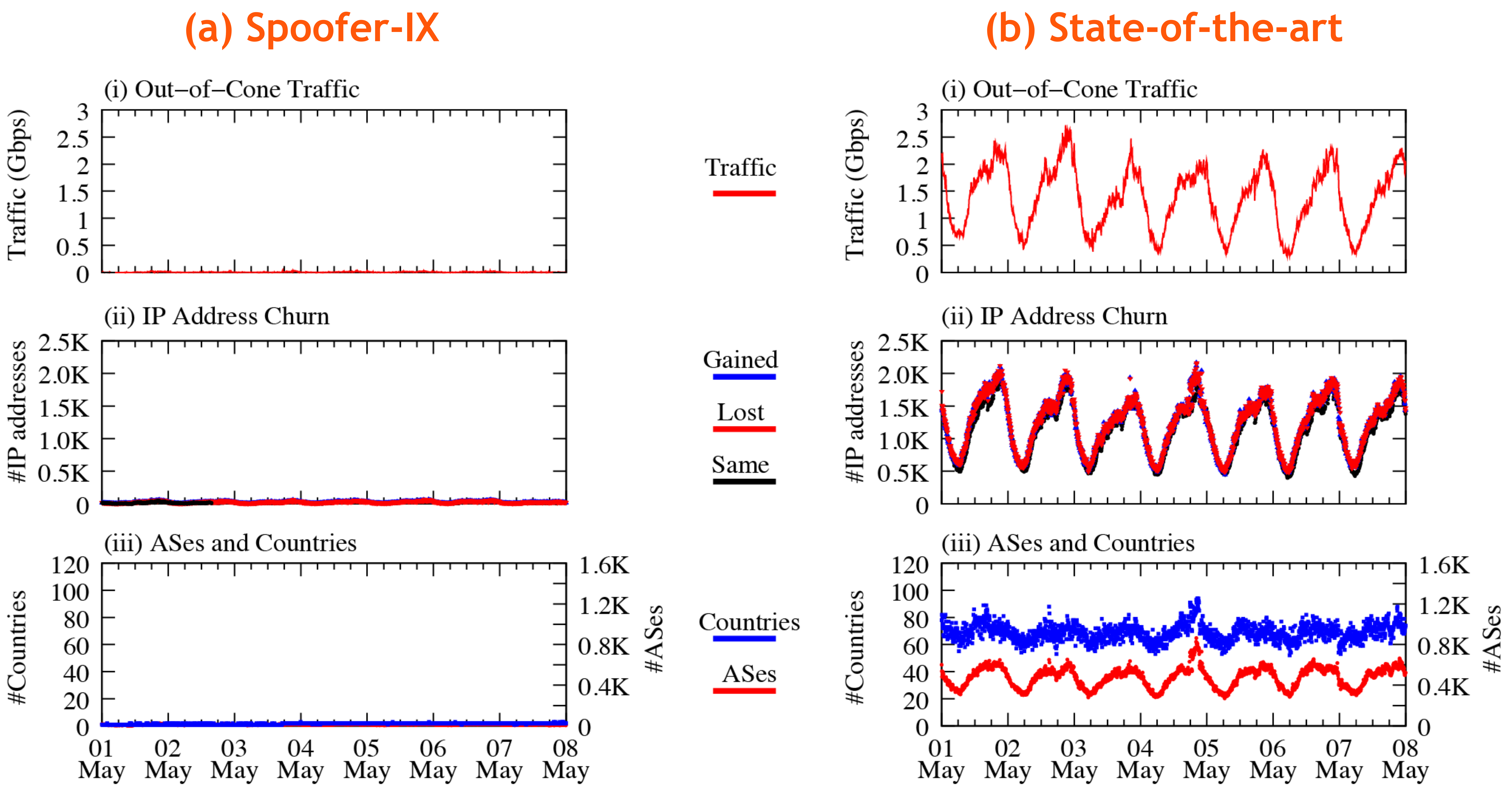
(a) Spoofer-IX

(b) State-of-the-art



spatio-temporal properties in active IP addresses

Comparison of Out-of-cone Traffic Inferred by Each Method



None of the metrics results correlated with a typical attack pattern

Takeaways

- Few efforts have tried to empirically measure SAV compliance for networks attached to the global Internet
- We have exposed fundamental challenges and developed a new method to classify traffic flows
- We hope that our work be used to further improve our collective ability to measure and expand deployment of SAV filtering

Takeaways

Thank you!
Questions?

Lucas Müller
lfmuller@inf.ufrgs.br

- Few efforts have tried to empirically measure SAV compliance for networks attached to the global Internet
- We have exposed fundamental challenges and developed a new method to classify traffic flows
- We hope that our work be used to further improve our collective ability to measure and expand deployment of SAV filtering