Illegitimate Source IP Addresses At Internet Exchange Points

@ DENOG8, Darmstadt

Franziska Lichtblau, **Florian Streibelt**, Philipp Richter, Anja Feldmann

23.11.2016

Internet Network Architectures, TU Berlin – www.inet.tu-berlin.de

Introduction

What are illegitimate source IP addresses?

Packets with source addresses that are not valid within the scope of the public Internet.

What are illegitimate source IP addresses?

- Intentionally spoofed traffic
- Internal traffic leaked by mistake
- General misconfiguration, unknown...

Packets with source addresses that are not valid within the scope of the public Internet.

Why looking at illegitimate source IPs?

- Includes attack traffic (DoS, DDoS, ...)
- Studying unwanted traffic can give insights to come up with mitigation strategies
- Potentially exposes information about internal infrastructure
- Utilizes (expensive) bandwidth

Illegitimate Traffic: Our Categories

- Bogon: RFC1918, IANA reserved, Multicast, Future Use, etc...
- Unrouted: Source IP address is not announced in the "global routing table"
- Invalid: Traffic sent by a network that is not responsible for the corresponding prefix

What is BCP38?

- IETF - Best Current Practice document 38, RFC 2827
- Network Ingress Filtering:
  Defeating Denial of Service Attacks which employ IP Source Address Spoofing
- Idea: Only allow traffic leaving your network with source adresses from legitimately advertised prefixes.

BCP38

> *In other words, if an ISP is aggregating routing announcements for multiple downstream networks, strict traffic filtering should be used to prohibit traffic which claims to have originated from outside of these aggregated announcements.*

(RFC2827/BCP38)

What we do...

- Previous studies like the Spoofer Project send probes to check for BCP38 compliance
- Our work is a passive approach to check for BCP38 deployment
- Provides insights about specific traffic volume and characteristics

Identifying Traffic

Identifying Bogon and Unrouted

Bogon

- RFC1918, Multicast, Future Use, IANA reserved

Unrouted

- Routing information: IXP Route Server, RIPE/RIS, RouteViews
- Compile a list of observed prefixes at all routing sources

Ignored: Announcements larger than /8 and smaller than /24

Traffic with a source address which is covered by this list is of class BOGON

Traffic with a source address which is **not** covered by this list is of class UNROUTED

Routing Information

We utilize as many data sources as possible to minimize false positives

- RIPE/RIS (14 collectors)
- RouteViews (16 collectors)
- Bogon/Martian prefix list as provided by Team Cymru

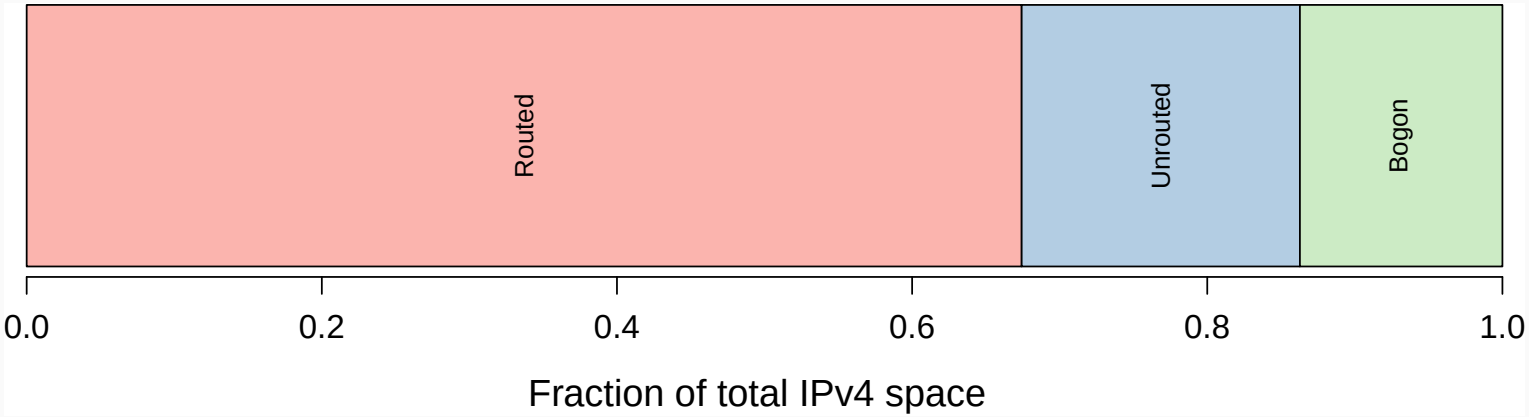
Bogon And Unrouted Overview

Bogon Prefixes

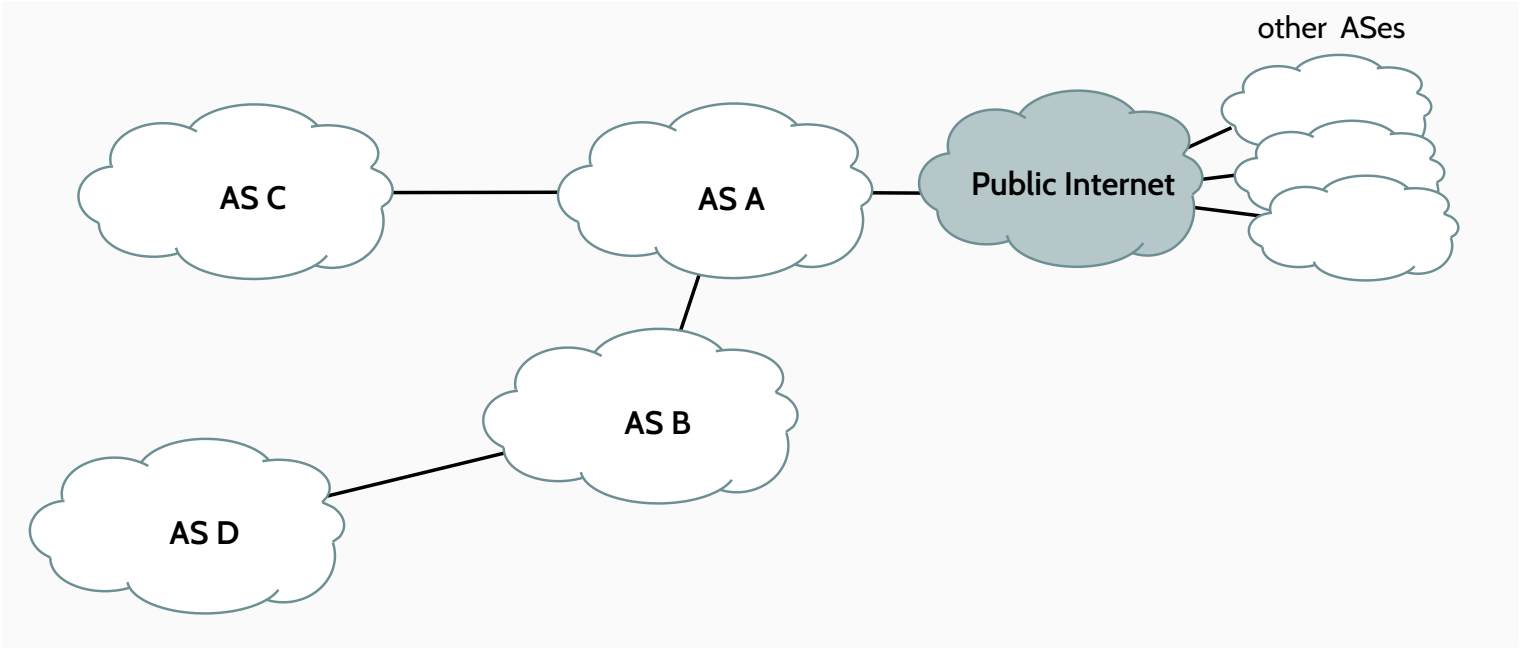
- As defined in RFC1918 and RFC5737
- 2.3M /24
- 14% of the IPv4 address space

Unrouted Prefixes

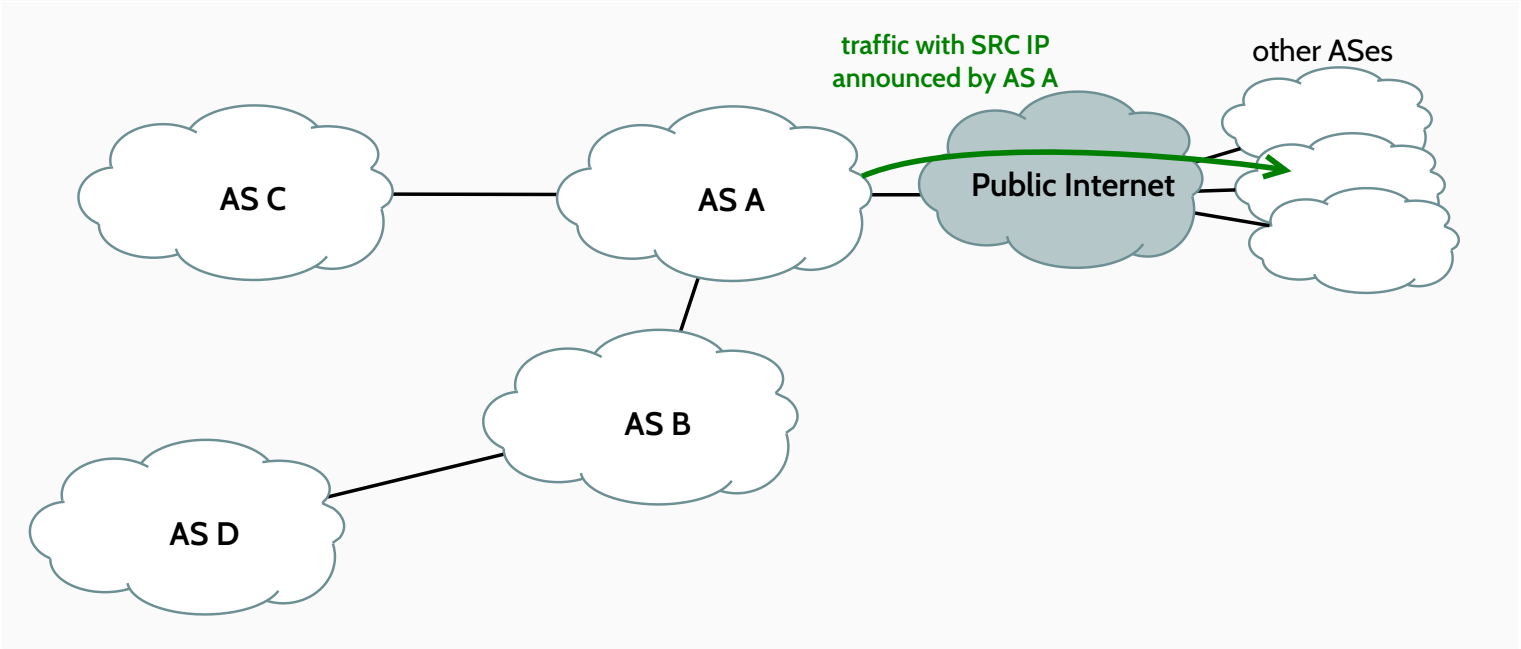
- 11.3M validly announce /24 (78% of the IPv4 address space)
- 3.16M unrouted /24 (excluding Bogon)



AS specific: Identifying Invalid

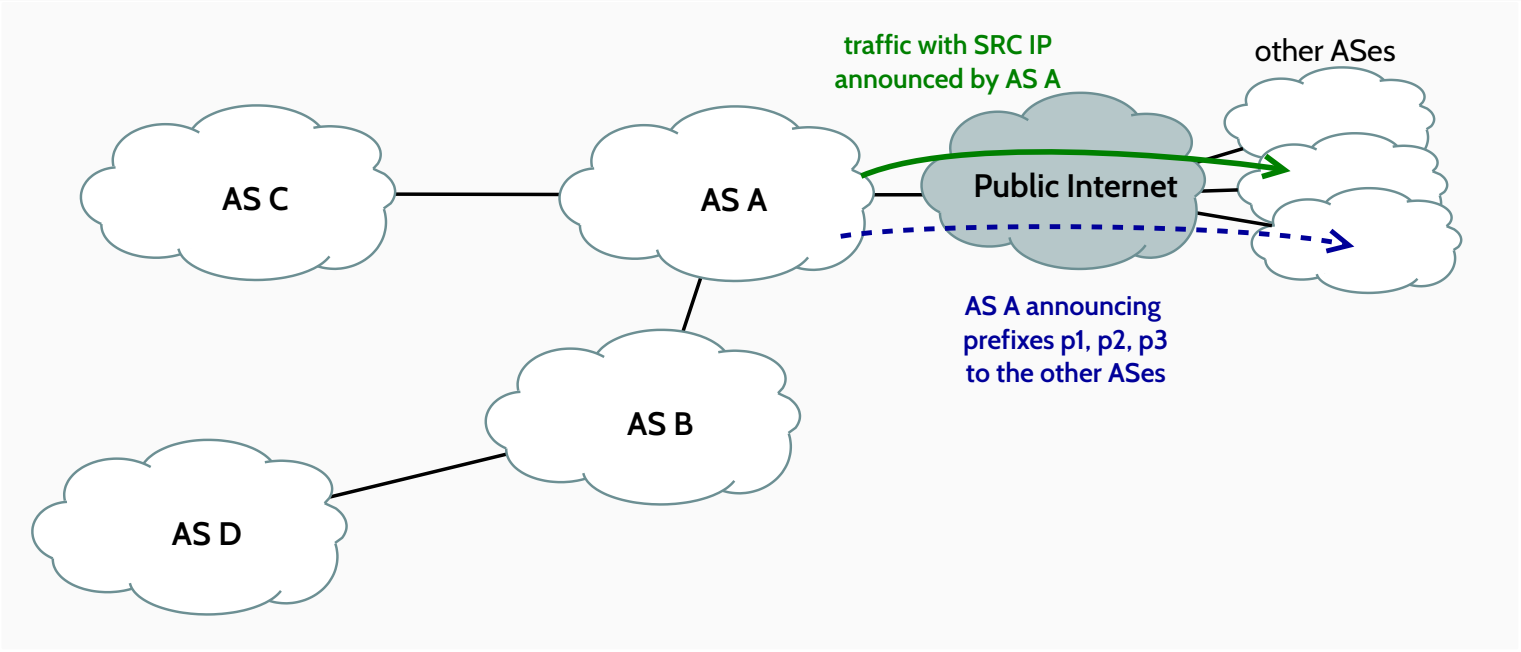


AS specific: Identifying Invalid

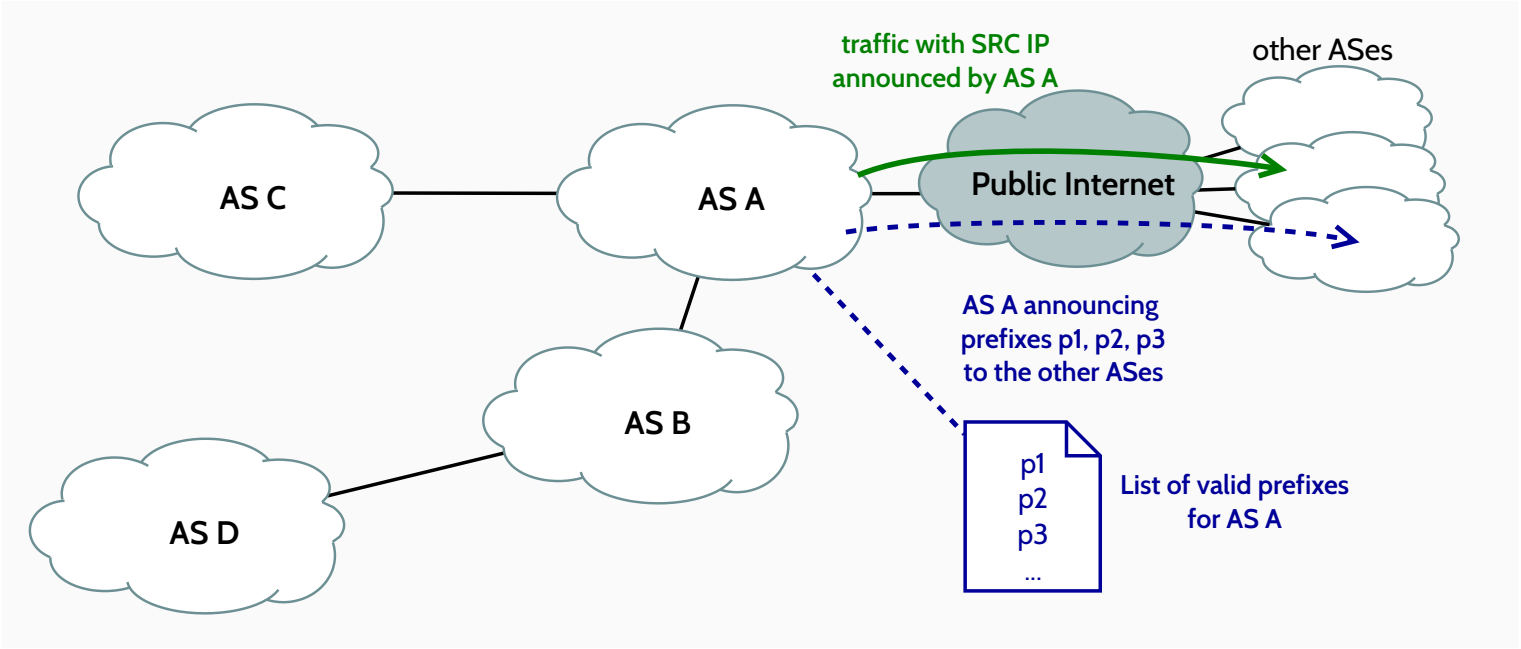


Assumption: An AS announcing a prefix is also a legitimate source for traffic originating from this prefix.

AS specific: Identifying Invalid

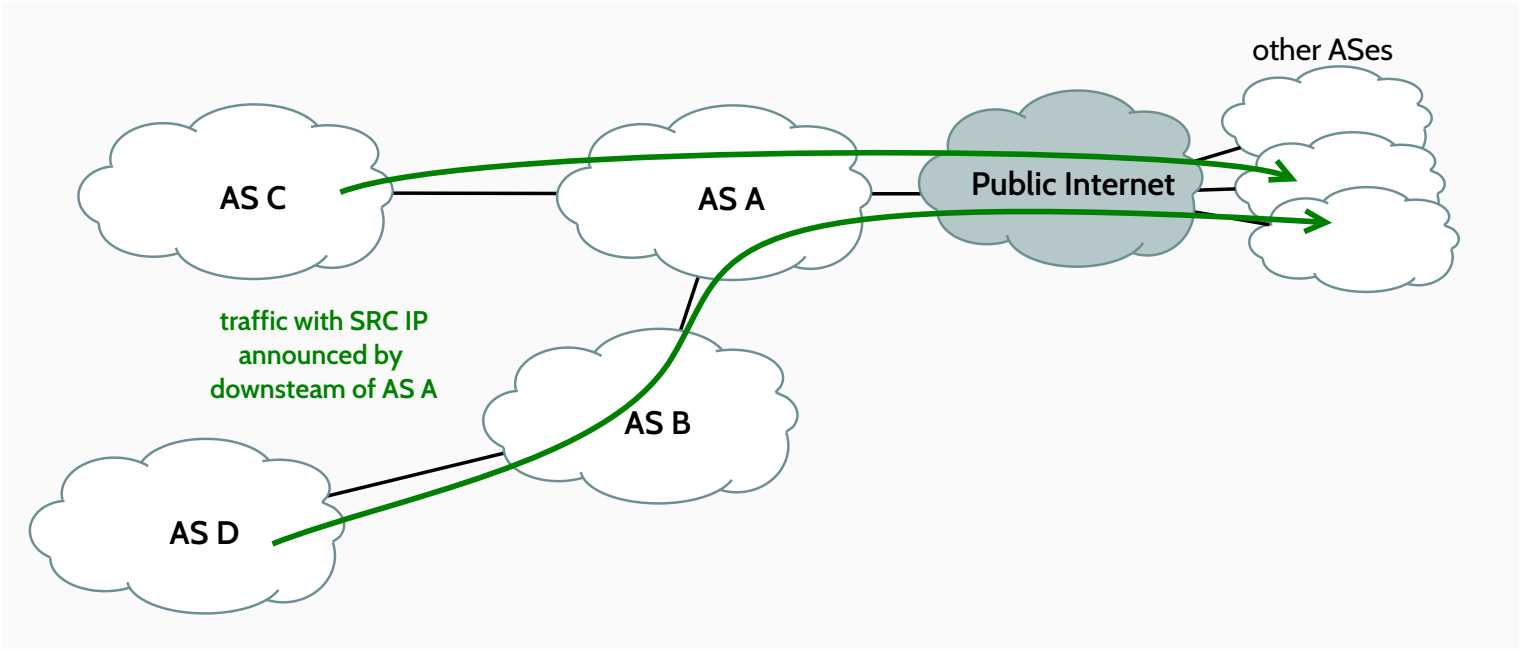


AS specific: Identifying Invalid

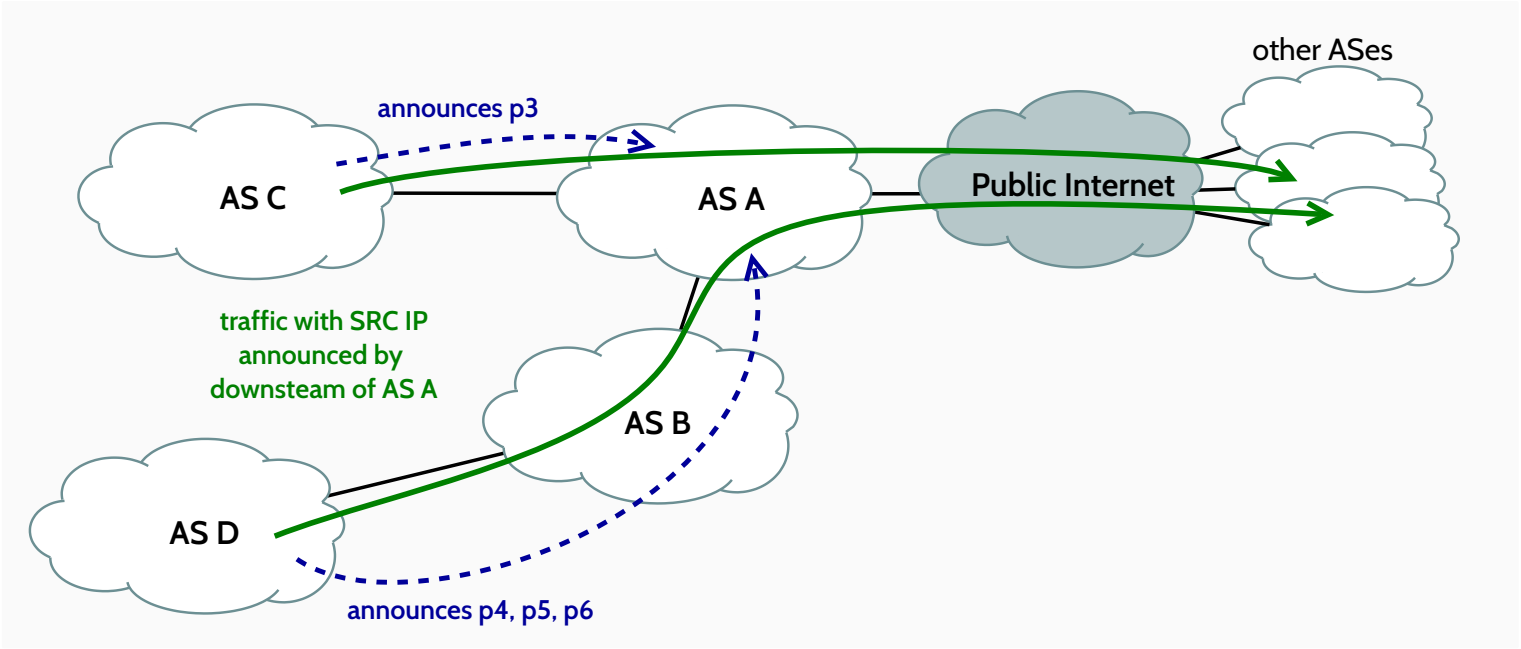


Construct list of valid prefixes for each AS

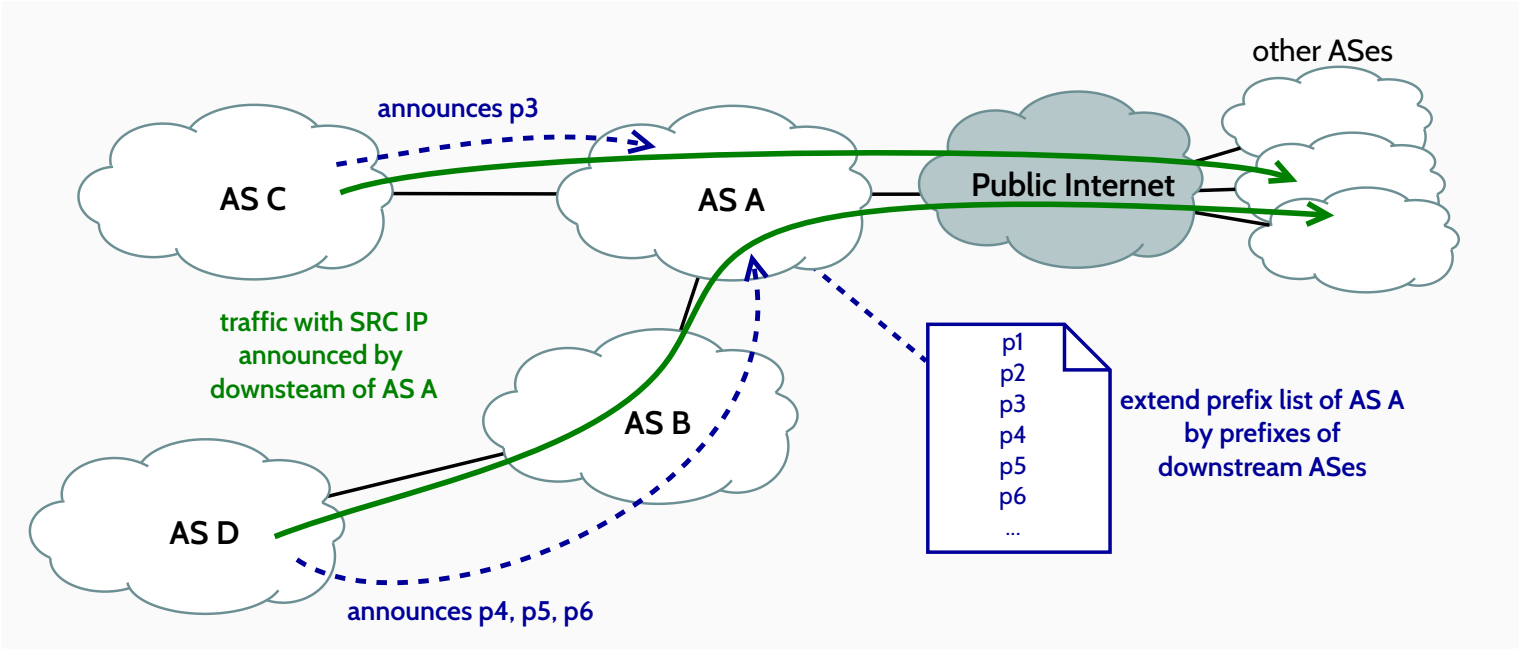
AS specific: Identifying Invalid



AS specific: Identifying Invalid

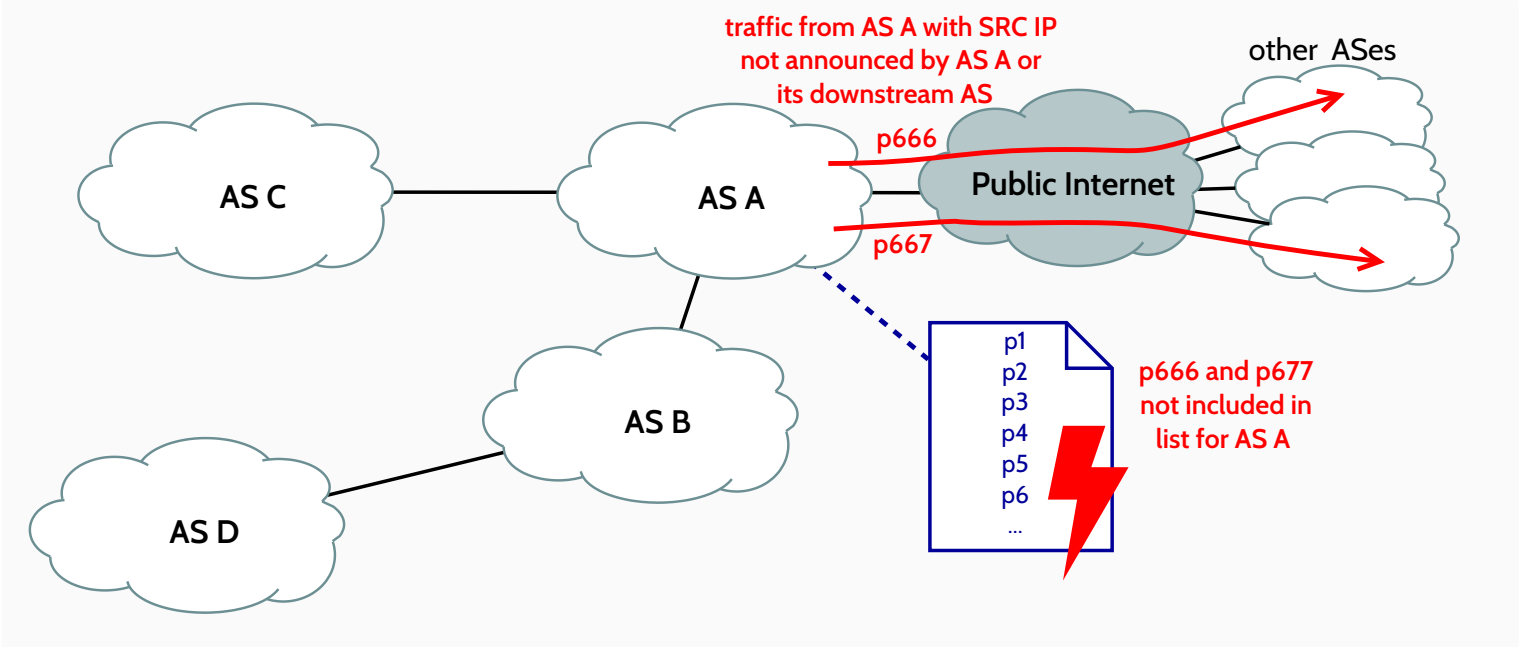


AS specific: Identifying Invalid



Prefix lists are also created for AS B, AS C and AS D (derived from public routing data) and added to the list of AS A

AS specific: Identifying Invalid



INVALID: Traffic with a SRC IP from a Prefix NOT covered by the prefix list of AS A

Identifying Invalid: Limitations

False positives

- No full picture of the complete BGP state
- Can not capture direct private interconnects

False negatives

- AS must just be *somewhere* on the AS Path to be valid source

Lots of number crunching involved

The process works completely offline, using a lot of computation time and memory.

Applying our methodology at a Large European IXP

Flow Data

- Measurements taken at a Large European IXP (LIXP)
- More than 700 members and peak traffic up to 5 Tb/s
- 5 weeks of uninterrupted IPFIX from
  2016-01-18 to 2016-02-21
- Sampling rate 1/32K
- We only considered IPv4 (until now...no need to queue for this question ;))

Fractions of Bogon, Unrouted, Invalid in terms of total traffic

	Absolute traffic	Bytes	Packets
Bogon	28.11 TB	0.004%	0.029%
Unrouted	72.56 TB	0.010%	0.053%
Invalid	509.68 TB	0.076%	0.087%

Fractions of Bogon, Unrouted, Invalid in terms of total traffic

	Absolute traffic	Bytes	Packets
Bogon	28.11 TB	0.004%	0.029%
Unrouted	72.56 TB	0.010%	0.053%
Invalid	509.68 TB	0.076%	0.087%

Relative amount is small, but absolutely we have 610TB of traffic for all 3 classes within one week.

Overview: Traffic Classes Over One Week

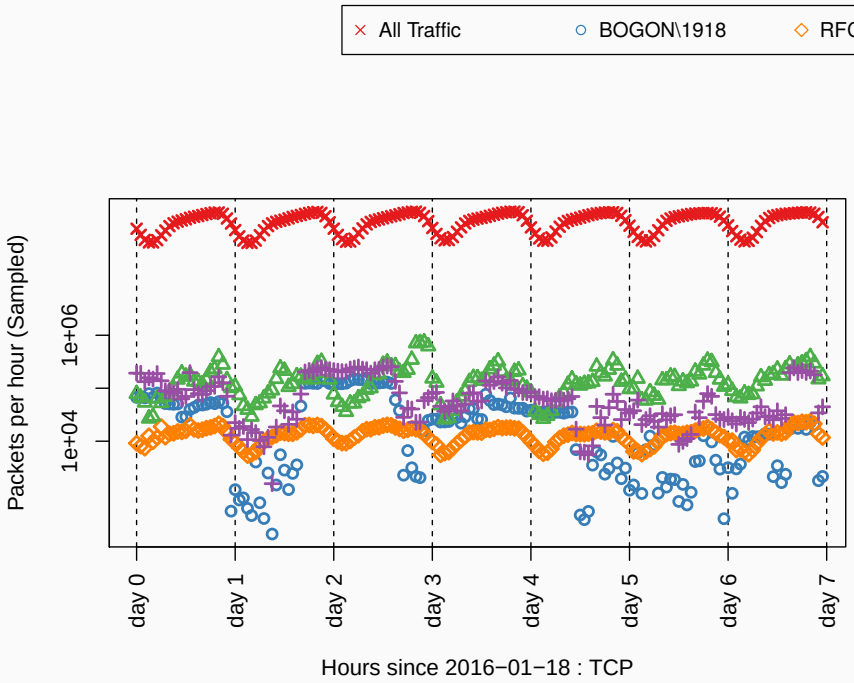


Figure 1: LIXP: TCP – Time series week 2016-01-18

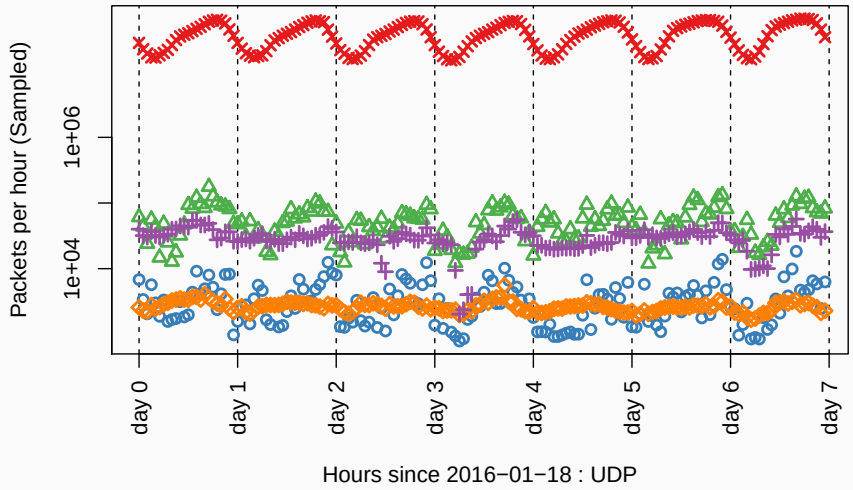
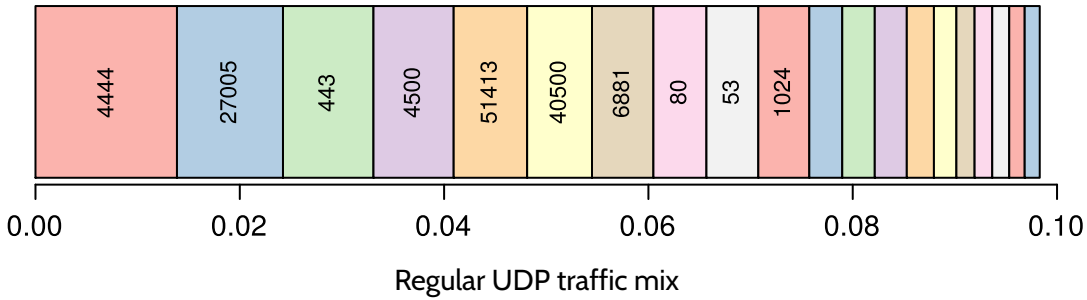
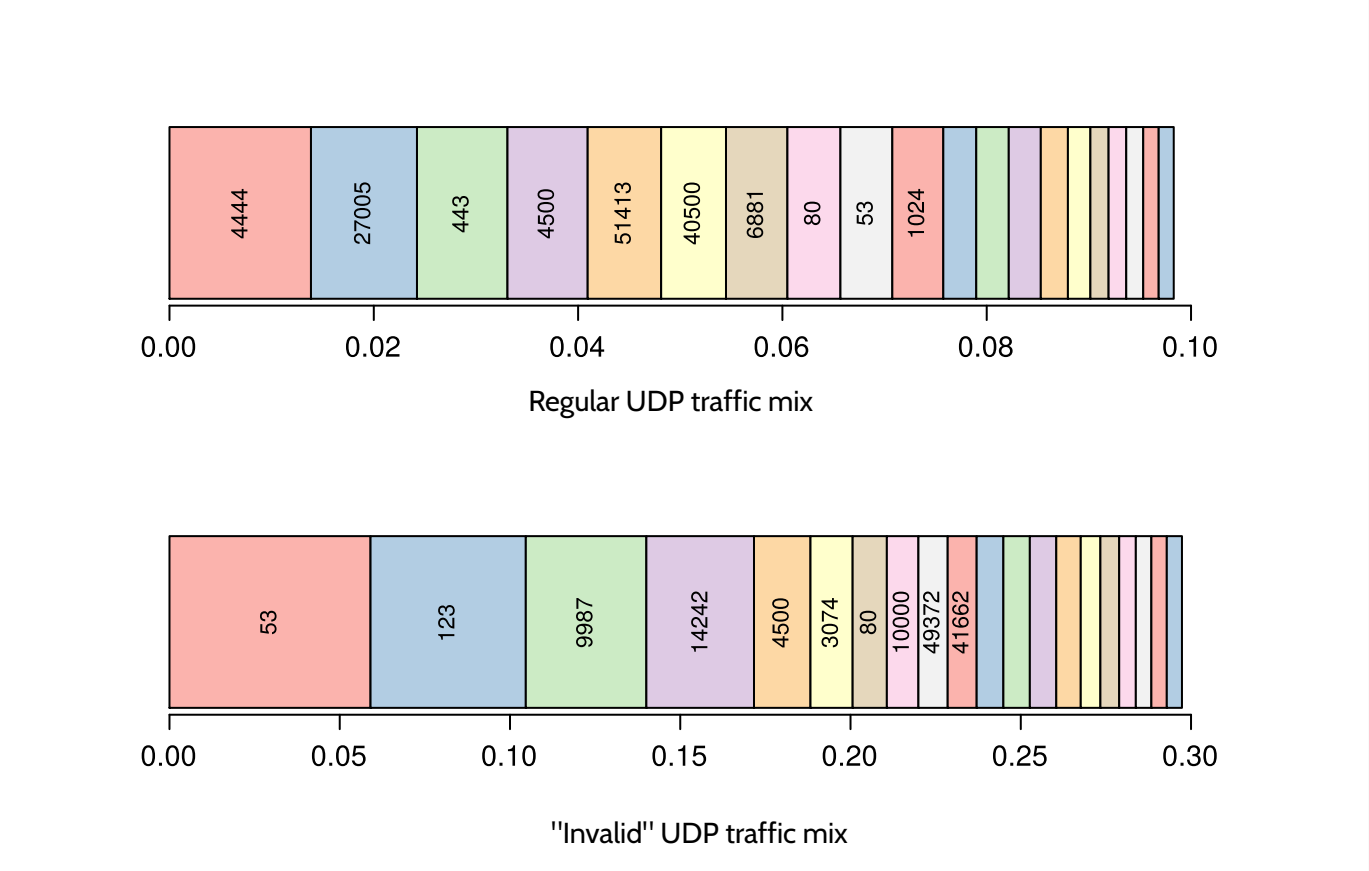


Figure 2: LIXP: UDP – Time series week 2016-01-18

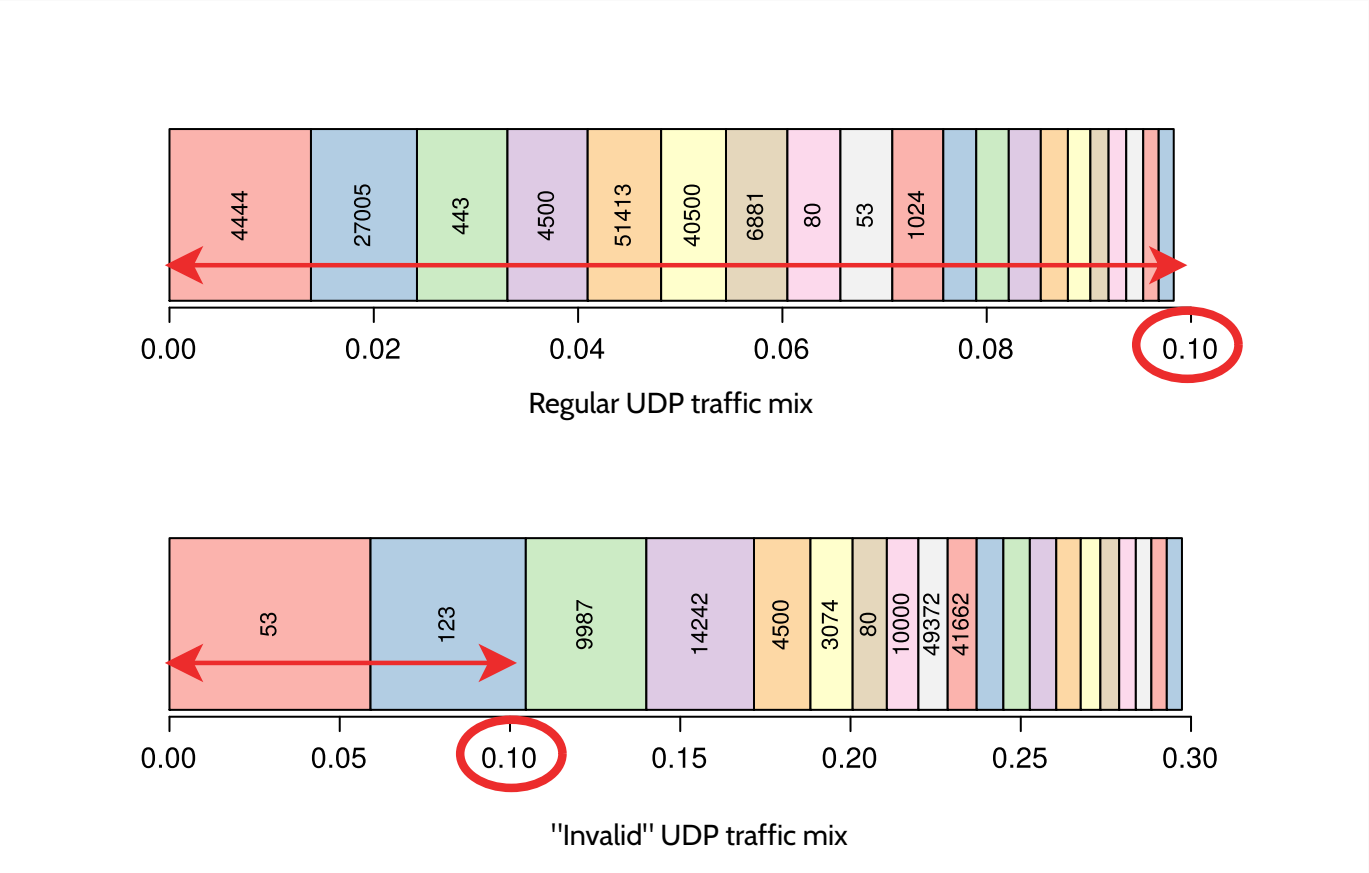
Top 20 UDP Destination Ports



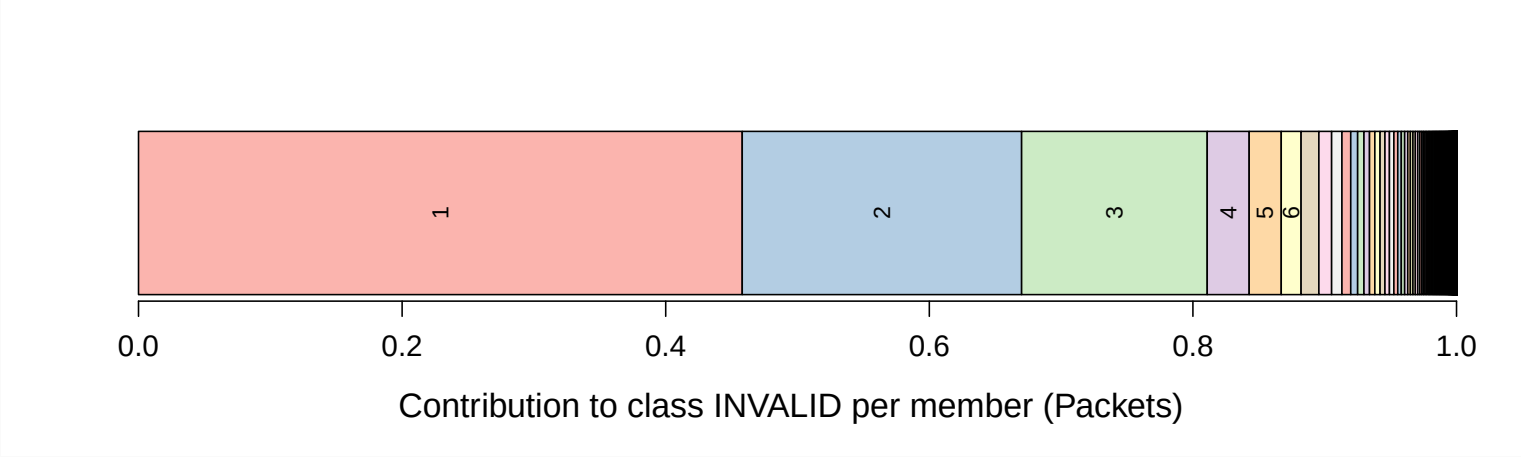
Top 20 UDP Destination Ports



Top 20 UDP Destination Ports



Contribution to invalid by IXP member



80% of the INVALID traffic can be attributed to 3 IXP members

Member Categorization (Bogon)

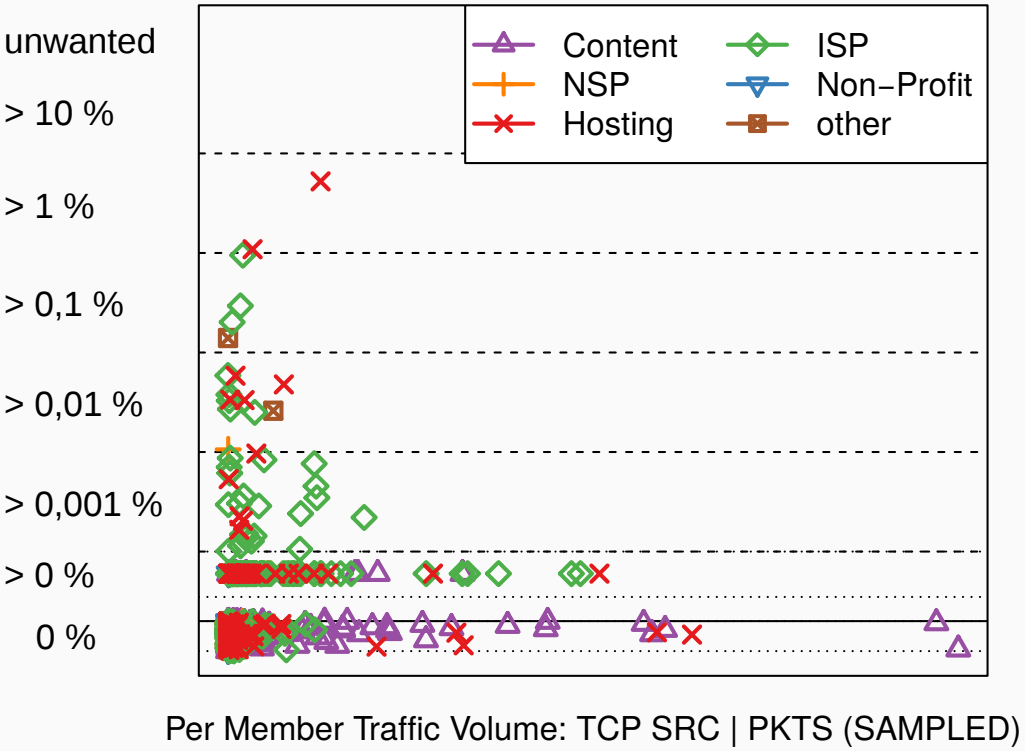


Figure 3: LIXP BOGON

Member Categorization (Bogon)

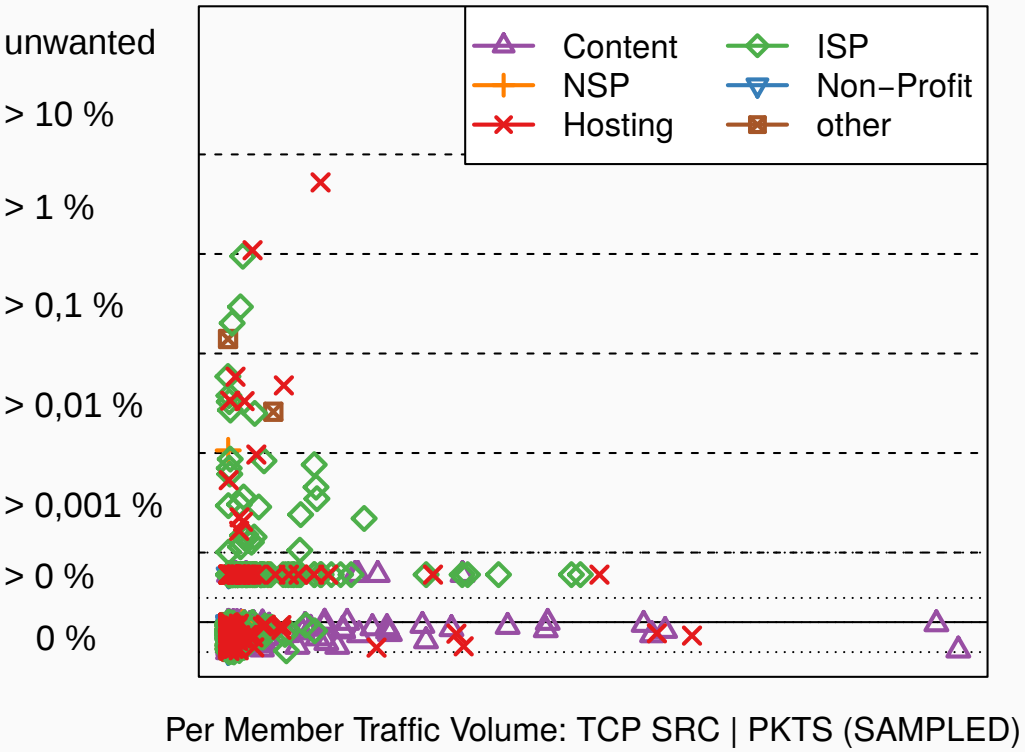


Figure 3: LIXP BOGON

- Majority does not leak anything
- TCP SYNs leaked: Probably misconfigured NAT
- Mostly low traffic ISPs and small hosters

Member Categorization (Unrouted and Invalid)

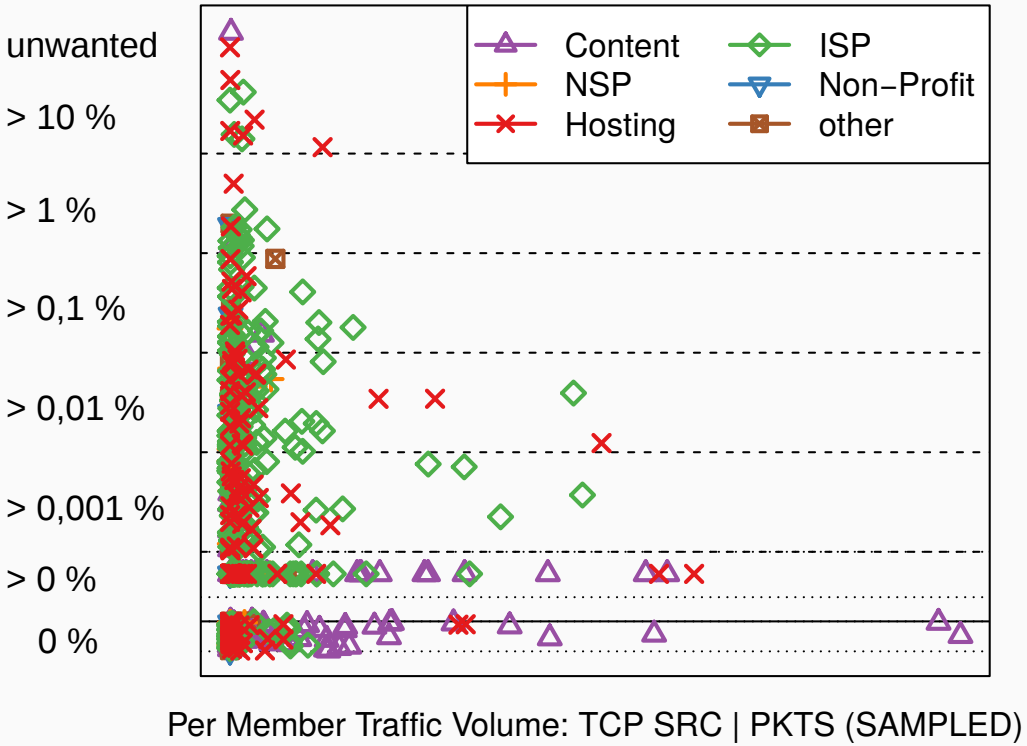


Figure 4: LIXP: Unrouted and Invalid

Member Categorization (Unrouted and Invalid)

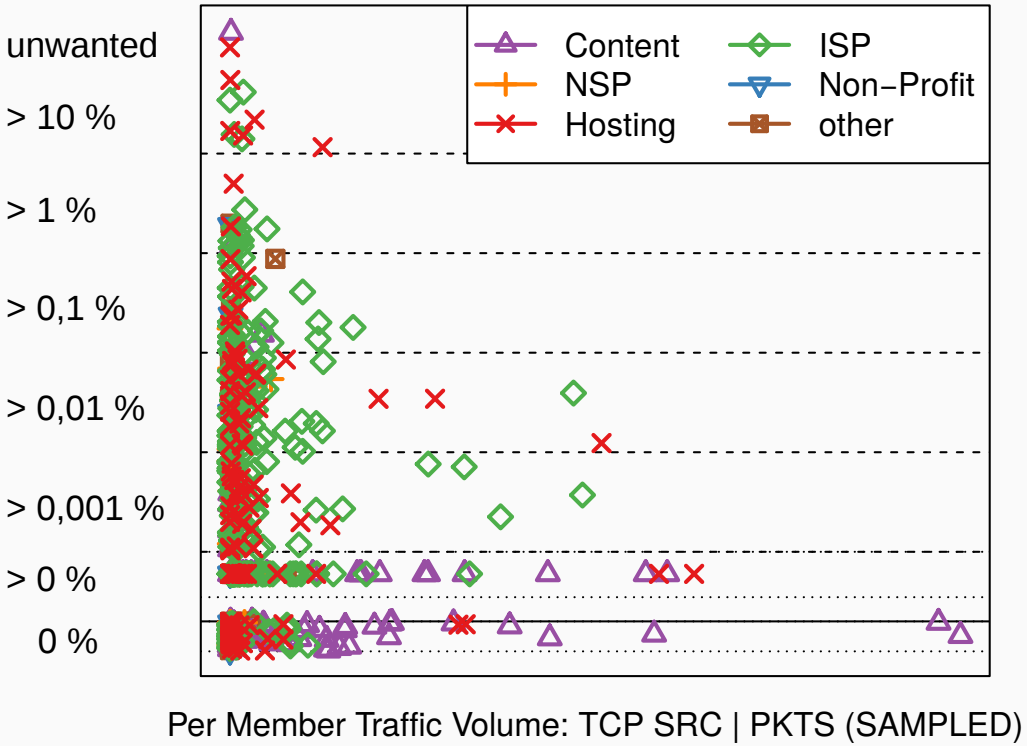


Figure 4: LIXP: UNROUTED and INVALID

- More members involved than in BOGON
- Still lots of members with 0%
- High traffic members have low unwanted level
- Lots of low traffic ISPs and hosters

Conclusion

What we found...

Network ingress filtering is not deployed everywhere, but some do it right...

What we found...

Network ingress filtering is not deployed everywhere, but some do it right...

- Large networks tend to deploy their filtering correctly – (Yes, it can be done!)
- Many small networks lack proper filtering
- Only a small amount of members contribute most of the unwanted traffic

What we found...

Network ingress filtering is not deployed everywhere, but some do it right...

- Large networks tend to deploy their filtering correctly – (Yes, it can be done!)
- Many small networks lack proper filtering
- Only a small amount of members contribute most of the unwanted traffic

Continue the ongoing efforts by the community to educate people and get rid of excuses!