Live Long and Prosper: Analyzing Long-Lived MOAS Prefixes in BGP

Presenter: Khwaja Zubair Sediqi
29 June 2023

Khwaja Zubair Sediqi
Max Planck Institute for Informatics
zsediqi@mpi-inf.mpg.de

Anja Feldmann
Max Planck Institute for Informatics
anja@mpi-inf.mpg.de

Oliver Gasser
Max Planck Institute for Informatics
oliver.gasser@mpi-inf.mpg.de
Introduction

1. MOAS Prefix (Hijacked Prefix)
   - Internet
   - AS1
   - AS2
   - 203.0.113.0/24

2. MOAS Prefix (Long-lived)
   - Internet
   - AS1
   - AS2
   - 203.0.113.0/24

We are interested in Long-lived MOAS prefixes

**Problem:** How to differentiate between both cases?
Motivation

IP to AS mapping  - > Geolocating problem

MOAS prefix usage for anycast services

Characteristics and users of MOAS prefixes
Identifying Long-Lived MOAS Prefixes

Daily RIBs from RIPE-RIS and Routeviews RCs

Measure the maximum lifetime of MOAS prefixes for six years (2017 – 2023)

Kneedle algorithm\(^1\) to determine the “elbow”, maximum curvature value, within the lifetime of all MOAS prefixes

All MOAS and Long-live MOAS

Huge Networks - DDoS Mitigation (AS264409) 143k prefixes

Angola Cables (AS37468) 90k prefixes

IPv4 MOAS increased from 1% to 2%
PREFIXES AND ORIGINS
RPKI Status of MOAS Prefixes

All Valid Origins increased 5% - 40%
  • MOAS -> not prefix hijacks

Not all origin ASes entered information in the RPKI database -> Partial Valid

Less than 1% All Invalid Origins
CIDR Sizes

Jazztel acquired by Orange (Orange Spain)

TTNet and Turk Telekomunikasyon

acquisition of KPN International by GTT

ASes use fine-granular CIDR sizes MOAS

Merger and acquisition lead to MOAS prefixes
Minimum and Maximum Visibility

For 99% of MOAS one Prefix Origing pair is visible by 100+ RC peers

For 40% MOAS at least one PO pair is visible only at one RC peer

One PO visible at 100 another barely visible

Hint: MOAS not mainly used for anycast
Anycast in MOAS Prefixes

Using bgp.tools anycast dataset
0.9% of IPv4 and 6.3% of IPv6 MOAS prefixes are **anycast** prefixes

Most of anycasted MOAS use **more than ten origin Ases**

**A** and **J** root DNS servers, use MOAS prefixes with a /24 CIDR size
USERS AND USAGE OF MOAS PREFIXES
Big players in the Internet

11 out of 16 Hypergiants$^1$ use MOAS prefixes

1. Verizon
2. Netflix
3. Google

to improve their network’s resilience, performance, and quality of experience

---

BGP Relationship of MOAS Prefix Origin ASes

Using CAIDA datasets

No relationship for 50% of origin AS pairs

Half of all origin AS pairs are C2P/P2C

Many MOAS prefixes are not related to sibling ASes
Business Type of MOAS Users

Using ASdb dataset

IT company pairs with other business types

Same company type for both origins being most common

40% of the cases, both MOAS origins fall into the “IT” category
Conclusion

Analyzed long-lived MOAS prefixes for a period of six years

Majority of MOAS prefixes
• valid ROV state in the RPKI
• mergers and acquisitions of companies
• customer-provider relationship
• users are IT companies

Rarely used for anycast purposes

We recommend network operators clean up the extra MOAS prefixes

zsediqi@mpi-inf.mpg.de
BACKUP SLIDES
**Lifetime Analysis**

*Six months* data from RC projects

**Lifetime** = duration a prefix is seen as a MOAS continuously

We use the *one day* sensitivity threshold
Using More Than One RIB per Day

Three RIBS per day **does not increase the Max Lifetime** of MOAS prefixes

How consistently prefixes are visible as MOAS?

- **Observability** = number of days out of the total days, when a prefix is observed as a MOAS

~ 80% of MOAS have > 95% observability
IPv4 long-lived MOAS prefixes increase from **10k** in 2017 to over **24k** prefixes at 2023

Number of origin ASes growing by about **50%** in the same time period.
95% IPv4 and 88% IPv6 MOAS have 2 origins ASes

60% of origin AS sets announce single MOAS

Few ASes announce large numbers of MOAS
Visibility Across Route Collector Peers

MOAS PO pairs around **50% visible in 100+ peers**

Followed by visibility of 3 or fewer peers