

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

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

Abstract—BGP exchanges reachability information in the form of prefixes, which are usually originated by a single Autonomous System (AS). If multiple ASes originate the same prefix, this is referred to as a Multiple Origin ASes (MOAS) prefix. One reason for MOAS prefixes are BGP prefix hijacks, which are mostly short-lived and have been studied extensively in the past years. In contrast to short-lived MOAS, long-lived MOAS have remained largely understudied.

In this paper, we focus on long-lived MOAS prefixes and perform an in-depth study over six years. We identify around 24k long-lived MOAS prefixes in IPv4 and 1.4k in IPv6 being announced in January 2023. By analyzing the RPKI status we find that more than 40% of MOAS prefixes have all origins registered correctly, with only a minority of MOAS having invalid origins. Moreover, we find that the most prominent CIDR size of MOAS prefixes is /24 for IPv4 and /48 for IPv6, suggesting their use for fine-grained traffic steering. We attribute a considerable number of MOAS prefixes to mergers and acquisitions of companies. Additionally, more than 90% of MOAS prefixes are originated by two origin ASes, with the majority of detected origin AS relations being customer-provider. Finally, we identify that the majority of MOAS users are IT companies, and just 0.9% of IPv4 MOAS and 6.3% of IPv6 MOAS prefixes are used for anycast.

I. INTRODUCTION

To exchange reachability information about IP addresses, different Autonomous Systems (ASes) in the Internet use BGP [1]. In BGP, each IP address prefix (i.e., collection of IP addresses) is usually originated by a single AS [2]. There are, however, also cases where multiple ASes originate the *same prefix*, this prefix is in turn called a Multi Origin AS (MOAS) prefix. Network operators use MOAS prefixes to e.g., provide resilience, load balancing, and multi-homing.

In addition to these uses, MOAS prefixes can also be a result of mergers of companies operating two ASes, misconfigurations [3], and—most problematically—prefix hijacks. This last case occurs if an attacker hijacks traffic to a specific prefix by announcing this prefix with its own AS as an origin. Unfortunately, prefix hijacks are happening relatively frequently [4], [5]. Consequently, prefix hijacks have been the focus of numerous studies over the past years [6]–[13].

Surprisingly, the use of long-lived MOAS prefixes—i.e., when they are visible for a longer time in BGP—remains understudied.

When analyzing RIB snapshots of all RIPE RIS [14] and Routeviews [15] route collectors, we find that the number of

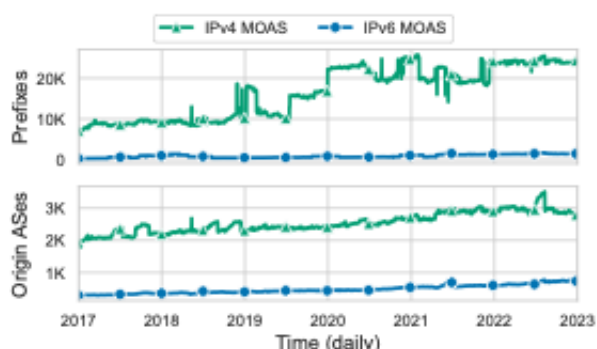


Fig. 1. Number of long-lived MOAS prefixes and origin ASes over time.

long-lived MOAS prefixes (i.e., visible for at least 30 days) is growing over time, as can be seen in Figure 1, both in terms of prefixes and origin ASes.

IPv4 long-lived MOAS prefixes increase from 10k in 2017 to over 24k prefixes at the beginning of 2023, with the number of origin ASes growing by about 50% in the same time period. Moreover, the fraction of long-lived MOAS prefixes out of all visible BGP prefixes is increasing as well (see Section III-D). In this paper, we focus on the analysis of these long-lived MOAS prefixes. We perform a longitudinal analysis across multiple dimensions to unveil prefix and origin characteristics, visibility, and users of MOAS prefixes. More specifically, the main contributions of this paper are:

- **Methodology to Detect Long-Lived MOAS Prefixes:** We apply a rigorous methodology to detect long-lived MOAS prefixes over a period of six years (see Section III). We use the Kneedle algorithm to discern long-lived from short-lived MOAS prefixes and perform a sensitivity analysis to analyze the influence of route collector artifacts.
- **MOAS Prefixes and Origins:** We perform a longitudinal analysis of MOAS prefixes and origin ASes (see Section IV). We find that more than 40% of long-lived MOAS prefixes have a valid RPKI status for all origins, hinting that hijacks are not prevalent among them. Moreover, we identify that the vast majority of MOAS prefixes are announced by two origin ASes. The most commonly used CIDR sizes are /24 for IPv4 and /48

978-3-903176-58-4 ©2023 IFIP