Position Paper: The Geolocation Conundrum for Small ISPs

Thomas (Tommy) Croghan

Lost Creek Technology, LLC

The Brothers WISP Podcast

tommy@lostcreek.tech

Introduction

As a consultant for numerous small to medium-sized Internet Service Providers (ISPs), I am writing to highlight the significant operational challenges we face regarding the current state of IP address geolocation. These issues not only impact our ability to deliver a consistent and reliable user experience but also consume valuable resources in a constant, often frustrating, battle against outdated and inaccurate data. The core problems are the lack of a standardized, timely feedback mechanism for corrections, the persistent misattribution of our networks, and the prolonged propagation delays for geolocation updates.

Gaps and Problems in Current Approaches

The existing IP geolocation ecosystem is fragmented and inefficient, lacking a unified approach for data submission and verification. For smaller ISPs, this results in several critical issues:

- **Delayed Updates and Lack of Feedback:** When we submit corrections for mislabeled IP addresses or subnets, the process is opaque and slow. It can take over a week for a simple update to be processed, if at all, and there is almost no feedback loop to confirm receipt or provide a timeline for correction. This high latency is a significant operational burden, as customer service teams are flooded with support requests from users who are unable to access region-locked content or whose accounts are flagged for suspicious activity. This can be even worse for ISPs who do not have excess IPv4 space to allocate when issues arise and customers become blacklisted.
- **Frequent Misattribution:** A common and particularly problematic issue is the mislabeling of our residential and business networks as commercial VPNs. This is likely due to the widespread use of Carrier-Grade Network Address Translation (**CG-NAT**) and the oversubscription of IP addresses. When a large number of users share a single public IPv4 address, it can be mistaken for a VPN server's traffic, leading to

service denials, captchas, or other authentication challenges on various websites and services. Furthermore, subnets that were previously used for malicious purposes and have since been recovered and re-allocated often carry a persistent "bad reputation" in various geolocation databases, further compounding the issue.

- **Long Propagation Delays:** Even after a correction is made with one geolocation provider, the new information can take months to propagate across all the different databases used by major content delivery networks (**CDNs**), streaming services, and other platforms. There is no central, authoritative source, leading to a constant cycle of individually contacting multiple, often unresponsive, organizations. The common refrain of "which geolocation database does -content provider- use?" in multiple industry forums highlights this fragmentation and the lack of a standardized solution. (I have managed the page: https://thebrotherswisp.com/index.php/geo-and-vpn for years now and it's routinely referenced across multiple industry forums)

Future Opportunities and Proposed Solutions

To address these challenges, we need a new approach that prioritizes standardization, transparency, and efficiency. Rather than relying on a disparate collection of private databases, a more effective solution would involve a collaborative, community-driven model. Preferably in conjunction with existing IP number allocation organizations (ARIN, APNIC, RIPE, etc.) and existing protocols/systems that show ownership (BGP, RPKI, IRR).

- **Standardized Submission and a Unified Database:** I propose the development of a standardized protocol for ISPs and network operators to submit geolocation data corrections. This would eliminate the "whack-a-mole" approach of updating each provider individually.
- **Reputation and Subnet History:** The proposed system could also include a mechanism to address the issue of misattributed reputation. When an IP block is recovered and re-allocated, the system could provide a way for the new holder to submit a "clean slate" request, effectively resetting its reputation score with major services. This would prevent new users from being unfairly penalized for the actions of previous tenants of the IP address space.
- **A "Beyond Geography" Approach:** Beyond simple latitude and longitude, a future solution could include more useful, privacy-preserving information. For example, a system could provide a way to convey the **type of last-mile network connection** (e.g., residential, business, mobile) and a confidence score for the geolocation data.

This would allow applications to make more informed decisions without relying solely on geographic location, which is often irrelevant to the user's intent. For instance, a streaming service might care more about whether a user is on a mobile network versus a residential one, rather than their exact city.

In conclusion, the current IP geolocation ecosystem is not fit for purpose in a modern, highly dynamic network environment. A collaborative and transparent approach is needed to resolve these issues and ensure that small ISPs can provide their customers with the reliable and accessible online experience users need.