GROW
Internet-Draft
Intended status: Informational
Expires: October 22, 2015

J. Mitchell

D. Rao
Cisco

R. Raszuk

April 20, 2015

Private Autonomous System (AS) Removal Requirements
draft-mitchell-grow-remove-private-as-04

Abstract

This document specifies operator's requirements for implementations that remove Private Use Autonomous System (AS) numbers from the AS path of routes sent to external Border Gateway Protocol (BGP) peers.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on October 22, 2015.

1. Introduction

After the original IANA reservation of Autonomous System Numbers (ASNs) for Private Use was allocated via [RFC1930] implementation specific features were released that removed ASNs from the Border Gateway Protocol AS_PATH attribute. The details of such implementations were driven by multiple operators use cases and varied accordingly. At times, implementation differences, mis-understanding of feature behavior and mis-configurations have led to operators leaking Private Use ASNs to the Internet. Since an additional range of Private Use ASNs has been documented in [RFC6996] implementations will likely require update and even more implementation variation is possible.

This document captures operator's requirements across various use cases, being cognizant of the operations of current implementations that remove Private Use ASNs, and provides a set of requirements for Private Use ASN removal implementations in the hopes of reducing inconsistencies and variations between implementations.

2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Basic Requirements

An implementation that removes Private Use ASNs MUST provide a configuration option to remove them from both the AS_PATH attribute of [RFC4271] and if Four-Octet AS Support [RFC6793] is present, the AS4_PATH attribute of the route. This configuration option MUST be configurable at least at the External Border Gateway Protocol (EBGP) peering session level, i.e. per neighbor, and will impact the as path attributes associated with any NLRI sent to the router to which is configured. The option SHOULD be configurable per AFI/SAFI so that implementations may provide different behaviors per address family. The implementation MUST remove all Private Use ASNs from the as path attributes up to the first non-Private Use AS in the as path, except as dictated by Section 4. An implementation MAY remove Private Use ASNs from the entire as path (past the first ASN in the as path attributes), however if it does so, it SHOULD provide an operator configurable option to disable this behavior if desired. The reason for this behavior is that operators would prefer visibility to which network is leaking Private Use ASNs to the global Internet (or any other network) so the behavior can be corrected directly by the upstream network providing connectivity to the Private Use ASN rather

than hiding the issue, which may not fully correct the problem if the downstream network has multiple providers.

4. Loop Prevention when using Private Use ASN Removal

Implementations of the Private Use ASN removal feature MAY provide basic loop prevention to prevent a dual-homed network utilizing a Private Use ASN which connects to a single ASN from receiving an update with it's own (Private) ASN removed that was sent back to the non-originating connection if the ASN to which it is connected has configured the feature towards it's other location. The implementation SHOULD validate that the peer ASN does not appear in the as path prior to removing Private ASNs from the path. If the peer ASN does appear, the Private Use removal feature should not manipulate the path. Otherwise, due to the standard BGP path selection process described in Section 9.1.2.2 of [RFC4271] EBGP routes will be preferred over IBGP routes which may have been from within the AS, so without further attribute manipulation, this can pose a risk of a routing information loop to some networks. Therefore a router SHOULD NOT remove Private Use ASN's from an AS_PATH or AS4_PATH attribute if it encounters the EBGP AS of the neighbor on which it is configured in the AS_PATH or AS4_PATH that would be removed.

5. Unnecessary Restrictions on Local or Peer AS

Implementations of this feature SHOULD NOT have any unnecessary restrictions on Private Use ASN use on either the local ASN of the router that is configuring the feature or the peer ASN that will be receiving the routes. Both use cases are prevalent in some networks as Private Use ASN removal features have sometimes been used in network mergers or other situations where masking the Private Use ASN's behind a particular AS, which may also be a Private Use ASN, is necessary to avoid conflict with Private Use ASN's inside the neighboring network. In these cases, as long as both the router with the feature configured and the peer have a unique Private ASN from each other, all routes originated from behind their networks containing Private ASN's can be masked to be their ASN. In the case where the AS where the feature is configured is a Private Use ASN and the router also has policy configured to prepend the local AS to the as path, an implementation SHOULD NOT remove the ASN's that have been locally prepended as per policy configuration, as it is expected that the local ASN cannot be removed from the path with the feature, and prepending is utilized by operators for various traffic engineering scenarios.

6. Private ASN Replacement Alternative

Implementations of this feature MAY include the capability to alternatively replace Private Use ASN's, or for that matter any arbitrary set of ASN's, in the AS Path with the local router ASN, thereby maintaining the original as path length when advertising the update to upstream networks. If this capability exists, it SHOULD NOT be the default behavior of the Private ASN removal feature and therefore MUST be operator configurable.

7. Behavior Towards other Special-Use ASNs

Implementations of this feature SHOULD NOT remove Documentation ASNs [RFC5398] as this may encourage their use by operators. These ASNs are not reserved for Private Use and use of them is likely the result of a misconfiguration. Due to historical reasons and lack of operator guidance on Last ASNs prior to [RFC7300] implementations MAY remove Last ASNs, which are deployed in some networks as if they are Private Use ASNs, even though this is not recommended to operators for the reasons specified in that document. If the implementation supports this, the behavior towards Last ASNs SHOULD be consistent with the behavior of the implementation towards Private Use ASNs as specified in this document.

8. Operational Considerations

It should be noted that removing items from the AS_PATH or AS4_PATH poses some risk and could introduce the chance of a routing loop. Further operational considerations for the use of Private Use ASNs are documented in [RFC6996].

9. IANA Considerations

There are no IANA actions required by this document. Current Private Use, Documentation and Last ASN registrations discussed in this document are located in the IANA AS Numbers registry [IANA.AS].

10. Security Considerations

There are no new security concerns in relation to the feature described in this document. General BGP security considerations are discussed in [RFC4271] and [RFC4272]. Identification of the originator of a route with a Private Use ASN in the AS path would have to be done by tracking the route back to the neighboring globally unique AS in the path or by inspecting other attributes.

11. References

11.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4271] Rekhter, Y., Li, T., and S. Hares, "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.

[RFC5398] Huston, G., "Autonomous System (AS) Number Reservation for Documentation Use", RFC 5398, December 2008.

[RFC6793] Vohra, Q. and E. Chen, "BGP Support for Four-Octet Autonomous System (AS) Number Space", RFC 6793, December 2012.

[RFC6996] Mitchell, J., "Autonomous System (AS) Reservation for Private Use", BCP 6, RFC 6996, July 2013.

[RFC7300] Haas, J. and J. Mitchell, "Reservation of Last Autonomous System (AS) Numbers", BCP 6, RFC 7300, July 2014.

11.2. Informative References

[IANA.AS] IANA, , "Autonomous System (AS) Numbers", April 2015, <http://www.iana.org/assignments/as-numbers/>.

[RFC1930] Hawkinson, J. and T. Bates, "Guidelines for creation, selection, and registration of an Autonomous System (AS)", BCP 6, RFC 1930, March 1996.

[RFC4272] Murphy, S., "BGP Security Vulnerabilities Analysis", RFC 4272, January 2006.

Appendix A. Acknowledgements

JM - Placeholder.

Authors' Addresses

Jon Mitchell

Email: jrmitche@puck.nether.net

Dhananjaya Rao
Cisco
170 West Tasman Dr.
San Jose, CA 95134
USA

Email: dhrao@cisco.com

Robert Raszuk

Email: robert@raszuk.net