BGP Prefix Origin Validation State Extended Community

Abstract

This document defines a new BGP opaque extended community to carry the origination Autonomous System (AS) validation state inside an autonomous system. Internal BGP (IBGP) speakers that receive this validation state can configure local policies that allow it to influence their decision process.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc8097.
Table of Contents

1.  Introduction . . . . . . . . . . . . . . . . . . . . . . . .   3
   1.1.  Requirements Language . . . . . . . . . . . . . . . . .   3
2.  Origin Validation State Extended Community . . . . . . . . .   3
3.  Deployment Considerations . . . . . . . . . . . . . . . . . .   4
4.  IANA Considerations . . . . . . . . . . . . . . . . . . . . .   4
5.  Security Considerations . . . . . . . . . . . . . . . . . . . .   4
6.  References . . . . . . . . . . . . . . . . . . . . . . . . . . .   5
   6.1.  Normative References . . . . . . . . . . . . . . . . . . .   5
   6.2.  Informative References . . . . . . . . . . . . . . . . . . .   5
Acknowledgements . . . . . . . . . . . . . . . . . . . . . . . . . .   6
Authors’ Addresses . . . . . . . . . . . . . . . . . . . . . . . . .   6
1. Introduction

This document defines a new BGP opaque extended community to carry the origination AS validation state inside an autonomous system. IBGP speakers that receive this validation state can configure local policies that allow it to influence their decision process.

1.1. 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 RFC 2119 [RFC2119].

2. Origin Validation State Extended Community

The origin validation state extended community is an opaque extended community [RFC4360] with the following encoding:

```
+--------+-----------------------------+
| Value  | Meaning                     |
+--------+-----------------------------+
| 0      | Lookup result = "valid"     |
| 1      | Lookup result = "not found" |
| 2      | Lookup result = "invalid"   |
+--------+-----------------------------+
```

If the router is configured to support the extensions defined in this document, it SHOULD attach the origin validation state extended community to BGP UPDATE messages sent to IBGP peers by mapping the computed validation state in the last octet of the extended...
community. Similarly, a receiving BGP speaker, in the absence of validation state set based on local data, SHOULD derive a validation state from the last octet of the extended community, if present.

An implementation SHOULD NOT send more than one instance of the origin validation state extended community. However, if more than one instance is received, an implementation MUST disregard all instances other than the one with the numerically greatest validation state value. If the value received is greater than the largest specified value (2), the implementation MUST apply a strategy similar to attribute discard [RFC7606] by discarding the erroneous community and logging the error for further analysis.

By default, implementations MUST drop the origin validation state extended community if received from an External BGP (EBGP) peer, without processing it further. Similarly, by default, an implementation SHOULD NOT send the community to EBGP peers. However, it SHOULD be possible to configure an implementation to send or accept the community when warranted. An example of a case where the community would reasonably be received from, or sent to, an EBGP peer is when two adjacent ASes are under control of the same administration. A second example is documented in [SIDR-RPKI].

3. Deployment Considerations

In deployment scenarios in which not all the speakers in an autonomous system are upgraded to support the extensions defined in this document, it is necessary to define policies that match on the origin validation extended community and set another BGP attribute [RFC6811] that influences selection of the best path in the same way that an implementation of this extension would.

4. IANA Considerations

IANA has registered the value 0x00, with the name "BGP Origin Validation State Extended Community", in the "Non-Transitive Opaque Extended Community Sub-Types" registry.

5. Security Considerations

Security considerations such as those described in [RFC4272] continue to apply. Because this document introduces an extended community that will generally be used to affect route selection, the analysis in Section 4.5 ("Falsification") of [RFC4593] is relevant. These issues are neither new nor unique to the origin validation extended community.
The security considerations provided in [RFC6811] apply equally to this application of origin validation. In addition, this document describes a scheme where router A outsources validation to some router B. If this scheme is used, the participating routers should have the appropriate trust relationship -- B should trust A either because they are under the same administrative control or for some other reason (for example, consider [SIDR-RPKI]). The security properties of the TCP connection between the two routers should also be considered. See Section 5.1 of [RFC7454] for advice regarding protection of the TCP connection.

6. References

6.1. Normative References


6.2. Informative References


Acknowledgements

The authors would like to acknowledge the valuable review and suggestions from Wesley George, Roque Gagliano, and Bruno Decraene on this document.

Authors’ Addresses

Pradosh Mohapatra  
Sproute Networks  
Email: mpradosh@yahoo.com

Keyur Patel  
Arrcus, Inc.  
Email: keyur@arrcus.com

John Scudder  
Juniper Networks  
1194 N. Mathilda Ave  
Sunnyvale, CA  94089  
United States of America  
Email: jgs@juniper.net

Dave Ward  
Cisco  
170 W. Tasman Drive  
San Jose, CA  95124  
United States of America  
Email: dward@cisco.com

Randy Bush  
Internet Initiative Japan, Inc.  
5147 Crystal Springs  
Bainbridge Island, WA  98110  
United States of America  
Email: randy@psg.com