

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 10, 2020

A. Azimov
E. Bogomazov
Qrator Labs
R. Bush
Internet Initiative Japan & Arccus
K. Patel
Arccus, Inc.
K. Sriram
US NIST
March 9, 2020

**Route Leak Prevention using Roles in Update and Open messages
draft-ietf-idr-bgp-open-policy-08**

Abstract

Route leaks are the propagation of BGP prefixes which violate assumptions of BGP topology relationships; e.g. passing a route learned from one peer to another peer or to a transit provider, passing a route learned from one transit provider to another transit provider or to a peer. Today, approaches to leak prevention rely on marking routes by operator configuration, with no check that the configuration corresponds to that of the BGP neighbor, or enforcement that the two BGP speakers agree on the relationship. This document enhances BGP OPEN to establish agreement of the (peer, customer, provider, Route Server, Route Server client) relationship of two neighboring BGP speakers to enforce appropriate configuration on both sides. Propagated routes are then marked with an OTC attribute according to the agreed relationship, allowing both prevention and detection of route leaks.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [BCP 14 \[RFC2119\]](#) [[RFC8174](#)] when, and only when, they appear in all capitals, as shown here.

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 <https://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 September 10, 2020.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

- [1.](#) Introduction [3](#)
- [2.](#) Peering Relationships [3](#)
- [3.](#) BGP Role [4](#)
- [4.](#) BGP Role Capability [4](#)
- [5.](#) Role correctness [5](#)
 - [5.1.](#) Strict mode [6](#)
- [6.](#) BGP Only to Customer (OTC) Attribute [6](#)
- [7.](#) Enforcement [7](#)
- [8.](#) Additional Considerations [7](#)
- [9.](#) IANA Considerations [7](#)
- [10.](#) Security Considerations [8](#)
- [11.](#) Acknowledgments [8](#)
- [12.](#) References [8](#)
 - [12.1.](#) Normative References [8](#)
 - [12.2.](#) Informative References [9](#)
- Authors' Addresses [10](#)

1. Introduction

A BGP route leak occurs when a route is learned from a transit provider or peer and then announced to another provider or peer. See [\[RFC7908\]](#). These are usually the result of misconfigured or absent BGP route filtering or lack of coordination between two BGP speakers.

The mechanism proposed in [\[I-D.ietf-grow-route-leak-detection-mitigation\]](#) uses large-communities to perform detection and mitigation of route leaks. While signaling using communities is easy to implement and deploy quickly, it normally relies on operator-maintained policy configuration, which is often vulnerable to misconfiguration and even attack [\[Streibelt\]](#). There is also the vulnerability that the community signal may be stripped, accidentally or maliciously.

This document provides configuration automation using 'BGP roles', which are negotiated using a new BGP Capability Code in OPEN message (see [Section 4 in \[RFC5492\]](#)). Either or both BGP speakers MAY be configured to require that this capability be agreed for the BGP OPEN to succeed.

A new BGP Path Attribute is specified that SHOULD be automatically configured using BGP roles. This attribute prevents networks from creating leaks, and detects leaks created by third parties.

2. Peering Relationships

Despite the use of terms such as "customer", "peer", etc. in this document, these are not necessarily business relationships based on payment agreements. These terms are used to represent restrictions on BGP route propagation, sometimes known as the Gao-Rexford model [\[Gao\]](#). The following is a list of various roles in BGP peering and the corresponding rules for route propagation:

Provider: MAY send to a customer all available prefixes.

Customer: MAY send to a provider their own prefixes and prefixes learned from any of their customers. A customer MUST NOT send to a provider prefixes learned from its peers, from other providers, or from Route Servers.

Route Server (RS): MAY send to an RS Client all available prefixes.

Route Server Client (RS-client): MAY send to an RS its own prefixes and prefixes learned from its customers. An RS-client MUST NOT send to an RS prefixes learned from its peers or providers, or from another RS.

Peer: MAY send to a peer its own prefixes and prefixes learned from its customers. A peer MUST NOT send to a peer prefixes learned from other peers, from its providers, or from RS(s).

Of course, any BGP speaker may apply policy to reduce what is announced, and a recipient may apply policy to reduce the set of routes they accept. Violation of the above rules may result in route leaks and MUST not be allowed. Automatic enforcement of these rules should significantly reduce route leaks that may otherwise occur due to manual configuration mistakes. While enforcing the above rules will address most BGP peering scenarios, their configuration is not part of BGP itself; therefore, configuration of ingress and egress prefix filters is still strongly advised.

3. BGP Role

BGP Role is new configuration option that SHOULD be configured on each BGP session. It reflects the real-world agreement between two BGP speakers about their relationship.

Allowed Role values for eBGP sessions are:

- o Provider - sender is a transit provider to neighbor;
- o Customer - sender is a transit customer of neighbor;
- o RS - sender is a Route Server, usually at an Internet exchange point (IX);
- o RS-Client - sender is client of an RS;
- o Peer - sender and neighbor are peers.

Since BGP Role reflects the relationship between two BGP speakers, it could also be used for other purposes besides route leak mitigation.

4. BGP Role Capability

The TLV (type, length, value) of the BGP Role capability are:

- o Type - <TBD1>;
- o Length - 1 (octet);
- o Value - integer corresponding to speaker's BGP Role.


```

+-----+-----+
| Value | Role name          |
+-----+-----+
|  0    | Sender is Provider |
|  1    | Sender is RS       |
|  2    | Sender is RS-Client|
|  3    | Sender is Customer |
|  4    | Sender is Peer     |
+-----+-----+

```

Table 1: Predefined BGP Role Values

5. Role correctness

Section 3 described how BGP Role encodes the relationship between two BGP speakers. But the mere presence of BGP Role doesn't automatically guarantee role agreement between two BGP peers.

To enforce correctness, the BGP Role check is applied with a set of constraints on how speakers' BGP Roles MUST correspond. Of course, each speaker MUST announce and accept the BGP Role capability in the BGP OPEN message exchange.

If a speaker receives a BGP Role capability, it MUST check the value of the received capability with its own BGP Role (if it is set). The allowed pairings are (first a sender's Role, second the receiver's Role):

```

+-----+-----+
| Sender Role | Receiver Role |
+-----+-----+
| Provider    | Customer      |
| Customer    | Provider      |
| RS          | RS-Client     |
| RS-Client   | RS            |
| Peer        | Peer          |
+-----+-----+

```

Table 2: Allowed Role Capabilities

If the observed Role pair is not in the above table, then the receiving speaker MUST send a Role Mismatch Notification (code 2, subcode <TBD2>) and reset the BGP session.

5.1. Strict mode

A new BGP configuration option "strict mode" is defined with values of true or false. If set to true, then the speaker MUST refuse to establish a BGP session with a neighbor which does not announce the BGP Role capability in the OPEN message. If a speaker rejects a connection, it MUST send a Connection Rejected Notification [[RFC4486](#)] (Notification with error code 6, subcode 5). By default, strict mode SHOULD be set to false for backward compatibility with BGP speakers that do not yet support this mechanism.

6. BGP Only to Customer (OTC) Attribute

Newly defined here, the Only to Customer (OTC) is an optional, 4 byte long, transitive BGP Path attribute with the Type Code <TBD3>. The purpose of this attribute is to guarantee that once route is sent to customer, peer or RS-client it will go only to customers. The semantics and usage of the OTC attribute are made clear by the ingress and egress policies described below.

The following ingress policy applies to the OTC attribute:

1. If a route with OTC attribute is received from a Customer or RS-client, then it is a route leak and MUST be rejected.
2. If a route with OTC attribute is received from a Peer and its value is not equal to the neighbor's ASN, then it is a route leak and MUST be rejected.
3. If a route is received from a Provider, Peer or RS and the OTC attribute is not present, then it MUST be added with value equal to the neighbor's AS number.

The egress policy MUST be:

1. A route with the OTC attribute set MUST NOT be sent to providers, peers, or RS(s).
2. If route is sent to a customer or peer, or an RS-Client and the OTC attribute is not present, then it MUST be added with value equal to AS number of the sender.

Once the OTC attribute has been set, it MUST be preserved unchanged.

7. Enforcement

Having the relationship unequivocally agreed between the two peers in BGP OPEN is critical; BGP implementations MUST enforce the relationship/role establishment rules (see [Section 5](#)) in order to overcome operator policy configuration errors (if any).

Similarly, the application of that relationship on prefix propagation using OTC MUST BE enforced by the BGP implementations, and not exposed to user mis-configuration.

As opposed to communities, BGP attributes may not be generally modified or filtered by the operator; BGP router implementations enforce such treatment. This is the desired property for the OTC marking. Hence, this document specifies OTC as an attribute.

8. Additional Considerations

There are peering relationships that are 'complex', i.e., both parties are intentionally sending prefixes received from each other to their non-transit peers and/or transit providers. If multiple BGP peerings can segregate the 'complex' parts of the relationship, the complex peering roles can be segregated into different normal BGP sessions, and BGP Roles MUST be used on each of the resulting normal (non-complex) BGP sessions.

No Roles SHOULD be configured on a 'complex' BGP session (assuming it is not segregated) and in that case, OTC MUST be set by configuration on a per-prefix basis. However, there are no built-in measures to check correctness of OTC use if BGP Role is not configured.

As the BGP Role reflects the peering relationship between neighbors, it might have other uses beyond the route leaks solution discussed so far. For example, BGP Role might affect route priority, or be used to distinguish borders of a network if a network consists of multiple ASs. Though such uses may be worthwhile, they are not the goal of this document. Note that such uses would require local policy control.

As BGP role configuration results in automatic creation of inbound/outbound filters, existence of roles should be treated as existence of Import and Export policy [[RFC8212](#)].

9. IANA Considerations

This document defines a new Capability Codes option [to be removed upon publication: <http://www.iana.org/assignments/capability-codes/>]

capability-codes.xhtml] [[RFC5492](#)], named "BGP Role" with an assigned value <TBD1>. The length of this capability is 1.

The BGP Role capability includes a Value field, for which IANA is requested to create and maintain a new sub-registry called "BGP Role Value". Assignments consist of Value and corresponding Role name. Initially this registry is to be populated with the data in Table 1. Future assignments may be made by a standard action procedure [[RFC5226](#)].

This document defines a new subcode, "Role Mismatch" with an assigned value <TBD2> in the OPEN Message Error subcodes registry [to be removed upon publication: <http://www.iana.org/assignments/bgp-parameters/bgp-parameters.xhtml#bgp-parameters-6>] [[RFC4271](#)].

This document defines a new optional, transitive BGP Path Attributes option, named "Only to Customer (OTC)" with an assigned value <TBD3> [To be removed upon publication: <http://www.iana.org/assignments/bgp-parameters/bgp-parameters.xhtml#bgp-parameters-2>] [[RFC4271](#)]. The length of this attribute is four bytes.

10. Security Considerations

This document proposes a mechanism for prevention of route leaks that are the result of BGP policy mis-configuration.

A misconfiguration in OTC setup may affect prefix propagation. But the automation that is provided by BGP roles should make such misconfiguration unlikely.

11. Acknowledgments

The authors wish to thank Douglas Montgomery, Brian Dickson, Andrei Robachevsky, and Daniel Ginsburg for their contributions to a variant of this work.

12. References

12.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.

- [RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", [RFC 4271](#), DOI 10.17487/RFC4271, January 2006, <<https://www.rfc-editor.org/info/rfc4271>>.
- [RFC4486] Chen, E. and V. Gillet, "Subcodes for BGP Cease Notification Message", [RFC 4486](#), DOI 10.17487/RFC4486, April 2006, <<https://www.rfc-editor.org/info/rfc4486>>.
- [RFC5492] Scudder, J. and R. Chandra, "Capabilities Advertisement with BGP-4", [RFC 5492](#), DOI 10.17487/RFC5492, February 2009, <<https://www.rfc-editor.org/info/rfc5492>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC 2119](#) Key Words", [BCP 14](#), [RFC 8174](#), DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.

12.2. Informative References

- [Gao] Gao, L. and J. Rexford, "Stable Internet routing without global coordination", IEEE/ACM Transactions on Networking, Volume 9, Issue 6, pp 689-692, DOI 10.1109/90.974523, December 2001, <<https://ieeexplore.ieee.org/document/974523>>.
- [I-D.ietf-grow-route-leak-detection-mitigation] Sriram, K. and A. Azimov, "Methods for Detection and Mitigation of BGP Route Leaks", [draft-ietf-grow-route-leak-detection-mitigation-01](#) (work in progress), July 2019.
- [RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [RFC 5226](#), DOI 10.17487/RFC5226, May 2008, <<https://www.rfc-editor.org/info/rfc5226>>.
- [RFC7908] Sriram, K., Montgomery, D., McPherson, D., Osterweil, E., and B. Dickson, "Problem Definition and Classification of BGP Route Leaks", [RFC 7908](#), DOI 10.17487/RFC7908, June 2016, <<https://www.rfc-editor.org/info/rfc7908>>.
- [RFC8212] Mauch, J., Snijders, J., and G. Hankins, "Default External BGP (EBGP) Route Propagation Behavior without Policies", [RFC 8212](#), DOI 10.17487/RFC8212, July 2017, <<https://www.rfc-editor.org/info/rfc8212>>.

[Streibelt]

Streibelt, F., Lichtblau, F., Beverly, R., Feldmann, A.,
Cristel, C., Smaragdakis, G., and R. Bush, "BGP
Communities: Even more Worms in the Routing Can",
<[https://people.mpi-inf.mpg.de/~fstreibelt/preprint/
communities-imc2018.pdf](https://people.mpi-inf.mpg.de/~fstreibelt/preprint/communities-imc2018.pdf)>.

Authors' Addresses

Alexander Azimov
Qrator Labs

Email: a.e.azimov@gmail.com

Eugene Bogomazov
Qrator Labs

Email: eb@qrator.net

Randy Bush
Internet Initiative Japan & Arccus

Email: randy@psg.com

Keyur Patel
Arccus, Inc.

Email: keyur@arccus.com

Kotikalapudi Sriram
US NIST

Email: ksriram@nist.gov

