Inter-Domain Routing
Internet-Draft
Intended status: Standards Track
Expires: 20 May 2026

D. Abraitis
NetDef

16 November 2025

BGP Route Flap Damping State Extended Community
draft-abraitis-bgp-rfd-state-ec-00

Abstract

This document defines a new BGP Opaque Extended Community to carry local route flap damping state information in BGP UPDATE messages. The community allows BGP speakers to expose the current damping penalty and configuration parameters associated with a route for visibility and troubleshooting purposes.

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 20 May 2026.

Table of Contents

1. Introduction 2
2. Specification of Requirements 3
3. The BGP Route Flap Damping State Extended Community 3
4. Operation 4
4.1. Sender Behaviour 4
4.2. Receiver Behaviour 5
4.3. Interaction with iBGP and eBGP 6
5. Deployment Considerations 6
6. IANA Considerations 7
7. Security Considerations 7
8. References 7
8.1. Normative References 7
Author's Address 8

1. Introduction

BGP Route Flap Damping (RFD) was originally specified in [RFC2439] as a mechanism to reduce the propagation of unstable routes in the Internet. Operational experience has shown that aggressive damping parameters can harm convergence, and [RFC7196] provides revised recommendations that make RFD more usable in modern networks.

Today, determining whether a route is being suppressed or penalized by damping at some point in the path typically requires out-of-band access to each router's local configuration and state. This opacity complicates troubleshooting, capacity planning, and understanding the stability characteristics of specific prefixes.

This document defines a new BGP Opaque Extended Community ([RFC4360]) referred to as the BGP Route Flap Damping State Extended Community. It allows a BGP speaker to attach a compact summary of its local damping state to a route advertisement. The information is primarily intended for visibility and troubleshooting; this document does not attempt to standardize any particular RFD algorithm or parameter set.

The design is intentionally similar in spirit to the BGP Prefix Origin Validation State Extended Community defined in [RFC8097], which carries RPKI origin validation state. In both cases, local state about routing policy is exported in-band using a transitive Opaque Extended Community.

2. Specification of Requirements

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.

3. The BGP Route Flap Damping State Extended Community

The BGP Route Flap Damping State Extended Community is an Opaque Extended Community as defined in [RFC4360]. Its high-order Type octet is taken from the "BGP Transitive Extended Community Types" registry as the Transitive Opaque Extended Community type, with value 0x03. The low-order Type octet (the Sub-Type) is allocated by IANA from the "Transitive Opaque Extended Community Sub-Types" registry ([RFC7153]).

The Extended Community is encoded as follows:

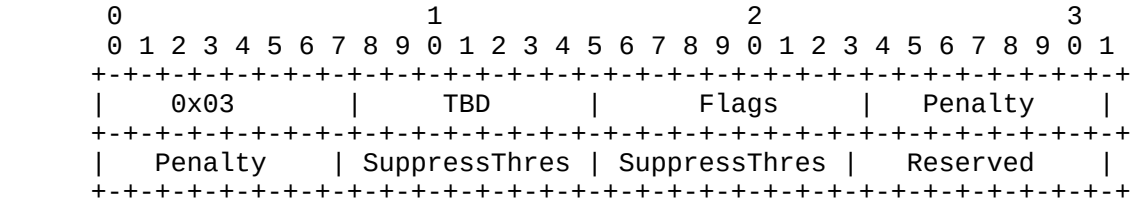

Figure 1: BGP Route Flap Damping State Extended Community

The fields are defined as follows:

Type (octet 0): The value 0x03 indicates a Transitive Opaque Extended Community.

Sub-Type (octet 1): The low-order Type octet is a Sub-Type allocated by IANA from the "Transitive Opaque Extended Community Sub-Types" registry. In this document it is referred to as the "BGP Route Flap Damping State Extended Community" and shown as "TBD".

Flags (octet 2): The Flags field contains the following bits, numbered from the most significant bit (bit 7) to the least significant bit (bit 0):

* Bit 7 (D - Damping Active): When set to 1, indicates that the advertising BGP speaker currently applies route flap damping to this route (that is, the route is subject to some form of RFD processing as described in [RFC2439] and/or [RFC7196]). When set to 0, the route is not currently subject to RFD at the advertising speaker.

* Bit 6 (R - Recently Reused): When set to 1, indicates that this route was previously suppressed by local RFD and has been reused (unsuppressed) within a locally configured "recent reuse interval". The precise duration of this interval is an implementation detail. When set to 0, either the route has not been suppressed since the last reset of RFD state, or the reuse event occurred sufficiently long ago that the implementation no longer considers it "recent".

* Bits 5-0: Reserved. These bits MUST be set to 0 on transmission and MUST be ignored on reception.

Penalty (octets 3-4): A 16-bit unsigned integer giving the current RFD penalty assigned to this route at the advertising speaker. The units are the implementation’s native penalty units, consistent with its damping algorithm. A value of 0 indicates that no penalty is currently applied.

SuppressThres (octets 5-6): A 16-bit unsigned integer giving the suppress threshold of the damping profile currently applied to this route, expressed in the same penalty units as the Penalty field. When the penalty equals or exceeds this value, the route is suppressed by the local RFD algorithm. A value of 0 indicates that the suppress threshold is not available or not being signalled.

Reserved (octet 7): This octet is reserved for future use. It MUST be set to 0 on transmission and MUST be ignored on reception.

4. Operation

4.1. Sender Behaviour

A BGP speaker that implements this specification and that applies route flap damping to a route MAY attach the BGP Route Flap Damping State Extended Community to UPDATE messages that advertise that route.

If the route is not subject to any local RFD processing, the speaker MUST NOT attach this Extended Community.

When attaching the community, the speaker:

* MUST set the D bit in the Flags field to 1.

* MUST set the Penalty field to the current penalty value for the route in the speaker’s RFD implementation.

* SHOULD set the SuppressThres field to the suppress threshold associated with the damping profile applied to this route. If this value is not available or not meaningful, it MUST be set to 0.

* SHOULD set the R bit to 1 if the route has transitioned from "suppressed" to "unsuppressed" within a locally configured "recent reuse interval". Otherwise it SHOULD set the R bit to 0.

A speaker SHOULD attach at most one instance of the BGP Route Flap Damping State Extended Community to a given path. If multiple instances would otherwise be attached, the speaker SHOULD retain only one.

4.2. Receiver Behaviour

A BGP speaker that receives a route with the BGP Route Flap Damping State Extended Community and that supports this specification:

* MAY use the information for operational visibility, logging, or external telemetry.

* MAY use the information as an input to local policy (for example, to de-prefer routes with high penalty values or to trigger additional monitoring for routes with frequent damping activity).

* MUST NOT treat the absence of this Extended Community as an error or as an indication that the route is not damped.

If multiple instances of the BGP Route Flap Damping State Extended Community are present for the same path, the speaker:

* MUST select a single instance to use and MUST ignore the rest.

If a Penalty or SuppressThres value is outside the acceptable range for the local implementation, the speaker MUST ignore that Extended Community instance and SHOULD log the condition for administrative review.

4.3. Interaction with iBGP and eBGP

The BGP Route Flap Damping State Extended Community is transitive and therefore propagates across both iBGP and eBGP sessions, subject to normal routing policy.

By default, an implementation:

* SHOULD propagate the BGP Route Flap Damping State Extended Community unchanged when advertising a route, unless local policy explicitly removes or modifies it.

* MAY be configured to strip, rewrite, or otherwise filter this Extended Community on a per-neighbor or per-policy basis.

Because the Extended Community is opaque, BGP speakers that do not implement this specification will treat it as an unknown transitive Extended Community and will propagate it as specified in [RFC4360].

For iBGP, normal propagation rules apply. A route reflector that receives a route with this Extended Community MAY reflect it to other clients, subject to local policy.

Although the mechanism was motivated primarily by intra-AS visibility and troubleshooting use cases, there is no protocol prohibition on using it across Autonomous Systems. Operators that exchange the BGP Route Flap Damping State Extended Community across eBGP sessions SHOULD ensure that there is an appropriate trust relationship and a shared understanding of how the information will be used.

5. Deployment Considerations

In many deployments, not all routers in an AS will support this specification. Operators MAY use routing policy to translate the information carried in the BGP Route Flap Damping State Extended Community into other attributes (for example, a local preference adjustment or a non-transitive community) that can be understood by legacy routers.

This document does not change the RFD algorithm, decay parameters, or recommended default values, which remain governed by [RFC2439] and [RFC7196]. Operators SHOULD continue to follow best practices for RFD configuration as described therein.

Because this Extended Community is transitive, information about local damping state may propagate beyond the originating Autonomous System. This can expose aspects of local policy (such as the use of RFD and the relative aggressiveness of configured thresholds) to

external networks. Operators that consider this information sensitive SHOULD apply export policies that remove or rewrite the Extended Community at AS boundaries.

6. IANA Considerations

IANA is requested to allocate a new Sub-Type from the "Transitive Opaque Extended Community Sub-Types" registry under "Border Gateway Protocol (BGP) Extended Communities" with the following entry:

Value	Description
TBD	BGP Route Flap Damping State Extended Community

Table 1

No other IANA actions are required by this document.

7. Security Considerations

The security considerations for BGP and RFD in general are discussed in [RFC4271], [RFC4272], [RFC4593], [RFC2439], and [RFC7196]. This document does not introduce new security mechanisms; it defines a new way to signal local RFD state.

When the Extended Community is permitted on eBGP sessions, the participating networks SHOULD have an appropriate trust relationship and a clear operational agreement regarding how the information will be interpreted and used.

Because this Extended Community is transitive, information about local damping state may propagate beyond the originating Autonomous System. Where this is considered sensitive, operators SHOULD use policy to control its export.

8. References

8.1. 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>.

[RFC2439] Villamizar, C., Chandra, R., and R. Govindan, "BGP Route Flap Damping", RFC 2439, DOI 10.17487/RFC2439, November 1998, <https://www.rfc-editor.org/info/rfc2439>.

[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>.

[RFC4272] Murphy, S., "BGP Security Vulnerabilities Analysis", RFC 4272, DOI 10.17487/RFC4272, January 2006, <https://www.rfc-editor.org/info/rfc4272>.

[RFC4360] Sangli, S., Tappan, D., and Y. Rekhter, "BGP Extended Communities Attribute", RFC 4360, DOI 10.17487/RFC4360, February 2006, <https://www.rfc-editor.org/info/rfc4360>.

[RFC4593] Barbir, A., Murphy, S., and Y. Yang, "Generic Threats to Routing Protocols", RFC 4593, DOI 10.17487/RFC4593, October 2006, <https://www.rfc-editor.org/info/rfc4593>.

[RFC7153] Rosen, E. and Y. Rekhter, "IANA Registries for BGP Extended Communities", RFC 7153, DOI 10.17487/RFC7153, March 2014, <https://www.rfc-editor.org/info/rfc7153>.

[RFC7196] Pelsser, C., Bush, R., Patel, K., Mohapatra, P., and O. Maennel, "Making Route Flap Damping Usable", RFC 7196, DOI 10.17487/RFC7196, May 2014, <https://www.rfc-editor.org/info/rfc7196>.

[RFC8097] Mohapatra, P., Patel, K., Scudder, J., Ward, D., and R. Bush, "BGP Prefix Origin Validation State Extended Community", RFC 8097, DOI 10.17487/RFC8097, March 2017, <https://www.rfc-editor.org/info/rfc8097>.

[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>.

Author’s Address

Donatas Abraitis
NetDef
Email: donatas.abraitis@gmail.com