Internet Engineering Task Force (IETF)
Request for Comments: 9104
Category: Standards Track
ISSN: 2070-1721

J. Tantsura
Microsoft
Z. Wang
Q. Wu
Huawei
K. Talaulikar
Cisco Systems

August 2021

Distribution of Traffic Engineering Extended Administrative Groups Using the Border Gateway Protocol - Link State (BGP-LS)

Abstract

Administrative groups are link attributes used for traffic engineering. This document defines an extension to the Border Gateway Protocol - Link State (BGP-LS) for advertisement of extended administrative groups (EAGs).

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 https://www.rfc-editor.org/info/rfc9104.

Table of Contents

1. Introduction

Administrative groups (commonly referred to as "colors" or "link colors") are link attributes that are advertised by link-state protocols like IS-IS [RFC1195], OSPFv2 [RFC2328], and OSPFv3 [RFC5340]. The Border Gateway Protocol - Link State (BGP-LS) advertisement of the originally defined (non-extended) administrative groups is encoded using the Administrative Group (color) TLV 1088 as defined in [RFC7752].

These administrative groups are defined as a fixed-length 32-bit bitmask. As networks grew and more use cases were introduced, the 32-bit length was found to be constraining, and hence extended administrative groups (EAGs) were introduced in [RFC7308].

The EAG TLV (Section 2) is not a replacement for the Administrative Group (color) TLV; as explained in [RFC7308], both values can coexist. It is out of scope for this document to specify the behavior of the BGP-LS consumer [RFC7752].

This document specifies an extension to BGP-LS for advertisement of the extended administrative groups.

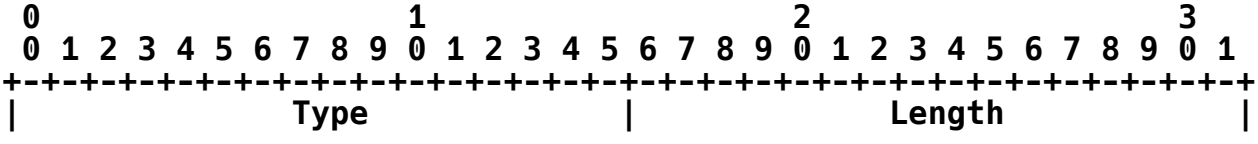
1.1. Requirements Language

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.

2. Advertising Extended Administrative Groups in BGP-LS

This document defines an extension that enables BGP-LS speakers to signal the EAG of links in a network to a BGP-LS consumer of network topology such as a centralized controller. The centralized controller can leverage this information in traffic engineering computations and other use cases. When a BGP-LS speaker is originating the topology learned via link-state routing protocols like OSPF or IS-IS, the EAG information of the links is sourced from the underlying extensions as defined in [RFC7308].

The EAG of a link is encoded in a new Link Attribute TLV [RFC7752] using the following format:



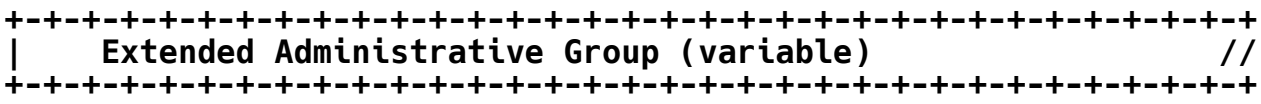


Figure 1: Extended Administrative Group TLV Format

Where:

Type: 1173

Length: variable length that represents the total length of the value field in octets. The length value MUST be a multiple of 4. If the length is not a multiple of 4, the TLV MUST be considered malformed.

Value: one or more sets of 32-bit bitmasks that indicate the administrative groups (colors) that are enabled on the link when those specific bits are set.

3. IANA Considerations

IANA has assigned a code point from the "BGP-LS Node Descriptor, Link Descriptor, Prefix Descriptor, and Attribute TLVs" registry as described in the following table.

Code Point	Description	IS-IS TLV/Sub-TLV
1173	Extended Administrative Group	22/14

Table 1

4. Manageability Considerations

The new protocol extensions introduced in this document augment the existing IGP topology information that is distributed via [RFC7752]. Procedures and protocol extensions defined in this document do not affect the BGP protocol operations and management other than as discussed in Section 6 ("Manageability Considerations") of [RFC7752]. Specifically, the tests for malformed attributes, to perform syntactic checks as described in Section 6.2.2 ("Fault Management") of [RFC7752], now encompass the new BGP-LS Attribute TLV defined in this document. The semantic or content checking for the TLV specified in this document and its association with the BGP-LS Network Layer Reachability Information (NLRI) types or its BGP-LS Attribute are left to the consumer of the BGP-LS information (e.g., an application or a controller) and not to BGP itself.

A consumer of the BGP-LS information retrieves this information over a BGP-LS session (refer to Sections 1 and 2 of [RFC7752]).

5. Security Considerations

The procedures and protocol extensions defined in this document do not affect the BGP security model. See the "Security Considerations"

section of [RFC4271] for a discussion of BGP security. This document only introduces a new Attribute TLV, and any syntactic error in it would result in the BGP-LS Attribute being discarded [RFC7752]. Also, refer to [RFC4272] and [RFC6952] for analyses of security issues for BGP. Security considerations for acquiring and distributing BGP-LS information are discussed in [RFC7752]. The TLV introduced in this document is used to propagate the EAG extensions defined in [RFC7308]. It is assumed that the IGP instances originating this TLV will support any required security mechanisms for OSPF and IS-IS, in order to prevent any security issues when propagating the Sub-TLVs into BGP-LS.

Security concerns for OSPF are addressed in [RFC7474], [RFC4552], and [RFC7166]. Further security analysis for the OSPF protocol is done in [RFC6863].

Security considerations for IS-IS are specified by [RFC5304].

The advertisement of the link attribute information defined in this document presents no significant additional risk beyond that associated with the existing link attribute information already supported in [RFC7752].

6. References

6.1. 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>.

[RFC7308] Osborne, E., "Extended Administrative Groups in MPLS Traffic Engineering (MPLS-TE)", RFC 7308, DOI 10.17487/RFC7308, July 2014, <https://www.rfc-editor.org/info/rfc7308>.

[RFC7752] Gredler, H., Ed., Medved, J., Previdi, S., Farrel, A., and S. Ray, "North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP", RFC 7752, DOI 10.17487/RFC7752, March 2016, <https://www.rfc-editor.org/info/rfc7752>.

[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>.

6.2. Informative References

[RFC1195] Callon, R., "Use of OSI IS-IS for routing in TCP/IP and dual environments", RFC 1195, DOI 10.17487/RFC1195, December 1990, <https://www.rfc-editor.org/info/rfc1195>.

[RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, DOI 10.17487/RFC2328, April 1998, <https://www.rfc-editor.org/info/rfc2328>.

[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>.

[RFC4552] Gupta, M. and N. Melam, "Authentication/Confidentiality for OSPFv3", RFC 4552, DOI 10.17487/RFC4552, June 2006, <https://www.rfc-editor.org/info/rfc4552>.

[RFC5304] Li, T. and R. Atkinson, "IS-IS Cryptographic Authentication", RFC 5304, DOI 10.17487/RFC5304, October 2008, <https://www.rfc-editor.org/info/rfc5304>.

[RFC5340] Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF for IPv6", RFC 5340, DOI 10.17487/RFC5340, July 2008, <https://www.rfc-editor.org/info/rfc5340>.

[RFC6863] Hartman, S. and D. Zhang, "Analysis of OSPF Security According to the Keying and Authentication for Routing Protocols (KARP) Design Guide", RFC 6863, DOI 10.17487/RFC6863, March 2013, <https://www.rfc-editor.org/info/rfc6863>.

[RFC6952] Jethanandani, M., Patel, K., and L. Zheng, "Analysis of BGP, LDP, PCEP, and MSDP Issues According to the Keying and Authentication for Routing Protocols (KARP) Design Guide", RFC 6952, DOI 10.17487/RFC6952, May 2013, <https://www.rfc-editor.org/info/rfc6952>.

[RFC7166] Bhatia, M., Manral, V., and A. Lindem, "Supporting Authentication Trailer for OSPFv3", RFC 7166, DOI 10.17487/RFC7166, March 2014, <https://www.rfc-editor.org/info/rfc7166>.

[RFC7474] Bhatia, M., Hartman, S., Zhang, D., and A. Lindem, Ed., "Security Extension for OSPFv2 When Using Manual Key Management", RFC 7474, DOI 10.17487/RFC7474, April 2015, <https://www.rfc-editor.org/info/rfc7474>.

Acknowledgments

The authors would like to thank Eric Osborne, Les Ginsberg, Tim Chown, Ben Niven-Jenkins, and Alvaro Retana for their reviews and valuable comments.

Authors' Addresses

Jeff Tantsura
Microsoft

Email: jefftant.ietf@gmail.com

Zitao Wang
Huawei
Yuhua District
101 Software Avenue
Nanjing
Jiangsu, 210012
China

Email: wangzitao@huawei.com

Qin Wu
Huawei
Yuhua District
101 Software Avenue
Nanjing
Jiangsu, 210012
China

Email: bill.wu@huawei.com

Ketan Talaulikar
Cisco Systems

Email: ketant@cisco.com