

IDR Working Group  
Internet-Draft  
Intended status: Informational  
Expires: 4 September 2025

S. Hares  
Hickory Hill Consulting  
3 March 2025

Guidance for Authors writing text for the BGP Tunnel Encapsulation  
Attribute  
draft-hares-idr-bess-tea-templates-00

## Abstract

The BGP (RFC4271) Tunnel Encapsulation Attribute (TEA) is defined in RFC9012. Currently proposed BGP specifications in the IDR and BESS Working groups have defined new tunnels and new parameters for these tunnels in Sub-TLV. The Segment Routing usage of the TEA has suggested a number of new Sub-TLVs. This document provides guidelines to help authors quickly write correct text for new tunnels (defined in tunnel TLVs) and new Sub-TLVs. These guidelines are given as "templates" to aid new authors. More experienced authors should view these templates as a list of expected content.

One additional challenge for tunnels using the PMSI tunnels is to carefully define the interaction between PMSI tunnels and TEA tunnels.

## 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 4 September 2025.

## Copyright Notice

Copyright (c) 2025 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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Tunnel TLV Specification Guidelines . . . . .	3
2.1. Do and Donts for Tunnel TLVs . . . . .	4
3. Sub-TLV Specification Guidelines . . . . .	5
3.1. Sub-TLVtemplate form with instructions: . . . . .	6
4. PMSI Interactions Specification Guidelines . . . . .	8
5. IANA Considerations . . . . .	8
6. Security Considerations . . . . .	9
7. References . . . . .	9
7.1. Normative References . . . . .	9
7.2. Informative References . . . . .	9
Author's Address . . . . .	9

## 1. Introduction

The BGP [RFC4271] Tunnel Encapsulation Attribute (TEA) [RFC9012] defines a BGP attribute that passes tunnel information. BGP passes this attribute to associate prefixes with a particular tunnel.

Currently proposed BGP specifications in the IDR and BESS Working groups have defined new tunnels and new parameters for these tunnels in Sub-TLV. This document provides guidelines to help authors quickly write correct text for new tunnels (defined in tunnel TLVs) and new Sub-TLVs. These guidelines are given as "templates" to aid new authors. More experience authors should view these templates as a list of expected content.

One additional challenge for tunnels defined by [RFC9012] TEA is the interaction with the PMSI tunnels ([RFC6514], [RFC7385]) is to carefully define the interaction between PMSI tunnels and TEA tunnels.

This set of guidelines comes from the lessons learned from reviewing the following different drafts for the BGP TEA:

draft-ietf-idr-sr-policy-safi: defines a BGP NLRI and a SR Policy

tunnel TLV for the BGP TEA, and several Sub-TLVs for the SR Policy Tunnel TLV based on the SR Policy architecture [RFC9552].

IDR drafts defining parameters for the SR Policy tunnel: This includes draft-ietf-idr-sr-policy-nrp, draft-idr-sr-policy-path-mtu, draft-ietf-idr-sr-policy-path-segment, and draft-ietf-sr-policy-seglist)

draft-ietf-idr-sdwan-edge-discovery: defines a Hybrid SDWAN Tunnel and several Sub-TLVs.

draft-ietf-bess-multicast-controller: defines two tunnels (Any Encapsulation tunnel (78), Load-Balancing Tunnel, Segment list Tunnel, and Sub-TLVs for these tunnels.

draft-ietf-bess-evpn-geneve: defines a Geneve tunnel type, and a Geneve Tunnel Option Sub-TLV.

The purpose behind the guidelines is content rather than form. In the draft-ietf-idr-sdwan-discovery-document, I used tables to refer to Sub-TLVs supported and sections with the description.

I will post prior to IETF-122 on the IDR wiki, reviews and suggested changes based on this document for the BESS and IDR draft using tunnels. This rough draft is to provide an snapshot of the Wiki prior to IETF-122.

## 2. Tunnel TLV Specification Guidelines

This section describes a guideline for information regarding new tunnel types. It is presented as a template to aid new authors.

Tunnel encapsulation specification requires the following things for each tunnel:

Name: Short name that will go in IANA allocation

Code: Code assigned by IANA

Description: Give a description of the tunnel and usage. The authors should strive to have a paragraph of description, but the description may point to other sections in the document.

List of all Sub-TLVs supported: This list should include the sub-TLV that may be sent in this tunnel TLV. This list should include mandatory and optional TLVs. Please denote which sub-TLVs are mandatory and which sub-TLVs are optional. Please note any sub-TLVs that are not listed are not supported.

List of all Sub-TLVs not supported: This list includes the Sub-TLVs which are not supported by this tunnel TLV. Note that any Sub-TLVs which are not explicitly defined as supported are by default unsupported.

A validation procedure: Each tunnel should have a set of procedures to determine if tunnel signaled by BGP is valid.

Multiple Tunnel interactions: Multiple Tunnel TLVs can be included in a single BGP TEA. If there are interactions between Tunnel TLVs, then this should be described in this section. For example, if one Tunnel TLV defines a security association that another TLV uses.

Security Considerations: A security section needs to provides specific comments regarding the information passed in the tunnel TLV. Tunnel TLVs can send critical information regarding a network infrastructure, and this critical information needs to be identified. After the critical information is identified, the security section should discuss how network operators should restrict access to such critical information.

Management Considerations: A management section includes comments on how the tunnel will be managed.

It is helpful for items 1-5 be clearly laid out in one section.

## 2.1. Do and Donts for Tunnel TLVs

### 1. Name: Do: Give a short name

Do not: Please do not replicate an existing tunnel or Sub-TLV name

### 2. Code: Do: Use a TBDxx unless assigned a number by IANA.

Do not: assign your own number for tunnel type.

### 3. Description: Do: Do you give a short description regarding the tunnel, and link to a more extended text block giving a detailed description.

Do not Forget: to give information in the longer text about conflicts with any other tunnels if both are attached to the same route, what network applications use the tunnel, and pros/cons about using tunnel.

### 4. List of all Sub-TLVs defined for this tunnel TLV Do: Look at RFC9012 and any other TEA document you reference

(e.g. draft-ietf-idr-sr-policy-safi).

Do: Gather a full list of Sub-TLVs from IANA lists and put it in a table with an indication for mandatory, optional, or not-supported. Report any errors in the IANA list to the IDR chairs.

Do: Provide a complete list with the form of name (code-number) for each item.

5. List of unsupported Sub-TLV: This contains a list of Sub-TLVs which are not supported for this tunnel TLV

6. Validation procedure(s): Do: Write up a validation procedure for each Tunnel.

Do: Look at existing validation procedures in [RFC9012]. Validation procedures may or may not include The Tunnel-Egress Endpoint.

Do Not Assume that one tunnel validation procedure matches another.

7. Multiple Tunnel Interactions Do: Consider if this tunnel interacts with another tunnel

specified for the prefixes (AFI/SAFI). If so, please give advice to the implementers.

Do not: Forget to look at all existing Tunnel types at the IANA site (<https://www.iana.org/assignments/bgp-tunnel-encapsulation/bgp-tunnel-encapsulation.xhtml>).

8. Security Considerations: Do: Please look draft-ietf-idr-sr-policy-safi for a good template.

Do: Consider what information is critical information or mission-critical information in the tunnel TLV or sub-TLV passed in tunnel TLV.

Do not: Forget to add the critical information in the security section.

9. Manageability section: How is the operator going to create the new tunnels in configuration? This section consider how easy this tunnel is to manage or configure.

### 3. Sub-TLV Specification Guidelines

A document specifying a new Sub-TLV needs include the following Information:

1. Title: Short title that goes in IANA documentation (10-15 characters).
2. Sub-TLV Type Code: Value for Type code.
3. Encoding of Value bytes: this information should include:
  - 3.1 diagram of value byte
  - 3.2 Description of each field in Encoding
  - 3.3 Error handling per field
4. Tunnel TLVs this Sub-TLV can appear in: The authors should list tunnel TLVs that support this Sub-TLV as mandatory or optional Sub-TLV
5. Sub-TLV role in validation: Please indicate whether this Sub-TLV play a part in validation in the validation of the validation of any Tunnel TLV.

It is helpful for items 1-5 be clearly laid out in one section. If new sub-TLVs are defined, it is helpful that these Sub-TLVs go before the list of all sub-TLVs.

In addition, the SUB-tLV may be part of discussions on:

- \* Multiple Tunnel interactions,
- \* security considerations with specific comments regarding critical information passed in a tunnel TLV in a BGP TEA,
- \* management considerations that includes comments on how the tunnel will be managed.

### 3.1. Sub-TLVtemplate form with instructions:

1. Title: One-line summary name that gets added to the IANA Sub-TLV list
2. Type: Type code values (assigned by IANA) in the form value (IANA) or TBDnnn.
3. Encoding of value byte 3.1 diagram of byte layout: Please use 32 bit layout.
  - 3.2 Description of each field: Each field should have

title:

definition:

limits on the field: what values the field can take. If the field is variable give some indication of what the range or how it is calculated.

3.3 Error handling: 1. Do: Specify what constitutes malformed Sub-TLV, and how

a malformed Sub-TLV is processed. RFC9012 specifies silently ignoring the Sub-TLV.

2. Do: Point to a description of content checking. If content checking is done in another process, still give a general hint on what that processing is.

Do not: Hide the Sub-TLV error processing in an error handling section.

Do: Provide an error handling section with an overall summary of error handling. Refer to this section, but provide the specific details for this Sub-TLV in this section.

4. Tunnel TLV this Sub-TLV can appear in Do: Give a list on what existing Tunnel types this Sub-TLV can go in as a required or an optional Sub-TLV.

Do: Give existing tunnel types tunnel types in RFCs and WG document.

Optionally: Authors may list tunnel types in individual drafts.

Do: Give the tunnel types by name and number.

5. Does this Sub-TLV play a part in validation Please indicate whether this Sub-TLV is involved in the validation of the tunnel.

Do: Indicate if multiple Sub-TLVs can be in the same tunnel TLV.

Do: Indicate whether on the first Sub-TLV is processed or if all Sub-TLV is processed.

Do: Consider cross-checking of Sub-TLVs within a Tunnel TLV and between two tunnel TLVs of the same type. Is there any restriction or cross checking?

5, Specific Security Considerations for this Sub-TLV: If this Sub-

TLV exposes critical information, how is it protected?

6. Specific Management issues regarding this Sub-TLV: If this Sub-TLV exposes a name or an identifier (e.g. binding SID) that helps the management systems track something for provisioning or debugging, give hints on how this might be gathered or passed to management system. One example, is that the BGP-LS might gather this information in an SR routing system.

#### 4. PMSI Interactions Specification Guidelines

The Tunnel Encapsulation [RFC9012] states that the consideration of "P-Multicast Service Interface Tunnel" (PMSI Tunnel) attribute are out of scope.

Please fill out the PMSI and TEA template below. Review of these interactions took a long time in [RFC9012], so think carefully about these questions.

Here's a few questions that must be answered in the Template:

- 1) When is the PMSI tunnel Attribute valid to attach by itself?
- 2) When is it valid to attach both the PMSI tunnel attribute and a BGP TEA?
  - 2a) In the case that it is valid to attach both PMSI + TEA, what happens if either is malformed?
  - 2b) In the case that it is required to attach both, what happens if either the PMSI or TEA is missing? Note: Malformed implies syntax checking.
  - 2c) When it is invalid to attach both PMSI and TEA, what is the error procedure if both are attached?

Is there content checking of the TEA that is impacted by PMSI?

- By content checking, this template document means that given valid TEA and PMSI attributes, some content checking must be done prior to installing the tunnel and/or a multicast tunnel.

#### 5. IANA Considerations

This section specifies no IANA considerations

## 6. Security Considerations

This document provides administrative guidelines for clearly specifying Tunnel Encapsulation [RFC9012] information in an Internet Draft or RFC.

Since this is an administrative document, no security consideration are appropriate.

## 7. References

### 7.1. Normative References

- [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>>.
- [RFC6514] Aggarwal, R., Rosen, E., Morin, T., and Y. Rekhter, "BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs", RFC 6514, DOI 10.17487/RFC6514, February 2012, <<https://www.rfc-editor.org/info/rfc6514>>.
- [RFC9012] Patel, K., Van de Velde, G., Sangli, S., and J. Scudder, "The BGP Tunnel Encapsulation Attribute", RFC 9012, DOI 10.17487/RFC9012, April 2021, <<https://www.rfc-editor.org/info/rfc9012>>.
- [RFC9552] Talaulikar, K., Ed., "Distribution of Link-State and Traffic Engineering Information Using BGP", RFC 9552, DOI 10.17487/RFC9552, December 2023, <<https://www.rfc-editor.org/info/rfc9552>>.

### 7.2. Informative References

- [RFC7385] Andersson, L. and G. Swallow, "IANA Registry for P-Multicast Service Interface (PMSI) Tunnel Type Code Points", RFC 7385, DOI 10.17487/RFC7385, October 2014, <<https://www.rfc-editor.org/info/rfc7385>>.

## Author's Address

Susan Hares  
Hickory Hill Consulting  
7453 Hickory Hill  
Saline, MI 48176  
United States of America  
Phone: +1-734-604-0332

Email: [shares@ndzh.com](mailto:shares@ndzh.com)