IDR Working Group
Internet-Draft
Intended status: Standards Track
Expires: 7 July 2026

X. He
A. Wang
China Telecom
W. Cheng
China Mobile
J. Dong
Huawei
X. Min
ZTE Corp.

3 January 2026

BGP Extensions to Enable BGP FlowSpec based IFIT
draft-he-idr-bgp-flowspec-ifit-02

Abstract

Border Gateway Protocol (BGP) Flow Specification (FlowSpec) is an extension to BGP that supports the dissemination of traffic flow specifications and resulting actions to be taken on packets in a specified flow. In-situ Flow Information Telemetry (IFIT) denotes a family of flow-oriented on-path telemetry techniques, which can provide high-precision flow insight and real-time network issue notification. This document defines BGP extensions to distribute BGP FlowSpec based traffic filtering carrying IFIT information. So IFIT behavior can be applied to the specified flow automatically.

Table of Contents

1. Introduction

Border Gateway Protocol (BGP) Flow Specification defined in [RFC8955] and [RFC8956] (FlowSpec) is an extension to BGP that supports the dissemination of traffic flow specifications and resulting actions to be taken on packets in a specified flow. It leverages the BGP Control Plane to simplify the distribution of ACLs (Access Control Lists). Using the Flow Specification extension, new filter rules can be injected to all BGP peers simultaneously without changing router configuration.

BGP Flow Specification [RFC8955] and [RFC8956] define some BGP Network Layer Reachability Information (NLRI) formats used to distribute traffic flow specification rules. The NLRI for (AFI=1, SAFI=133) specifies IPv4 unicast filtering and the NLRI for (AFI=1, SAFI=134) specifies IPv4 BGP/MPLS VPN filtering [RFC7432]. The NLRI for (AFI=2, SAFI=133) specifies IPv6 unicast filtering and the NLRI for (AFI=2, SAFI=134) specifies IPv6 BGP/MPLS VPN filtering. The Flow Specification match part defined in [RFC8955]and[RFC8956]include L3/L4 information like IPv4/6 source/destination prefix, protocol, ports.

In-situ Flow Information Telemetry (IFIT) denotes a family of flow-oriented on-path telemetry techniques,which can provide high-precision flow insight and real-time network issue notification.In particular, IFIT refers to network OAM (Operations, Administration, and Maintenance) data plane on-path telemetry techniques, including In-situ OAM (IOAM) [RFC9197] and Alternate Marking [RFC9341]. It can provide flow information on the entire forwarding path on a per-packet basis in real time.

With the evolution of IP carried networks towards the intent-based and autonomous networks,flexible deployment of IFIT based on network dynamics and service requirements is getting a must. [I-D.draft-ietf-idr-sr-policy-ifit] defines BGP extensions to distribute SR policies carrying IFIT information so that IFIT behavior can be enabled automatically when the SR policy is applied. IFIT Attributes Sub-TLV is encoded in the Tunnel Encapsulation Attribute (23) defined in [RFC9012] using a new Tunnel-Type called SR Policy Type with codepoint 15. Once the IFIT attributes are signalled, if a packet arrives at the headend and, based on the types of steering described in [RFC9256], it may get steered into an SR Policy where IFIT methods are applied. However, in this way, IFIT is only applicable to SR policy environment. On the other hand, it cannot leverage the BGP FlowSpec to automatically configure traffic flow filtering to steer a packet flow into a valid SR Policy.

This document defines the BGP extensions to distribute BGP FlowSpec based traffic filtering together with IFIT information. So the IFIT behavior can be applied to the specified flow automatically. In this way, IFIT is automatically enabled and running.

2. Conventions

2.1. 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.

2.2. Terminology

Abbreviations used in this document:

ACL: Access Control List

AFI: Address Family Identifier

AS: Autonomous System

DEX: Direct Exporting

IFIT: In-situ Flow Information Telemetry

IOAM: In situ Operation, Administration, and Maintenance

NLRI: Network Layer Reachability Information

OAM: Operation, Administration, and Maintenance

SAFI: Subsequent Address Family Identifier

3. IFIT Attribute

IFIT attribute is an optional non-transitive BGP path attribute. IANA is requested to allocate the reserved value as the type code of the attribute in the "BGP Path Attributes" registry [IANA-BGP-PARAMS]. The attribute is composed of a set of Type-Length-Value (TLV) encodings. Each TLV contains information corresponding to a particular IFIT type. An IFIT TLV is structured as shown in Figure 1.

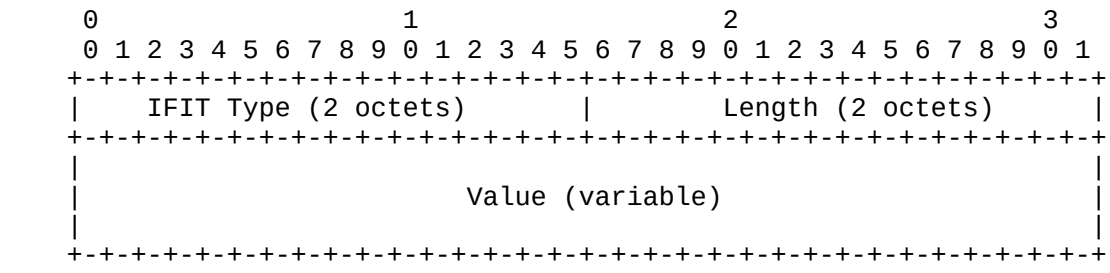

Figure 1: IFIT TLV

IFIT Type (2 octets): Identifies a type of IFIT. This document defines two types of IFIT as follows.

* When the IFIT Type is 1, it is the IOAM Type [RFC9197], [RFC9326].

* When the IFIT Type is 2, it is the AltMark Type [RFC9343].

Length (2 octets): The total number of octets of the Value field.

Value (variable): Comprised of one or multiple sub-TLVs.

Each sub-TLV consists of three fields: A 1-octet type, a 1-octet length, and zero or more octets of value. A sub-TLV is structured as shown in Figure 2.

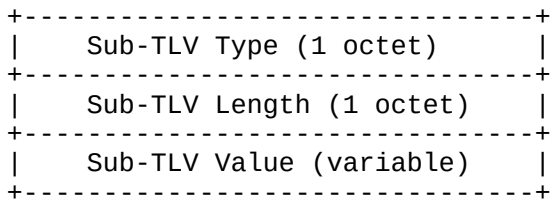

Figure 2: IFIT Sub-TLV

Sub-TLV Type (1 octet): Each sub-TLV type defines a certain OAM option about the IFIT TLV that contains this sub-TLV.

Sub-TLV Length (1 octet): The total number of octets of the Sub-TLV Value field.

Sub-TLV Value (variable): Encoding of the Value field depends on the sub-TLV type. The following subsections define the encoding in detail.

4. IFIT Attribute Sub-TLVs

This section specifies a number of sub-TLVs. These sub-TLVs can be included in two TLVs of the IFIT attribute.

For IFIT Type 1, namely the IOAM Type, four sub-TLVs are defined in this document as follows:

* IOAM Pre-allocated Trace Option [RFC9197] Sub-TLV, Type=1.

* IOAM Incremental Trace Option [RFC9197] Sub-TLV, Type=2.

* IOAM Directly Export (DEX) Option [RFC9326] Sub-TLV, Type=3.

* IOAM Edge-to-Edge Option [RFC9197] Sub-TLV, Type=4.

For IFIT Type 2, namely the AltMark Type, two sub-TLVs are defined in this document as follows:

* Alternate Marking [RFC9343] Sub-TLV, Type=1.

* Enhanced Alternate Marking sub-TLV, Type=2.

4.1. IOAM Sub-TLVs

IOAM Sub-TLVs include four sub-TLVs, and every sub-TLV structure is defined in the following subsections.

4.1.1. IOAM Pre-allocated Trace Option Sub-TLV

The IOAM tracing data is expected to be collected at every node that a packet traverses to ensure visibility into the entire path a packet takes within an IOAM domain. The preallocated tracing option will create pre-allocated space for each node to populate its information. The structure of IOAM pre-allocated trace option sub-TLV is defined as follows:

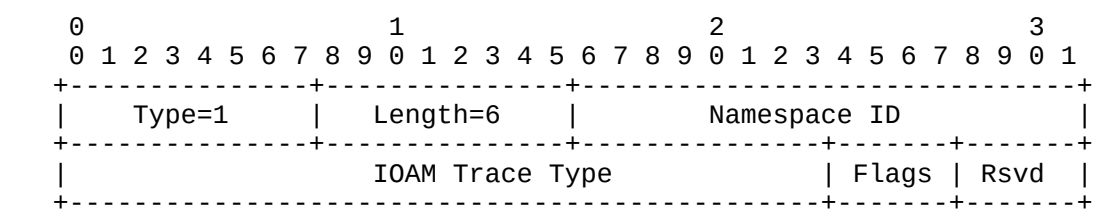

Figure 3: IOAM Pre-allocated Trace Option Sub-TLV

Type: 1 (to be assigned by IANA).

Length: 6, the total number of octets of the Sub-TLV Value field.

Namespace ID: A 16-bit identifier of an IOAM-Namespace. The definition is described in section 4.4 of [RFC9197].

IOAM Trace Type: A 24-bit identifier which specifies which data types are used in the node data list. The definition is described in section 4.4 of [RFC9197].

Flags: A 4-bit field. The definition is described in [RFC9322] and section 4.4 of [RFC9197].

Rsvd: A 4-bit field reserved for further usage. It MUST be zero and ignored on receipt.

4.1.2. IOAM Incremental Trace Option Sub-TLV

The incremental tracing option contains a variable node data fields where each node allocates and pushes its node data immediately following the option header. The structure of IOAM incremental trace option sub-TLV is defined as follows:

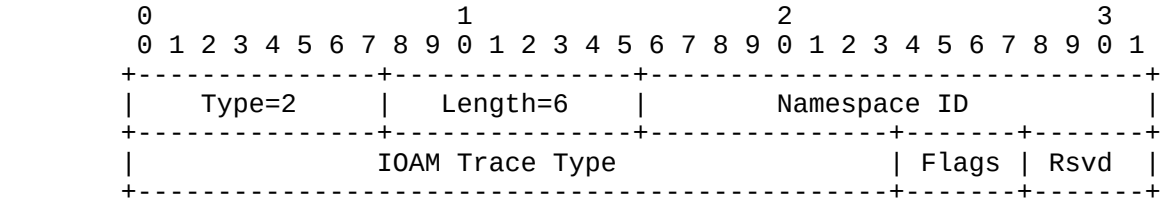

Figure 4: IOAM Incremental Trace Option Sub-TLV

Type: 2 (to be assigned by IANA).

Length: 6, the total number of octets of the Sub-TLV Value field.

All the other fields definitions are the same as the pre-allocated trace option sub-TLV in section 4.1.1.

4.1.3. IOAM Directly Export (DEX) Option Sub-TLV

IOAM DEX option is used as a trigger for IOAM data to be directly exported to a collector without being pushed into in-flight data packets. The structure of IOAM DEX sub-TLV is defined as follows:

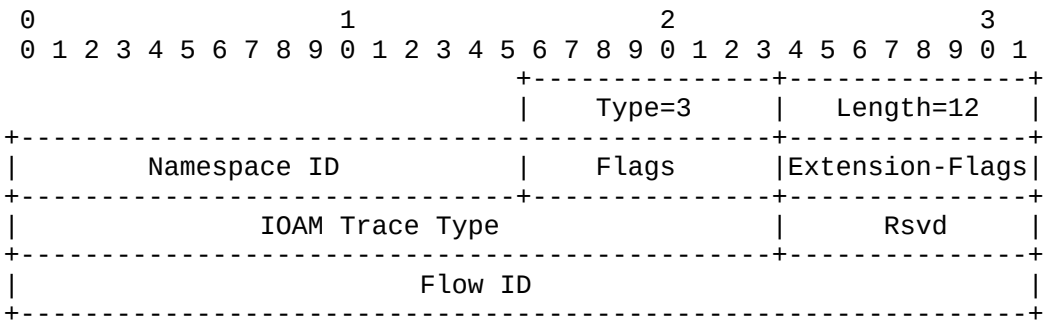

Figure 5: IOAM DEX Option Sub-TLV

Type: 3 (to be assigned by IANA).

Length: 12, the total number of octets of the Sub-TLV Value field.

Namespace ID: A 16-bit identifier of an IOAM-Namespace. The definition is described in section 4.4 of [RFC9197].

Flags: A 8-bit field. The definition is described in section 3.2 of [RFC9326].

Extension-Flags: A 8-bit field. The definition is described in section 3.2 of [RFC9326]. Every bit in the Extension-Flag field that is set to 1 indicates the existence of a corresponding optional 4-octet field. Bit 0 (the most significant bit) is defined as Flow ID and bit 1 as Sequence Number. Flow ID may be uniquely assigned by the collector. In this document, when bit 1 is set to 1, Sequence Number MUST be sequently assigned by the headend device (encapsulating node).

IOAM Trace Type: A 24-bit identifier which specifies which data types are used in the node data list. The definition is described in section 4.4 of [RFC9197].

Rsvd: A 4-bit field reserved for further usage. It MUST be zero and ignored on receipt.

Flow ID: A 32-bit flow identifier. The definition is described in section 3.2 of [RFC9326]. Flow ID may be uniquely assigned by the collector.

4.1.4. IOAM Edge-to-Edge Option Sub-TLV

The IOAM edge-to-edge option is to carry data that is added by the IOAM encapsulating node and interpreted by IOAM decapsulating node. The structure of IOAM edge-to-edge option sub-TLV is defined as follows:

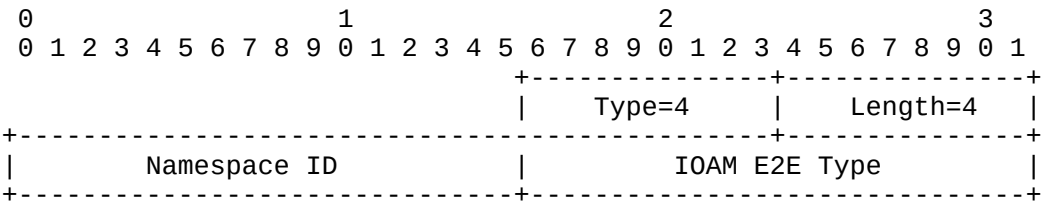

Figure 6: IOAM Edge-to-Edge Option Sub-TLV

Type: 4 (to be assigned by IANA).

Length: 4, the total number of octets of the Sub-TLV Value field.

Namespace ID: A 16-bit identifier of an IOAM-Namespace. The definition is described in section 4.4 of [RFC9197].

IOAM E2E Type: A 16-bit identifier which specifies which data types are used in the E2E option data. The definition is described in section 4.6 of [RFC9197].

4.2. AltMark Sub-TLVs

AltMark Sub-TLVs include two sub-TLVs, and every sub-TLV structure is defined in the following subsections.

4.2.1. Alternate Marking Sub-TLV

The structure of Alternate Marking sub-TLV is defined as follows:

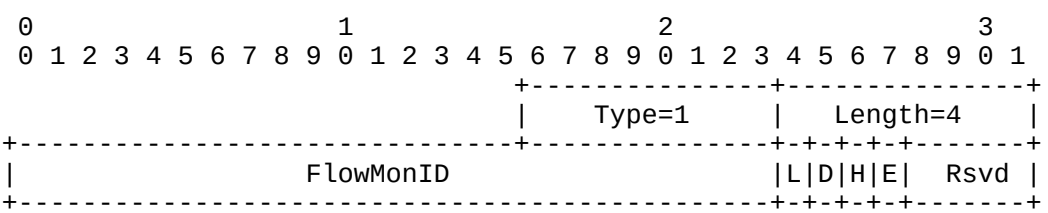

Figure 7: Alternate Marking Sub-TLV

Type: 1 (to be assigned by IANA).

Length: 4, the total number of octets of the Sub-TLV Value field.

FlowMonID: A 20-bit identifier to uniquely identify a monitored flow within the measurement domain. The definition is described in section 5.3 of [RFC9343].

L: 1-bit Loss flag set to 1 indicating Packet Loss Measurement as described in Section 5.1 of [RFC9343].

D: 1-bit Delay flag set to 1 indicating Packet Delay Measurement as described in Section 5.2 of [RFC9343].

H: 1-bit flag set to 1 indicating that the measurement is Hop-by-Hop.

E: 1-bit flag set to 1 indicating that the measurement is End-to-End.

Rsvd: 4-bit field reserved for further usage. It MUST be zero and ignored on receipt.

4.2.2. Enhanced Alternate Marking Sub-TLV

The structure of Enhanced Alternate Marking sub-TLV is defined as follows:

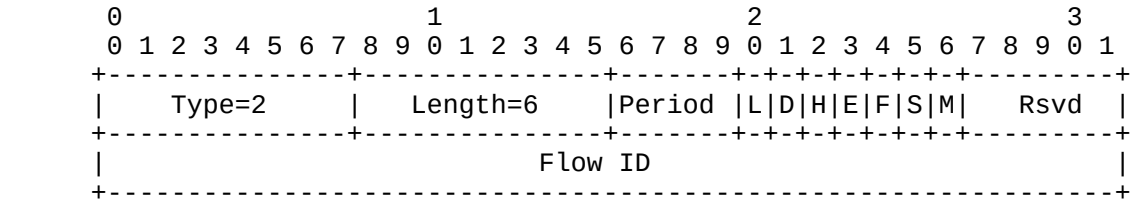

Figure 8: Enhanced Alternate Marking Sub-TLV

Type: 2 (to be assigned by IANA).

Length: 6, the total number of octets of the Sub-TLV Value field.

Period: 4-bit field used for encoding at most 16 measuement periods. The definition of its value and the corresponding measuement period is out of this document.

L: 1-bit Loss flag set to 1 indicating Packet Loss Measurement as described in Section 5.1 of [RFC9343].

D: 1-bit Delay flag set to 1 indicating Delay Measurement as described in Section 5.2 of [RFC9343].

H: 1-bit flag set to 1 indicating that the measurement is Hop-by-Hop.

E: 1-bit flag set to 1 indicating that the measurement is End-to-End.

F: 1-bit flag set to 1 indicating 32-bit Flow ID, which uniquely identify a monitored flow within the measurement domain. The definition and usage is described in section 7 of [I-D.draft-he-ippm-ioam-dex-extensions-incorporating-am-03]. In the centralized way, Flow ID is uniquely assigned by the controller; in the distributed way, Flow ID is locally assigned by the headend device (encapsulating node).

S: 1-bit flag set to 1 indicating an optional 32-bit Sequence Number, starting from 0 and incremented by 1 for each packet from the same flow at the encapsulating node. The field is set at the encapsulating node and exported to the receiving entity by the forwarding nodes. The Sequence Number, when combined with the Flow ID, provides a convenient approach to correlate the exported data from the same user packet.In this document, when bit S is set to 1, Sequence Number MUST be sequently assigned by the headend device (encapsulating node).

M: 1-bit flag set to 1 indicating an optional 32-bit Measurement Period Number(MPN), starting from 0 and incremented by 1 for the specified flow with the same Flow ID. The field is set at the encapsulating node and exported to the receiving entity by the forwarding nodes. The MPN, when combined with the Flow ID, provides a convenient approach to correlate the exported data of the same flow during the same measurement period from multiple nodes. In this document, when bit M is set to 1, MPN MUST be sequently assigned by the headend device (encapsulating node).

Rsvd: 5-bit field reserved for further usage. It MUST be zero and ignored on receipt.

5. Traffic Sampling Action

IFIT may be applied on all the traffic flow or a subset of the traffic. For the IOAM Type, take IOAM trace monitoring as example, when an IOAM encapsulating node incorporates the IOAM Pre-allocated Trace Option type (passport mode) or the DEX Option type (postcard mode) into all packets of the user traffic it forwards, more bandwidth and processing resources are required. So it is appropriate for an IOAM encapsulating node to apply the IOAM functionality to the selected subset of the traffic. But for the AltMark Type, it is more perferable for an encapsulating node to color all the traffic of interest it forwards, not a subset of the traffic, thus the fidelity of performance measurement for user

traffic flow (e.g., packet loss, delay and jitter) can be ensured.

This document defines a new Traffic Sampling Action that it standardizes as BGP Extended Communities [RFC4360].

5.1. Traffic Sampling Extended Community

The structure of the traffic sampling Extended Community is defined as follows:

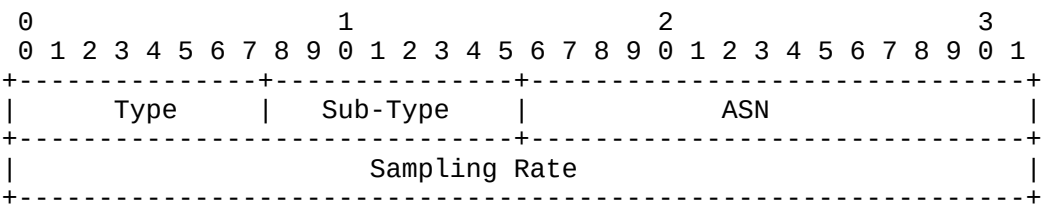

Figure 9: Traffic Sampling Extended Community

Type: 1-octet, BGP Transitive Extended Community Type, set to 0x80.

Sub-Type: 1-octet, TBA (to be assigned by IANA).

ASN: 2-octet AS number, which can be assigned from a 2-octet AS number. When a 4-octet AS number is locally present, the 2 least significant octets of such an AS number can be used. This value is purely informational and SHOULD NOT be interpreted by the implementation.

Sampling Rate: 4-octet float, which carries the sampling rate information in IEEE floating point [IEEE.754.1985] format. A sampling rate of 0 should result on no packet for the particular flow to be applied to IFIT, and a sampling rate of 100% should result on all traffic for the particular flow to be be applied to IFIT. On encoding, the sampling rate MUST NOT be negative.

6. BGP FlowSpec Operations with IFIT Attributes

A Flow Specification is an n-tuple consisting of several matching criteria that can be applied to IP traffic flow. A given IP packet is said to match the defined Flow Specification if it matches all the specified criteria. This n-tuple is encoded into a BGP NLRI. Flow Specifications can be seen as more specific routing entries to a unicast prefix, and the routing system can take advantage of the ACL (Access Control List) capabilities in the router’s forwarding path.

Generally, in operator network, the centralized controller determines the particular user traffic to be monitored according to service requirements; at the same time, the centralized controller also need to determine th IFIT type applied to the specified traffic flow. Based on BGP FlowSpec, the centralized controller sends the BGP FlowSpec update message to the headend device (i.e,. IOAM encapsulating node), carrying NLRI and IFIT attributes along with the traffic sampling Extended Community(if present). The BGP FlowSpec update message is used to instruct the headend device to perform IFIT automatic configuration on the monitored traffic flows. The headend device automatically generates ACLs according to the received traffic filter rules, and encapsulates IFIT for the incoming specified traffic flow packets, achieving the automated configuration for the monitored traffic flows.

Once the centralized controller determines to terminate monitoring the specified traffic flow, it can withdraw the corresponding NRLI routes, indicating that the headend device will remove the ACLs related to the traffic filter rules and stop encapsulating IFIT for the incoming specified traffic flow packets.

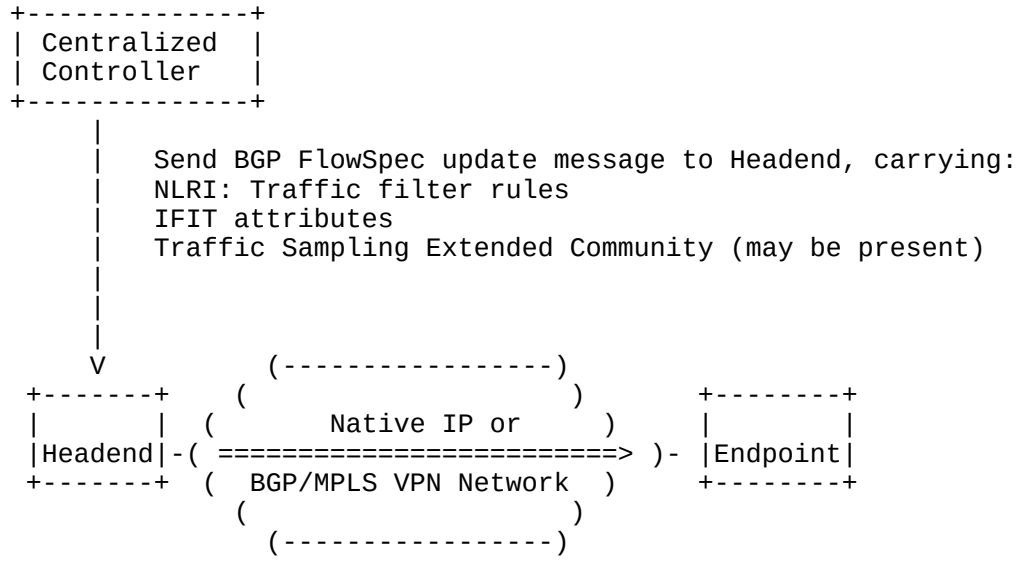

Figure 10: IFIT applied to the specified traffic flow

7. Validation Procedure and Error Handling

The validation procedure is the same as specified in Section 6 of [RFC8955] and Section 5 of [RFC8955].

Additionally, The IFIT Attribute MUST be attached to the BGP Update and MUST have an IFIT Type TLV set to the IOAM Type (1) or the AltMark Type (2).

When the IFIT Type TLV includes any sub-TLV that is unrecognized or unsupported, the update SHOULD NOT be considered usable. An implementation MAY provide an option for ignoring unsupported sub-TLVs.

A router that receives an BGP update that is not valid according to these criteria MUST treat the update as malformed.

The validation of the TLVs/sub-TLVs introduced in this document and defined in their respective sub-sections of Section 4 MUST be performed to determine if they are malformed or invalid. In case of any error detected, either at the attribute or its TLV/sub-TLV level, the "treat-as-withdraw" strategy MUST be applied. This is because a BGP Flowspec update without a valid IFIT Attribute (comprising of all valid TLVs/sub-TLVs) is not usable.

A BGP Flowspec update that is determined to be not valid, and therefore malformed, MUST be handled by the "treat-as-withdraw" strategy.

An implementation SHOULD log any errors found during the above validation for further analysis.

8. IANA Considerations

8.1. IFIT Attribute Type Code

IANA is requested to allocate the reserved value as the type code of the attribute in the "BGP Path Attributes" registry [IANA-BGP-PARAMS].

Type Code	Description	Reference
TBA	IFIT Attribute	This document

8.2. IFIT Type

IANA is requested to create a IFIT Type registry. IANA is requested to allocate the following values as the type code of the IFIT Attribute TLVs. Unassigned Type values will be assigned on a First Come First Served (FCFS) basis.

Value	Description	Reference
1	IOAM Type	This document
2	AltMark Type	This document

8.3. IFIT Attribute Sub-TLVs

8.3.1. IOAM Type Sub-TLVs

IANA is requested to create a IOAM Type registry. IANA is requested to allocate the following values as the type code of the IOAM Type Sub-TLVs. Unassigned Type values will be assigned on a First Come First Served (FCFS) basis.

Value	Description	Reference
1	IOAM Pre-allocated Trace Option Sub-TLV	This document
2	IOAM Incremental Trace Option Sub-TLV	This document
3	IOAM Directly Export (DEX) Option Sub-TLV	This document
4	IOAM Edge-to-Edge Option Sub-TLV	This document

8.3.2. AltMark Type Sub-TLVs

IANA is requested to create an AltMark Type registry. IANA is requested to allocate the following values as the type code of the AltMark Type Sub-TLVs. Unassigned Type values will be assigned on a First Come First Served (FCFS) basis.

Value	Description	Reference
1	Alternate Marking Sub-TLV	This document
2	Enhanced Alternate Marking sub-TLV	This document

8.4. Traffic Sampling Extended Community

IANA is requested to allocate the reserved value as the Sub-type code of Traffic Sampling Extended Community in the registry entitled "Generic Transitive Experimental Use Extended Community Sub-Types".

Type Value	Sub-Type Value	Description	Reference
0x80	TBA	Traffic Sampling	This document

9. Security Considerations

The security mechanisms of the base BGP security model apply to the extensions described in this document as well. See the Security Considerations section of [RFC4271] for a discussion of BGP security.

The BGP extensions specified in this document enable IFIT within an controlled domain, as defined in [RFC9378] and [I.D.draft-ietf-ippm-alt-mark-deployment]. IFIT operates within a controlled domain and its security considerations also apply to BGP sessions when carrying IFIT information. The IFIT configurations distributed by BGP are expected to be used entirely within this trusted IFIT domain which comprises a single AS or multiple ASes/ domains within a single provider network. Therefore, precaution is necessary to ensure that the IFIT information advertised via BGP sessions is limited to nodes in a secure manner within this trusted IFIT domain.

Flow Specification BGP speakers (e.g., the centralized controller) also need to be cautious for sending BGP updates. For example, sending updates at a high rate, or generating a high number of Flow Specifications may stress the receiving systems (the Headend devices), or exceed their capabilities.

Another major concern is that enabling IFIT on all the traffic flows may have some impact on network forwarding performance, thus the traffic sampling action is needed for protecting network resources. In particular, settting the appropriate traffic sampling rate for the IOAM trace monitoring is also necessary.

10. References

10.1. Normative References

[IEEE.754.1985]
IEEE, "IEEE Standard for Binary Floating-Point Arithmetic", IEEE ANSI/IEEE 754-1985, DOI 10.1109/IEEESTD.1985.82928, 5 April 2019, <https://ieeexplore.ieee.org/document/30711>.

[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>.

[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>.

[RFC4760] Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC 4760, DOI 10.17487/RFC4760, January 2007, <https://www.rfc-editor.org/info/rfc4760>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[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>.

[RFC8955] Loibl, C., Hares, S., Raszuk, R., McPherson, D., and M. Bacher, "Dissemination of Flow Specification Rules", RFC 8955, DOI 10.17487/RFC8955, December 2020, <https://www.rfc-editor.org/info/rfc8955>.

[RFC8956] Loibl, C., Ed., Raszuk, R., Ed., and S. Hares, Ed., "Dissemination of Flow Specification Rules for IPv6", RFC 8956, DOI 10.17487/RFC8956, December 2020, <https://www.rfc-editor.org/info/rfc8956>.

[RFC9197] Brockners, F., Ed., Bhandari, S., Ed., and T. Mizrahi, Ed., "Data Fields for In Situ Operations, Administration, and Maintenance (IOAM)", RFC 9197, DOI 10.17487/RFC9197, May 2022, <https://www.rfc-editor.org/info/rfc9197>.

[RFC9326] Song, H., Gafni, B., Brockners, F., Bhandari, S., and T. Mizrahi, "In Situ Operations, Administration, and Maintenance (IOAM) Direct Exporting", RFC 9326, DOI 10.17487/RFC9326, November 2022, <https://www.rfc-editor.org/info/rfc9326>.

[RFC9341] Fioccola, G., Ed., Cociglio, M., Mirsky, G., Mizrahi, T., and T. Zhou, "Alternate-Marking Method", RFC 9341, DOI 10.17487/RFC9341, December 2022, <https://www.rfc-editor.org/info/rfc9341>.

[RFC9343] Fioccola, G., Zhou, T., Cociglio, M., Qin, F., and R. Pang, "IPv6 Application of the Alternate-Marking Method", RFC 9343, DOI 10.17487/RFC9343, December 2022, <https://www.rfc-editor.org/info/rfc9343>.

10.2. Informative References

[I-D.he-ippm-ioam-dex-extensions-incorporating-am]
hexiaoming, X., Brockners, F., Song, H., Fioccola, G., and A. Wang, "IOAM Direct Exporting (DEX) Option Extensions for Incorporating the Alternate-Marking Method", Work in Progress, Internet-Draft, draft-he-ippm-ioam-dex-extensions-incorporating-am-03, 13 November 2025, <https://datatracker.ietf.org/doc/html/draft-he-ippm-ioam-dex-extensions-incorporating-am-03>.

[I-D.he-ippm-ioam-extensions-incorporating-am]
hexiaoming, X., Min, X., Brockners, F., Fioccola, G., and C. Xie, "IOAM Trace Option Extensions for Incorporating the Alternate-Marking Method", Work in Progress, Internet-Draft, draft-he-ippm-ioam-extensions-incorporating-am-05, 13 November 2025, <https://datatracker.ietf.org/doc/html/draft-he-ippm-ioam-extensions-incorporating-am-05>.

[I-D.ietf-idr-sr-policy-ifit]
Qin, F., Yuan, H., Yang, S., Zhou, T., and G. Fioccola, "BGP SR Policy Extensions to Enable IFIT", Work in Progress, Internet-Draft, draft-ietf-idr-sr-policy-ifit-11, 15 October 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-idr-sr-policy-ifit-11>.

[I-D.ietf-ippm-alt-mark-deployment]
Fioccola, G., Zhu, K., Graf, T., Nilo, M., and L. Zhang, "Alternate Marking Deployment Framework", Work in Progress, Internet-Draft, draft-ietf-ippm-alt-mark-deployment-04, 29 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-ippm-alt-mark-deployment-04>.

[RFC9378] Brockners, F., Ed., Bhandari, S., Ed., Bernier, D., and T. Mizrahi, Ed., "In Situ Operations, Administration, and Maintenance (IOAM) Deployment", RFC 9378, DOI 10.17487/RFC9378, April 2023, <https://www.rfc-editor.org/info/rfc9378>.

Authors' Addresses

Xiaoming He
China Telecom
Email: hexm4@chinatelecom.cn

Aijun Wang
China Telecom
Email: wangaj3@chinatelecom.cn

Weiqiang Cheng
China Mobile
Email: chengweiqiang@chinamobile.com

Jie Dong
Huawei
Email: jie.dong@huawei.com

Xiao Min
ZTE Corp.
Email: xiao.min2@zte.com.cn