GROW
Internet-Draft
Intended status: Standards Track
Expires: 27 October 2026

C. Lin
New H3C Technologies
P. Narasimha
Cisco
M. Srivastava
Juniper Networks
J. Li
China Mobile

25 April 2026

Peer Capability Update Notification in BGP Monitoring Protocol (BMP)
draft-lin-grow-bmp-cap-notification-01

Abstract

When BGP Dynamic Capability is supported, dynamic updates of capabilities are allowed over an established BGP session. At present, after the BGP session is established, the monitored router sends a BMP Peer Up Notification message first, containing the initial capabilities. If BGP Dynamic Capability is supported, using BMP Peer Up Notification messages to report subsequent capability changes for a BGP session becomes inappropriate. This document defines a new Peer Capability Update Notification message type in BMP to report peer capability changes.

Table of Contents

1. Introduction

[I-D.ietf-idr-dynamic-cap] introduces BGP Dynamic Capability, which enables dynamic updates of capabilities over an established BGP session. This feature allows BGP speakers to negotiate capabilities without disrupting the existing session.

When a BGP session is established, a BMP Peer UP Notification message containing the initial capabilities is first sent to monitor this session [RFC7854]. If BGP Dynamic Capability is implemented, subsequent capability changes can be reported to the monitoring station by resending a Peer UP Notification message that includes all current capabilities. The capabilities in the latter message must override those in the former.

Normally, a BMP Peer Up Notification message should only be sent once when a BGP session is established. If the BMP Peer Up Notification message is sent multiple times, the monitoring station may mistakenly interpret the event as a peer session re-established, potentially causing the clearing of previously received route monitoring messages for the affected peers in that session. In this case, all routing monitoring messages for those peers must be resent, significantly increasing the network load.

Therefore, when BGP Dynamic Capability is implemented, using BMP Peer Up Notification messages to report subsequent capability changes becomes unsuitable.

To avoid potential problems caused by the above solution, this document defines a new BMP message type, Peer Capability Update Notification, for reporting BGP dynamic capability changes.

2. Terminology

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. Peer Capability Update Notification Message

This section defines a new BMP message type for monitoring BGP dynamic capabilities. The assigned value for this message type is placed in the Message Type field of the common header.

Message Type = TBD: Peer Capability Update Notification

3.1. Message Format

This section defines the Peer Capability Update Notification BMP message format, as illustrated in Figure 1. The message consists of four components: a Common Header, a Per-Peer Header, a CAP Flags, and a BGP Dynamic Capability PDU.

The Common Header and Per-Peer Header follow the same format as defined in Sections 4.1 and 4.2 of [RFC7854] respectively. The BGP Dynamic Capability PDU uses the format specified in Section 3 of [I-D.ietf-idr-dynamic-cap]. The Peer CAP Flags field is defined as follows:

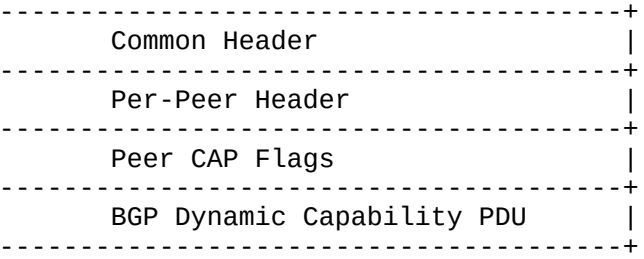
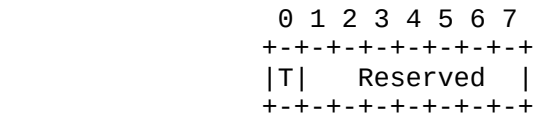


Figure 1: Peer Capability Update Notification Message Format

Peer CAP Flags (1 byte): This field provides status information about the Capability Update, including the direction of the BGP Dynamic Capability PDU. The direction flag fields are defined as follows:



The T flag (1 bit) signals the direction of the BGP Dynamic Capability PDU:

* 1: Received from a peer.

* 0: Sent to a peer.

The remaining bits are reserved for future use. They MUST be transmitted as 0 and their values MUST be ignored on receipt.

The BMP Peer Capability Update Notification MUST be sent before sending any Route Monitoring message corresponding to the updated capability for the Peer.

4. Example and Use Case

The Peer Capability Update Notification message of BMP provides real-time notifications of BGP dynamic capability changes.

Consider a BGP speaker with a peer that supports both BGP Dynamic Capability and VPNv4 Address Family Identifier/Subsequent Address Family Identifier (AFI/SAFI) [RFC4364], where the corresponding BGP session is already established. When this peer subsequently enables the EVPN address family [RFC7432], the BGP speaker will send a BGP Dynamic Capability message containing Multiprotocol Extensions Capability for BGP-4 (including EVPN AFI/SAFI information) [RFC4760]. If the peer is being monitored via BMP, the BGP speaker must generate a BMP Peer Capability Update Notification message (with the T flag set to 0) to report this capability change, before sending any Route Monitoring Messages for EVPN address family.

5. Operational Considerations

When a BGP speaker sends a BGP Dynamic Capability message to its peer, the generation of a corresponding BMP Peer Capability Update Notification message (with the T flag set to 0) should be generated immediately and not need to await successful receipt of the BGP Dynamic Capability acknowledgment (ACK), per the procedures in [I-D.ietf-idr-dynamic-cap].

When a BGP speaker receives a BGP Dynamic Capability message from its peer, a corresponding BMP Peer Capability Update Notification message (with the T flag set to 1) should be generated immediately.

If a new BGP capability is added, after both the corresponding BMP Peer Capability Update Notification message with the T flag set to 0 and that with the T flag set to 1 are sent to monitoring station, the route information and End-of-RIB (EOR) of corresponding peer will be sent via BMP.

If an existing BGP capability is removed, only the corresponding BMP Peer Capability Update Notification messages will be sent, but the route withdrawal information of corresponding peer will not be sent via BMP.

6. Security Considerations

The security considerations in Section 11 of [RFC7854] apply to this document. It is also believed that this document does not add any additional security considerations.

7. IANA Considerations

This document requests IANA to assign the following new parameter in the BMP Parameters registry (maintained at https://www.iana.org/assignments/bmp-parameters/bmp-parameters.xhtml).

New BMP Message Type:

Value: TBD (to be assigned by IANA)

Name: Peer Capability Update Notification

Reference: This document

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>.

[RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, DOI 10.17487/RFC4364, February 2006, <https://www.rfc-editor.org/info/rfc4364>.

[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>.

[RFC7432] Sajassi, A., Ed., Aggarwal, R., Bitar, N., Isaac, A., Uttaro, J., Drake, J., and W. Henderickx, "BGP MPLS-Based Ethernet VPN", RFC 7432, DOI 10.17487/RFC7432, February 2015, <https://www.rfc-editor.org/info/rfc7432>.

[RFC7854] Scudder, J., Ed., Fernando, R., and S. Stuart, "BGP Monitoring Protocol (BMP)", RFC 7854, DOI 10.17487/RFC7854, June 2016, <https://www.rfc-editor.org/info/rfc7854>.

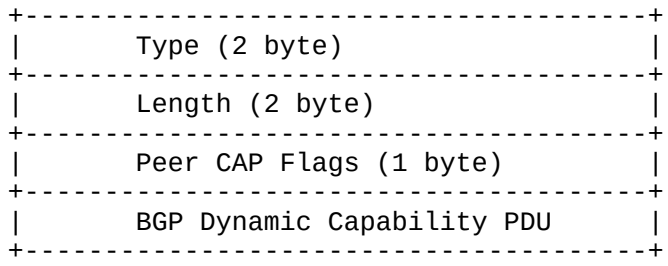
[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[I-D.ietf-idr-dynamic-cap] Chen, E. and S. R. Sangli, "Dynamic Capability for BGP-4", Work in Progress, Internet-Draft, draft-ietf-idr-dynamic-cap-19, 15 February 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-idr-dynamic-cap-19>.

Appendix A. Option 1

In addition to the aforementioned solutions (Using New BMP Type or Peer Up Notification) to report the BGP Capability changes, This document can also define a New TLV as part of Peer Up Notification or other available BMP Message types defined in existing documents.

The New TLV format is defined below:



Type = TBD: Peer Capability Update Notification;

Length: indicates the length of value in this TLV, including Peer CAP Flags and BGP Dynamic Capability PDU;

Peer CAP Flags and BGP Dynamic Capability PDU is same with the definition of Section 3.1 in this document.

Authors' Addresses

Changwang Lin
New H3C Technologies
8 Yongjia North Road
Beijing
Haidian District, 100094
China
Email: linchangwang.04414@h3c.com

Prasad S. Narasimha
Cisco
Cessna Business Park SEZ, Kadubeesanahalli
Bangalore
India
Email: snprasad@cisco.com

Mukul Srivastava
Juniper Networks
10 Technology Park Dr
Westford, MA 01886
United States of America
Email: msri@juniper.net

Jinming Li
China Mobile
32 Xuanwumen West Street
Beijing
Xicheng District, 100053
China
Email: lijinming@chinamobile.com