Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 20 September 2026

S. Zhuang
N. Geng
H. Wang
Huawei

19 March 2026

Monitoring BGP Parameters Using BMP
draft-zhuang-grow-monitoring-bgp-parameters-02

Abstract

The BGP Monitoring Protocol (BMP) [RFC7854] is designed to monitor BGP [RFC4271] running status, such as BGP peer relationship establishment and termination and route updates. Without BMP, manual query is required if you want to know about BGP running status.

This document provides the use cases that the BMP station can get the optional parameters that are supported by the monitored network device and default configure parameters of the monitored network device via BMP.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of This Memo

Table of Contents

1. Terminology

This memo makes use of the terms defined in [RFC7854].

BMP: BGP Monitoring Protocol

BMS: BGP Monitoring Station

Initiation message: Reports to the monitoring server such information as the router vendor and its software version.

2. Introduction

The Border Gateway Protocol (BGP) is a dynamic routing protocol operating on an Autonomous System (AS) and typically configured on a network device. The BGP typically can support a number of optional parameters[RFC5492], e.g., IPv4 Unicast, IPv4 Multicast, IPv6 Unicast, and other Multiple-Protocol Extended Capabilities, Route Refresh Capability, Outbound Route Filtering Capability, Graceful Restart Capability, Support for 4-octet AS number capability etc., and the different BGP implementations may support a different number of different capabilities. The network device configured with the

BGP typically may not enable all optional capabilities supported in the configured BGP, but enable some currently required BGP optional capabilities as required for a current task.

The BGP Monitoring Protocol (BMP) introduces the availability of monitoring BGP running status, such as BGP peer relationship establishment and termination and route updates. Without BMP, manual query is required if you want to know about BGP running status. With BMP, a router can be connected to a monitoring station and configured to report BGP running statistics to the station for monitoring, which improves the network monitoring efficiency. BMP facilitates the monitoring of BGP running status and reports security threats in real time so that preventive measures can be taken promptly.

In order to monitor and manage effectively the operating states of the BGP configured on the respective network devices in the network, the existing practice is that a monitoring station obtains BGP information of the respective network devices in the network to monitor and manage centrally the network devices configured with the BGP in the network. By way of an example of a flow in which the monitoring station obtains the BGP information, after a BGP connection is set up between network devices A and B configured with the BGP (or between peers), taking the network device A as an example, the network devices A and B negotiate about their own enabled BGP optional capabilities in OPEN messages under a BGP rule, and the network device A further includes a BGP Monitoring Protocol (BMP) module connected with the monitoring station, where the BMP module can obtain the enabled BGP optional capabilities of the network device A, and the enabled BGP capabilities of the network device B as a result of negotiation about the enabled BGP capabilities, so that if the BMP module of the network device A sends the configured BGP information of the network device to the monitoring station in a Peer Up Notification message, then the BGP optional capabilities will include only the BGP capabilities enabled on the network device A.

However, sometimes it’s not sufficient to report only the capabilities currently enabled at the monitored device to the BMS. In order to better optimize the network, the BMS may want to access all the capabilities that are supported at each monitored devices, as well as the current configuration informations.

3. Use cases

* BGP Optional Parameters Supported/Enabled: The Open Message reported to BMS contains only the currently enabled capabilities at the monitored device. If all the supported capabilities of the monitored devices, both the enabled and not yet enabled ones, are informed to the BMS, the BMS can use the more comprehensive and valid inputs to make decisions about the whole network optimization. For example, if the Graceful Restart Capability is not enabled for a BGP Peer, and thus the BGP Open Message (i.e., the Peer Up Notification in BMP) would not include the GR capability. However, if the BMS or the operator has the knowledge that both devices support the GR capability, and enables it at both devices, it could improve the operational stability of the network.

* BGP Default Behavior Parameters: As one of the concern from the operators, that in multi-vendor environment, some default configurations or behaviors of devices are vendor-specific, and may cause various issues during the interoperation test or any time after. Take the protocol preferences (distance) of different BGP routes for example: Vendor A assigns value 255 to eBGP, iBGP and BGP local routes by default, while vendor B assigns 20 to eBGP, 200 to iBGP and 200 to BGP local routes by default. In addition, value 255 is not recognized by vendor B, and routes assigned such distance would be ignored.

4. Extension of BMP Initiation Message

As described in Section 4.3 of [RFC7854], the initiation message provides a means for the monitored router to inform the monitoring station of its vendor, software version, and so on.

The initiation message consists of the common BMP header followed by two or more Information TLVs (Section 4.4 of [RFC7854]) containing information about the monitored router. Currently defined types are:

Type = 0: String.

Type = 1: sysDescr.

Type = 2: sysName.

Figure 1

This document defines 3 new categories of TLV types: the BGP Optional Parameters and the BGP Default Behavior Parameters.

Type = TBD1: Optional Parameters Supported. The Information field specifies all BGP optional parameters supported by the monitored device. Each parameter is encoded as a triplet: <Parameter Type, Parameter Length, Parameter Value>.

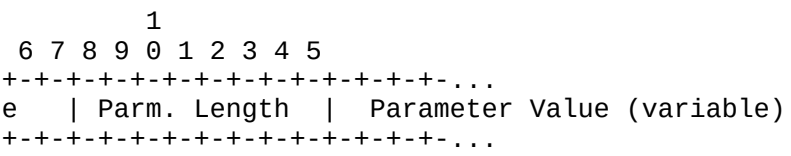

Figure 2: BGP Optional Parameters Information TLV

Parameter Type is a one octet field that unambiguously identifies individual parameters. Parameter Length is a one octet field that contains the length of the Parameter Value field in octets. Parameter Value is a variable length field that is interpreted according to the value of the Parameter Type field. RFC 5492 [RFC5492] defines the Capabilities Optional Parameter.

Type = TBD2: Optional Parameters Enabled. The Information field specifies all BGP optional parameters enabled by the monitored device. Each parameter is encoded as a triplet: <Parameter Type, Parameter Length, Parameter Value>.

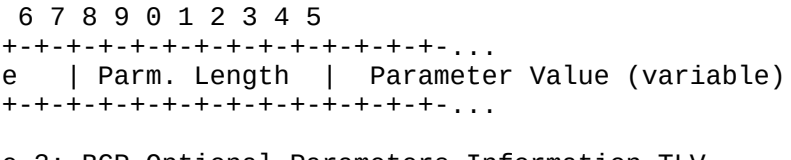

Figure 3: BGP Optional Parameters Information TLV

Parameter Type is a one octet field that unambiguously identifies individual parameters. Parameter Length is a one octet field that contains the length of the Parameter Value field in octets. Parameter Value is a variable length field that is interpreted according to the value of the Parameter Type field. RFC 5492 [RFC5492] defines the Capabilities Optional Parameter.

Type = TBD3: Default Behavior Parameters. The Information field contains a list of default behavior parameters, in which each parameter is encoded as a Default Behavior sub TLV <Default Behavior Type, Default Behavior Length, Default Behavior Value>, which is defined as follows:

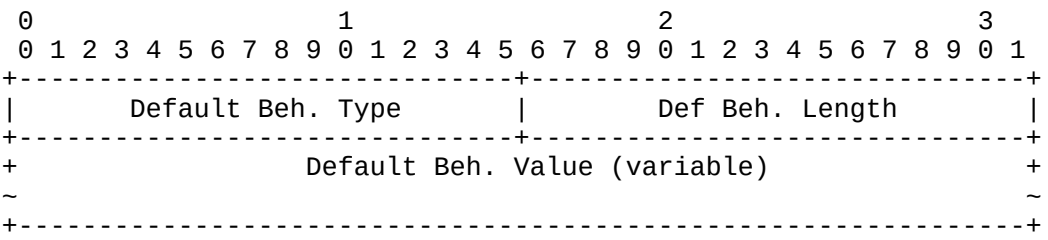

Figure 4: Default Behavior Parameters sub TLV

The Default Behavior Type is a one octet field that identifies the default behavior type parameter. Parameter Length is a one octet field that contains the length of the Parameter Value field in octets. Parameter Value is a variable length field that is interpreted according to the value of the Parameter Type field:

* Type = TBD4, (32-bit integer) Value of default Protocol Preference for Local route

* Type = TBD5, (32-bit integer) Value of default Protocol Preference for EBGP route

* Type = TBD6, (32-bit integer) Value of default Protocol Preference for IBGP route

* Type = TBD7, (32-bit integer) Value of default BGP connect-retry timer time

* Type = TBD8, (32-bit integer) Value of default BGP Keepalive time

* Type = TBD9, (32-bit integer) Value of default BGP hold time

* Type = TBD10, (32-bit integer) Value of EBGP route-update-interval

* Type = TBD11, (32-bit integer) Value of IBGP route-update-interval

* Type = TBD12, (32-bit integer) Value of Default local-preference

* Type = TBD13, (32-bit integer) Value of Default MED

5. Acknowledgements

TBD.

6. IANA Considerations

TBD.

7. Security Considerations

TBD.

8. 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>.

[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>.

[RFC5492] Scudder, J. and R. Chandra, "Capabilities Advertisement with BGP-4", RFC 5492, DOI 10.17487/RFC5492, February 2009, <https://www.rfc-editor.org/info/rfc5492>.

[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>.

Authors' Addresses

Shunwan Zhuang
Huawei
Huawei Bld., No.156 Beiqing Rd.
Beijing 100095
China
Email: zhuangshunwan@huawei.com

Nang Geng
Huawei
Huawei Bld., No.156 Beiqing Rd.
Beijing 100095
China

Email: gengnan@huawei.com

Haibo Wang
Huawei
Huawei Bld., No.156 Beiqing Rd.
Beijing 100095
China
Email: rainsword.wang@huawei.com