BMP YANG Module
draft-cptb-grow-bmp-yang-03

Abstract

This document proposes a YANG module for BMP (BGP Monitoring Protocol) configuration and monitoring. A complementary RPC triggers a refresh of the session of a BMP station.

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 10 January 2023.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.
1. 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.

Routing Information Bases, peers, monitoring stations are defined in [RFC7854].

2. Introduction

This document specifies a YANG module for configuring and monitoring the BGP Monitoring Protocol (BMP) [RFC7854]. The model provides parameters for defining BMP monitoring stations, the selection of the BGP Routing Information Bases (RIBs), provides operational metrics and enables to reset BMP monitoring sessions.
3. Model summary

The BMP YANG model provides the methods for managing BMP monitoring stations. It includes:

* Connectivity parameters, including station IP address and destination port.

* BMP session parameters, such as defining the BMP initiation message or the interval for statistics messages.

* BGP Data sources. The model requires the explicit configuration of the Network instance, RIBs and address family to send to each monitoring station. For Adj-RIB-in and Adj-RIB-out, both post and pre policy, the model also requires to reference the peer. In those RIBs, the value "all_peers" can be used if the operators desire to receive data of all peers.

* Per BMP station status and statistics, such as established status, number of route-monitoring messages, number of route-mirroring messages, number of peer-down and peer-up messages, number of initiation messages.

* BMP session reset RPC action.

4. Base ietf-bmp YANG module

4.1. Tree View

The following tree diagram provides an overview of the ietf-bmp.yang data model.

```
module: ietf-bmp
  +--rw bmp
  |  +--rw stations
  |     +--rw station* [id]
  |     |  +--rw id               string
  |     |  +--rw connection
  |     |     +--rw (passive_or_active)?
  |     |     |  +--rw active
  |     |     |     +--rw network-instance    leafref
  |     |     |     +--rw station-address     inet:ip-address
  |     |     |     +--rw station-port     inet:port-number
  |     |     |     +--rw local-address     inet:ip-address
  |     |     |     +--rw local-port?     inet:port-number
  |     |     |  +--:(active)
  |     |     |     +--rw passive
  |     |     +--:(passive)
  |     +--rw passive
```

---rw network-instance leafref
---rw station-address inet:ip-address
---rw station-port? inet:port-number
---rw local-address? inet:ip-address
---rw local-port? inet:port-number
---rw max-segment-size? uint16
---rw mtu-discovery? boolean
---rw keepalives! {keepalives-supported}?
  ---rw idle-time uint16
  ---rw max-probes uint16
  ---rw probe-interval uint16
---rw secure-session-enable? boolean
---rw secure-session
  ---rw (authentication)?
    ---:(ao)
      ---rw enable-ao? boolean
      ---rw send-id? uint8
      ---rw recv-id? uint8
      ---rw include-tcp-options? boolean
      ---rw accept-key-mismatch? boolean
      ---ro r-next-key-id? uint8
    ---:(md5)
      ---rw enable-md5? boolean
---rw bmp_session
  ---rw initiation-message? string
  ---rw statistics-interval? uint32
---rw bmp_sources
  ---rw network-instances
    ---rw network-instance* [network-instance-id]
      ---rw network-instance-id union
      ---rw adj-rib-in-pre
        ---rw enabled? boolean
        ---rw address-families
          ---rw address-family* [name]
            ---rw name leafref
            ---rw peers* union
      ---rw adj-rib-in-post
        ---rw enabled? boolean
        ---rw address-families
          ---rw address-family* [name]
            ---rw name leafref
            ---rw peers* union
      ---rw local-rib
        ---rw enabled? boolean
        ---rw address-families* identityref
      ---rw adj-rib-out-pre
        ---rw enabled? boolean
        ---rw address-families
4.2. YANG Module

<CODE BEGINS> file "ietf-bmp@2022-01-27.yang"

module ietf-bmp {
  yang-version 1.1;
  namespace "urn:ietf:params:xml:ns:yang:ietf-bmp";
  prefix bmp;

  import ietf-yang-types {
    prefix yang;
  }

  import ietf-inet-types {
    prefix inet;
    reference
      "RFC 6991: Common YANG Data Types";
  }
  import ietf-routing {
    prefix rt;
  }

import ietf-bgp-types {
    prefix bt;
    reference
    "RFC XXXX: BGP YANG module for Service Provider Network.
    RFC-EDITOR: please update XXX with the RFC ID assigned
to I-D.ietf-idr-bgp-model";
}

import ietf-bgp {
    prefix bgp;
    reference
    "RFC XXXX: BGP YANG module for Service Provider Network.
    RFC-EDITOR: please update XXX with the RFC ID assigned
to I-D.ietf-idr-bgp-model";
}

import ietf-netconf-acm {
    prefix nacm;
    reference
    "RFC 8341: Network Configuration Access Control Model";
}

import ietf-tcp-common {
    prefix "tcpcmn";
    reference
    "I-D.ietf-netconf-tcp-client-server: YANG Groupings for TCP
    Clients and TCP Servers."
}

import ietf-tcp {
    prefix "tcp";
    reference
    "I-D.ietf-tcpm-yang-tcp: A YANG Model for
    Transmission Control Protocol (TCP) Configuration";
}

import ietf-network-instance {
    prefix "ni";
    reference
    "RFC 8529: YANG Data Model for Network Instances";
}

organization

"IETF GROW Working Group";
contact
"WG Web: <https://datatracker.ietf.org/wg/grow/>
WG List: <mailto:grow@ietf.org>

Author: Camilo Cardona
<mailto:camilo@ntt.net>

Author: Paolo Lucente
<mailto:cpaolo@ntt.net>

Author: Thomas Graf
<mailto:thomas.graf@swisscom.com>

Author: Benoit Claise
<mailto:benoit.claise@huawei.com>"

description
"This module specifies a structure for BMP
(BGP Monitoring Protocol) configuration and monitoring.

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 (RFC 2119)
(RFC 8174) when, and only when, they appear in all
capitals, as shown here.

Copyright (c) 2022 IETF Trust and the persons identified as
authors of the code. All rights reserved.

Redistribution and use in source and binary forms, with or
without modification, is permitted pursuant to, and subject to
the license terms contained in, the Revised BSD License set
forth in Section 4.c of the IETF Trust’s Legal Provisions
Relating to IETF Documents

This version of this YANG module is part of RFC 9196
(https://www.rfc-editor.org/info/rfc9196); see the RFC itself
for full legal notices."

revision 2022-01-27 {

description
"initial version";

reference
"RFC YYYY: BMP YANG Module
RFC-EDITOR: please update YYYY with this RFC ID";
}
identity bmp-peer-types-idty {
    description "Enum values for peer selection specific for BMP";
}

identity bmp-peer-types-all-peers-idty {
    base bmp-peer-types-idty;
    description "This identify is an explicit way of defining that the device should send the updates from all peers to the station for a particular RIB/AFI."
}

identity bmp-ni-types-idty {
    description "Enum values for network instances specific for BMP";
}

identity bmp-ni-types-all-ni-idty {
    base bmp-ni-types-idty;
    description "The identify is an explicit way of defining that the device should send the updates from all network instances.";
}

grouping bmp-tcp-options {
    description "TCP options for the connection to the station";
    leaf maximum-segment-size {
        type uint16;
        description "Maximum segment size for the TCP connections.";
    }
    // Taken from the bgp yang module
    leaf mtu-discovery {
        type boolean;
        default "true";
        description "Turns path mtu discovery for the TCP sessions on (true) or off (false).";
        reference "RFC 1191: Path MTU discovery.";
    }
    uses tcpcmn:tcp-common-grouping;
    // taken from the bgp yang module but using groupings
    leaf secure-session-enable {
        type boolean;
        default "false";
    }
container secure-session {
  when "../secure-session-enable = 'true'";
  description "Container for describing how a particular BGP session is to be secured.";
  choice authentication {
    case ao {
      uses tcp:ao;
      description "Use TCP-AO to secure the connection.";
    }
    case md5 {
      uses tcp:md5;
      description "Use TCP-MD5 to secure the connection.";
    }
  }
  description "Choice of TCP authentication.";
}

grouping bmp-ip-connection {
  description "common elements for defining connectivity to a bmp station";
  choice passive_or_active {
    description "Choice for active or passive connection";
    case active {
      description "The device starts the connection to the station";
      container active {
        description "The device starts the connection to the station";
        leaf network-instance {
          type leafref {
            path "/ni:network-instances/ni:network-instance/" + "ni:name";
          }
        }
      }
    }
  }
}
leaf network-instance {
  type leafref {
    path "/ni:network-instances/ni:network-instance/
      + "ni:name";
  }
  mandatory true;
  description
    "Network-instance to used to reach the station.";
}

leaf station-address {
  type inet:ip-address;
  mandatory true;
  description
    "Destination IP address of station";
}

leaf station-port {
  type inet:port-number;
  mandatory true;
  description
    "Destination port of the station";
}

leaf local-address {
  type inet:ip-address;
  mandatory true;
  description
    "Local IP address to source active connection";
}

leaf local-port {
  type inet:port-number;
  description
    "Optional Local port for active connection";
}

case passive {
  description
    "The device waits for the connection to
     start the connection to a local endpoint";
  container passive {
    description
      "The device waits for the connection
       to start the connection to a local endpoint";
    leaf network-instance {
      type leafref {
        path "/ni:network-instances/ni:network-instance/
          + "ni:name";
      }
      mandatory true;
      description

leaf station-address {
  type inet:ip-address;
  mandatory true;
  description "address of station";
}
leaf station-port {
  type inet:port-number;
  description "Optional port identifying the connection, if provided it must match";
}
leaf local-address {
  type inet:ip-address;
  description "Local IP address to wait for the connection";
}
leaf local-port {
  type inet:port-number;
  description "Local port to wait for the connection";
}

grouping bmp-peer-ribs-filter {
  description "Leaves for configuring RIBs where origin/destination peers are well defined."
  leaf enabled {
    type boolean;
    description "Enables the specified RIB";
  }
  container address-families {
    description "container for lists of address-families"
    list address-family {
      key "name";
      description "List of address families.";
    }
  }
}
The name of the address family, as defined in the BGP model is used for keying.

leaf name {
  type leafref {
    path "/rt:routing/rt:control-plane-protocols/
      + "rt:control-plane-protocol/bgp:bgp/
        + "bgp:global/bgp:afi-safis/bgp:afi-safi/bgp:name";
  }
  description "Name of the address family";
}

leaf-list peers {
  type union {
    type leafref {
      path "/rt:routing/rt:control-plane-protocols/
        + "rt:control-plane-protocol/bgp:bgp/
          + "bgp:neighbors/bgp:neighbor/bgp:remote-address";
    }
    type bt:peer-type;
    type identityref {
      base bmp-peer-types-idty;
    }
  }
  description "Peers can be identified by a remote-address, or by an enum value corresponding to groups of peers. This way an operator can select all external peers, all internal peers, or all peers.";
}

grouping bmp-route-monitoring-sources {
  description "Route monitoring sources";
  container network-instances {
    description "container for lists of network-instances";
    list network-instance {
      key "network-instance-id";
      description "Network instance to monitory using BMP.";
      leaf network-instance-id {
        type union {
          type leafref {
            path "/ni:network-instances/ni:network-instance/"
+ "ni:name";
}
type identityref {
    base bmp-ni-types-all-ni-idty;
}
}
description
"Identification of a network-instance. Network instances can be identified directly by their path or one can define all of them using an identity";

container adj-rib-in-pre {
    description
        "Configuration for the adj-rib-in pre-policy";
    reference
        "RFC7854: BGP Monitoring Protocol (BMP), Section 2.";
    uses bmp-peer-ribs-filter;
}
container adj-rib-in-post {
    description
        "Configuration for the adj-rib-in post-policy";
    reference
        "RFC7854: BGP Monitoring Protocol (BMP), Section 2.";
    uses bmp-peer-ribs-filter;
}
container local-rib {
    description
        "Configuration for the local-rib";
    reference
        "RFC9069: Support for Local RIB in the BGP Monitoring Protocol (BMP), Section 3.";
    leaf enabled {
        type boolean;
        description
            "Enables the specified RIB";
    }
    leaf-list address-families {
        type identityref {
            base bt:afi-safi-type;
        }
        description
            "List of address families to enable for local-rib.";
    }
container adj-rib-out-pre {
  description
    "Configuration for the adj-rib-out pre-policy";
  uses bmp-peer-ribs-filter;
  reference
    "RFC8671: Support for Adj-RIB-Out in the BGP Monitoring Protocol (BMP), Section 3.";
}

container adj-rib-out-post {
  description
    "Configuration for the adj-rib-out post-policy";
  uses bmp-peer-ribs-filter;
  reference
    "RFC8671: Support for Adj-RIB-Out in the BGP Monitoring Protocol (BMP), Section 3.";
}

grouping bmp-session-options {
  description
    "leaves for configuration of the bmp session";
  leaf initiation-message {
    type string;
    description
      "User defined message to append to the initiation message";
  }
  leaf statistics-interval {
    type uint32;
    description
      "Default Interval for statistic message.";
  }
}

container bmp {
  description
    "Main level for BMP configuration";
  container stations {
    description
      "Container for the list of BMP stations";
    list station {

key "id";
description
  "Configuration for BMP stations.";
leaf id {
  type string;
  description
  "Identification string for the station";
}
// Connection, missing tcp tuning params
// like keep-alives, segment sizes, etc.
container connection {
  description
  "Connection details for the station";
  uses bmp-ip-connection;
  uses bmp-tcp-options;
}
container bmp_session {
  description
  "BMP session options for the station";
  uses bmp-session-options;
}
container bmp_sources {
  description
  "Configuration of the data sources for the station";
  uses bmp-route-monitoring-sources;
}
container session-stats {
  description
  "Stats and operational values for the station";

  leaf discontinuity-time {
    type yang:date-and-time;
    mandatory true;
    description
    "The time on the most recent occasion at which any one or more of this station’s counters suffered a discontinuity. If no such discontinuities have occurred since the last re-initialization of the local management subsystem, then this node contains the time the local management subsystem re-initialized itself.";
  }

  leaf established-session {
    type boolean;
    config false;
    description

"Value indicating if the session is currently established";
}
leaf total-route-monitoring-messages {
    type uint64;
    config false;
    description
    "Number of route-monitoring messages sent since last successful connection";
}
leaf total-statistics-messages {
    type uint64;
    config false;
    description
    "Number of statistics messages sent since last successful connection";
}
leaf total-peer-down-messages {
    type uint64;
    config false;
    description
    "Number of peer-down messages sent since last successful connection";
}
leaf total-peer-up-messages {
    type uint64;
    config false;
    description
    "Number of peer-up messages sent since last successful connection";
}
leaf total-initiation-messages {
    type uint64;
    config false;
    description
    "Number of initiation messages sent since last successful connection";
}
leaf total-route-mirroring-messages {
    type uint64;
    config false;
    description
    "Number of route-mirroring messages sent since last successful connection";
}
container actions {
 nacm:default-deny-all;
 description
 "Container with the actions for the BMP operation";
 action session-reset {
  description
  "Resets the session for a station.";
  output {
   choice outcome {
    description
    "Output of the reset operation. Either a success or
    failure. For the latter, the reason for the
    error is provided.";
    leaf success {
     type empty;
     description
     "Reset successful";
    }
    leaf failure {
     type string;
     description
     "Reset could not be performed. Reason is included in the field";
    }
   }
  }
}
}

5. Security Considerations

The YANG module specified in this document defines a schema for data that is designed to be accessed via network management protocols such as NETCONF [RFC6241] or RESTCONF [RFC8040]. The lowest NETCONF layer is the secure transport layer, and the mandatory-to-implement secure transport is Secure Shell (SSH) [RFC6242]. The lowest RESTCONF layer is HTTPS, and the mandatory-to-implement secure transport is TLS [RFC8446]. The NETCONF Access Control Model (NACM) [RFC8341] provides the means to restrict access for NETCONF or RESTCONF users.
to a preconfigured subset of all available NETCONF or RESTCONF protocol operations and content.

BGP data is sensible for security considerations. The model described in this document could be used to send BGP information to malicious BMP stations. Write access to this model should therefore be properly protected.

The session-reset action can demand considerable amount of resources from network elements. It should thus be protected from illegal access.

6. IANA Considerations

6.1. The IETF XML Registry

This document registers a URIs in the IETF XML registry [RFC3688]. Following the format in [RFC3688], the following registrations are requested:

Registrant Contact: The IESG.
XML: N/A, the requested URI is an XML namespace.

6.2. The YANG Module Name Registration

This document registers the following YANG module in the " YANG Module Names" registry registry [RFC6020]:

Name: ietf-bmp
Prefix: bmp
Reference: [This RFC-to-be]

7. Open Issues

Shall we leverage other IETF models to specify TCP parameters?

The security considerations section will have to be aligned with https://trac.ietf.org/trac/ops/wiki/yang-security-guidelines

8. Normative References
[I-D.ietf-idr-bgp-model]


Appendix A. Examples

This section shows an example of a BMP configuration using the model. In the example, the device will send information from the global network instance, the adj-rib-out-pre RIB, IPv4 AFI, and only from peers that are external.
<bmp xmlns="urn:ietf:params:xml:ns:yang:ietf-bmp">
  <stations>
    <station>
      <id>1</id>
      <connection>
        <active>
          <network-instance>global</network-instance>
          <station-address>203.0.113.1</station-address>
          <station-port>27716</station-port>
          <local-address>203.0.113.2</local-address>
        </active>
      </connection>
    </station>
  </stations>
  <bmp_sources>
    <network-instances>
      <network-instance>
        <network-instance-id>global</network-instance-id>
        <adj-rib-in-pre>
          <enabled>true</enabled>
          <address-families>
            <address-family>
              <name xmlns:bt="urn:ietf:params:xml:ns:yang:
                          ietf-bgp-types">bt:ipv4-unicast</name>
              <peers>external</peers>
            </address-family>
          </address-families>
        </adj-rib-out-pre>
      </network-instance>
    </network-instances>
  </bmp_sources>
</bmp>

Acknowledgements

The authors would like to thank Pierre Vander Vorst and Tom Petch for their review and feedback.

Authors’ Addresses

Camilo Cardona
NTT
164–168, Carrer de Numancia
08029 Barcelona
Spain
Email: camilo@ntt.net
Paolo Lucente
NTT
Siriusdreef 70-72
2132 Hoofddorp
Netherlands
Email: paolo@tt.net

Thomas Graf
Swisscom
Binzring 17
CH- Zurich 8045
Switzerland
Email: thomas.graf@swisscom.com

Benoit Claise
Huawei
Email: benoit.claise@huawei.com