I2RS working group   S. Hares
Internet-Draft   Q. Wu
Intended status: Standards Track   Huawei
Expires: September 9, 2015   J. Tantsura
                                                            R. White
                                                             Ericsson
                                                        March 8, 2015

       An Information Model for Basic Network Policy and Filter Rules
                   draft-hares-i2rs-bnp-info-model-02

Abstract

   This document contains the Basic Network Policy and Filters (BNP IM)
   Information Model which provides a generic model for representing an
   ordered list of routing policy or filter rules. Filter rules which
   combine match-condition with action (forwarding or sets) are
   supported by this policy.

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 http://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 September 9, 2015.

Table of Contents

1. Introduction

   This generic network policy provide a model to support an ordered
   list of routing policy or an ordered list of filter rule. An ordered
   list of policy can be used in protocols such as BGP. An ordered list
   of filters can be used in filtering for routing data traffic or
   flows. Two examples of the ordered-based filters is the I2RS Filter-
   based RIBS or flow specification filtering. This generic model can
   be used to combine filter rules such as: ACLs, Prefix-filtering, and
   complex filter match-actions rules (match, set, modify, set).

   This generic model combines rules for filter/policy into groups of
   groups. project.

   Antecedents to this generic policy are the generic policy work done
   in PCIM WG. The PCIM work contains a Policy Core Information Model
   (PCIM) [RFC3060], Policy Core Informational Model Extensions
   [RFC3460] and the Quality of Service (QoS) Policy Information Model
   (QPIM) ([RFC3644]) From PCIM comes the concept that policy rules
   which are combined into policy groups. PCIM also refined a concept
   of policy sets that allowed the nesting and aggregation of policy
   groups. This generic model did not utilize the concept of sets of
   groups, but could be expanded to include sets of gorups in the
   future.

   Policy rules may include specific filters such as ACL or prefix
   filters by simple reference. The following drafts provide these more
   specific filters;

   o ACL policy [I-D.ietf-netmod-acl-model]

   o BGP Prefix filter policy [I-D.zhdankin-idr-bgp-cfg]

2. Definitions and Acronyms

      BGP: Border Gateway Protocol

      CLI: Command Line Interface

      IGP: Interior Gateway Protocol

      Information Model: An abstract model of a conceptual domain,
      independent of a specific implementations or data representation

      INSTANCE: Routing Code often has the ability to spin up multiple
      copies of itself into virtual machines. Each Routing code
      instance or each protocol instance is denoted as Foo_INSTANCE in
      the text below.

      NETCONF: The Network Configuration Protocol

      PCIM - Policy Core Information Model

      RESTconf - http programmatic protocol to access yang modules

3. Generic Route Filters/Policy Overview

   This generic policy model represents filter or routing policies as
   rules and groups of rules.

   The basic concept are:

   Rule Group

      A rule group is is an ordered set of rules .

   Rule

      A Rule is represented by the semantics "If Condition then Action".
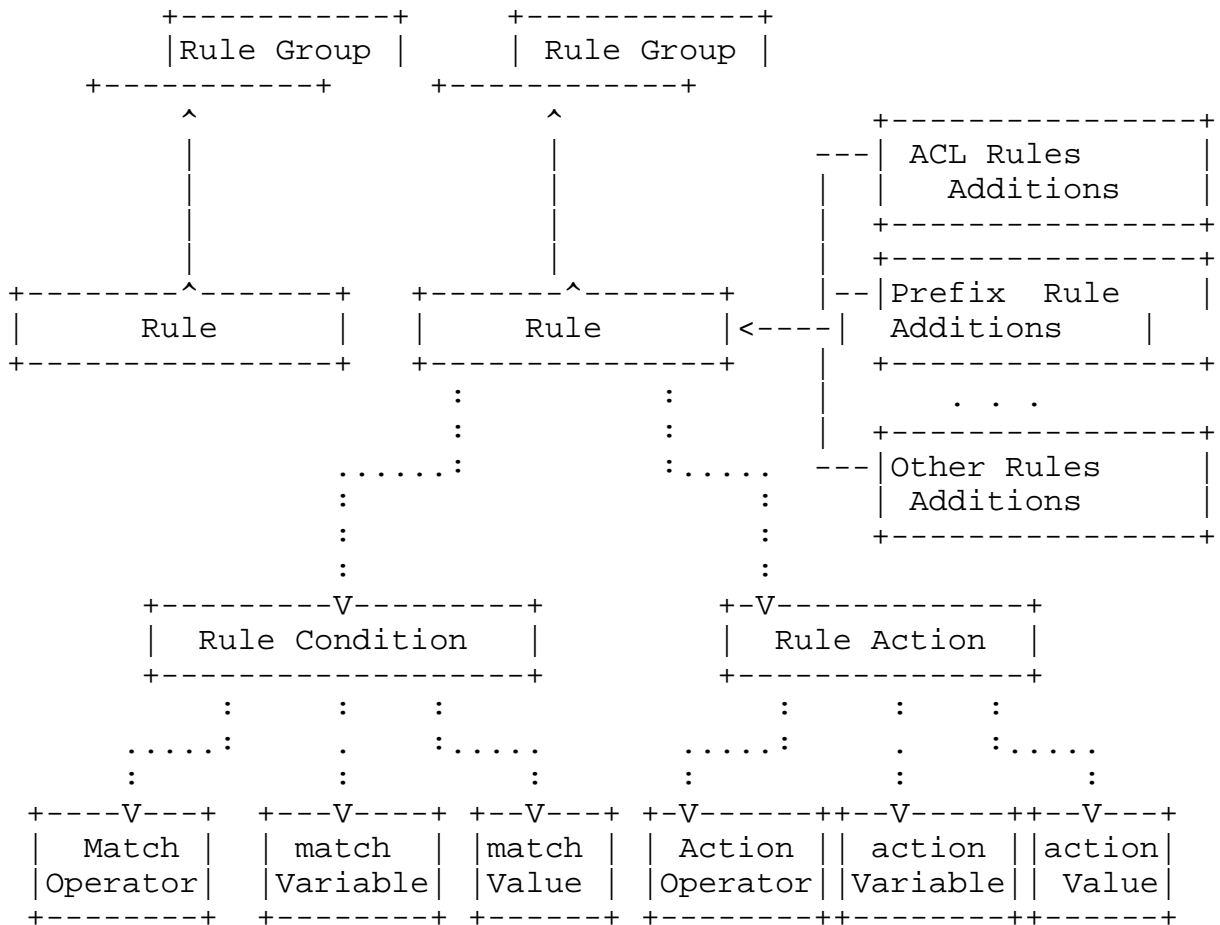   A Rule may have a priority assigned to it.

```
        +----------+       +-----------+
        |Rule Group |       | Rule Group |
        +----------+       +-----------+              +----------------+
             ^                   ^                  ---| ACL Rules      |
             |                   |                 |  |    Additions   |
             |                   |                 |  +----------------+
             |                   |                 |  +----------------+
 +---------^-------+   +-------^-------+   |--|Prefix  Rule    |
 |     Rule        |   |     Rule      |<----|    Additions    |
 +----------------+   +--------------+   |  +----------------+
                           :         :      |      . . .
                           :         :      |  +----------------+
                     ......:         :..... ---|Other Rules      |
                           :         :         |   Additions     |
                           :         :         +----------------+
                           :         :
        +---------V---------+       +-V-------------+
        |  Rule Condition   |       |  Rule Action  |
        +------------------+       +--------------+
           :      :      :              :      :      :
       ....:      .      :.....     ....:      .      :.....
           :      :      :              :      :      :
 +----V---+  +---V----+ +--V---+  +-V------++--V-----++--V---+
 |  Match |  | match  | |match |  | Action || action ||action|
 |Operator|  |Variable| |Value |  |Operator||Variable|| Value|
 +--------+  +--------+ +------+  +--------++--------++------+
```

                    Figure 1: BNP structure

4. BNP Rule Groups

    Rule groups have the following elements:

    o name that identifies the grouping of policy rules

    o role - that is a combination of target resource (E.g. IPv4 FB-FIB
       filters) and a scope (read, read-write, write-only).

    o list of rules

    The rule has the following elements: name, order, status, priority,
    reference cnt, and match-action as shown as shown in figure 2. The
    order indicates the order of the rule within the list. The status of
    the rule is (active, inactive). The priority is the priority within
    a specific order of policy/filter rules. A reference count (refcnt)
    indicates the number of entities (E.g. network modules) using this
    policy. The generic rule match-action conditions have match

operator, a match variable and a match value. The rule actions have
an action operator, action variable, and an action value.

The generic rules can be included with other types of rules as figure
2 shows.

```
                    Figure 2 - Rule Group
      +-------------------------------------+ (optional)
      |              Rule Group              |....
      +-------------------------------------+   :
        *         *                  *      ^   :
        |         |                  |      :....:
        |         |                  |
        |         |                  |
   +------+  +-----+      +------------------+
   | Name |  |Role |      |     Rule_list    |
   |      |  |     |      |                  |
   +------+  +-----+      +------|-----------+
        *         *       +------|-----------+
        |         |       |    rule          |
        |         |       +--|---------------+
        |         |          |
      +--+        |          | +----------+
      |           |-|        | |   Name   |
      |           |          | +----------+
   +----+---+  ++-----+      | +----------+
   |Resource|  |Scope |      | |  + Rule  |
   +--------+  +-----+       |-|  order   |
                            |  +----------+
                            |  +----------+
                            |-|  Status  |
                            |  +----------+
                            |  +----------+
                            |-|  priority |
                            |  +----------+
                            |  +----------+
                            |-|  refcnt   |
                            |  +----------+
                            |  +-------------+
                            |-|     Rule     |
                            |  | match/action |
                            +-----|--------+
                                  |
      +-----|---------------|----|----------+
      |              |           |          |
   +-------|-------+ +----|--------+ +----|--------+  . . .
   | bnp generic   | | Access rule  | | Prefix-list  |
   | match/action  | | match/action | | rule         |
   +-------------+   +------------+   +------------+
```
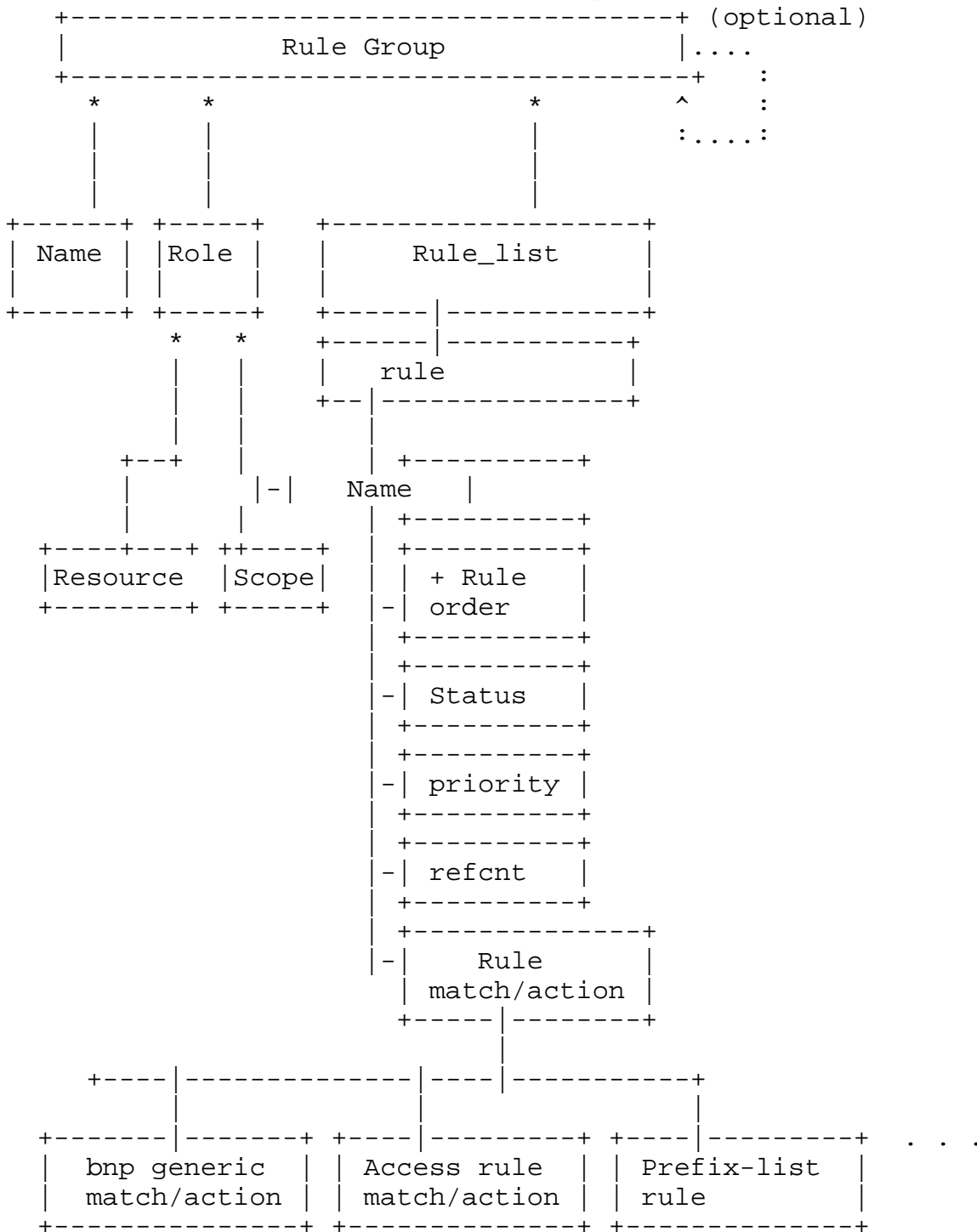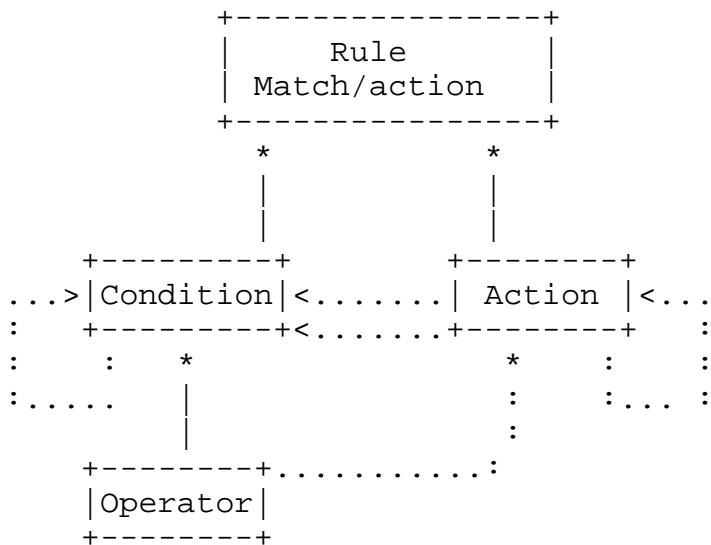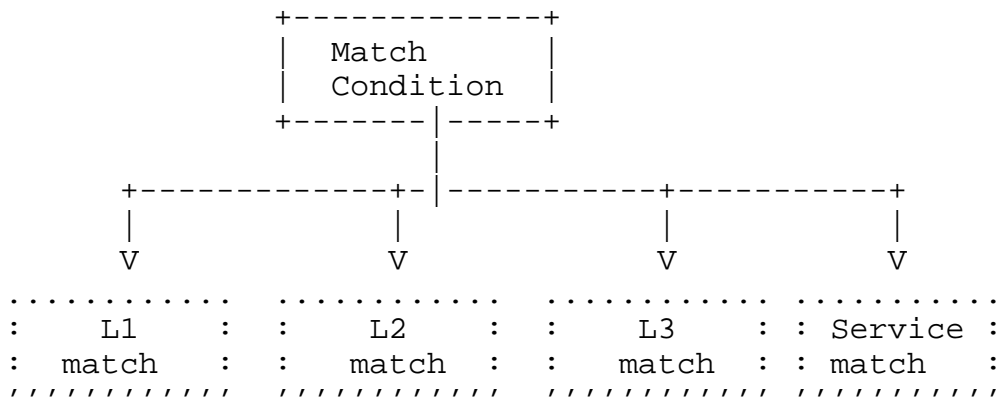
   The conditions in one rule may cause actions to set values (E.g. BGP
   communities) that are examined in a second rule as shown in figure 3.

Figure 3 - Rule's match-condition

```
              +----------------+
              |     Rule       |
              | Match/action   |
              +----------------+
                  *           *
                  |           |
                  |           |
          +--------+        +--------+
     ...>|Condition|<.......| Action |<...
      :   +--------+<.......+--------+   :
      :     :    *               *   :    :
      :.....      |              :    :... :
                  |              :
          +-------+..........:
          |Operator|
          +--------+
```

The generic match conditions are specific to a particular layer are
refined by matches to a specific layer (as figure 4 shows), and
figure 5's high-level yang defines. The general actions may be
generic actions that are specific to a particular layer (L1, L2, L3,
service layer) or general forwarding by interface or nexthop. The
high-level yang diagram for the matches in figure 5.

```
          Figure 4
                +-------------+
                |   Match     |
                | Condition   |
                +-------|-----+
                        |
        +------------+-|-----------+-----------+
        |            |             |           |
        V            V             V           V
    ...........  ...........  ........... ...........
    :   L1    :  :   L2    :  :   L3    : : Service :
    :  match  :  :  match  :  :  match  : : match   :
    '''''''''''  '''''''''''  ''''''''''' '''''''''''
```

5. BNP Generic Info Model in High Level Yang

   Below is the high level yang diagram for the

```
      Figure 5
          module:bnp-generic-rules
            import ietf-acl
            import ietf-interface
            +-rw rule-group* [group-name]
              +--rw group-name
              +--rw group-scope
              | +--resource  tree-identity
              | +--access    access-identity
        +--rw group-installer install-identity
        +--rw rule*  [rule-name]
            +--rw rule-name string
            +--rw order unit16
                  +--rw installer
            +--rw status enumeration
            | +--ro rules-status
            | +--ro rule-inactive-reason
            | +--ro rule-installer
            +--rw priority unit16
            +--rw refcnt unit16
            +--rw rule-match-act
                +--rw match-act-type match-act-type-identity
                    +--case: BNP-GENERIC-MATCH-ACTION
                    | +--rw bnp-term-match
                    | | +--case: interface-match
                    | | +--case: L1-header-match
                    | | +--case: L2-header-match
                    | | +--case: L3-header-match
                    | | +--case: L4-header-match
                    | | +--case: Service-header-match
                    | +--rw bnp-action
                    | | +--rw genric-actions [nbr-act]
                    | | | +--rw n-acts
                    | | | +--rw qos-action
                    | | | | +--case L1-action
                    | | | | +--case L2-action
                    | | | | +--case L3-action
                    | | | | +--case L4-action
                    | | | | +--case service-action
                    | +--rw bnp-forward
                    | | +--rw forward
                    | | | +--rw interface interface-ref
                    | | | +--rw next-hop  rib-nexthop-ref
                    | | | +--rw route-attributes
                    | | | +--rw rib-route-attributes-ref
                    | | +--rw fb-std-drop
                    +--case: ACL-MATCH-ACTION
                        +--rw acl-match-act acl-list-entry-name
```

6. Example of use in filters

    The following is an example is an example structure for the rrule
    match-condition applied to Filter-Based RIB containing a list of
    routes

```
          figure 6
     module: FB-RIB
      +--rw FB-RIB-instance-name
      +--rw RB-RIB-router-id  uint32
            +--rw FB-RIB-interface*
            |  +--rw FB-RIB-interface interface-ref-id
            +--rw FB-Default-RIB rib-ref
        +--rw FB-RIB
              +--rw FB-RIB-Name
                  +--rw FB-RIB-AFI
                  +--rw FB-RIB-intf*
                  +--rw FB-FIB-status-info
                  |  +--rw fb-rib-update-ref uint64
                  +--rw FB-RIB-Ordered-Filters  rule-group-list-ref
                uses /nt:bnp-generic-rules

        rule-group-list-ref points to rule-group-list
```

7. IANA Considerations

    This draft includes no request to IANA.

8. Security Considerations

    These generic filters are used in the I2RS FB-RIBs to filter packets
    in a traffic stream, act to modify packets, and forward data packets.
    These I2RS filters operate dynamically at same level as currently
    deployed configured filter-based RIBs to filter, change, and forward
    traffic. The dynamic nature of this protocol requires that I2RS
    Filters track the installer of group information and rules.

    This section will be augmented after a discussion with security
    experts.

9. Informative References

    [I-D.hares-i2rs-usecase-reqs-summary]
              Hares, S. and M. Chen, "Summary of I2RS Use Case
              Requirements", draft-hares-i2rs-usecase-reqs-summary-01
              (work in progress), October 2014.

   [I-D.ietf-i2rs-architecture]
              Atlas, A., Halpern, J., Hares, S., Ward, D., and T.
              Nadeau, "An Architecture for the Interface to the Routing
              System", draft-ietf-i2rs-architecture-09 (work in
              progress), March 2015.

   [I-D.ietf-i2rs-rib-info-model]
              Bahadur, N., Folkes, R., Kini, S., and J. Medved, "Routing
              Information Base Info Model", draft-ietf-i2rs-rib-info-
              model-05 (work in progress), January 2015.

   [I-D.ietf-netconf-restconf]
              Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF
              Protocol", draft-ietf-netconf-restconf-04 (work in
              progress), January 2015.

   [I-D.ietf-netmod-acl-model]
              Bogdanovic, D., Sreenivasa, K., Huang, L., and D. Blair,
              "Network Access Control List (ACL) YANG Data Model",
              draft-ietf-netmod-acl-model-02 (work in progress), March
              2015.

   [I-D.zhdankin-idr-bgp-cfg]
              Alex, A., Patel, K., Clemm, A., Hares, S., Jethanandani,
              M., and X. Liu, "Yang Data Model for BGP Protocol", draft-
              zhdankin-idr-bgp-cfg-00 (work in progress), January 2015.

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC3060] Moore, B., Ellesson, E., Strassner, J., and A. Westerinen,
              "Policy Core Information Model -- Version 1
              Specification", RFC 3060, February 2001.

   [RFC3460] Moore, B., "Policy Core Information Model (PCIM)
              Extensions", RFC 3460, January 2003.

   [RFC3644] Snir, Y., Ramberg, Y., Strassner, J., Cohen, R., and B.
              Moore, "Policy Quality of Service (QoS) Information
              Model", RFC 3644, November 2003.

   [RFC5511] Farrel, A., "Routing Backus-Naur Form (RBNF): A Syntax
              Used to Form Encoding Rules in Various Routing Protocol
              Specifications", RFC 5511, April 2009.

Authors' Addresses

   Susan Hares
   Huawei
   7453 Hickory Hill
   Saline, MI 48176
   USA

   Email: shares@ndzh.com

   Qin Wu
   Huawei
   101 Software Avenue, Yuhua District
   Nanjing, Jiangsu 210012
   China

   Email: bill.wu@huawei.com

   Jeff Tantsura
   Ericsson

   Email: Jeff Tantsura jeff.tantsura@ericsson.com

   Russ White
   Ericsson

   Email: russw@riw.us