

I2RS working group
Internet-Draft
Intended status: Standards Track
Expires: April 30, 2015

S. Hares
Q. Wu
Huawei
October 27, 2014

An Information Model for Basic Network Policy
draft-hares-i2rs-bnp-info-model-01

Abstract

This document contains the Basic Network Policy (BNP IM) Information Model which is an instantiation and extension of the PCIM work (RFC3060, RFC 3460, RFC 3644) that supports both the configuration models and the I2RS ephemeral models. The PCIM work contains a Policy Core Information Model (PCIM) (RFC3060) and the Quality of Service (QoS) Policy Information Model (QPIM)(RFC3644) and policy based routing. The PCIM work provided a framework to incorporate ACL filters, prefix filters, and more complex filters. This extension to PCIM model incorporate ACLs, Prefix-filtering, and complex policy (match, set, modify, set) into the PCIM framework. Complex policy is needed by I2RS programmatic interface to BGP, flow specification filtering, Policy Based Routing (PBR), MPLS topology management, and flow specification filtering.

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 April 30, 2015.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction	2
2. Definitions and Acronyms	3
3. PCIM Overview	3
4. Top-Down yang Diagram for PCIM	5
4.1. Policy Set Structures	5
4.2. Policy Group Expansion for Basic Network Policy (BNP)	6
5. Example of use in BGP	9
6. IANA Considerations	9
7. Security Considerations	10
8. Informative References	10
Authors' Addresses	11

1. Introduction

The Interface to the Routing System (I2RS) provides read and write access to the information and state within the routing process within routing elements. The I2RS client interacts with one or more I2RS agents to collect information from network routing systems. The processing of collecting information at the I2RS agent may require the I2RS Agent to filter certain information, group pieces of information, or perform actions on the I2RS collected information based on specific I2RS policies.

The generic policy work done in PCIM WG has been has been recast into I2RS work. 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]) The basic concept of PCIM is that there are policy rules which are combined into policy groups. If nesting and aggregation of policy groups is necessary, the PCIM work defines a policy set that operates under specific rules. Policy Groups can be used without using policy sets. This concept of a policy group as an entity that contains a set of policy rules is also reference utilized by the OpenDaylight group policy project.

In initial work for I2RS or netmod, the policy group that simply combines and orders policies rules will be sufficient.

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.bogdanovic-netmod-acl-model]
- o BGP Prefix filter policy [I-D.zhdankin-netmod-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. PCIM Overview

The PCIM work created the concepts of Policy Set, Policy Group, and Policy Rule. This section reviews these concepts as background for the application of these concepts to current configuration and I2RS policy. In addition, this section suggests placement of policy rule concepts.

The basic PCIM concepts are:

Policy Set

is a class which derived from Policy, and it is inserted into the inheritance hierarchy above both PolicyGroup and PolicyRule (as figure 1 shows). The Policy set is a coherent set of rules that

has two properties of PolicyDecisionStrategy and PolicyRoles, and supports PolicySetComponent subclass. The PolicySetComponent is an aggregation class that allows aggregation of policy groups and under policy groups the a set of rules. The PolicySet contains rules for nesting policies that include matching strategies (all-matching or first-match), priorities between rules, and roles. One of the roles that must be conditionally matched is the models denotation of "read-only" or "read-write".

Policy Group

Policy is described by a set of policy rules that may be grouped into subsets. [RFC3060] defines policy groups as either a group of policy rules or group of policy groups - but not both. A policy group is used to provide a hierarchical policy definition that provides the model context or scope for sub-rule actions. The policy group is identified by a policy group name, and contains policy rules. Policy groups can be nested within other policy rules only within Policy sets.

Policy Rule

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

Figure 2 - Policy Set Yang

```

module: ietf-pcim
  +--rw policy-set [policy-set-name]
  |   +--rw policy-set-name string
  |   +--rw matching-strategy enumeration
  |   +--rw policy-roles enumeration
  |   +--rw default-rule-priority uint16
  |   +--rw policy-group* [policy-group-name]

```

Figure 2 - PSET Yang level

4.2. Policy Group Expansion for Basic Network Policy (BNP)

Policy groups within the PCIM work have a name that identifies the grouping of policy rules. In PCIM, the policy rule has a name, status, priority, match condition with an action. The status for the policy rule is enabled or disabled. The priority is the priority within the policy rule order. This expansion of the PCIM policy rule adds a policy-rule order field, a reference count (pr-refcnt). It expands the PCIM match/condition methods to include a reference to other match-action fields.

I2RS which requires that a read/write scope be tied to a particular portion of the ephemeral tree. This requirement is instantiated as the I2RS-role at the policy group level. However, it is anticipated this will be replaced by an expansion of [I-D.ietf-netconf-restconf] functionality surrounding the xpath feature. This element is left in this model to until these restconf xpath additions have been finalized.

The logical structure is below in figure 3 with an expansion of the pcim match-action-operation in figure 4.

Figure 3 - Policy Group

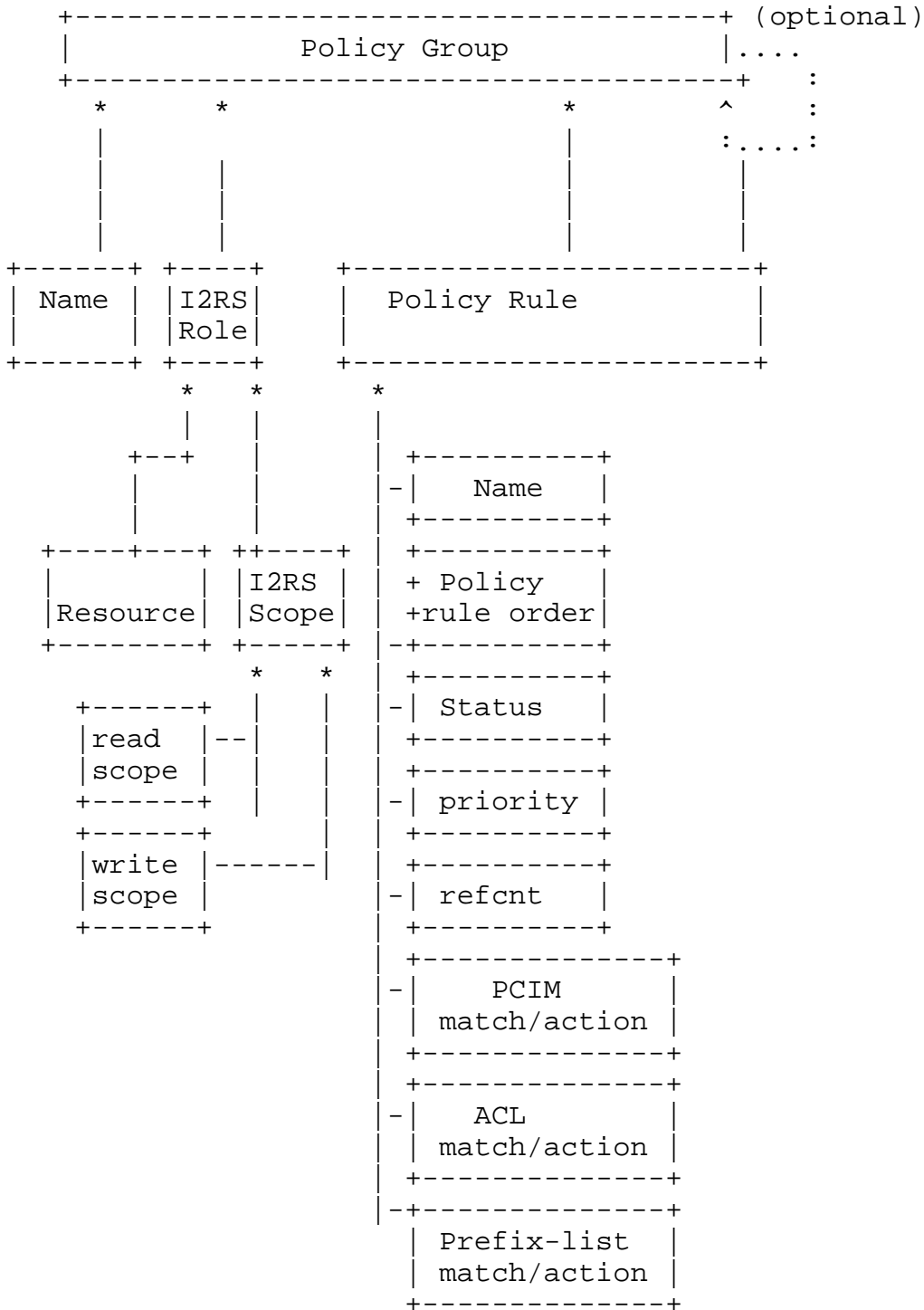
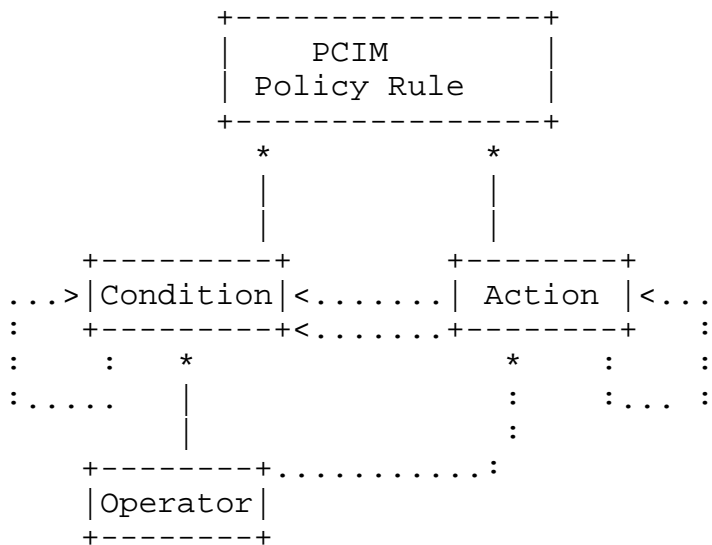


Figure 5 - Policy Rule's match-condition



The basic yang high-level structure for the policy group is included below in figure 6.

Figure 6

```

module: ietf-pcim
+--rw policy-set [policy-set-name]
|
|   ....
|   +--rw policy-group* [policy-group-name]
|   |   +--rw policy-group-name
|   |   +--rw i2rs-scope
|   |   |   +--tree-xpath
|   |   |   +--access enumeration
|   |   +--rw policy-rule* [policy-rule-name]
|   |   |   +--rw pr-name string
|   |   |   +--rw pr-order unit16
|   |   |   +--rw pr-status enumeration
|   |   |   +--rw pr-priority unit16
|   |   |   +--rw pr-refcnt unit16
|   |   |   +--rw pr-match-act
|   |   |   |   +--rw pr-match-act-type
|   |   |   |   +case: pcim match-act ref-cnt
|   |   |   |   +case: acl acl-ref
|   |   |   |   +case: Prefix-list prefix-list-ref
|   |   |   +
|   |   +case: pbr-pcim-match-act pbr-pcim-match-act-ref

```


5. Example of use in BGP

The PCIM suggests a patch structure of match-field, operator for match, action (send packet), and set value. The following is an example structure for the pcim of the match-condition applied to BGP.

figure 7

```

+--rw bnp-match-act
|
|  +--rw bnp-match-act-bgp-i2rs
|  |
|  |  +--rw bgp-match-field
|  |  |
|  |  |  +--rw bgp-afi
|  |  |  +--rw bgp-local-rib
|  |  |  +--rw bgp-peer
|  |  |  +--rw bgp-rib-in
|  |  |  |  +--bgp-rib-in-policy-type
|  |  |  |  +--bgp-rib-in-policy
|  |  |  |  +--case: policy-set pcim-policy-set-name
|  |  |  |  +--case: policy-group pcim-policy-group-name
|  |  |  +--rw bgp-rib-out
|  |  |  |  +--bgp-rib-out-policy-type
|  |  |  |  +--bgp-rib-out-policy
|  |  |  |  +--case: policy-set pcim-policy-set-name
|  |  |  |  +--case: policy-group pcim-policy-group-name
|  |  |  +--rw bgp-route-prefix
|  |  |  |  .. prefix or prefix-range
|  |  |  +--rw bgp-attribute-list
|  |  |  |  ... bgp attributes
|  |  |  +--rw bgp-state-info
|  |  |  |  ... bgp state
|  |  +--rw bgp-match-operator
|  |  |  +--rw operator-type enumeration
|  |  |  +--rw bgp-prefix-range-operator
|  |  |  +--rw bgp-attribute-operator
|  |  |  +--rw bgp-state-operator
|  |  +--rw bgp-action
|  |  |  +--bgp-act enumeration
|  |  |  +--bgp-act value
|  |  +--rw bgp-set
|  |  |  +--bgp-set enumeration
|  |  |  +--bgp-set value

```

6. IANA Considerations

This draft includes no request to IANA.

7. Security Considerations

TBD

8. Informative References

[I-D.bogdanovic-netmod-acl-model]

Bogdanovic, D., Sreenivasa, K., Huang, L., and D. Blair, "Network Access Control List (ACL) YANG Data Model", draft-bogdanovic-netmod-acl-model-02 (work in progress), October 2014.

[I-D.hares-i2rs-bgp-im]

Hares, S., Wang, L., and S. Zhuang, "An I2RS BGP Information Model", draft-hares-i2rs-bgp-im-01 (work in progress), October 2014.

[I-D.hares-i2rs-usecase-reqs-summary]

Hares, S., "Summary of I2RS Use Case Requirements", draft-hares-i2rs-usecase-reqs-summary-00 (work in progress), July 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-05 (work in progress), July 2014.

[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-03 (work in progress), May 2014.

[I-D.ietf-netconf-restconf]

Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", draft-ietf-netconf-restconf-02 (work in progress), October 2014.

[I-D.zhdankin-netmod-bgp-cfg]

Alex, A., Patel, K., and A. Clemm, "Yang Data Model for BGP Protocol", draft-zhdankin-netmod-bgp-cfg-01 (work in progress), October 2014.

[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@endzh.com

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

Email: bill.wu@huawei.com