I2RS working group S. Hares
Internet-Draft Hickory Hill Consulting
Intended status: Standards Track Q. Wu
Expires: September 4, 2014 Huawei
March 3, 2014

An Information Model for Network policy
draft-hares-i2rs-info-model-policy-02

Abstract

This document introduces an information model for network policies. This model operates as policy model that can be linked to other information model such as the I2RS RIB information model.

Some applications that utilize the services of I2RS client may require specific set of data in response to network events or conditions based on pre-established rules. In order to reduce the data flow through the network, the I2RS client needs to signal the I2RS agent to filter some of the collected data or events prior to transmission, or group the data prior to transmission to the i2rs client. This functionality is necessary to meet the requirements i2rs enabled services which include service-layer routing improvements, and control of traffic flows and exit points.

The information model is based on extensible information model for representing policies, for example, the Policy Core Information Model (PCIM) (RFC3060), and an extension to this model to address the need for QoS management, called the Quality of Service (QoS) Policy Information Model (QPIM)(RFC3644) and policy based routing.

Status of This Memo

Copyright Notice

Table of Contents

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.

Processing of collected information at the I2RS agent may require the I2RS Agent to filter certain information or group pieces of information in order to reduce the data flow through the network to the I2RS client. Some applications that that utilize the services of I2RS client may also wish to require specific data in response to network events or conditions based on pre-established rules. This functionality is necessary to meet the requirements of i2rs enabled services which include service-layer routing improvements, and control of traffic flows and exit points.

This document introduces a basic information model for network policies. This policy model can be linked with other information models such as the I2RS RIB informational model [I-D.ietf-i2rs-rib-info-model] as a generic policy module. This basic policy model can be easily extended beyond the basic functions. The [I-D.ietf-i2rs-architecture] suggests that associated with the the i2RS RIB model there will be "Policy-based Routing (ACLs)" and RIB "policy controls". These basic policy functions can operate as part of this functional blocks providing the basic model for policy operators. This model can also be considered as the substance of the policy templates.

The basic but extendable policy model is a product of the industry approach to I2RS. The initial I2RS work is focusing on the initial RIB module, and basic functions to make the initial RIB model function within real networks. Subsequent drafts will provide building blocks upon this policy model that can be used to create network functions.

This information model leverages previous work done on extensible information model for representing policies, for example, the Policy Core Information Model (PCIM) [RFC3060] [RFC3060], and an extension to this model to address the need for QoS management, called the Quality of Service (QoS) Policy Information Model (QPIM) [RFC3644] [RFC3644].

Most policy within routing and forwarding systems has become hierarchical with individual specific policies being grouped as a set policy. The hierarchical policy rule definition enhances policy readability and reusability. Groups of network policies have labels to aid operational use. Named groups of policy are easily identified and reused as blocks.

The information model contains the following three components:

Policy Group

> Policy is described by a set of policy rules that may be grouped into subsets. A Policy group is used to provide a hierarchical policy definition that provides the model context or scope for sub-rule actions. The model context includes identity, scope, role, precedence, priority and security model. In a policy group policy rules and policy groups can be nested within other policy rules.

Network-Policy

contains a generic network policy model. It can be thought of as a coherent set of rules to administer, manage, and control access to network resources and defines a network policy at its most general level of abstraction. It models aspects such as actions and conditions that constitute a policy element relationship, as well as operators contained in the both condition and action that can either be used to overwrite an old value of the variable or imply match relationship. Policies vary in level of abstraction, for example policy at parent level or policy at child level. The model therefore allows to show relationships between policies, as well as dependencies between condition and action across policy.

Local Config

defines information kept that kept in policy database that is leveraged by CLI, SNMP, NetConf.

1.1. Currently Out of Scope for I2RS

An I2RS client may also interact with other elements of the policy and provisioning system to retrieve policy to transmit to an I2RS agent to be use in processing collected information, or to pass to policy information bases (PIBs) within the routing system. How the I2RS client interacts with the policy and provision systems is currently outside the scope of I2RS.

I2RS architecture allows multiple I2RS Clients to communicate with the same agent I2RS agent, but requires that only one I2RS client has write control over one element. Specification on how the I2RS Clients handle multiple client interactions it out of scope at this time. The i2rs-architecture document specifies in section x.x that I2RS clients should avoid writing the same element. In the future, the I2RS WG may decide to specify these interactions. Therefore, this document’s policy information allows for extensions that will allow multiple clients.

2. Definitions and Acronyms

IGP: Interior Gateway Protocol

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

CLI: Command Line Interface

SNMP: The Simple Network Management Protocol

NETCONF:The Network Configuration Protocol

RBNF: Routing Backus-Naur Form

3. Network Policy Model Overview

I2RS needs its own implicit and explicit policy. This section provides an overview of the network policy model. The network policy model is defined by the following components, whose relationship is roughly depicted in the figure below.

```
         +-----------------------+
         |    Network-Policy     |
         +-----------+-----------+
                     ^
                    /|\
                     | "extends"
         +-----------^-------------+
         |       Policy Set        |
         +--+-------------------+--+
            ^                   ^               +-----------------+
           /|\                 /|\           ---|Local Policy Rule|
            | "extends"         | "extends"  |  +-----------------+
   +--------^-------+   +-------^-------+    |
   | Policy Group   |   | Policy Rule   |<---|
   +----------------+   +---------------+    |
                          :          :       |  +-------------+
                    ......:          :.....  ---|  PBR Rule   |
                    :                     :     +-------------+
                    :                     :
          +---------V---------+         +-V-------------+
          |  Policy Condition |         | Policy Action |
          +-------------------+         +---------------+
              :     :    :                 :     :    :
         .....:     .    :.....       .....:     .    :.....
         :          :         :       :          :         :
    +----V---+  +---V----+ +--V---+ +-V------++--V-----++--V---+
    |  Match |  |Policy  | |Policy| |  Set   || Policy ||Policy|
    |Operator|  |Variable| |Value | |Operator||Variable|| Value|
    +--------+  +--------+ +------+ +--------++--------++------+
```

Figure 1: Overall model structure

The policy group component defines the basic network policy Group model. In addition, the Network-policy component defines the basic network policy rule model.

PolicySet, is introduced to provide an abstraction for a set of rules. It is derived from Policy, and it is inserted into the inheritance hierarchy above both PolicyGroup and PolicyRule. This reflects the additional structural flexibility and semantic capability of both subclasses.

Policy Rule is represented by semantics "If Condition then Action", therefore condition and action comprise Policy Rule model. Condition models the elementary match operation "<variable> match <value>". Action models the elementary set operation. "SET <variable> TO <value>". In Condition model, the ’Match’ operator is usually implied while in the action model, the ’Set’ operator is explicitly used.

The Local Config Component is extended from Policy Rule and contains a set of local policy state related to I2RS operation that the I2RS agent controls. The local system’s local policy state linked to a particular information base (E.g. I2RS RIB) may have a write scope that one or more clients may write. The same write scope with that of one or more clients using an agent. An agent must check to determine if a local configuration state overlaps with existing installed state.

The Policy Based Routing Rule is also extended from Policy Rule and Contain a set of condition, action and attributes that are inherited from Policy Group Component. Routing decisions in policy based routing are based on several criteria beyond destination address, such as packet size, application, protocol used, and identity of the end system.

4. Network Policy Information Model

This section specifies the network policy information model in Routing Backus-Naur Form (RBNF, [RFC5511]). It also provides diagrams of the main entities that the information model is comprised of.

4.1. The Policy Group Component

In order to provide hierarchical policy definition and associate policy rule with other constraint, the basic policy group model needs to be defined. The corresponding extensions are introduced in a component, whose structure is informally depicted in the following diagram.

```
          +------------------------------------+
          |           Policy Group             |....
          +------------------------------------+   :
            *      *          *     *     *   ^    :
            |      |          |     |     |   :....:
            |      |          |     |     |
            |      |          |     |     |
            |      |          |     |     |
    +--------+ +--------+ +--------+|   +-----------+
    |Identity| | Role   | |Priority||   |Policy Rule|
    +--------+ +--------+ +--------+|   +-----------+
               *      *             |    *      *  *
               |      |             |     |     |  |
            +---      |             |  +---+---+ | ++----+
            |         |             |  |Enabled| | |Usage|
            |         |             |  +-------+ | +-----+
       +-----+----+ +------+        |            |
       | Resource | |Scope |        |            |
       +----------+ +------+        |            |
                    *    *          |         +--+------+
                    |    |     +----+------+  |Mandatory|
                    |    |     | Precedence|  +---------+
                    |    |     +-----------+
                    |    |
                 +-----++-----+
                 | Read||Write|
                 |Scope||Scope|
                 +-----++-----+
```

The basic information model works as follows: Within the policy group information model, hierarchy is used to model context or scope for the sub-rule actions. A policy group contains Identity, scope, priority,precedence, policy rule and policy group. Policy rule or policy group can be nested into policy group. Policy rule can inherit context from policy group as properties and also policy rule can have its own properties, eg., enabled, mandatory, usage properties.

A more formal depiction in RBNF format follows below:

```
      <Policy-Group> ::= <Identity>
                         <Role>
                         <priority>
                         <precedence>
                         <Policy-Rule>
                         [<Supporting-Policy-Group>]
                         [<Policy-Group-Extension>]

      <Scope> ::= <Read-Scope> |<Write-Scope>

      <Role> ::= <Resource> | <Scope>

      <Policy-Group-Extension> ::= <>
       ...
```

The elements of the Policy Group information model are as follows:

- o Each policy group is captured in its own list, distinguished via a identity, role, priority, precedence.

- o A policy group has a certain role, such as resource or scope. A policy group can even have multiple roles simultaneously. The role, are captured in the list of "role" component.

- o A policy role has a certain Scope, such as read scope or write scope. A policy group can even have multiple scope simultaneously. The scope, or scopes, are captured in the list of "scope" components.

- o A policy has a certain priority, such as priority 0-255. A policy can only have one priority. The priority is captured in the list of "priority" component.

- o A policy rule can inherit properties (e.g., identity,role,priority, precedence) from policy group. A policy rule also can have its own properties, e.g., enabled, mandatory, usage.

- o The policy, policy group elements can be extended with policy-specific components (policy-extensions, policy-group-extension respectively).

4.2. The Network-Policy Rule Component

The following diagram contains an informal graphical depiction of the main elements of the information model:

```
               +----------------+
               |   Policy Rule  |<...
               +----------------+   :
                 *           *  :   :
                 |           |  :...:
                 |           |
        +---------+        +--------+
    ...>|Condition|<.......| Action |<...
    :   +---------+<.......+--------+   :
    :    :   *                *    :    :
    :.....   |                :    :... :
             |                :
        +--------+...........:
        |Operator|
        +--------+
```

Roughly speaking, the basic information model works as follows: A policy rule contains conditions and actions. Each condition or each action in turn contains operator. A operator connects variable and value in the action or condition. Condition can map onto and be supported by other condition, while action can map onto and be supported by other actions. Policy rule can map onto other, policy rules.

The information model for the Network-policy component is more formally shown in the following diagram.

```
     <network-policy-rule> ::= (<policy-rule>...)

     <policy-rule> ::= <Identity>
                       <priority>
                       <precedence>
                       <Role>
                       (<Condition>
                       (<Action>...)
                       <Security-Model>
                       [<policy-rule-extension>]

     <Scope> ::= (<Read> [<read-scope>]) |
                 (<Write> [<write-scope>])

     <Role> ::= <Resource> | <Scope>

     <Security-Model> ::= <First-Matching>|<All-Matching>

     <policy-rule-extension> ::= <i2rs-policy-extension> |
                                 ...

      <condition> ::= <variable>
                      (<value>...)
                      [<Match-Operator>]
                      [<condition-extension>]

      <Match-Operator> ::= <IS-SET-MEMBER’>
                          |<IN-INTEGER-RANGE>
                          |<IP-ADDRESS-AS-RESOLVED-BY-DNS>
                          |<Match-Operator-extension>

      <condition-extension> ::= <i2rs-condition-extension> |
                                ...

      <action> ::= <variable>
                   <value>
                   <Set-Operator>
                   [<action-extension> ]

      <action-extension> ::= <i2rs-action-extension> |
                             ...
```

The elements of the Network-Policy Rule information model are as follows:

- A policy can in turn be part of a hierarchy of policies, building on top of other policies. Each policy is captured in its own level, distinguished via a policy-identity.

- Policy rule inherit scope from policy group. A policy role has a certain Scope, such as read scope or write scope. A policy rule can even have multiple scope simultaneously. The scope, or scopes, are captured in the list of "scope" components.

- Furthermore, a policy rule contains conditions and actions, each captured in their own list.

- A condition contains a variable and a value and use a match operator, to connect variable with value. An examples of an operator might be a" IP ADDRESS AS RESOLVED BYDNS" or "Set to a member". Also, a condition can in turn map onto other condition in an underlay policy. This is captured in list"supporting-condition".

- An action contains a variable and a value. An action uses Set operator to connect variable with value. Analogous to a node, an action can in turn map onto other actions in an underlay policy. This is captured in list "supporting-action".

- The policy, condition, action and operator elements can be extended with policy-specific components (policy-extensions, condition-extension, action-extension and operator-extension respectively).

4.3. The Policy Based Routing Rule Component

4.3.1. Policy based Routing Overview

Policy based Routing is a technique used to make routing decisions based on policies set by the network administrator. PBR enables network administrator to forward the packet based on other criteria than the destination address in the packet, which is used to lookup an entry in the routing table.

The policy based routing problem can be viewed as a resource allocation problem that incorporates business decision.

Policy based routing provides many benefits, including cost saving, load balancing and basic QoS.

Routing decisions in policy based routing are based on several criteria beyond destination address, such as packet size, application, protocol used, and identity of the end system.

Policy constraints are applied before applying QoS constraints since policy constraint overrides QoS constraint.

Policy constraints may be exchanged by routing protocols while updating routing information.

Policy based routing MUST tackle the following difficult questions:

- How is policy management strategy selected? Centralized or distributed.

- At which point in a network domain are policy constraints checked and enforced? i.e., policy coverage, here policy constraint can be exchanged by routing protocol?

- How are policy constraints exchanged within a domain?

- How is policy data stored, refreshed and retrieved from policy repository?

- How are policy rule conflicts avoided?

4.3.2. PBR Rule Component

A PBR rule is constructed using condition, action and attributes that are inherited from Policy Group Component.

```
            +-----------------------+
            |     Policy Rule       |
            +-----------+-----------+
                        ^
                       /|\ "extends"
            +-----------^-----------+
            |       PBR Rule        |
            +--+-----------------+--+
               :                 :
               :                 :     .......
               :                 :     :     :
      +--------V-------+ +-------V-------+   :
      | PBR Condition  | |   PBR Action  |<...
      +----------------+ +-+----------+--+
                          /|\        /|\
                  "extends"|          | "extends"
                       +---+          +--------+
                       |                       |
               +-------^-------+         +-----^---------+
               |  QoS Action   |         |Forward Action |
               +---------------+         +---------------+
                 :     :    :                 :     :    :
             ....:     :    :.....       .....:     :    :.....
             :         :         :       :          :         :
        +----V---+ +---V----+ +--V---+ +-V------++--V-----++--V-----+
        |Set     | |QoS     | |QoS   | |Forward ||Next Hop||Next Hop|
        |Operator| |Variable| |Value | |Operator||Variable||Value   |
        +--------+ +--------+ +------+ +--------++--+-----++--------+
                                                   /|\
                                                    | "extends"
                                                +---^----+
                                                |Next Hop|
                                                |Type    |
                                                +--------+
```

Figure 3: Policy based routing IM structure

4.3.3. Relationship between PBR Rule Model and RIB Information Model

As descried in [I.D-ietf-i2rs-rib-info-model], Routing instance contains a collection of RIBs, interfaces, and routing parameters.

- The set of interfaces indicates which interfaces are associated with this routing instance.

- The RIBs specify how incoming traffic is to be forwarded based on destination.

- the routing parameters control the information in the RIBs/PIBs.

PIB and RIB can not be used at the same time

- If a router doesn’t support policy based routing, a router MUST use rib and MUST not use PIB.

- If a router supports policy based routing,

  * PIB is used if several criteria beyond destination address is matched.

  * RIB is used if several criteria beyond destination address is not matched.

Policy constraints information either comes from RSVP,BGP/IGP, or comes from manual configuration or policy configuration tool. Therefore PIB may has the following field:

- Interface-list: The interface list contains a list of identifiers, with each identifier uniquely identifying an interface.

- Origin: an indication used to identify from which protocols (e.g., ISIS, OSPF, BGP, I2RS, CLI etc.) the policy based route is.

4.4. The Local Config Component

The Local Config Component is the information links to the policy functions associated with a information model it is linked to. This component defines a set of groupings with auxiliary information required and shared by those other components.

Since the I2RS RIB model is the only currently agreed upon model, an example from this model may be helpful. The I2RS RIB model contains a RIB definition of routing instance that has 0-N interfaces and 1-N RIBs. Each RIB contains a set of routes. This policy operates on the elements of I2RS RIB model by combining one of the elements defined in the I2RS RIB model (Routing instance 1, RIB 1, route-attribute) within the context of a policy rule. The [I-D.ietf-i2rs-architecture] shows this as the RIB Policy Controls that impact the policy routing. The I2RS agent may only collect information on this RIB. On Write, the RIB Policy Rules may determine what portion of the Policy-Based RIBs are altered to provide the early exit or service routing features needed by the I2RS client.

The key benefit of this Policy Information Model is that it provides a common model of interactions of policy which can be saved as templates, and then enacted for specific functions associated with another model. The policy element an identity, scope, role, and security model. This allows the specific element to be easily tailor to identified by operations, enable for specific operations (via scope and role), and at a correct security level. As the example demonstrates, this blends with the I2RS RIB model to set conditions and actions. Additional drafts will show that it provides other service routing.

```
      <local-policy-rule> ::= (<local-policy-rule>...)
      <local-policy-rule> ::= <Identity>
                              <priority>
                              <precedence>
                              <Role>
                              (<Condition>)
                              (<Action>...)
                              <Security-Model>

      <Scope> ::= (<Read> [<read-scope>]) |
                        (<Write> [<write-scope>])

      <Role> ::= <Resource> |
                    <Scope>

      <Security-Model> ::= <First-Matching>|
                             <All-Matching>
                               ...
      <condition> ::= <variable>
                        (<value>...)
                        [<Match-Operator>]
                        [<condition-extension>]

      <Match-Operator> ::= <IS-SET-MEMBER'>
                             |<IN-INTEGER-RANGE>
                             |<IP-ADDRESS-AS-RESOLVED-BY-DNS>
                             |<Match-Operator-extension>
      <condition-extension> ::= <i2rs-condition-extension> |
                                 ...

      <action> ::= <variable>
                    <value>
                    <Set-Operator>
                    [<action-extension>]
      <action-extension> ::= <i2rs-action-extension> |
                              ...
```

The model extends the original network-policy model as follows:

- A local policy rule can in turn be part of a hierarchy of policies, building on top of other policies. Each local configuration policy is captured in its own level, distinguished via a policy identity.

- A local policy rule inherit scope from policy group. A local policy rule has a certain Scope, such as read scope or write scope. A local policy rule can even have multiple scope simultaneously. The scope, or scopes, are captured in the list of "scope" components.

- Furthermore, a local policy contains conditions and actions, each captured in their own list.

- A condition contains a variable and a value and use a match operator, to connect variable with value. An examples of an operator might be a" IP ADDRESS AS RESOLVED BYDNS" or "Set to a member". Also, a condition can in turn map onto other condition in an underlay policy. This is captured in list "supporting-condition".

- An action contains a variable and a value. An action uses Set operator to connect variable with value. Analogous to a node, an action can in turn map onto other actions in an underlay policy. This is captured in list "supporting-action".

- The local policy, condition, action and operator elements can be extended with policy-specific components (condition-extension, action-extension and operator-extension respectively).

Drafts that specify examples for this blended I2RS model are:

- An Traffic balancing using the I2RS RIB Model [draft-hares-i2rs-TE-exit-balance]

- Utilizing BGP Information regarding Service Chaining [draft-hares-i2rs-bgp-chains]

- Information model for service topology [draft-hares-i2rs-info-model-service-topo]

- In future revision of I2rs, this may link to other I2RS information models or linked through the I2RS agent to things configured by the CLI, SNMP, or via the NETCONF interface.

5. IANA Considerations

This draft includes no request to IANA.

6. Security Considerations

TBD.

7. Informative References

[I-D.atlas-i2rs-policy-framework]
Atlas, A., Hares, S., and J. Halpern, "A Policy Framework for the Interface to the Routing System", draft-atlas-i2rs-policy-framework-00 (work in progress), February 2013.

[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-02 (work in progress), February 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-02 (work in progress), February 2014.

[I-D.white-i2rs-use-case]
White, R., Hares, S., and A. Retana, "Protocol Independent Use Cases for an Interface to the Routing System", draft-white-i2rs-use-case-02 (work in progress), February 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.

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

[RFC5394] Bryskin, I., Papadimitriou, D., Berger, L., and J. Ash, "Policy-Enabled Path Computation Framework", RFC 5394, December 2008.

[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
Hickory Hill Consulting
7453 Hickory Hill
Saline, CA 48176
USA

Email: shares@ndzh.com

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

Email: sunseawq@huawei.com