I2RS working group
Internet-Draft
Intended status: Standards Track
Expires: November 6, 2016

S. Hares
Huawei
A. Dass
Ericsson
May 5, 2016

# I2RS Data Flow Requirements
# draft-hares-i2rs-dataflow-req-04.txt

Abstract

This document covers requests to the netmod and netconf Working Groups for functionality to support the data flows described in the I2RS architecture and the I2RS use cases requirements summary.

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 November 6, 2016.

Table of Contents



## 1. Introduction

The Interface to the Routing System (I2RS) Working Group is chartered with providing architecture and mechanisms to inject into and retrieve information from the routing system. The I2RS Architecture document [I-D.ietf-i2rs-architecture] abstractly documents a number of requirements for implementing the I2RS requirements.

The I2RS Working Group has chosen to use the YANG data modeling language [RFC6020] as the basis to implement its mechanisms.

Additionally, the I2RS Working group has chosen to use the NETCONF [RFC6241] and its similar but lighter-weight relative RESTCONF [I-D.ietf-netconf-restconf] as the protocols for carrying I2RS. NETCONF and RESTCONF are suitable for handling the configuration portion of the I2RS protocol, but need extensions to handle the I2RS use cases described in [I-D.ietf-i2rs-usecase-reqs-summary]. The requirements for these functionalities have been specified:

- ephemeral state - as defined in [I-D.ietf-i2rs-ephemeral-state]

- notifications and events - as defined in [I-D.ietf-i2rs-pub-sub-requirements]

- traceability - as defined in [I-D.ietf-i2rs-traceability]

- protocol security - as defined in [I-D.ietf-i2rs-protocol-security-requirements]

The requirements for the data flows in the following use cases have not been specified:

Generic interfaces to Protocol Local-RIBs or Policy Data bases,

Large data flows,

Traffic monitoring data,

Data flows for action sequences, and

data flows during network outages or attacks

This document describes the protocol requirements for these last five types of requirements. The first summarizes the data flow requirements for the I2RS protocol version 1, and data flow requirements that may occur in future I2RS protocol versions.

Section 3 provides details on the data flow requirements for the generic interfaces. Section 4 considers large data flows and traffic monitoring data flows. Section 5 considers data flows and constraints during action and attacks.

## 1.1. 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].

## 2. Summary of I2RS Data Flow Requirements

The following are the data flow related requirements for I2RS protocol version 1:

I2RS-DF-REQ-01:No Validation RPCs I2RS generic interfaces in I2RS protocol independent modules or I2RS protocol dependent modules should be able to optionally create rpcs which store configuration data in the I2RS ephemeral data store without the normal configuration checking. The only thing check will be the syntax within the protocol packets. The data models allowing must provide a "no-checking flag" at the level the rpc stores the data. For example, the I2RS RIB could create a rpc for a route-add that

allowed a flag that indicates validation status ("full or no-checks")

I2RS-DF-REQ-02: XML and JSON: encoding formats SHOULD be supported in RESTCONF and NETCONF.

I2RS-DF-REQ-03: Transport Protocols: MAY be negotiated between I2RS client and I2RS agent from a list of mandatory transports and optional transports.

I2RS-DF-REQ-04: Insecure Transport: For a few select data models, the communication between the I2RS client and I2RS agent MAY run over an insecure transports. The I2RS client and I2RS agent should negotiate this insecure protocol, and the portion of the data model which can be sent via the insecure transport SHOULD be marked in YANG data model with "i2rs-insecure-transport ok".

I2RS-DF-REQ-05: Resource Contraints on the I2RS Agent: should have the ability to constraints for OAM functions operating to limit CPU processing, data rate across a transport, the rate of publication of data in a subscription, and logging rates.

I2RS-DF-REQ-06: Alternative Transport protocols or ports: The I2RS should be able to support an OAM actions that select alternate transports from available list of transports, and to support selection of alternate ports for these protocols. The alternate transports may have constraints specified for security levels, sizes of messages, or data flow priorities.

I2RS-DF-REQ-07: Priorization of Data Flows: The I2RS Agent should be able to prioritize some of the management data flows in the I2RS Agent-I2RS Client data flows. This prioriziation can for data schedule for publication, data flows within a single transport, or data flows flows within a single transport, or between multiple data flow streams an I2RS Agent is sending. This priorization may be for the data flows the I2RS Agent is receiving.

DF-REQ-08: Yang indicates rpc with no validation: Yang MUST have a way to indicate rpc can write without validating data except for syntax of data because I2RS client has validated data.

ephemeral-validation nocheck"

DF-REQ-09: Yang for Data sent over insecure transport : Yang MUST have a way to indicate in a data model that insecure transmission is ok.

i2rs-transport-insecure ok"

Requirement for Future versions of I2RS Protocol:

SHOULD be supported as an optional component protocol by the I2RS protocol.

## 3. Generic Interfaces to Routing Functions

The generic interfaces to the routing system includes generic interface to the RIB, forwarding policies, and an interface to the topology information. The existing I2RS protocol independent data models have provided these generic models in the I2RS RIB ([I-D.ietf-i2rs-rib-info-model], [I-D.ietf-i2rs-rib-data-model]), the I2RS Filter-Based RIB ([I-D.kini-i2rs-fb-rib-info-model], [I-D.hares-i2rs-fb-rib-data-model]), and the topology genetric model ([I-D.ietf-i2rs-yang-network-topo]) and plus layer models ([I-D.ietf-i2rs-yang-l2-network-topology], [I-D.ietf-i2rs-yang-l3-topology].

The only addition to the generic model is the ability for the I2RS client to be able to do all of the data value checking, and simply download the data to the I2RS Agent. The I2RS RIB updates are done with rpcs (rib-add, rib-delete, route-add, route-delete, route-update, nh-add, nh-delete). The I2RS FB-RIB updates are done with rpcs (fset-add, fs-dete, fpolicy-add, fpolicy-delete, fpolicy-update, fgroup-add, fgoup-delete, fgroup-update). The requirement is to allow create rpcs that do not require validation, but simply input syntax.

### 3.1. I2RS Data Flow Requirements

[DF-REQ-01:No Validation RPCs I2RS generic interfaces in I2RS protocol independent modules or I2RS protocol dependent modules should be able to optionally create rpcs which store configuration data in the I2RS ephemeral data store without the normal configuration checking. The only thing check will be the syntax within the protocol packets. The data models allowing must provide a "no-checking flag" at the level the rpc stores the data. For example, the I2RS RIB could create a rpc for a route-add that allowed a flag that indicates no validation checks.

## 4. Large Data Flow Requirements

This section decribes the I2RS management data flow requirements for data transfers for large data flows, traffic measurments, and non-secure data flows.

Large data transfers to/from the I2RS Agent can be from tables relating to generic interfaces (RIB, FIB, Filter-Based RIB policy, generic connectivity topologies), protocol state, traffic measurements or user state. The generic interfaces were described in the section above.

The I2RS interaction with the protocol are to configure the protocols, and retrieve general state information (RIB, FIB, topologies and policy). The data flow for the management of protocol state has the same type of flows.

The unique type of data flows are management flows based on traffic flow measurement or I2RS data traveling across insecure connections. These requirements are described in this section.

Traffic monitoring can occur in a network under DDoS with high levels of congestion and loss the use of these protocols which rely on transport-level retransmission may not be as resilient as needed. The data flow problems involved in sending monitoring data during network congestion or outage are considered in section 5 on operations during network outages or congestoin.

## 4.1. Use Case Requirements for Traffic Flow Measurements

The I2RS requirements for the Protocol independent use cases requires the support of traffic flow measurements protocols (requirements PI-REQ-05, PI-REQ06 in [I-D.ietf-i2rs-usecase-reqs-summary]), and operational state regarding flow filtering.

The following IETF protocol pass traffic flow measurements:

- IPFIX - IP Flow Information ([RFC7011]) that reports on a wide variety of routing system statistics, and

- IPPM - IP Performance mangement ([RFC2330], [RFC7312]) that reports on one-way or two-way end-to-end network performance statistics,

In addition the SFLOW([RFC3176]) of layer 2 devices is supported by many routers. Other traffic flows may be measured in support of IDS/IPS, but these will be covered in the section on security flows.

Flow Filtering data models with policy rules (BGP Flow Specification, I2RS Filter-Based RIB, and n-tuple policy routing RIB) often save operational state on how often these policies are match.

Traffic flow data can provide large streams of traffic. The I2RS mechanism for handling the data bursts in these protocols is to

utilize a traffic monitoring protocol, IPFIX) or to utilize a publication/subscription service in order to send just what clients want.

## 4.2. Protocol Requirements based on Traffic Measurement Data Flows

Due to the potentially large data flow the traffic measurment statistics generate, these statistics are best handled by publication techniques within NETCONF or a separate protocol such as IPFIX. The publication/subscription model within NETCONF could use either push pub-sub model or a pull pub-sub model. Thresholds for reporting can be set per data models or per client so the pub-sub model allows the I2RS client-I2RS Agent to meter the amount of data flow these statistics carry. The push portion of the pub-sub model is supported by [I-D.ietf-netconf-yang-push], but the pull portion of the pub-sub model is not defined.

The support of IPFIX protocol ([RFC7011]) as a component protocol in I2RS requires the I2RS Agent supports an IPFIX exporting process sending data to a I2RS client running an IPFIX collector process. The IPFIX templates could be stored as ephemeral state or reference configured state. The IPFIX data flows may run over SCTP, UDP, or TCP utilizing the congestion services at each time. The IPFIX connections assumes that: a) congestion is an temporary anomaly, b) dropping data during a congestion is reported, and c) for some exporiting process it is acceptable to have drop data in a reliable protocol. The I2RS protocol must support the establishment of an IPFIX connection.

## 4.3. Publication/Subscription Service

All use case requirements for the publication/subscription service for the push service from large data requirements 01-04 and 6-12 is found in [I-D.ietf-i2rs-pub-sub-requirements], and an example protocol addition to netconf is include in [I-D.ietf-netconf-yang-push].

The requirements for the publication/subscription service for the pull model are not specified in the [I-D.ietf-i2rs-pub-sub-requirements], but a majority of the pub-sub requirements and mechanisms can be reused. In a pull, the publisher prepares the data that is pulled by a few receivers who then distribute it to the receivers. The pull mechanism would have a different "pull latency" versus the push latencey, and a set of parameters which indicate the amount of data stored if receivers did not pull the data within a certain time.

At this time, the pull-model of the publication/subscription model is not being requested by vendors or operators.

### 4.4. Data Flow Requirements for Transports

The use case requirements ([I-D.ietf-i2rs-usecase-reqs-summary]) for large data flows also include support for data flows via any transport (L-Dat-REQ-04) and any data format (L-Data-REQ-05).

One of the requirements is to be able to support an insecure transport for a small set of data. Examples of this type of data may be outage/restoration information the operator wishes to make public.

### 4.5. I2RS Requirements for Large Data Flow

Current Data Flow Requirements:

I2RS-DF-REQ-02: XML and JSON: encoding formats SHOULD be supported in RESTCONF and NETCONF.

I2RS-DF-REQ-03: Transport Protocols: MAY be negotiated between I2RS client and I2RS agent from a list of mandatory transports and optional transports.

I2RS-DF-REQ-04: Insecure Transport: For a few select data models, the communication between the I2RS client and I2RS agent MAY run over an insecure transports. The I2RS client and I2RS agent should negotiate this insecure protocol, and the portion of the data model which can be sent via the insecure transport SHOULD be marked in YANG data model with "i2rs-insecure-transport ok".

Future Data Flow Requirements:

Future-DF-REQ-01: IPFIX Protocol and templates: SHOULD be supported as an optional component protocol by the I2RS protocol.

## 5. I2RS Data Flow during OAM or Outages

The data flow requirements for Operations and Management (OAM) actions must be able to be constrained in order not to impact the routing system. During periods of normal connectivity, it is important that any OAM function not impact the the routing systems function. During periods of outage, the I2RS protocol must operate when data bandwidth is reduced and network connectivity fluctuates. The constraints on the I2RS client-agent communication may be increased or decreased from the normal state depending on what management traffic needs to flow in order to help detect outages or resist attacks.

I2RS agents must be able to adjust operation of event notifications, logging, or data traffic during these outage periods. Data Models and I2RS agent configuration must allow operator-applied policy to prioritize data during this period. The I2RS Agent should be able to signal the I2RS Client that such a time period is occuring.

A quick list of some of the types of outages may illustrate why the I2RS agent need the ability to balance internal processing and the rate of communication with the I2RS client. Network Outages may occur due connectivity failures or security attacks. Security attacks can be distributed or target incidents that exploit vulnerabilities in software, network devices, protocols using botnets, malware attacks, identity theft, port spams, icmp blasts, and other attacks. Some outages are caused by Distributed Denial of Service (DDoS) attacks may impact multiple routing systems so the constraints on management data flow may be required even when the routing system is not the specific device under attack.

## 5.1. I2RS Data Flow Requirements during OAM or Outages

I2RS-DF-REQ-05: Resource Contraints on the I2RS Agent: should have the ability to constraints for OAM functions operating to limit CPU processing, data rate across a transport, the rate of publication of data in a subscription, and logging rates.

I2RS-DF-REQ-06: Alternative Transport protocols or ports: The I2RS should be able to support an OAM actions that select alternate transports from available list of transports, and to support selection of alternate ports for these protocols. The alternate transports may have constraints specified for security levels, sizes of messages, or priority

I2RS-DF-REQ-07: Priorization of Data Flows: The I2RS Agent should be able to prioritize some of the management data flows in the I2RS Agent-I2RS Client data flows. This prioriziation can for data schedule for publication, data flows within a single transport, or data flows flows within a single transport, or between multiple data flow streams an I2RS Agent is sending.

## 6. Changes to YANG

To support the above requirements, the yang modules will need to support the following features:

DF-REQ-08: Yang indicates rpc with no validation: Yang MUST have a way to indicate rpc can write without validating data except for syntax of data because I2RS client has validated data.

ephemeral-validation nocheck"

DF-REQ-09: Yang for Data sent over insecure transport : Yang MUST have a way to indicate in a data model that insecure transmission is ok.

i2rs-transport-insecure ok"

## 7. IANA Considerations

There are no IANA requirements for this document.

## 8. Security Considerations

The security requirements for the I2RS protocol are covered in [I-D.ietf-i2rs-protocol-security-requirements] document.

## 9. Acknowledgements

The following people have aided in the discuss

- Russ White,
- Joel Halpern,
- Linda Dunbar,
- Frank Xia, and
- Robert Moskowitz

## 10. References

### 10.1. 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, <http://www.rfc-editor.org/info/rfc2119>.

### 10.2. Informative References

[I-D.hares-i2rs-fb-rib-data-model] Hares, S., Kini, S., Dunbar, L., Krishnan, R., Bogdanovic, D., and R. White, "Filter-Based RIB Data Model", draft-hares-i2rs-fb-rib-data-model-03 (work in progress), March 2016.

[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-15 (work in progress), April 2016.

[I-D.ietf-i2rs-ephemeral-state]
Haas, J. and S. Hares, "I2RS Ephemeral State Requirements", draft-ietf-i2rs-ephemeral-state-05 (work in progress), March 2016.

[I-D.ietf-i2rs-protocol-security-requirements]
Hares, S., Migault, D., and J. Halpern, "I2RS Security Related Requirements", draft-ietf-i2rs-protocol-security-requirements-03 (work in progress), March 2016.

[I-D.ietf-i2rs-pub-sub-requirements]
Voit, E., Clemm, A., and A. Prieto, "Requirements for Subscription to YANG Datastores", draft-ietf-i2rs-pub-sub-requirements-07 (work in progress), May 2016.

[I-D.ietf-i2rs-rib-data-model]
Wang, L., Ananthakrishnan, H., Chen, M., amit.dass@ericsson.com, a., Kini, S., and N. Bahadur, "A YANG Data Model for Routing Information Base (RIB)", draft-ietf-i2rs-rib-data-model-05 (work in progress), March 2016.

[I-D.ietf-i2rs-rib-info-model]
Bahadur, N., Kini, S., and J. Medved, "Routing Information Base Info Model", draft-ietf-i2rs-rib-info-model-08 (work in progress), October 2015.

[I-D.ietf-i2rs-traceability]
Clarke, J., Salgueiro, G., and C. Pignataro, "Interface to the Routing System (I2RS) Traceability: Framework and Information Model", draft-ietf-i2rs-traceability-09 (work in progress), May 2016.

[I-D.ietf-i2rs-usecase-reqs-summary]
Hares, S. and M. Chen, "Summary of I2RS Use Case Requirements", draft-ietf-i2rs-usecase-reqs-summary-02 (work in progress), March 2016.

[I-D.ietf-i2rs-yang-l2-network-topology]
Dong, J. and X. Wei, "A YANG Data Model for Layer-2 Network Topologies", draft-ietf-i2rs-yang-l2-network-topology-02 (work in progress), December 2015.

[I-D.ietf-i2rs-yang-l3-topology]
Clemm, A., Medved, J., Varga, R., Tkacik, T., Liu, X., Bryskin, I., Guo, A., Ananthakrishnan, H., Bahadur, N., and V. Beeram, "A YANG Data Model for Layer 3 Topologies", draft-ietf-i2rs-yang-l3-topology-01 (work in progress), December 2015.

[I-D.ietf-i2rs-yang-network-topo]
Clemm, A., Medved, J., Varga, R., Tkacik, T., Bahadur, N., and H. Ananthakrishnan, "A Data Model for Network Topologies", draft-ietf-i2rs-yang-network-topo-02 (work in progress), December 2015.

[I-D.ietf-netconf-restconf]
Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", draft-ietf-netconf-restconf-13 (work in progress), April 2016.

[I-D.ietf-netconf-yang-push]
Clemm, A., Prieto, A., Voit, E., Tripathy, A., and E. Einar, "Subscribing to YANG datastore push updates", draft-ietf-netconf-yang-push-02 (work in progress), March 2016.

[I-D.kini-i2rs-fb-rib-info-model]
Kini, S., Hares, S., Dunbar, L., Ghanwani, A., Krishnan, R., Bogdanovic, D., and R. White, "Filter-Based RIB Information Model", draft-kini-i2rs-fb-rib-info-model-03 (work in progress), February 2016.

[RFC2330] Paxson, V., Almes, G., Mahdavi, J., and M. Mathis, "Framework for IP Performance Metrics", RFC 2330, DOI 10.17487/RFC2330, May 1998, <http://www.rfc-editor.org/info/rfc2330>.

[RFC3176] Phaal, P., Panchen, S., and N. McKee, "InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks", RFC 3176, DOI 10.17487/RFC3176, September 2001, <http://www.rfc-editor.org/info/rfc3176>.

[RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <http://www.rfc-editor.org/info/rfc6020>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <http://www.rfc-editor.org/info/rfc6241>.

[RFC7011] Claise, B., Ed., Trammell, B., Ed., and P. Aitken, "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information", STD 77, RFC 7011, DOI 10.17487/RFC7011, September 2013, <http://www.rfc-editor.org/info/rfc7011>.

[RFC7312] Fabini, J. and A. Morton, "Advanced Stream and Sampling Framework for IP Performance Metrics (IPPM)", RFC 7312, DOI 10.17487/RFC7312, August 2014, <http://www.rfc-editor.org/info/rfc7312>.

## Authors' Addresses

Susan Hares
Huawei
Saline
US

Email: shares@ndzh.com

Amit Daas
Ericsson

Email: amit.dass@ericsson.com