I2RS working group
Internet-Draft
Intended status: Standards Track
Expires: September 17, 2016

S. Hares
Huawei

March 16, 2016

I2RS Data Flow Requirements
draft-hares-i2rs-dataflow-req-02.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 September 17, 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 include:

- 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]
- 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 section summarizes the data flow requirements. Section 2 details how the I2RS use case requirements for Generic interfaces to protocol RIBS or policy data base do not add any requirements to the I2RS protocol. Section 3 describes how the describes

2. Summary of I2RS Data Flow Requirements

Additional requirements from Generic Interface:None

The additional Data flow requirements are:

DF-REQ-01: Support writing to the ephemeral copy of the Local RIB with three different types of checks: minimal data reception checks (TLVs of data oacket valid), all non-referential checks (e.g. do not do leafref, MUST, instance identifiers), and do referential checks via three different rpcs.

DF-REQ-02: The support of large data transfers in a data format agnostic format. This the I2RS protocol should support transport of data in any format including: XML, JSON, MTL (ALias/Waveformat, .mtl), protobufs, and ascii text.

DF-REQ-03: Support of I2RS Agent and I2RS Client negotiating specific transport and transport options,

DF-REQ-04: Support for the ability to send traffic monitoring information using IPFIX protocol and IPFIX templates,

DF-REQ-05: Support of transmitting traffic statistics for filter-based policies (BGP-FS, I2RS FB-RIB, policy routing), IPPM, SFLOW, and others in yang data model format or IPFIX templates formats over XML or JSON.

DF-REQ-06: I2RS should be able to support an action which allocates internal resources for the I2RS agent (memory, processing time, interrupts) and outbound data flow bandwidth. It is expected that an action would be included in a data model in an "rpc"-like format in yang.

DF-REQ-07: The I2RS should be able to support an action that interacts with routing OAM functions.

DF-REQ-08:I2RS Agent must be able signals that it will be using different protocol with different constraints (security, priority of data, or transport) or different constraints on the existing protocol (smaller message sizes, different priorities on data carried, or different security levels).

DF-REQ-09: Yang MUST have a way to indicate in a data model has actions which allow: different transports, different resource constraints, or different security.

DF-REQ-10: Yang MUST have a way to indicate a data model has different levels of checking where: lowest level is message form only, medium level checks message format plus data syntax, and highest level uses the message format, data syntax and referential check netconf configuration does. The default level for I2RS is message format plus data syntax.

3. Generic Interfaces to Routing Functions

The I2RS use case requirement suggests that a generic interface be created to protocol local RIBs and a generic interface be available to configure policies.

3.1. I2RS-Generic Interface to Local-RIB

The I2RS requirements ([I-D.ietf-i2rs-usecase-reqs-summary]) require that a generic interface be defined to the local-RIB in protocols. This type of data flow does not require a new type of data flow, but

the definition of a new data model that creates a generic local RIB and has operations to funnel this generic Local-RIB to a specific protocol.

The Protocol Independent Use case (PI-REQ-11) Local RIB use case suggest the I2RS protocol has three levels of checks: minimal data reception checks (TLVs of data align), all non-referential checks (e.g. do not do leafref, MUST, instance identifiers), and do referential checks. This feature could be supported through different rpc calls to the LOCAL RIB.

3.2. I2RS-Generic interfaces to Policies

The I2RS requirements suggest that I2RS have a generic interface to routing policies for protocols, routing distribution, or routing protocols. This generic interface is currently being implemented as common definitions for data models. At this time, This generic interface does not need additional protocol requirements.

3.3. I2RS Data Flow Requirements

[DF-REQ-01] Support writing to the ephemeral copy of the Local RIB with three different types of checks: minimal data reception checks (TLVs of data oacket valid), all non-referential checks (e.g. do not do leafref, MUST, instance identifiers), and do referential checks via three different rpcs.

4. Large Data Flow Requirements

This section decribes the data flow requirements for large data flows, traffic flows measurements, CDNI traffic flows, OAM and Action rqeuests, data flows during outages or network attacks (DDoS (Distributed Denial of Service) or other network attacks), and non-secure data flows. These data flows are data flows which are not configuration based data flows.

4.1. Large Data Flow Use Case Requirements

The I2RS use case for Large Data Collection systems [I-D.ietf-i2rs-usecase-reqs-summary] requires the I2RS protocol and data models:

- be able to be done at a high frequency and resolution with minimal impact to devices memory or CPU (L-Data-REQ-01) ,
- use a data model which allows definition of the form as part of the data model (L-Data-REQ-02) ,

- support a publication/subscription mechanism with push/pull mechanism (L-Data-REQ-03),

- (supports capability negotiation for level of transport, security, and error handling as a general configurations, per I2RS client-agent protocol for all interfaces and all time instance, or per I2RS interface client-agent protocol per specific interface or per time instances. (L-Data-REQ-04,L-Data-REQ-06, L-Data-REQ-07, L-Data-REQ-08, and L-Data-REQ-09),

- dynamic subscription model set-up via IPFIX (L-REQ-12c),

- support of subscriber and consumer I2RS-Agent pairs (L-REQ-12d),

- remapping of Node’s databases,

- data format agnostic (L-Data-REQ-05),

- data models and I2RS protocol additions that support of query, introspection using data-base model that support a set of capabilities, data filters, and error handling (stale data, repeated transport failures, and other errors.) Introspection supports data verification, inclusion of legacy data, and merging of data flows based on meta-data. (L-Data-REQ-11, L-Data-REQ-13),

- Support of push of data synchronously or asyncronously via registered subscriptions (L-Data-REQ-12a).

- Pull of data in one-shot or multiple sequences (L-Data-REQ-12b), and

- dynamic subscription model set-up via IPFIX Feed (L-REQ-12c)

4.1.1. Data Requirements Supported in pub-sub Requirements

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.

4.1.2. Data Flow Requirements Outside of Pub/Sub Requirements

The data flow requirements for large data flows also include support for data flows outside of publication/subscription via any transport (L-Dat-REQ-04) and any data format (L-Data-REQ-05). Support for the IPFIX protocol or just the IPFIX data formats is required.

4.1.3. I2RS Data Flow Requirements

The following requirements are additional data flow requirements for large data flows.

(DF-REQ-02): Support of any data format including: XML, JSON, (MTL (Alias/WaveFormat,.mtl), protobufs, and ascii,

DF-REQ-03: Support of I2RS Agent and I2RS Client negotiating specific transport and transport options,

(DF-REQ-04): support of the ability send information using IPFIX templates as a reporting structure over the IPFIX protocol.

[I-D.ietf-netconf-yang-push] supports XML and JSON in its first release, and provides an ability to register extra formats, but these requirements should also support large data flows sent outside of the publication-subscription service.

4.2. Traffic Flow Measurements

The I2RS requirements for the Protocol independent use cases requires the support off interactions with traffic flow and other network management Protocols (requirements PI-REQ-05, PI-REQ06) in [I-D.ietf-i2rs-usecase-reqs-summary]).

The following IETF protocol pass traffic related information:

- BGP Flow Specification (BGP-FS) ([RFC5575]
- 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.

Additional traffic flow models are being defined to configure traffic flow policy and to monitor the statistics on the use of the traffic flow statistics:

- BGP Flow Specification (BGP-FS) yang model [I-D.wu-idr-flowspec-yang-cfg] contains flow filter match statistics.

- I2RS Filter-Based RIB yang model ([I-D.kini-i2rs-fb-rib-info-model], [I-D.hares-i2rs-fb-rib-data-model])- yang model contains ephemeral flow statistics,

- Filter-Based RIB (draft-hares-rtgwg-fb-rib-data-model) contains both flow filter match statistics,

4.2.1. Protocol Requirements based on Traffic Flows

Due to the potentially large data flow these statistics should be handle by push pub-sub model or a pull pub-sub model. Thresholds for data models may be passed by the event portion of the push/pull pub-sub model. The pub-sub model will allow 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.

Alternatively I2RS can use the the IPFIX protocol ([RFC7011]) as a component protocol. I2RS processes can support an IPFIX exporting process sendinging dta to a node to a node on a collector process. The IPFIX templates can be configured as ephemeral state or configuration 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.

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 for network security functions (NSF). These are considered in section 5 on operations during network outages or congestoin.

The Flow Filtering data models with policy rules (BGP Flow Specification, I2RS Filter-Based RIB, and n-tuple policy routing RIB) often track how often these policies are match. These statistics can also be pushed/pulled in a publication/subscription with yang data-model defined format or an IPFIX exporting process format. Similarly IPPM statistics or SFLOW data, be sent via publication/subscription service in yang data model format or in a IPFIX Template or as XML or JSON representation of a yang data model. These additional sources do not change the requirements for the push publication/subscription or expand the

Summary: The pub-sub model push or pull may have to support additional formats (E.g. SFLOW, IPFIX) as well as yang data models.

4.2.2. I2RS Data Flow Requirements

DF-REQ-04: Support for the ability to send traffic monitoring information using IPFIX protocol and IPFIX templates,

(DF-REQ-05): Support of traffic statistics for filter-based policies (BGP-FS, I2RS FB-RIB, policy routing), IPPM, SFLOW, and others in yang data model format or IPFIX template formats over XML or JSON.

4.3. Action sequences in Data Models

Several of the I2RS requirements from the use cases require a sequence of events with the following actions:

1. query data in protocol independent model (topology, RIB, Filter-RIB), or protocol),
2. start calculation (or re-calculation) in protocol function,
3. Report results,
4. install topology or RIB calculated,
5. check results,
6. recycle.

The actions included looking for overlapping BGP routes, IGP LFA calculation, ECMP load balancing traffic, optimizing paths via MPLS-TE, CCNE re-optimization, and virtual topology creation.

An alternate pattern within the requirements is if the topology is calculated off-line, and uploaded.

These action patterns may involve an interaction of the I2RS action sequences with existing OAM functions in the routing system.

NETCONF/RESTCONF have the concepts of an "rpc" for a configuration enabled action, but these action sequences should have the abilty to have the following characteristics:

- o the ability to request a reservation of resources for this effort so the action sequence does not start unless there is enough calculation or response bandwidth in a node,

- o the abilty ability to have validation on off-line calculated data so this critical data does not have errors

- o the ability to "prioritize" notification or reports ahead of other I2RS data streams to allow process to work.

4.3.1. I2RS Data Flow Requirement

I2RS-DF-REQ-06: I2RS should be able to support an action which allocates internal resources for the I2RS agent (memory, processing time, interrupts) and outbound data flow bandwidth. It is expected that an action would be included in a data model in an "rpc"-like format in yang.

DF-REQ-07: The I2RS should be able to support an action that interacts with routing OAM functions.

4.4. Operation during network outages or attacks

The router needs dynamic management during periods of outage or periods of security attack.

4.4.1. Periods of Network Outage

During periods of outage, the I2RS protocol must operate when data bandwidth is reduced and network connectivity fluctuates. I2RS agents must be able to adjust operation of event notifications, logging, or data traffic during this period. 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.

4.4.2. I2RS Data Flow Requirements

DF-REQ-08: The I2RS Agent must be able signals that it will be using different protocol with different constraints (security, priority of data, or transport) or different constraints on the existing protocol (smaller message sizes, different priorities on data carried, or different security levels).

5. Changes to YANG

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

- DF-REQ-09: Yang MUST have a way to indicate in a data model has actions which allow: different transports, different resource constraints, or different security.

- DF-REQ-10: Yang MUST have a way to indicate a data model has different levels of checking where: lowest level is message form only, medium level checks message format plus data syntax, and highest level uses the message format, data syntax and referential check netconf configuration does. The default level for I2RS is message format plus data syntax.

6. IANA Considerations

There are no IANA requirements for this document.

7. Security Considerations

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

8. Acknowledgements

The following people have aided in the discuss

- Russ White,and

- Robert Moskowitz.

9. References

9.1. 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>.

9.2. 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-02 (work in progress), February 2016.

[I-D.ietf-dots-requirements] Mortensen, A., Moskowitz, R., and T. Reddy, "DDoS Open Threat Signaling Requirements", draft-ietf-dots-requirements-00 (work in progress), October 2015.

[I-D.ietf-i2nsf-problem-and-use-cases] Hares, S., Dunbar, L., Lopez, D., Zarny, M., and C. Jacquenet, "I2NSF Problem Statement and Use cases", draft-ietf-i2nsf-problem-and-use-cases-00 (work in progress), February 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-13 (work in progress), February 2016.

[I-D.ietf-i2rs-ephemeral-state] Haas, J. and S. Hares, "I2RS Ephemeral State Requirements", draft-ietf-i2rs-ephemeral-state-04 (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-05 (work in progress), February 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-07 (work in progress), February 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-01 (work in progress), May 2015.

[I-D.ietf-mile-rfc5070-bis]
Danyliw, R., "The Incident Object Description Exchange Format v2", draft-ietf-mile-rfc5070-bis-16 (work in progress), February 2016.

[I-D.ietf-netconf-restconf]
Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", draft-ietf-netconf-restconf-09 (work in progress), December 2015.

[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-01 (work in progress), February 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.

[I-D.wu-idr-flowspec-yang-cfg]
Wu, N., Zhuang, S., and A. Choudhary, "A YANG Data Model for Flow Specification", draft-wu-idr-flowspec-yang-cfg-02 (work in progress), October 2015.

[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>.

[RFC5070] Danyliw, R., Meijer, J., and Y. Demchenko, "The Incident Object Description Exchange Format", RFC 5070, DOI 10.17487/RFC5070, December 2007, <http://www.rfc-editor.org/info/rfc5070>.

[RFC5575] Marques, P., Sheth, N., Raszuk, R., Greene, B., Mauch, J., and D. McPherson, "Dissemination of Flow Specification Rules", RFC 5575, DOI 10.17487/RFC5575, August 2009, <http://www.rfc-editor.org/info/rfc5575>.

[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>.

[RFC6536] Bierman, A. and M. Bjorklund, "Network Configuration Protocol (NETCONF) Access Control Model", RFC 6536, DOI 10.17487/RFC6536, March 2012, <http://www.rfc-editor.org/info/rfc6536>.

[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>.

Author's Address

Susan Hares
Huawei
Saline
US

Email: shares@ndzh.com