Internet Engineering Task Force (IETF)
Request for Comments: 7920
Category: Informational
ISSN: 2070-1721

A. Atlas, Ed.
Juniper Networks
T. Nadeau, Ed.
Brocade
D. Ward
Cisco Systems

June 2016

Problem Statement for the Interface to the Routing System

Постановка задачи для интерфейса в систему маршрутизации

Аннотация

Традиционно системы маршрутизации реализуют сигнализацию (например, MPLS) и маршрутизацию для управления трафиком, пересылаемым в сеть. Расчёт маршрутов контролируется относительно статическими правилами, определяющими стоимость каналов и маршрутов или политику импорта-экспорта маршрутов. Появление динамичных сетей центров обработки данных (ЦОД), услуг WAN по запросам, динамического управления трафиком на основе правил, объединения (цепочек) услуг, а также необходимость защиты в реальном масштабе времени для всего трафика и парадигма отделения принятия решений от самих маршрутизаторов вызвали потребности в более динамичном управлении и программировании систем маршрутизации. Это должно разрешить контроль над данными маршрутизации и путями трафика, а также извлечение сведений о сетевой топологии, статистике трафика и другой сетевой аналитики из систем маршрутизации.

В этом документе предлагается реализовать эти потребности через интерфейс с системой маршрутизации (Interface to the Routing System или I2RS).

Статус документа

Документ не относится к категории Internet Standards Track и публикуется лишь для информации.

Документ является результатом работы IETF[1] и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG[2]. Не все документы, одобренные IESG, претендуют на статус стандартов. Дополнительную информацию о стандартах Internet можно найти в разделе 2 RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке http://www.rfc-editor.org/info/rfc7920.

Оглавление

1. Введение

Традиционно системы маршрутизации реализуют сигнализацию (например, MPLS) и маршрутизацию для управления трафиком, пересылаемым в сеть. Расчёт маршрутов контролируется относительно статическими правилами, определяющими стоимость каналов и маршрутов или политику импорта-экспорта маршрутов. Появление динамичных сетей центров обработки данных (ЦОД), услуг WAN по запросам, динамического управления трафиком на основе правил, объединения (цепочек) услуг, а также необходимость защиты в реальном масштабе времени для всего трафика и парадигма отделения принятия решений от самих маршрутизаторов вызвали потребности в более динамичном управлении и программировании систем маршрутизации.

[1]Internet Engineering Task Force - комиссия по решению инженерных задач Internet.
[2]Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

Поскольку масштабы и сложность современных сетей продолжают расти, а желаемая политика становится всё сложнее и динамичней, требуется поддержка быстрого контроля и аналитики. Масштабы современных сетей и ЦОД, а также связанные с ними операционные расходы требуют автоматизации даже простейших операций. Возможность быстрого взаимодействия с помощью более сложных операций для поддержки динамических правил ещё важнее.

Чтобы сетевые приложения имели доступ и контроль над сведениями из систем маршрутизации разных производителей, нужен интерфейс с общедоступной документацией. Интерфейс должен поддерживать асинхронные взаимодействия в реальном масштабе времени, используя эффективные модели данных и кодирование, основанные на расширении заданных ранее. Кроме того, интерфейс должен обеспечивать прочную основу для различных вариантов возможного применения.

Для поддержки требований оркестрации программ и автоматизированных сетевых приложений динамического изменения сетей требуется изучение топологии, сетевой аналитики и имеющихся состояний сети, а также создание или обновление маршрутной информации и сетевых путей. Нужен контур обратной связи для проверки изменений и обучения приложений с целью изучения и реагирования на изменения в сети.

Фирменные (proprietary) решения для частичного выполнения означенных требований были разработаны под конкретные ситуации и задачи. Стандартизация интерфейса с системой маршрутизации упростит её интеграцию в сеть. Наличие фирменных частных решений позволяет считать задачу стандартизации общего интерфейса разрешимой.

Следует отметить, что в этом документе термин «приложение» (applications) используется для исполняемых программ того или иного вида, имеющих доступ в сеть (например, IP или MPLS) через систему маршрутизации.

2. Модель I2RS и область задач для IETF

Управление сетью систем, работающих с разными протоколами маршрутизации и/или предоставляющих дополнительные услуги (например, пересылку, классификацию и контроль, межсетевое экранирование), включает взаимодействие между множеством компонентов этих систем. Некоторые из этих систем или системных компонентов могут быть виртуализованными, размещёнными в одной физической системе или распределёнными. Во всех случаях желательно разрешать сетевым приложениям управлять и контролировать услуги, предоставляемые многими (если не всеми) компонентами в соответствии с аутентифицированным и полномочным доступом и правилами.

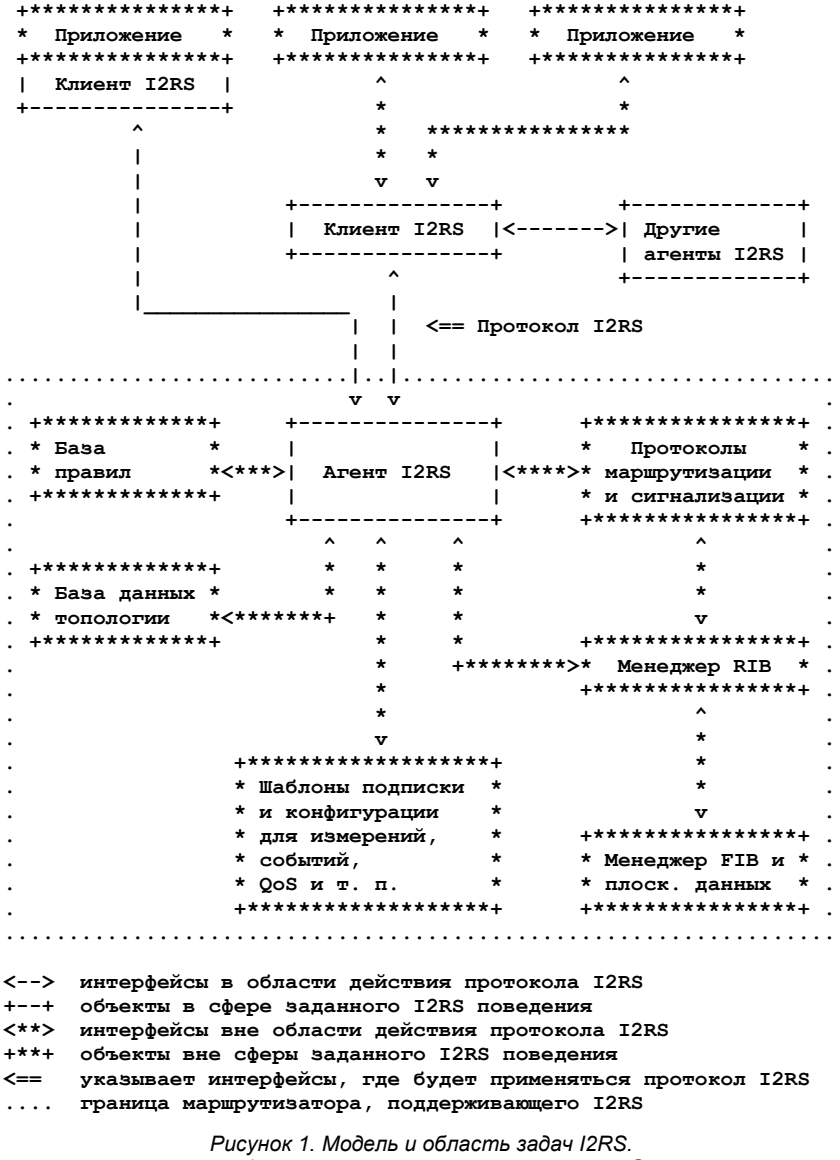

Рисунок 1. Модель и область задач I2RS.

Нужен управляемый моделью данных интерфейс с системой маршрутизации. Это позволит увеличить объем сведений, которые можно считывать и контролировать, а также обеспечит гибкость в будущем. Нужен хотя бы один сопроводительны протокол с чётко заданными операциями. Подходящие протоколы могут бать идентифицированы и расширены для поддержки требований к интерфейсу I2RS. Нужно разработать решения для облегчения быстрых,

изолированных, защищённых и динамичных изменений в системе маршрутизации устройств. Это будет способствовать широкому внедрению функционально совместимых приложений и систем маршрутизации.

Модель I2RS и область задач для работы IETF показаны на рисунке 1. В документе применяется терминология из [RFC7921]. Агент I2RS связан с маршрутизирующим элементом, который может быть размещён вместе с плоскостью данных. Клиент I2RS может быть интегрирован в сетевое приложение или контролироваться и применяться одним или несколькими отдельными сетевыми приложениями. Например, клиент I2RS может быть предоставлен контроллером сети или системой оркестровки, которая обеспечивает отличный от I2RS интерфейс для сетевых приложений и интерфейс I2RS с агентами I2RS на управляемых системах. Область действия моделей данных, применяемых I2RS, охватывает всю систему маршрутизации и выбранные протоколы для I2RS.

Как показано на рисунке 1, клиент I2RS и агент I2RS в системе маршрутизации являются объектами области действия I2RS. Выбранные протоколы для I2RS размещаются между клиентом и агентом I2RS. Остальные объекты на рисунке 1 выходят за рамки стандартизации I2RS. Протоколам передачи сообщений между клиентами и агентами I2RS следует поддерживать основные свойства, указанные в разделе 5. Аспекты, рассматриваемые для протокола I2RS.

I2RS будет применять набор значимых моделей данных для информации в системе маршрутизации и базе данных топологии. Каждой модели данных следует описывать назначение и связи моделируемых элементов. Модели данных следует разделять по свойствам управляемых компонентов, иметь версии и поддерживать расширение. Как показано на рисунке 1, I2RS нужно взаимодействовать с несколькими логическими компонентами маршрутизирующего элемента - базой правил, топологической базой, настройкой и подпиской на динамические измерения и события, протоколам маршрутизации и сигнализации и их менеджером RIB. Эти взаимодействия включают как запись (например, в базу правил или менеджер RIB), так и чтение (например, динамические измерения или база данных топологии). Приложению следует иметь возможность комбинировать данные от отдельных элементов маршрутизации для обеспечения моделей данных в масштабе сети.

Моделям данных следует поддерживать трансляцию в сжатый (concise) синтаксис передачи для отправки по протоколу I2RS, который прост в применении для приложений (например, для парадигмы создания web-приложений). При передаче информации следует применять имеющиеся транспортные протоколы, обеспечивающие отказоустойчивость, безопасность и своевременную доставку, подходящие для конкретных данных.

3. Стандартные модели данных состояния маршрутизации

Как указано в разделе 1, необходима возможность точно контролировать состояние маршрутизации и сигнализации на основе правил или внешних мер. Одним из наборов моделей данных, на котором следует сосредоточить I2RS, предназначен для взаимодействия с уровнем RIB (например, RIB, LIB[1], групповая RIB, маршрутизация на основе правил) для обеспечения гибкости и абстракций маршрутизации. Например, желаемое состояние маршрутизации и сигнализации может варьироваться от простых статических маршрутов до маршрутизации на основе правил и статической групповой репликации и статуса маршрутизации. Это значит, что для эффективного моделирования следующего узла (nexthop) применяемая модель данных должна обрабатывать косвенность (indirection) nexthop и рекурсию (например, префикс X маршрутизируется аналогично префиксу Y), а также разные типы туннелирования и инкапсуляции.

Усилия по обеспечению такого уровня контроля были сосредоточены на стандартизации моделей данных, описывающих плоскость пересылки (например, ForCES[2] [RFC3746]). I2RS признает, что система маршрутизации и ОС маршрутизатора обеспечивают полезные механизмы, которые приложения могут применять для достижения целей на своём уровне. Применение косвенности маршрутов, рекурсии и базовых абстракций маршрутизации (например, туннелей, LSP[3] и т. п.) обеспечивает значительную гибкость и функциональность по сравнению с отдельными маршрутами в FIB, которые нужно менять индивидуально при возникновении изменений.

В дополнение к интерфейсам управления уровнем RIB нужно динамически настраивать правила и значения параметров для различных протоколов маршрутизации и сигнализации на основе решений политики прикладного уровня.

4. Изучение сведений от маршрутизаторов

У маршрутизатора имеются сведения, которые могут потребоваться приложениям для понимания сети, проверки установленного программируемого состояния, измерения поведения различных потоков и понимания существующей конфигурации и статуса маршрутизатора. I2RS следует предоставлять приложениям модель для регистрации на получение асинхронных уведомлений и запроса конкретной информации.

Хотя попытки расширить доступную технологическую информацию предпринимаются, даже лучшие из них (например, , BGP-LS [RFC7752]) по-прежнему предоставляют лишь текущее активное состояние, наблюдаемое на уровнях IGP и BGP. Приложениям нужно подробное состояние топологии с большим объёмом информации (например, активные пути и каналы). Примеры отсутствующих сведений включают пути или каналы (например, отключённые административно), которые потенциально доступны или неизвестны (например, партнёры или клиенты) топологии маршрутов.

Чтобы у приложений была обратная связь, осведомленная о соответствующем трафике, приложение должно иметь возможность запросить измерение и своевременные, масштабируемые отчёты о результатах. Хотя такие механизмы, как экспорт сведений о потоке IP (IP Flow Information Export или IPFIX) [RFC5470], могут способствовать доставке данных, важно предоставить приложениям возможность динамически запрашивать у таких механизмов выполнение измерений и доставку данных.

Имеется много событий, которые приложения могут использовать для проверки состояния маршрутизатора до того, как изменится другое состояние сети (например, будет установлен маршрут), и заблаговременно выполнять действия в ответ на изменения соответствующих маршрутов или события в маршрутизаторе (например, включение или выключение канала). Хотя что-то (например, включение или выключение канала) доступно сегодня через уведомления MIB, полный диапазон (например, установка или изменение маршрута, смена основного LSP) остаются недоступными.

---

[1] Label Information Base - база сведений о метках.
[2] Forwarding and Control Element Separation - разделение элементов управления и пересылки.
[3] Label Switched Path - путь с коммутацией по меткам.

5. Аспекты, рассматриваемые для протокола I2RS

В этом разделе рассматриваются требуемые аспекты протокола, который может поддерживать I2RS. Реализация протокола путём расширения имеющихся механизмов или разработки новых требует дополнительного исследования.

Ниже указаны основные свойства, необходимые для интерфейса с системой маршрутизации.

Множество одновременных асинхронных операций
Отдельное приложение должно иметь возможность передать несколько независимых неделимых (atomic) операций через I2RS, не дожидаясь выполнения каждой перед отправкой следующей.

Тонкая детализация блокировки данных для записи
При выполнении операции I2RS требуется тонкая детализация блокируемых данных (например, конкретный префикс и маршрут), а не грубая блокировка как при записи конфигурации. Это должно повысить число одновременно выполняемых операций I2RS и снизить задержки на блокировку.

Контроль из разных источников
Несколько приложений могут взаимодействовать с одним агентом I2RS при минимальной координации. Нужно, чтобы агент I2RS мог обрабатывать несколько запросов известным способом, определяемым правилами. Записанные данные могут принадлежать разным клиентам I2RS в разные моменты времени, данные могут быть переопределены другим клиентом I2RS. Дателли такой обработки рассмотрены в [RFC7921].

Дуплекс
Взаимодействие может организовать клиент (т. е. оно происходит в приложении или используется им для взаимодействия с агентом I2RS) или агент I2RS. Точно так же события, подтверждения, отказы, операции и т. п. могут передаваться в любой момент как маршрутизатором, так и приложением. I2RS не является чистой моделью вытягивания (pull), где лишь приложение запрашивает отклики.

Высокая пропускная способность
Агенту I2RS и связанному с ним маршрутизатору следует, по меньшей мере, иметь возможность обработки значительного числа операций в секунду (например, 10000 для обработки множества индивидуальных маршрутов в абонентам, меняющихся одновременно).

Малая задержка
Следует обеспечивать выполнение простых операций (например, чтение или запись одного маршрута для префикса) за доли секунды.

Множество каналов
Следует предусмотреть возможность взаимодействия через интерфейсы различных компонентов маршрутизатора без работы через один канал. Например, для масштабирования некоторые экспортируемые данные или события будет лучше передать напрямую из плоскости пересылки, а другие взаимодействия могут проходить через плоскость управления. Один канал с проверкой подлинности и полномочий может считаться основным, по которому может запросить доставку данных лишь уполномоченный клиент. Записи от клиентов ожидаются лишь на каналах, поддерживающих проверку подлинности и полномочий.

Масштабируемый и фильтруемый доступ к информации
Для масштабируемого извлечения сведений, которое проще использовать приложениям, очень ценна возможность указывать фильтры в операциях запроса данных или асинхронных уведомлений.

Защищённое управление и доступ
Любая возможность манипулирования состоянием маршрутизации должна подвергаться проверке подлинности и полномочий. Конфиденциальные сведения о маршрутах могут потребовать доставки клиенту I2RS по защищённому каналу. Для таких взаимодействий нужна защита целостности, а большинство взаимодействий требует защиты конфиденциальности.

Расширяемость и функциональная совместимость
Протокол и модели I2RS должны быть расширяемыми и совместимыми между разными версиями протокола и моделей.

6. Вопросы безопасности

Безопасность является важнейшим аспектом любого протокола, который позволяет задавать состояния и извлекать детали состояния маршрутизатора. Необходимость защищённого управления и доступа отмечена в разделе 5. Большинство архитектурных соображений безопасности рассмотрено в [RFC7921]. Предполагается, что агент I2RS имеет отдельный канал проверки подлинности и полномочий, через который можно проверить отождествление и права клиента I2RS. Требуется взаимное согласование между клиентом и агентом I2RS. С разными аспектами I2RS связаны различные уровни защиты целостности и конфиденциальности, а также предотвращения повторного использования (replay).

7. Литература

7.1. Нормативные документы

[RFC7921] Atlas, A., Halpern, J., Hares, S., Ward, D., and T. Nadeau, "An Architecture for the Interface to the Routing System", RFC 7921, DOI 10.17487/RFC7921, June 2016, <http://www.rfc-editor.org/info/rfc7921>.

7.2. Дополнительная литература

[RFC3746] Yang, L., Dantu, R., Anderson, T., and R. Gopal, "Forwarding and Control Element Separation (ForCES) Framework", RFC 3746, DOI 10.17487/RFC3746, April 2004, <http://www.rfc-editor.org/info/rfc3746>.

[RFC5470] Sadasivan, G., Brownlee, N., Claise, B., and J. Quittek, "Architecture for IP Flow Information Export", RFC 5470, DOI 10.17487/RFC5470, March 2009, <http://www.rfc-editor.org/info/rfc5470>.

[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, <https://www.rfc-editor.org/info/rfc6241>.

[RFC7752] Gredler, H., Ed., Medved, J., Previdi, S., Farrel, A., and S. Ray, "North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP", RFC 7752, DOI 10.17487/RFC7752, March 2016, <http://www.rfc-editor.org/info/rfc7752>.

Приложение A. Имеющиеся интерфейсы управления

Здесь сочетание абстрактных моделей данных, их представления на языке данных и протокола передачи рассматривается как единое целое. Хотя возможны иные комбинации этих имеющихся стандартных технологий, описанные способы являются одними из наиболее распространённых.

Есть 3 основных способа управления маршрутизаторами. Наиболее популярным является командный интерфейс (command-line interface или CLI), позволяющий настраивать и изучать состояние устройства. Это фирменный (proprietary) интерфейс, напоминающий оболочки UNIX, который позволяет очень селективно настраивать устройство и наблюдать за ним и, что особенно интересно в нашем случае, работать в его системой маршрутизации. Та или иная форма этого интерфейса имеется почти на каждом устройстве (виртуальном или ином). Обработка сведений, возвращаемых в CLI (называется «скоблением» экрана - screen scraping) - обременительное занятие, поскольку данные обычно форматируются для человека, а их схема может меняться от устройства к устройству и от версии к версии. Несмотря на повсеместное распространение, это интерфейс не стандартизован и вряд ли когда-либо будет стандартизован. Стандартизация CLI не рассматривается как возможное решение для I2RS.

Другим распространенным интерфейсом для опроса состояния устройства, статистики и конфигурации является простой протокол сетевого управления (Simple Network Management Protocol или SNMP) с набором стандартизованных и фирменных модулей MIB[1]. SNMP давно применяется администраторами сетей для сбора сведений о статистике и состояниях устройств, включая системы маршрутизации. Однако SNMP очень редко служит для настройки устройств или каких-либо их систем по причине очень сильной зависимости от оператора сети. К таким причинам относятся сложность, отсутствие желаемой семантики настройки (например, отката конфигурации, «песочниц», версий конфигурации) и сложности применения семантики (или её отсутствия), определённой в модулях MIB, для настройки функций устройств. Поэтому SNMP не рассматривается как возможное решение для I2RS.

Протокол IETF для настройки сети (Network Configuration Protocol или NETCONF) [RFC6241] существенно продвинулся в части преодоления большинства отмеченных ограничений, связанных с настройкой. Однако это новая технология и ещё нет стандартных моделей, поэтому внедрение NETCONF идёт достаточно медленно. При необходимости I2RS будет идентифицировать и определять информацию и модели данных для поддержки приложений I2RS. В NETCONF и/или соответствующие модели данных может потребоваться добавить расширения для управления из нескольких мест.

Благодарности

Авторы благодарны Ken Gray, Ed Crabbe, Nic Leymann, Carlos Pignataro, Kwang-koog Lee, Linda Dunbar, Sue Hares, Russ Housley, Eric Grey, Qin Wu, Stephen Kent, Nabil Bitar, Deborah Brungard, Sarah Banks за их предложения и рецензии.

Адреса авторов

Alia Atlas (editor)
Juniper Networks
Email: akatlas@juniper.net

Thomas D. Nadeau (editor)
Brocade
Email: tnadeau@lucidvision.com

Dave Ward
Cisco Systems
Email: wardd@cisco.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

[1]Management Information Base - база информации управления.