Internet Engineering Task Force (IETF)
Request for Comments: 9232
Category: Informational
ISSN: 2070-1721

H. Song
Futurewei
F. Qin
China Mobile
P. Martinez-Julia
NICT
L. Ciavaglia
Rakuten Mobile
A. Wang
China Telecom

May 2022

Network Telemetry Framework

Модель сетевой телеметрии

Аннотация

Сетевая телеметрия - это технология для получения данных о сети и облегчения эффективного автоматизированного управления сетью. Она включает различные методы удалённой генерации, сбора, сопоставления и применения данных. В этом документе описана архитектурная модель сетевой телеметрии, основанная на задачах, возникающих при работе сетей, и вытекающих из этого требований. Документ разъясняет терминологию и классифицирует модули и компоненты сетевой телеметрии с различных точек зрения. Схема и таксономия помогают создать единую основу для сбора связанных работ и обеспечивают рекомендации для соответствующих методов и разработки стандартов.

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 одобренные IESG документы являются кандидатами в Internet Standard, см раздел 2 RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке https://www.rfc-editor.org/info/rfc9232.

Оглавление

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

1. Введение

Видимость сети - это способность инструментов управления видеть состояние и поведение сети, что важно для её успешной работы. Сетевая телеметрия сосредоточена на данных, которые могут:

1) помогать в получении данных о текущем состоянии сети, включая плоскости устройств, пересылки, управления и администрирования (management);

2) генерироваться и собираться с использованием различных технологий, включая сетевые инструменты и измерения, а также иные средства;

3) обрабатываться с разными целями от обеспечения сервиса до безопасности сети с использованием широкого спектра методов анализа.

В этом документе к сетевой телеметрии относятся как сами данные (т. е. данные сетевой телеметрии), так и методы и процессы, служащие для генерации, экспорта, сбора и применения этих данных в потенциально автоматизируемых приложениях управления сетью. Сетевая телеметрия выходит за рамки традиционных методов эксплуатации, администрирования и поддержки (Operations, Administration, and Management или OAM) и от неё ожидается большая гибкость, расширяемость, точность, область охвата и производительность.

Однако у термина «сетевая телеметрия» нет однозначного определения. Область действия термина вызывает путаницу и недопонимание. Полезно разъяснить концепцию и представить чёткую архитектурную модель для сетевой телеметрии, что можно было сформулировать техническую область и более точно согласовать связанные с ней методы и работу над стандартами.

Для решения задачи сначала обсуждаются некоторые важные характеристики сетевой телеметрии, которые задают её чёткое отличие от традиционных технологий OAM и показывают возможность применения некоторых технологий OAM в сетевой телеметрии. Затем рассматривается архитектурная модель сетевой телеметрии, включающая 4 модуля, каждый из которых связан со своей категорией данных телеметрии и соответствующими процедурами. Все эти модули имеют одинаковую внутреннюю структуру, включая компоненты, позволяющие оператору выбирать источники данных в части генерации сведений и их предоставления клиентским приложениям, инструменты для базовых источников данных и компоненты, фактически выполняющие сбор, представление и экспорт полученных данных. Показано, как модель сетевой телеметрии может обеспечить преимущества для имеющихся и будущих сетей. На основе выделения модулей и функций можно сопоставить имеющиеся и будущие методы и протоколы с предлагаемой моделью. Модель также способна упростить разработку, поддержку и понимание систем сетевой телеметрии. Кроме того, описываются стадии развития систем сетевой телеметрии и обсуждаются возможные проблемы безопасности.

Целью модели и таксономии является создание единой основы для набора связанных работ и предоставление рекомендаций по разработке новых методов и стандартов. Насколько известно авторам, этот документ является первой работой в данном направлении среди организаций, занимающихся отраслевыми стандартами. Документ не определяет конкретных технологий.

1.1. Заявление о применимости

Масштабный сбор данных в сети представляет собой основную угрозу приватности пользователей и может быть неотличим от глубокого всеобъемлющего мониторинга [RFC7258]. Представленную здесь модель сетевой телеметрии недопустимо применять для генерации, экспорта, сбора, анализа или хранения данных конкретных пользователей или каких-либо сведений, позволяющих идентифицировать конечного пользователя или характеризовать его поведение без согласия пользователя. С учётом этого принципа модель сетевой телеметрии не применима для сетей, где конечные точки представляют индивидуальных пользователей, таких как общественные сети доступа.

1.2. Глоссарий

Перед дальнейшим обсуждением приведём основные термины и сокращения, применяемые в документе. Между толкованием терминов в сетевой телеметрии и OAM имеются различия. Однако следует понимать, что эти концепции не имеют жёстких границ и сетевая телеметрия скорее является расширением OAM. Она охватывает имеющиеся протоколы OAM, уделяя дополнительное внимание новым и разрабатываемым методам и протоколам, касающимся всех аспектов данных о сети от их получения до применения.

AI (Artificial Intelligence) - искусственный интеллект

В сфере сетей AI относится к основанным на машинном обучении технологиям автоматизированной эксплуатации сетей и решения других задач.

AM (Alternate Marking) - чередующаяся маркировка
Метод измерения производительности потоков, описанный в [RFC8321].

BMP (BGP Monitoring Protocol) - протокол мониторинга BGP
Описан в [RFC7854].

DPI (Deep Packet Inspection) - глубокая инспекция пакетов
Методы проверки пакетов за пределами заголовков L3/L4.

GNMI (gRPC Network Management Interface) - интерфейс сетевого управления gRPC
Протокол сетевого управления от OpenConfig Operator Working Group, разработанный в основном Google. Подробности приведены в [gnmi].

GPB (Google Protocol Buffer) - протокольный буфер Google
Расширяемый механизм представления структурированных данных в последовательной форме. Подробности приведены в [gpb].

GRPC (gRPC Remote Procedure Call) - обобщенный вызов удалённых процедур
Модель высокопроизводительных вызовов RPC с открытым исходным кодом, на которой основан интерфейс gNMI. Подробности приведены в [grpc].

IPFIX (IP Flow Information Export Protocol) - протокол экспорта сведений о потоке IP
Описан в [RFC7011].

IOAM
In situ (на месте) OAM [RFC9197]. Метод телеметрии путей в плоскости данных.

JSON (JavaScript Object Notation) - обозначение объектов JavaScript
Открытый стандарт формата файлов и обмена данными, использующий человекочитаемый текст для сохранения и передачи объектов данных. Описан в [RFC8259].

MIB (Management Information Base) - база информации для управления
Набор данных, применяемых для управления объектами сети.

NETCONF (Network Configuration Protocol) - протокол настройки сети
Описан в [RFC6241].

NetFlow
Протокол компании Cisco, служащий для сбора записей о потоках, как указано в [RFC3954].

Network Telemetry - сетевая телеметрия
Процессы и инструменты для удалённого получения и использования данных о сети для мониторинга и эксплуатации. Базовый термин для большого набора методов и протоколов наблюдения за сетью, связанных с генерацией, сбором, сопоставлением и применением данных. Сетевая телеметрия решает текущие проблемы эксплуатации сетей и позволяет плавно перейти к будущим системам с управлением на основе намерений.

NMS (Network Management System) - система управления сетью
Приложения, позволяющие администраторам управлять сетью.

OAM (Operations, Administration, and Maintenance) - эксплуатация, администрирование, поддержка
Группа функций поддержки сетей, обеспечивающих индикацию и локализацию отказов, сбор сведений о производительности, а также данные и функции диагностики. Большинство современных методов и протоколов мониторинга сетей относится к OAM.

PBT (Postcard-Based Telemetry)
Метод телеметрии путей в плоскости данных. Один из вариантов описан в [IPPM-IOAM-DIRECT-EXPORT].

RESTCONF
Работающий на основе HTTP протокол, который обеспечивает программный интерфейс для доступа к данным, определенным в YANG, с использованием концепции хранилища, определённой в NETCONF [RFC8040].

SMIv2 (Structure of Management Information Version 2) - структура управляющей информации версии 2
Определяет объекты MIB, как описано в [RFC2578].

SNMP (Simple Network Management Protocol) - простой протокол управления сетью
Версии 1, 2, 3 заданы в [RFC1157], [RFC3416], [RFC3411], соответственно.

XML (Extensible Markup Language) - расширяемый язык разметки
Язык разметки для представления данных в человекочитаемом и машинном формате, как указано W3C [W3C.REC-xml-20081126].

YANG
Язык моделирования для определения данных, передаваемых протоколами управления сетью, такими как NETCONF и RESTCONF. Определение YANG дано в [RFC6020] и [RFC7950].

YANG ECA
Модель YANG для правил событие-условие-действие (Event-Condition-Action) [NETMOD-ECA-POLICY].

YANG-Push
Механизм, позволяющий приложениям подписчиков запросить поток обновлений из хранилища YANG на сетевом устройстве. Подробности приведены в [RFC8639] и [RFC8641].

2. Основы

Термин «большие данные» (big data) служит для описания чрезвычайно крупных наборов данных, которые можно анализировать вычислительными средствами для выявления закономерностей, тенденций и связей. Сети несомненно является источником больших данных из-за своих масштабов и объёма пересылаемого трафика. Когда оконечные точки сети не представляют индивидуальных пользователей, например, в контексте предприятия, ЦОД или инфраструктуры), сетевые операции зачастую могут выигрывать от крупномасштабного сбора данных без нарушения приватности пользователей.

Сегодня можно получить доступ к расширенным возможностям анализа данных на основе открытых платформ (например, Apache Hadoop), инструментов (например, Apache Spark) и методов (например, машинное обучение). Благодаря развитию технологий вычислений и хранения, анализ больших данных даёт сетевым операторам возможность получить более точное представление о сети и перейти к самоуправляемости сетей. Некоторые операторы начали применять искусственный интеллект (AI) для понимания сетевых данных. Программные инструменты могут использовать данные о сетях для обнаружения отказов, аномалий, нарушений правил и реагирования на них, а также для предсказания будущих событий. В свою очередь, могут применяться обновления сетевых правил для планирования, предотвращения вторжений, оптимизации и самовосстановления.

Вполне возможно, что самоуправляемые сети [RFC7575] являются следующим логическим шагом развития сетей вслед за программно управляемыми сетями (Software-Defined Networking или SDN), направленным на сокращение (или даже исключение) человеческого труда, более эффективное использование ресурсов сетей и предоставления более качественных услуг в соответствии с потребностями клиентов. Рабочая группа IETF ANIMA занимается разработкой и поддержкой протоколов и процедур для автоматизированного управления сетями и контроля профессионально управляемых сетей. Родственный подход сетей на основе намерений (Intent-Based Networking или IBN) [NMRG-IBN-CONCEPTS-DEFINITIONS] требует видимости сетей и данных телеметрии для обеспечения должного поведения сетей.

Однако, несмотря на расширение возможностей обработки данных и рост потребностей приложений в данных для более качественного функционирования, сети отстают в части извлечения и трансляции сетевых данных в полезные и применимые сведения эффективными способами. Узкие места систем смещаются от потребления данных к их предоставлению. Число узлов сетей и пропускная способность для трафика продолжают быстро возрастать. Конфигурацию сетей и правила приходиться менять чаще, чем раньше. Более тонкие события и детализированные данные от всех плоскостей (уровней) сети требуется извлекать и экспортировать в реальном масштабе времени. В результате получение достаточного объёма высококачественных данных из сети эффективным, своевременным и гибким способом усложняется. Поэтому требуется изучить имеющиеся технологии и протоколы и выявить все возможные проблемы.

Дале в этом разделе сначала разясняется сфера охвата для сетевых данных (т. е. данных телеметрии), затем рассматриваются некоторые важные примеры использования сетевых операций сегодня и в будущем. Далее показано, почему имеющихся технологий и протоколов OAM не достаточно для таких случаев. Подчёркивается потребность в новых методах и протоколах, а также расширениях для имеющихся средств, которые описаны как сетевая телеметрия.

2.1. Охват данными телеметрии

Любая информация, которую можно извлечь из сети (включая плоскости данных, управления и администрирования) и использовать для обеспечения видимости или в качестве основы для действий, считается данными телеметрии. Это включает статистику, записи событий и системных журналов (log), снимки состояния, данные конфигурации и т. п. Телеметрия также включает выходные данные любых активных или пассивных измерений [RFC7799]. В некоторых случаях «сырые» (raw) данные обрабатываются в сети до их отправки потребителю. Обработанные данные также относятся к телеметрии. Значения данных телеметрии меняются. В некоторых случаях, если это приемлемо, лучше отдать предпочтение меньшему объёму высококачественных данных, нежели большому объёму данных низкого качества. Классификация данных телеметрии приведена в разделе 3. Для сохранения приватности конечных пользователей не следует собирать содержимое их пакетов. В частности, объектам данных, генерируемым, экспортируемым и собираемым приложениями сетевой телеметрии, не следует включать какое-либо содержимое из пакетов, связанных с системами конечных пользователей.

2.2. Примеры использования

Ниже приведён список вариантов использования, важных для сетевых операторов. Список не является исчерпывающим, но его достаточно для выделения требований к скорости передачи, разнообразию, объёму и достоверности, а также атрибутам больших данных в сети.

- Безопасность. Системам обнаружения и предотвращения вторжений в сеть нужно отслеживать сетевой трафик и действия для реагирования на аномалии. Учитывая все более изощренные направления атак в сочетании со все более серьезными последствиями нарушений безопасности, нужно разрабатывать новые инструменты и методы, основанные на более широком и глубоком анализе сетей. Конечная цель заключается в минимизации или исключении участия человека в этих процессах и отсутвии помех для легитимного трафика.

- Соответствие правилам и намерениям. Политика сети представляет собой набор правил, ограничивающих доступ служб к сети в целях дифференциации или принудительно применяющих специальную обработку трафика. Например, цепочка сервисных функций может являться политикой, требующей прохождения отдельных потоков через набор упорядоченных сетевых функций. Намерение, как указано в [NMRG-IBN-CONCEPTS-DEFINITIONS], - это набор операционных целей, которые сети следует поддерживать, и результатов, которые сети следует обеспечивать, заданных декларативно без указания способов достижения или реализации. Намерения требуют сложной трансляции и отображения процессов до применения в сети. Применение политики или намерения требуется непрерывная проверка соответствия и мониторинг, основанные на видимости, обеспечиваемой сетевой телеметрией. Обо всех нарушениях требуется сообщать незамедлительно, т. е. информировать администратора сети о нарушении, что может приводить к изменению применяемой политики или намерений для обеспечения их соблюдения в сети.

- Соответствие SLA. Соглашение об уровне обслеживания (Service Level Agreement или SLA) является контрактом между сервис-провайдером и клиентом, включающим показатели для оценки сервиса, а также меры и санкции в случае нарушения контракта. Пользователям требуется проверять получение обещанных услуг, а операторам - оценивать способы предоставления услуг в соответствии с SLA в реальном масштабе времени на основе данных сетевой телеметрии, включая данные сетевых измерений.

- Анализ первопричин. Многие отказы в сетях могут быть следствиями цепочки событий. Для поиска неполадок и восстановления нужна быстрая идентификация корня возникающих проблем. Однако это не всегда просто, особенно при спорадических отказах и большом числе сообщений о событиях как связанных с отказом, так и иных. Хотя такие технологии, как машинное обучение, могут служить для анализа первопричины, именно сеть видит и предоставляет соответствующие диагностические данные, которые вводятся активно или пассивно собираются приложениями для анализа первопричин.

- Оптимизация сети. Методы краткосрочной и долгосрочной оптимизации сети, включая балансировку нагрузки, организацию трафика (Traffic Engineering или TE) и планирование сети. Операторы стремятся оптимизировать использование своих сетей для ускорения возврата инвестиций (Return on Investment или ROI) и снижения капитальных расходов (Capital Expenditure или CAPEX). Первым шагом является получение в реальном масштабе времени состояния сети до применения правил управления трафиком. В некоторых случаях нужно обнаружение микропиков трафика в течение очень коротких интервалов для тонкого управления трафиком с

целью предотвращения перегрузок в сети. Долгосрочное планирование пропускной способности и топологии сети требует анализа фактических данных сетевой телеметрии, собранных в течение длительного времени.

- Отслеживание и предсказание событий. Видимость путей и производительности сетевого трафика очень важна для служб и приложений, зависящих от работоспособности сети. Для операторов представляют интерес многочисленные события в сети. Например, оператору могут потребоваться сведения о местах и причинах отбрасывания пакетов в потоках приложений или он может захотеть получать предупреждения о возможных проблемах, чтобы заранее предпринять соответствующие действия и избежать серьёзных последствий.

2.3. Задачи

Долгое время сетевые операторы полагались на SNMP [RFC3416], командный интерфейс (Command-Line Interface или CLI), Syslog [RFC5424] для мониторинга своей сети. Некоторые методы OAM, как описано в [RFC7276], также применялись для облегчения устранения неполадок в сети. Этих традиционных методов недостаточно для поддержки указанных выше вариантов по целому ряду причин.

- В большинстве случаев нужен постоянный мониторинг сети и динамическое переопределение сбора данных в режиме реального времени. Сбор данных путём опроса плохо подходит для таких случаев. Основанные на подписке потоковые данные, передаваемые напрямую от источника данных (например, микросхемы пересылки), предпочтительней в плане достаточности объёма данных и точности в масштабе.

- Нужны всесторонние данные - от механизмов обработки пакетов менеджерам трафика, от линейных плат основному устройству, от пользовательских потоков в протоколы управления пакетами, от конфигурации устройств в сетевые операции, от физических уровней на прикладные. Традиционные методы OAM удовлетворяют лишь часть этих потребностей (например, SNMP обрабатывает лишь данные MIB). Классические сетевые устройства не могут предложить все требуемые датчики, поэтому нужны более открытые и программируемые сетевые устройства.

- Во многих приложениях требуется сопоставлять в масштабе сети данные из разных источников (например, от распределенных сетевых устройств, разных компонент устройства, разных плоскостей сети). Частным решениям зачастую не достает возможностей консолидировать данные из разных источников. Состав полного решения, частично предложенный в архитектуре самоуправления ресурсами (Autonomic Resource Control Architecture - ARCA) [NMRG-ANTICIPATED-ADAPTATION], будет расширен для работы в комплексной модели.

- Некоторые традиционные методы OAM (например, CLI и Syslog) не имеют формальных моделей данных. Отсутствие структуры данных препятствует автоматизации инструментов и расширяемости. Стандартизованные модели данных важны для поддержки программируемых сетей.

- Хотя некоторые традиционные методы OAM поддерживают выталкивание (push) данных (например, SNMP Trap [RFC2981][RFC3877], Syslog, sFlow [RFC3176]), передаваемые данные ограничены предопределенным набором предупреждения плоскости администрирования (например, SNMP Trap) или выборкой пользовательских пакетов (например, sFlow). Операторам сетей нужны данные из произвольных источников, с разной детализацией и точностью, что превосходит возможности имеющихся технологий.

- Традиционные методы пассивных измерений могут потреблять чрезмерные сетевые ресурсы, создавать избыточные данные или давать неточные результаты. Традиционные активные методы измерений могут мешать пользовательскому трафику, а их результаты являются лишь косвенными. Более подходят методы, способные собирать данные напрямую или по запросу из пользовательского трафика.

Эти проблемы решены в новых стандартах и методах (например, IPFIX/Netflow, Packet Sampling (PSAMP), IOAM, YANG-Push), но возникают новые проблемы. Эти стандарты и методы нужно принять и включить в новую модель.

2.4. Сетевая телеметрия

Сетевая телеметрия стала основным техническим термином для обозначения методов сбора и применения сетевых данных. Несколько методов и протоколов сетевой телеметрии (например, IPFIX [RFC7011] и gRPC [grpc]) уже получили широкое распространение. Сетевая телеметрия позволяет разным объектам получать данные от сетевых устройств так, что эти данные можно анализировать и визуализировать для поддержки мониторинга и работы сети. Сетевая телеметрия охватывает традиционные методы OAM и имеет более широкую область действия. Например, ожидается, что сетевая телеметрия сможет обеспечить данные о сети, требуемые для самоуправления и устранения недостатков традиционных методов OAM.

В сетевой телеметрии обычно предполагается применение данных машинами, а не человеком-оператором. Поэтому сетевая телеметрия может напрямую инициировать в сети операции самоуправления, тогда как традиционные инструменты OAM были созданы для использования человеком с целью мониторинга и диагностики сетей, а также управления работой сети вручную. Эти предложения ведут к очень различающимся методам.

Хотя новые методы сетевой телеметрии появляются и постоянно развиваются, некоторые аспекты сетевой телеметрии уже получили широкое распространения. Отметим, что термин «сетевая телеметрия» предназначен для использования в качестве общего термина, охватывающего широкий спектр методов, поэтому не предплагается, что перечисленные ниже характеристики будут присущи каждому из методов.

- Выталкивание и потоковая передача. Вместо опросв сетевых устройств для получения данные коллекторы телеметрии подписываются на потоковые данные, выталкиваемые источниками из сетевых устройств.

- Объем и скорость. Данные телеметрии предназначены для машинного применения, а не для человека напрямую. Поэтому объем данных может быть очень большим, а обработка оптимизируется под нужны автоматизации в реальном масштабе времени.

- Нормализация и унификация. Телеметрия нацелена на выполнение задач автоматизации сетей. Прилагаются усилия по нормализации представления данных и унификации протоколов для упрощения анализа данных и обеспечения интегрированного анализа для разнородных устройств и источников данных в сети.

- Основа на модели. Данные телеметрии заранее моделируются, что позволяет приложениям легко настраивать и применять данные.
- Слияние данных. Данные для одного приложения могут поступать из разных источников (например, из разных доменов, устройств, уровней), основанных на общих именах (идентификаторах) для сопоставления.
- Динамичность и интерактивность. Поскольку сетевая телеметрия предназначена для применения в замкнутом контуре управления, она должна работать непрерывно и адаптироваться к интерактивным запросам контроллеров, управляющих работой сети.

Идеальное решение для сетевой телеметрии должно также иметь указанные ниже свойства или возможности.

- Настройка в сети. Генерируемые данные можно настроить в сети в процессе работы в соответствии с потребностями конкретных приложений. Для этого нужна поддержка программируемой плоскости данных, которая позволяет гибко задавать датчики с настраиваемыми функциями в нужных местах.
- Агрегирование и сопоставление данных в сети. Сетевые устройства и точки агрегирования могут определять, какие события и данные нужно сохранять, сообщать или отбрасывать, снижая нагрузку на центральные точки сбора и обработки при сохранении готовности нужной информации к своевременной обработке.
- Обработка в сети. Иногда не обязательно или нежелательно собирать все данные в центральной точке для обработки и применения действий. Можно выполнять обработку данных в сети, разрешая применять реактивные действия локально.
- Прямой экспорт плоскости данных. Сведения от микровсем пересылки в плоскости данных могут напрямую экспортироваться потребителям в целях эффективности, особенно при достаточной пропускной способности и необходимости обработки в реальном масштабе времени.
- Сбор данных в основной полосе (In-Band). В дополнение к активному и пассивному сбору данных новый гибридный подход позволяет собирать данные на прямую для любого целевого потока на всем пути его пересылки [OPSAWG-IFIT-FRAMEWORK].

Следует отметить, что для сетевой телеметрии не следует нарушать обычные сетевые операции и следует избегать «эффекта наблюдателя», т. е. не следует изменять поведение сети или влиять на поведение пересылки. Кроме того, большой объем трафика сетевой телеметрии может вызывать перегрузку сети, если не принять подобающих мер изоляции, методов организации трафика или механизмов контроля перегрузок, обеспечивающих отключение трафика телеметрии в случае нехватки сетевых возможностей. Для этого подойдут механизмы, описанные в [RFC8084] и [RFC8085] (Best Current Practice или BCP).

Хотя во многих случаях система для сбора данных сетевой телеметрии включает удалённые объекты сбора и применения данных, важно понимать, что что не существует неотъемлемых допущений об устройстве и архитектуре системы. Хотя сетевая архитектура с централизованным контроллером (например, SDN) представляется естественным решением для сетевой телеметрии, возможна работа системы телеметрии и в распределенной манере. Например, поставщики и потребители данных телеметрии могут иметь партнерские (peer-to-peer) отношения, где сетевой узел может напрямую потреблять данные телеметрии от других узлов.

2.5. Потребность в модели сетевой телеметрии

Аналитика сетевых данных (например, машинное обучение) применяется для автоматизации работы сетей на основе обширных и согласованных данных из сетей. Сбора данных, ограниченного одним источником и статического по своей природе, во многих случаях недостаточно для удовлетворения потребностей приложений в данных телеметрии. В результате требуется объединять множество источников данных, использующих различные методы и стандарты. Желаетльно иметь модель, классифицирующую и организующую источники и типы данных телеметрии, определять различные компоненты систем сетевой телеметрии и их взаимодействия, а также помогать в координации и интеграфии нескольких телеметрических подходов на разных уровнях. Это позволит гибко сочетать данные для разных приложений, нормализуя и упрощая интерфейсы. В частности, такая модель будет полезна при разработке приложений для работы в сети, как отмечено ниже.

- Будущие сети с самоуправлением или без него будут зависеть от целостной и всеобъемлющей видимости сети. Приложения будут работать лучше при единообразной и согласованной поддержке с использованием интегрированных конвергентных механизмов и общего представления данных телеметрии, когда это возможно. Поэтому следует консолидировать механизмы и протоколы в минимальный, но всеобъемлющий набор. Модель телеметрии может помочь в нормализации развития техники.
- Видимость сети представляется с разных точек зрения. Например, устройство воспринимает сетевую инфраструктуру как объект мониторинга для которого можно получить сведения о топологии сети и состоянии устройств, а с точки зрения трафика объектами мониторинга являются пакеты или потоки, от которых можно получить объёмы трафика и пути через сеть. Приложению может потребоваться смена точки зрения в процессе работы, а также может потребоваться сопоставить услугу и её воздействие с восприятием пользователя (user experience или UE) для получения исчерпывающей инфомации.
- Приложениям требуется эластичность сетевой телеметрии для обеспечения эффективного использования ресурсов сети и снижения влияния связанной с телеметрией обработки на производительность сети. Например, рутинный мониторинг должен охватывать сеть целиком с невысокой скоростью выборки данных. Лишь при возникновении проблем или критических тенденций следует менять источники телеметрических данных и повышать при необходимости частоту выборки.
- Эффективное агрегирование данных важно для приложений, чтобы снизить общий объем данных и повысить точность анализа.

Модель телеметрии объединяет все работы по телеметрии из разных источников и рабочих групп IETF. Это позволяет собрать комплексную систему сетевой телеметрии и избежать повторения уже сделанной работы. Модели следует охватывать концепции и компоненты с точки зрения стандартизации. В этом документе описаны модули, образующие

структуру сетевой телеметрии и разбивающие систему телеметрии на компоненты, которые легко отображаются на выполненные и будущие работы.

3. Модель сетевой телеметрии

На верхнем уровне модели сетевой телеметрии выделены 4 модуля по источникам объектов данных и представлены их взаимосвязи. Получив данные из этих модулей приложение может анализировать данные и выполнять действия. На следующем уровне модели каждый модуль делится на блоки, имеющие одинаковую базовую структуру. Один блок предназначен для настройки источников данных и подписки, другой - для кодирования и экспорта данных, третий отвечает за генерацию телеметрии, связанной с базовыми ресурсами. В модели применяется один набор абстракций механизмов получения данных и типов данных (3.3. Абстракции механизмов извлечения и типов данных). Двухуровневая архитектура с унифицированными абстракциями помогает точно определить положение протоколов и методов в модели и при необходимости разделить систему телеметрии на управляемые части.

3.1. Модули верхнего уровня

Телеметрию можно применять в плоскостях пересылки, управления и администрирования (management), а также для внешних источников, как показано на рисунке 1. Поэтому телеметрия разделена на 4 модуля (плоскости администрирования, управления и пересылки, а также внешние источники данных и событий). Каждый из которых имеет свой интерфейс с приложениями управления сетью.

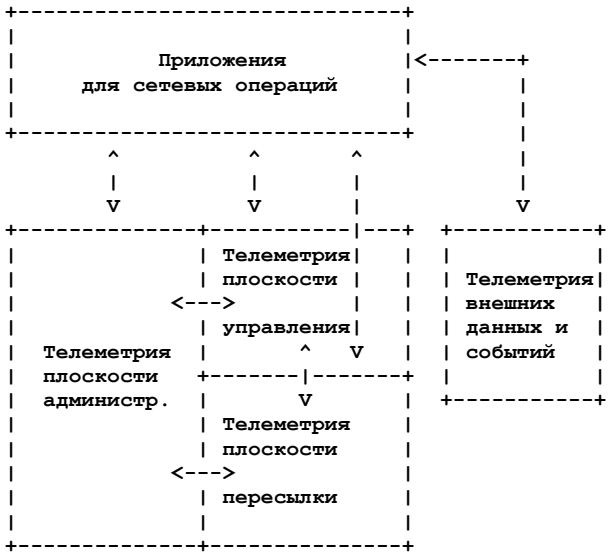

Рисунок 1. Категории модулей сетевой телеметрии.

Это разделение основано на разных объектах данных телеметрии, ведущее к различиям в источниках данных и местах экспорта. Различия оказывают серьезное влияние на возможности программирования и обработки данных в сети, кодирования данных и транспортные протоколы, а также требования к пропускной способности и задержкам. Данные могут передаваться напрямую или через плоскости управления и администрирования. У каждого из этих подходов есть свои преимущества и недостатки.

Отметим, что в некоторых случаях сетевой контроллер сам может служить источником данных телеметрии, которые уникальны для него или выводятся из данных от элементов сети. Некоторые принципы и таксономия, относящиеся к телеметрии плоскостей управления и администрирования, могут применяться к контроллеру для обеспечения данных телеметрии внешним приложениям управления сетью. Этот документ сконцентрирован на телеметрии элементов сети и детали, относящиеся к контроллерам выходят за рамки документа.

Сводка основных различий этих 4 модулей дана в таблице 1 с шести точек зрения:

- объекты данных;
- местоположение (цель) экспорта данных;
- модель данных;
- представление данных;
- прикладной протокол телеметрии;
- метод доставки данных.

Объекты данных являются целями или источниками для каждого модуля. Поскольку источники данных могут меняться, место, куда наиболее удобно экспортировать данные, также может меняться. Например, данные плоскости пересылки в основном поступают как данные, экспортируемые из микросхем пересылки (Application-Specific Integrated Circuit или ASIC), тогда ка данные плоскости управления исходят обычно от протокольных демонов, работающих на процессорах управления (CPU). Для удобства и эффективности предпочтительно экспортировать данные в устройства, расположенные ближе к источнику. Поскольку места для экспорта данных различаются по возможностям, для баланса производительности и расходов применяются разные модели данных, кодирование и методы транспортировки. Например, микросхемы пересылки имеют высокую пропускную способность, но ограниченные возможности обработки комплексных данных и поддержки состояния, а основной процессор управления способен обрабатывать сложные данные и состояния, но имеет ограниченную пропускную способность. В результате протоколы телеметрии для модулей могут различаться. Некоторые методы представлены в соответствующих ячейках таблицы, чтобы подчеркнуть техническое различие модулей. Отметим, что выбранные методы просто отражают фактический уровень и не являются

исчерпывающими (например, IPFIX может работать по протоколам TCP и SCTP, но это не рекомендуется для плоскости пересылки). Важно подчеркнуть, что не следует ожидать универсального протокола для всех случаев.

Таблица 1. Сравнение модулей объектов данных.

Модуль	***Плоскость администрирования***	***Плоскость управления***	***Плоскость пересылки***	***Внешние данные***
Object (объект)	Конфигурация и рабочее состояние	Протокол управления и сигнализации, RIB	QoS пакетов и потоков, статистика трафика, статистика буферов и очередей, FIB, списки управления доступом (ACL)	терминал, социальные данные, окружение
Export Location (цель экспорта)	Основной процессор (CPU) управления	Основной процессор (CPU) управления, CPU линейной платы или микросхема пересылки	Микросхема пересылки или CPU линейной платы; основной процессор маловероятен	Разные
Data Model (модель данных)	YANG, MIB, syslog	YANG, пользовательская	YANG, пользовательская	YANG, пользовательская
Data Encoding (кодирование данных	GPB, JSON, XML	GPB, JSON, XML, текст	текст	GPB, JSON, XML, текст
Application Protocol (прикладные протоколы)	gRPC, NETCONF, RESTCONF	gRPC, NETCONF, IPFIX, отражение трафика	IPFIX, отражение трафика, gRPC, NETFLOW	gRPC
Data Transport (доставка данных)	HTTP(S), TCP	HTTP(S), TCP, UDP	UDP	HTTP(S), TCP, UDP

Отметим, что взаимодействие с приложениями, потребляющими данные сетевой телеметрии, может быть косвенным. Возможна передача некоторых данных внутри устройства. Например, плоскости администрирования могут потребоваться данные от плоскости управления. Некоторые операционные состояния можно вывести лишь из сведений от источников в плоскости данных, примером могут служить состояния интерфейсов и статистика. Для получения данных телеметрии плоскости управления может потребоваться доступ к таблицам пересылки (Forwarding Information Base или FIB) в плоскости данных.

Приложение может включать более одной плоскости и взаимодействовать с несколькими плоскостями одновременно. Например, приложению контроля SLA может потребоваться телеметрия плоскостей данных и управления.

Требования и задачи для каждого модуля описаны ниже (отметим, что требования могут относиться ко всем модулям телеметрии, но здесь выделены те, которые наиболее ярко выражены для конкретной плоскости).

3.1.1. Телеметрия плоскости администрирования

Телеметрия плоскости администрирования (управления элементами сети) взаимодействует с системой управления сетью (Network Management System или NMS) и обеспечивает такие сведения, как данные производительности, данные сетевых журналов и данные о предупреждениях и дефектах в сети, а также сетевую статистику и данные о состоянии. Плоскость администрирования включает множество протоколов, в том числе классические SNMP и syslog. Независимо от протокола телеметрия плоскости администрирования должна удовлетворять приведённым ниже требованиям.

- Удобная подписка на данные. Приложениям следует обеспечивать свободу выбора экспортируемых данных (см. параграф 3.3), способы и частоту экспорта (например, при изменении или периодически).
- Структурированные данные. В сети с самоуправлением машины заменят людей по вопросам осмысления сетевых данных. Языки моделирования данных, такие как YANG, позволяют эффективно описывать структурированные данные, а также нормализовать представление и преобразования данных.
- Высокоскоростной транспорт. Чтобы не отставать от скорости поступления информации, источники данных должны быть способны передавать большие объёмы данных с высокой частотой. Нужны форматы компактного кодирования и схемы сжатия для повышения эффективности передачи данных. Режим подписки, заменяющий режим запроса, сокращает взаимодействие между клиентами и серверами, помогая повысить эффективность источников данных.
- Предотвращение перегрузок в сети. Приложение должно защищать сеть с помощью механизмов контроля перегрузок или хотя бы «выключателей» (circuit breaker). Некоторые решения даны в [RFC8084] и [RFC8085].

3.1.2. Телеметрия плоскости управления

Телеметрия плоскости управления относится к мониторингу работоспособности различных протоколов управления на всех уровнях протокольного стека. Отслеживание операционного состояния этих протоколов полезно для обнаружения, локализации и даже предсказания проблем в сети, а также для оптимизации сети в реальном масштабе времени с высоким уровнем детализации. Некоторые из задач и вопросов телеметрии плоскости управления указаны ниже.

- Способ сопоставления сквозных индикаторов KPI (End-to-End Key Performance Indicator) с KPI конкретных уровней. Например, пользователи IPTV могут оценить сервис плавностью и чёткостью изображения. В случае необычно низкого UE KPI или прерывания сервиса нетривиальной задачей становится обнаружение проблемы в стеке протоколов (например, транспортный или сетевой уровень) и её границ, конкретного протокола (например, IS-IS или BGP на сетевом уровне) и устройства.
- Традиционный подход на основе OAM для измерения KPI плоскости управления, включая Ping (L3), Traceroute (L3), Y.1731 [y1731] (L2) и т. д. Общей проблемой, связанной с этими методами является то, что они лишь измеряют KPI, не отражая реального статуса протоколов, что снижает их эффективность и действенность при поиске неполадок в плоскости управления и оптимизации сети.

- Какие дополнительные исследования нужны для протокола мониторинга BGP (BMP). BMP является примером телеметрии плоскости управления, он применяется сейчас для мониторинга маршрутов BGP и позволяет применять многофункциональные приложения, такие как анализ партнёров BGP, автономных систем (AS), префиксов и безопасности. Однако мониторинг других уровней, протоколов, а также кроссуровневые и кросспротокольные корреляции KPI всё ещё нахотядся в зачаточном состоянии (например, мониторинг IGP не так обширен, как BMP) и требуют дополнительных исследований.

Отметим, что требования и решения по предотвращению перегрузок относятся и к телеметрии плоскости управления.

3.1.3. Телеметрия плоскости пересылки

Эффективная телеметрия плоскости пересылки полагается на данные, которые может раскрыть сетевое устройство. Качество, объем, своевременность данных должны соответствовать ряду строгих требований. Это создаёт некоторые сложности для сетевых устройств плоскости пересылки, откуда исходят первичные данные.

- Основной задачей устройств плоскости данных является обработка и пересылка пользовательского трафика. Хотя поддержка видимости сети важна, телеметрия является лишь вспомогательной функцией и ей не следует мешать обычной обработке и пересылке трафика (т. е. поведение пересылки следует сохранять, а компромисс между телеметрией и производительностью пересылки должен быть чётко сбалансирован).

- Приложениям сетевых операций требуется сквозная видимость разных источников, что может приводить к очень большим объёмам данных. Однако этим данным недопустимо истощать пропускную способность, независимо от подхода к доставке (основная полоса или отдельный канал).

- Устройства плоскости данных должны своевременно предоставлять данные с минимально возможной задержкой. Длительная обработка, хранение и анализ могут влиять на эффективность контура управления и даже делать данные бесполезными.

- Данные следует структурировать и помечать для упрощения их разбора и применения приложениями. Требуемые приложениями типы данных могут существенно различаться. Устройства плоскости данных должны обеспечивать гибкость и программируемость для предоставления точных данных приложениям.

- Телеметрии плоскости данных следует поддерживать поэтапное развёртывание и работу даже при наличии устройств, не знающих о телеметрии.

- Требования и решения по предотвращению перегрузок относятся и к телеметрии плоскости пересылки.

Хотя эти проблемы относятся не только к плоскости пересылки, здесь они усугубляются ограниченностью ресурсов и гибкости. Программируемость плоскости данных важна для поддержки сетевой телеметрии. Новые микросхемы пересылки имеют расширенные возможности телеметрии для поддержки настраиваемых функций телеметрии.

Техническая таксономия относится к тому, как используется телеметрия и возможно несколько критериев для классификации методов телеметрии в плоскости пересылки.

- Активная, пассивная и гибридная. Этот критерий относится к сквозным измерениям. Активные и пассивные методы (а также гибридные типы) хорошо описаны в [RFC7799]. Пассивные методы включают TCPDUMP, IPFIX [RFC7011], sFlow, отражение трафика. Эти методы обычно охватывают малую область данных. Расход пропускной способности очень высок, что не позволяет расширить охват. Активные методы включают Ping, OWAMP [RFC4656], TWAMP [RFC5357], STAMP [RFC8762], и Cisco SLA Protocol [RFC6812]. Эти интрузивные методы обеспечивают лишь косвенные измерения. Гибридные методы включают IOAM [RFC9197], Alternate Marking (AM) [RFC8321], Multipoint Alternate Marking [RFC8889] и обеспечивают хорошо сбалансированный и более гибкий подход. Однако реализация гибридных методов более сложна.

- Внутри- или внеполосные данные. Данные телеметрии, передаваемые в пользовательских пакетах до экспорта в коллектор (например, IOAM [RFC9197]), считаюся внутриполосными (in-band). Данные, экспортируемые в коллектор напрямую (например, как описано в Приложении A.3.5), считаются внеполосными (out-of-band). Возможны также гибридные методы, где в пользовательских пакетах передаётся лишь часть данных и инструкции телеметрии (например, AM [RFC8321]).

- Сквозная или внутрисетевая. Сквозные методы организуются между конечными хостами сети (например, Ping), внутрисетевые методы работают в сети и незаметны (прозрачны) для конечных хостов. Однако при необходимости внутрисетевые методы можно легко распространить на конечные хосты.

- Субъект данных. В зависимости от целей телеметрии методы могут основываться на потоках (например, IOAM [RFC9197]), путях (например, Traceroute) и узлах (например, IPFIX [RFC7011]). Объектами данных могут быть пакеты, записи о потоках, измерения, состояния, сигналы.

3.1.4. Телеметрия внешних данных

События за пределами сети также являются важным источником сетевой телеметрии. Сопоставление внутренней телеметрии и внешних событий с требованиями сетевой системы, как описано в [NMRG-ANTICIPATED-ADAPTATION], обеспечивает стратегические и функциональные преимущества для операций управления.

Как и другие источники данных телеметрии, внешние данные и события должны удовлетворять строгим требованиям, особенно в части своевременности, что необходимо для подобающего встраивания сведений о внешних событиях в приложения управления сетью. Конкретные вопросы и проблемы указаны ниже.

- Внешними детекторами событий могут быть разные элементы, включая оборудование (например, физические датчики, такие как сейсмометры) и программы (например, источники больших данных, способные анализировать потоки сообщений, такие как сообщения Twitter). Поэтому должна поддерживаться передача данных разной формы, при этом схема должна быть единой, но расширяемой.

- Поскольку основной функцией внешних детекторов является отправка уведомлений, предполагается их своевременность. После отправки сообщений их нужно быстро собрать и внедрить в плоскость управления с разными приоритетами, зависящими от важности источников и событий.

- Используемая внешними детекторами схема должна легко приспосабливаться к имеющимся и будущим устройствам и приложениям. Поэтому она должна легко сопоставляться с имеющимися моделями данных, такими как YANG.

- Поскольку взаимодействие с внешними объектами за пределами сети провайдера может происходить через Internet, риск перегрузки в этом случае играет очень важную роль и требует принятия соответствующих мер. Требуются решения, подобные автоматическим выключателям на уровне сетевого транспорта.

Объединение внутренней и внешней телеметрии будет играть важную роль для применения возможностей управления в имеющихся и будущих сетевых системах, что отражается во включении когнитивных (познавательных) возможностей в новое оборудование и программные (виртуальные) элементы.

3.2. Блоки функций второго уровня

Модули телеметрии в каждой плоскости можно дополнительно разделить на 5 концептуальных блоков.

- Запрос, анализ и хранение данных. Этот блок работает с приложением сетевых операций, показанным на рисунке 1. Обычно это является частью системы управления сетью на приёмной стороне. Этот блок отвечает за формирование требований к данным. Интересующие данные могут моделироваться через конфигурацию или пользовательские программы моделирования. Данные могут извлекаться по запросам , а также через подписку на события или потоковые данные. Блок принимает, хранит и обрабатывает возвращённые сетевыми устройствами данные. Анализ данных может быть интерактивным для создания последующих запросов. Блок функций может быть централизованным или распределенным и может иметь 1 или несколько экземпляров.

- Настройка данных и подписка. Этот блок управляет запросами данных на устройствах. Он определяет для приложений протокол и канал получения желаемых данных, а также отвечает за настройку нужных данных, которые могут быть недоступны от источника напрямую. Подписку можно описать моделями, шаблонами или программами.

- Кодирование и экспорт данных. Этот блок определяет, как данные телеметрии будут доставляться для анализа и хранения с контролем доступа. Кодирование данных и протоколы доставки могут меняться в зависимости от цели (местоположения) экспорта.

- Генерация и обработка данных. Запрошенные данные должны быть собраны, отфильтрованы, обработаны и форматированы в сетевых устройствах из «сырых» данных от источников. Это может включать расчёты и обработку на быстром или медленном пути в устройствах.

- Объект и источник данных. Этот блок определяет объекты мониторинга и исходные источники данных в устройстве. Источник обычно просто отдаёт «сырые» данные, которые требуют дальнейшей обработки. Каждый источник данных можно считать датчиком. Некоторые источники могут создаваться динамически.

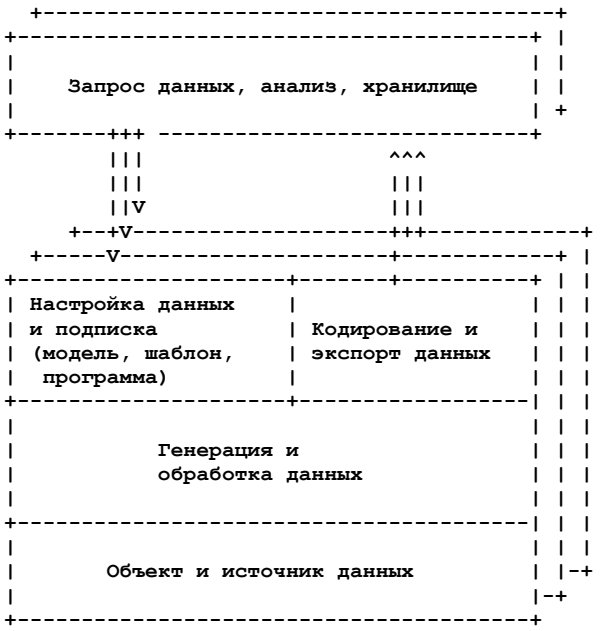

Рисунок 2. Блоки модели сетевой телеметрии.

3.3. Абстракции механизмов извлечения и типов данных

В общем случае сетевые данные могут быть получены через подписку (push) и запросы (poll). Подписка - это соглашение между издателем и подписчиком. После организации подписки указанные в ней данные автоматически доставляются зарегистрированным подписчикам, пока соглашение действует. Есть два варианта подписки с получение предопределённых или выбираемых подписчиком данных.

Запросы применяются в тех случаях, когда клиент ожидает незамедлительного разового отклика от сетевых устройств. Запрошенные данные могут напрямую извлекаться из указанного источника или синтезироваться и обрабатываться на основе «сырых» данных. Запросы удобны для интерактивных приложений сетевой телеметрии.

В общем случае данные можно извлекать (запрашивать) по мере необходимости, но во многих случаях выталкивание данных (подписка) более эффективно и может снижать задержку на обнаружение изменений клиентом. С точки зрения потребителя имеется 4 типа данных от сетевых устройств, которые он может запрашивать или получать по подписке:

- Простые данные. Данные, которые уже доступны в каком-либо хранилище или статическом датчике сетевого устройства.

- Производные данные. Данные, которые нужно синтезировать или обрабатывать в сети на основе «сырых» данных от одного или нескольких сетевых устройств. Функция обработки данных может быть статической или загружаться в сетевое устройство динамически.

- Вызванные событиями данные. Данные, которые извлекаются в результате каких-либо событий, например, переход рабочего состояния интерфейса между включённым и отключённым (up, down). Такие данные могут активно выталкиваться через подписку или извлекаться (poll) по запросам. Есть много способов моделирования событий, включая использование конечных автоматов (Finite State Machine или FSM) и действия по событиям (Event Condition Action или ECA) [NETMOD-ECA-POLICY].

- Потоковые данные. Это может быть временной срез или дамп базы данных, например, счётчик пакетов на интерфейсе, экспортируемый каждую секунду. Потоковые данные отражают состояние сети и показатели в реальном масштабе времени, поэтому для них нужна высокая пропускная способность и вычислительная мощность. Потоковые данные всегда активно выталкиваются подписчикам.

Указанные типы данных телеметрии не являются взаимоисключающими и зачастую типы будут композитными. Производные данные состоят из простых данных, сведения, инициированные событиями, могут быть простыми или производными данными, а потоковые данные могут быть основаны на неких повторяющихся событиях. Связи между типами данных показаны на рисунке 3.

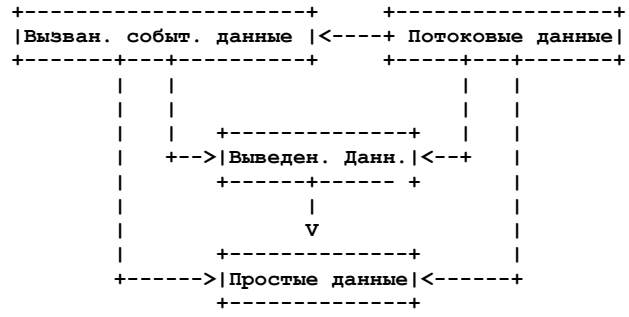

Рисунок 3. Связи между типами данных.

Подписка обычно имеет дело с данными, вызванными событиями, и потоковыми данными, а по запросам обычно передаются простые и производные данные, но возможны и иные варианты. Усовершенствованные методы сетевой телеметрии предназначены в основном для подписки на вызванные событиями или потоковые данные, а также для запросов производных данных.

3.4. Сопоставление модели с имеющимися механизмами

В таблице 2 показано размещение имеющихся механизмов (прежде всего опубликованных IETF и связанных с новейшими технологиями) в модели телеметрии. Учитывая разнообразие выполняемых работ, невозможно представить исчерпывающий список, поэтому приведённые в таблице механизмы следует считать просто примерами. Кроме того, некоторые полнофункциональные протоколы и методы могут охватывать несколько аспектов или модулей модели, поэтому название блока подчёркивает лишь одну его характеристику. Более подробные описания некоторых механизмов представлены в Приложении А.

Таблица 2. Сопоставление существующих работ

	Плоскость администрирования	***Плоскость управления***	***Плоскость пересылки***
Генерация данных и подписка	gNMI, NETCONF, RESTCONF, SNMP, YANG-Push	gNMI, NETCONF, RESTCONF, YANG-Push	NETCONF, RESTCONF, YANG-Push
Генерация и обработка данных	MIB, YANG	YANG	IOAM, PSAMP, PBT, AM
Кодирование и экспорт данных	gRPC, HTTP, TCP	BMP, TCP	IPFIX, UDP

Хотя модель в общем случае подходит для любой сетевой среды, в многодоменной телеметрии возникают вопросы, которые заслуживают дальнейшего архитектурного рассмотрения, но выходят за рамки документа.

4. Развитие приложений сетевой телеметрии

Сетевая телеметрия - это развивающаяся техническая область. По мере перехода сетей к самоуправлению приложения сетевой телеметрии проходят несколько этапов развития, задающих новые уровни требований к методам телеметрии базовых сетей. Каждый этап строится на методах, принятых предыдущими этапами, и вносит некоторые новые требования.

Этап 0 - Статическая телеметрия

Источники и типы данных телеметрии задаются при разработке. Операторы сетей могут лишь настраивать их использование с ограниченной гибкостью.

Этап 1 - Динамическая телеметрия

Заданные пользователем данные телеметрии могут динамически настраиваться или программироваться в процессе работы без прерывания сетевых операций, что позволяет найти компромисс между ресурсами, производительностью, гибкостью и сферой охвата.

Этап 2 - Интерактивная телеметрия

Сетевые операторы могут в любой момент настраивать и юстировать набор данных телеметрии в реальном масштабе времени в соответствии с требованиями к видимости сетей. По сравнению с этапом 1 изменения происходят более часто на основе обратной связи в реальном масштабе времени. На этом этапе некоторые задачи могут быть автоматизированы, но по-прежнему требуется присутствие человека для принятия решений.

Этап 3 - Телеметрия с обратной связью

Телеметрия освобождается от участия людей-операторов за исключением генерации отчётов. Интеллектуальный механизм управления сетью автоматически выдаёт запросы на данные телеметрии, анализирует данные и обновляет сетевые операции в контуре управления с обратной связью (замкнутом).

Имеющиеся технологии соответствуют этапам 0 и 1, имеются также отдельные приложения для этапов 2 и 3. Однако в будущем сетям с самоуправлением потребуется полнофункциональная система управления операциями, соответствующая этапам 2 и 3 для охвата всех сетевых операций. Чётко заданная модель сетевой телеметрии является первым шагом в этом направлении.

5. Вопросы безопасности

Сложность сетевой телеметрии оказывает существенное влияние на безопасность. Например, данными телеметрии можно манипулировать для истощения сетевых ресурсов, а также ресурсов потребителя данных, подмена или искажение данных могут исказить процессы принятия решений и парализовать работу сети, а неправильная настройка или программирование для телеметрии могут наносить вред. Данные телеметрии являются конфиденциальными, поскольку раскрывают сведения о сети и её конфигурации. Часть сведений (например, подробности об используемых программах и исправлениях для них) может значительно упростить организацию атак на сеть и позволить злоумышленникам определить, какое из устройств уязвимо.

Учитывая, что в этом документе предложена модель для сетевой телеметрии, а рассматриваемые механизмы выходят за рамки (по частоте сообщений и объёму трафика) традиционных концепций OAM, требуется осознать возможность возникновения новых проблем безопасности. Уже имеется много методов защиты для плоскостей пересылки, управления и администрирования в сети, но важно понять, не будут ли активизированы новые направления атак с использованием процедур и механизмов сетевой телеметрии.

Этот документ предлагает концептуальную архитектуру для сбора, транспортировки и анализа широкого спектра данных от разных источников для поддержки сетевых приложений. Протоколы, форматы данных и конфигурации, выбранные для реализации этой модели будут определять конкретные соображения безопасности, которые могут включать перечисленные ниже.

- Модели доверия и правил для телеметрии.
- Управление ролями и контроль доступа для включения и отключения возможностей телеметрии.
- Транспорт, применяемый для данных телеметрии и присущие ему свойства безопасности.
- Хранилища данных телеметрии, методы доступа и практика хранения.
- Отслеживание событий и аномалий телеметрии, которые могут указывать на атаки, использующие интерфейсы телеметрии.
- Проверка подлинности и целостности телеметрических данных для повешения доверия к ним.
- Отделение трафика телеметрии от трафика данных в сети (например, данные управления и телеметрии могут передаваться через отдельную сеть управления).

Некоторые из указанных выше вопросов безопасности могут быть исключены или минимизированы за счёт управления правилами сетевой телеметрии. При развёртывании телеметрии целесообразно разделить возможности телеметрии по разным классам, например «управление по ролям», «действия по событиям». Возможные конфликты между механизмами сетевой телеметрии должны обнаруживаться точно и быстро устраняться для предотвращения ненужного распространения трафика телеметрии, способного стать предусмотренной или нечаянной атакой на службы (DoS).

Потребуется дальнейшее изучение вопросов безопасности и предполагается, что будут разработаны и развёрнуты протоколы и механизмы защиты вместе с системами сетевой телеметрии.

6. Взаимодействие с IANA

Этот документ не требует действий IANA.

7. Литература

[gnmi] Shakir, R., Shaikh, A., Borman, P., Hines, M., Lebsack, C., and C. Marrow, "gRPC Network Management Interface", IETF 98, March 2017, <https://datatracker.ietf.org/meeting/98/materials/slides-98-rtgwg-gnmi-intro-draft-openconfig-rtgwg-gnmi-spec-00>.

[gpb] Google Developers, "Protocol Buffers", <https://developers.google.com/protocol-buffers>.

[grpc] gRPC, "gPPC: A high performance, open source universal RPC framework", <https://grpc.io>.

[IPPM-IOAM-DIRECT-EXPORT] Song, H., Gafni, B., Zhou, T., Li, Z., Brockners, F., Bhandari, S., Ed., Sivakolundu, R., and T. Mizrahi, Ed., "In-situ OAM Direct Exporting", Work in Progress, Internet-Draft, draft-ietf-ippm-ioam-direct-export-07, 13 October 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-ippm-ioam-direct-export-07>.

[IPPM-POSTCARD-BASED-TELEMETRY] Song, H., Mirsky, G., Filsfils, C., Abdelsalam, A., Zhou, T., Li, Z., Mishra, G., Shin, J., and K. Lee, "In-Situ OAM Marking-based Direct Export", Work in Progress, Internet-Draft, draft-song-ippm-postcard-based-telemetry-12, 12 May 2022, <https://datatracker.ietf.org/doc/html/draft-song-ippm-postcard-based-telemetry-12>.

[NETCONF-DISTRIB-NOTIF] Zhou, T., Zheng, G., Voit, E., Graf, T., and P. Francois, "Subscription to Distributed Notifications", Work in Progress, Internet-Draft, draft-ietf-netconf-distributed-notif-03, 10 January 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-netconf-distributed-notif-03>.

[NETCONF-UDP-NOTIF] Zheng, G., Zhou, T., Graf, T., Francois, P., Feng, A. H., and P. Lucente, "UDP-based Transport for Configured Subscriptions", Work in Progress, Internet-Draft, draft-ietf-netconf-udp-notif-05, 4 March 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-netconf-udp-notif-05>.

[NETMOD-ECA-POLICY] Wu, Q., Bryskin, I., Birkholz, H., Liu, X., and B. Claise, "A YANG Data model for ECA Policy Management", Work in Progress, Internet-Draft, draft-ietf-netmod-eca-policy-01, 19 February 2021, <https://datatracker.ietf.org/doc/html/draft-ietf-netmod-eca-policy-01>.

[NMRG-ANTICIPATED-ADAPTATION] Martinez-Julia, P., Ed., "Exploiting External Event Detectors to Anticipate Resource Requirements for the Elastic Adaptation of SDN/NFV Systems", Work in Progress, Internet-Draft, draft-pedro-nmrg-anticipated-adaptation-02, 29 June 2018, <https://datatracker.ietf.org/doc/html/draft-pedro-nmrg-anticipated-adaptation-02>.

[NMRG-IBN-CONCEPTS-DEFINITIONS] Clemm, A., Ciavaglia, L., Granville, L. Z., and J. Tantsura, "Intent-Based Networking - Concepts and Definitions", Work in Progress, Internet-Draft, draft-irtf-nmrg-ibn-concepts-definitions-09, 24 March 2022, <https://datatracker.ietf.org/doc/html/draft-irtf-nmrg-ibn-concepts-definitions-09>.

[OPSAWG-DNP4IQ] Song, H., Ed. and J. Gong, "Requirements for Interactive Query with Dynamic Network Probes", Work in Progress, Internet-Draft, draft-song-opsawg-dnp4iq-01, 19 June 2017, <https://datatracker.ietf.org/doc/html/draft-song-opsawg-dnp4iq-01>.

[OPSAWG-IFIT-FRAMEWORK] Song, H., Qin, F., Chen, H., Jin, J., and J. Shin, "A Framework for In-situ Flow Information Telemetry", Work in Progress, Internet-Draft, draft-song-opsawg-ifit-framework-17, 22 February 2022, <https://datatracker.ietf.org/doc/html/draft-song-opsawg-ifit-framework-17>.

[RFC1157] Case, J., Fedor, M., Schoffstall, M., and J. Davin, "Simple Network Management Protocol (SNMP)", RFC 1157, DOI 10.17487/RFC1157, May 1990, <https://www.rfc-editor.org/info/rfc1157>.

[RFC2578] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Structure of Management Information Version 2 (SMIv2)", STD 58, RFC 2578, DOI 10.17487/RFC2578, April 1999, <https://www.rfc-editor.org/info/rfc2578>.

[RFC2981] Kavasseri, R., Ed., "Event MIB", RFC 2981, DOI 10.17487/RFC2981, October 2000, <https://www.rfc-editor.org/info/rfc2981>.

[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, <https://www.rfc-editor.org/info/rfc3176>.

[RFC3411] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, DOI 10.17487/RFC3411, December 2002, <https://www.rfc-editor.org/info/rfc3411>.

[RFC3416] Presuhn, R., Ed., "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3416, DOI 10.17487/RFC3416, December 2002, <https://www.rfc-editor.org/info/rfc3416>.

[RFC3877] Chisholm, S. and D. Romascanu, "Alarm Management Information Base (MIB)", RFC 3877, DOI 10.17487/RFC3877, September 2004, <https://www.rfc-editor.org/info/rfc3877>.

[RFC3954] Claise, B., Ed., "Cisco Systems NetFlow Services Export Version 9", RFC 3954, DOI 10.17487/RFC3954, October 2004, <https://www.rfc-editor.org/info/rfc3954>.

[RFC4656] Shalunov, S., Teitelbaum, B., Karp, A., Boote, J., and M. Zekauskas, "A One-way Active Measurement Protocol (OWAMP)", RFC 4656, DOI 10.17487/RFC4656, September 2006, <https://www.rfc-editor.org/info/rfc4656>.

[RFC5085] Nadeau, T., Ed. and C. Pignataro, Ed., "Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires", RFC 5085, DOI 10.17487/RFC5085, December 2007, <https://www.rfc-editor.org/info/rfc5085>.

[RFC5357] Hedayat, K., Krzanowski, R., Morton, A., Yum, K., and J. Babiarz, "A Two-Way Active Measurement Protocol (TWAMP)", RFC 5357, DOI 10.17487/RFC5357, October 2008, <https://www.rfc-editor.org/info/rfc5357>.

[RFC5424] Gerhards, R., "The Syslog Protocol", RFC 5424, DOI 10.17487/RFC5424, March 2009, <https://www.rfc-editor.org/info/rfc5424>.

[RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <https://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, <https://www.rfc-editor.org/info/rfc6241>.

[RFC6812] Chiba, M., Clemm, A., Medley, S., Salowey, J., Thombare, S., and E. Yedavalli, "Cisco Service-Level Assurance Protocol", RFC 6812, DOI 10.17487/RFC6812, January 2013, <https://www.rfc-editor.org/info/rfc6812>.

[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, <https://www.rfc-editor.org/info/rfc7011>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <https://www.rfc-editor.org/info/rfc7258>.

[RFC7276] Mizrahi, T., Sprecher, N., Bellagamba, E., and Y. Weingarten, "An Overview of Operations, Administration, and Maintenance (OAM) Tools", RFC 7276, DOI 10.17487/RFC7276, June 2014, <https://www.rfc-editor.org/info/rfc7276>.

[RFC7540] Belshe, M., Peon, R., and M. Thomson, Ed., "Hypertext Transfer Protocol Version 2 (HTTP/2)", RFC 7540, DOI 10.17487/RFC7540, May 2015, <https://www.rfc-editor.org/info/rfc7540>.

[RFC7575] Behringer, M., Pritikin, M., Bjarnason, S., Clemm, A., Carpenter, B., Jiang, S., and L. Ciavaglia, "Autonomic Networking: Definitions and Design Goals", RFC 7575, DOI 10.17487/RFC7575, June 2015, <https://www.rfc-editor.org/info/rfc7575>.

[RFC7799] Morton, A., "Active and Passive Metrics and Methods (with Hybrid Types In-Between)", RFC 7799, DOI 10.17487/RFC7799, May 2016, <https://www.rfc-editor.org/info/rfc7799>.

[RFC7854] Scudder, J., Ed., Fernando, R., and S. Stuart, "BGP Monitoring Protocol (BMP)", RFC 7854, DOI 10.17487/RFC7854, June 2016, <https://www.rfc-editor.org/info/rfc7854>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

[RFC8084] Fairhurst, G., "Network Transport Circuit Breakers", BCP 208, RFC 8084, DOI 10.17487/RFC8084, March 2017, <https://www.rfc-editor.org/info/rfc8084>.

[RFC8085] Eggert, L., Fairhurst, G., and G. Shepherd, "UDP Usage Guidelines", BCP 145, RFC 8085, DOI 10.17487/RFC8085, March 2017, <https://www.rfc-editor.org/info/rfc8085>.

[RFC8259] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <https://www.rfc-editor.org/info/rfc8259>.

[RFC8321] Fioccola, G., Ed., Capello, A., Cociglio, M., Castaldelli, L., Chen, M., Zheng, L., Mirsky, G., and T. Mizrahi, "Alternate-Marking Method for Passive and Hybrid Performance Monitoring", RFC 8321, DOI 10.17487/RFC8321, January 2018, <https://www.rfc-editor.org/info/rfc8321>.

[RFC8639] Voit, E., Clemm, A., Gonzalez Prieto, A., Nilsen-Nygaard, E., and A. Tripathy, "Subscription to YANG Notifications", RFC 8639, DOI 10.17487/RFC8639, September 2019, <https://www.rfc-editor.org/info/rfc8639>.

[RFC8641] Clemm, A. and E. Voit, "Subscription to YANG Notifications for Datastore Updates", RFC 8641, DOI 10.17487/RFC8641, September 2019, <https://www.rfc-editor.org/info/rfc8641>.

[RFC8671] Evens, T., Bayraktar, S., Lucente, P., Mi, P., and S. Zhuang, "Support for Adj-RIB-Out in the BGP Monitoring Protocol (BMP)", RFC 8671, DOI 10.17487/RFC8671, November 2019, <https://www.rfc-editor.org/info/rfc8671>.

[RFC8762] Mirsky, G., Jun, G., Nydell, H., and R. Foote, "Simple Two-Way Active Measurement Protocol", RFC 8762, DOI 10.17487/RFC8762, March 2020, <https://www.rfc-editor.org/info/rfc8762>.

[RFC8889] Fioccola, G., Ed., Cociglio, M., Sapio, A., and R. Sisto, "Multipoint Alternate-Marking Method for Passive and Hybrid Performance Monitoring", RFC 8889, DOI 10.17487/RFC8889, August 2020, <https://www.rfc-editor.org/info/rfc8889>.

[RFC8924] Aldrin, S., Pignataro, C., Ed., Kumar, N., Ed., Krishnan, R., and A. Ghanwani, "Service Function Chaining (SFC) Operations, Administration, and Maintenance (OAM) Framework", RFC 8924, DOI 10.17487/RFC8924, October 2020, <https://www.rfc-editor.org/info/rfc8924>.

[RFC9069] Evens, T., Bayraktar, S., Bhardwaj, M., and P. Lucente, "Support for Local RIB in the BGP Monitoring Protocol (BMP)", RFC 9069, DOI 10.17487/RFC9069, February 2022, <https://www.rfc-editor.org/info/rfc9069>.

[RFC9197] Brockners, F., Ed., Bhandari, S., Ed., and T. Mizrahi, Ed., "Data Fields for In Situ Operations, Administration, and Maintenance (IOAM)", RFC 9197, DOI 10.17487/RFC9197, May 2022, <https://www.rfc-editor.org/info/rfc9197>.

[W3C.REC-xml-20081126] Bray, T., Paoli, J., Sperberg-McQueen, M., Maler, E., and F. Yergeau, "Extensible Markup Language (XML) 1.0 (Fifth Edition)", World Wide Web Consortium Recommendation REC-xml-20081126, November 2008, <https://www.w3.org/TR/2008/REC-xml-20081126>.

[y1731] ITU-T, "Operations, administration and maintenance (OAM) functions and mechanisms for Ethernet-based networks", ITU-T Recommendation G.8013/Y.1731, August 2015, <https://www.itu.int/rec/T-REC-Y.1731/en>.

Приложение A. Обзор имеющихся методов сетевой телеметрии

В этом ненормативном приложении представлен обзор некоторых имеющихся методов и предложенных стандартов для каждого из модулей сетевой телеметрии.

A.1. Телеметрия плоскости администрирования

A.1.1. Расширения NETCONF для выталкивания

NETCONF [RFC6241] - это популярный протокол сетевого управления, рекомендуемый IETF. Его основное назначение состоит в управлении конфигурацией, но протокол пригоден и для сбора данных. Модель YANG-Push [RFC8639] [RFC8641] расширяет NETCONF и разрешает подписчикам запрашивать непрерывный, настраиваемый поток обновления из хранилища YANG. Видимость изменений, вносимых в конфигурацию YANG и работающие объекты даёт новые возможности, основанные на удалённом отображении (mirroring) конфигурации и операционного состояния. Кроме того, механизм распределенного сбора данных [NETCONF-DISTRIB-NOTIF] с помощью канала публикации UDP [NETCONF-UDP-NOTIF] обеспечивает рост эффективности телеметрии на основе NETCONF.

A.1.2. Интерфейс управления gRPC

Интерфейс сетевого управления gRPC (gRPC Network Management Interface или gNMI) [gnmi] обеспечивает протокол управления сетью на основе модели удалённого вызова процедур gRPC [grpc] (Remote Procedure Call или RPC). Одно определение службы gRPC позволяет охватить настройку конфигурации и телеметрию. Коммуникационная модель gRPC с открытым исходным кодом основана на HTTP/2 [RFC7540] и обеспечивает многочисленные возможности для сетевой телеметрии, включая указанные ниже.

- Модель полнодуплексной транспортировки в комбинации с двоичным кодированием обеспечивает высокую эффективность телеметрии.
- Согласованность функций верхних уровней на разных платформах, которую обычно не обеспечивают базовые библиотеки HTTP/2. Это свойство особенно важно, поскольку сборщики данных телеметрии обычно работают на разных платформах.
- Встроенный механизм балансировки и аварийного переключения.

A.2. Телеметрия плоскости управления

A.2.1. Протокол мониторинга BGP

Протокол BMP [RFC7854] служит для мониторинга сессий BGP и предназначен для обеспечения удобного интерфейса при получении представлений маршрутов (route view).

Маршрутные данные BGP собираются с отслеживаемых устройств на станцию мониторинга BMP через организованную сессию BMP TCP. Партнёры BGP отслеживаются с помощью уведомлений BMP Peer Up и Peer Down. Маршруты BGP (включая Adj_RIB_In [RFC7854], Adj_RIB_out [RFC8671], и локальную базу RIB [RFC9069]) инкапсулируются в сообщения BMP Route Monitoring и BMP Route Mirroring, обеспечивающие исходный дамп таблицы и обновления маршрутов в реальном масштабе времени. В дополнение к этому передаётся статистика BGP в сообщениях BMP Stats Report Message, которые могут передаваться по таймеру или событиям. Будущие расширения BMP могут дополнительно обогатить приложения для мониторинга BGP.

A.3. Телеметрия плоскости данных

A.3.1. Технология чередующейся маркировки (AM)

Метод чередующейся маркировки (Alternate-Marking) позволяет эффективно измерять потери пакетов, задержку и её вариации в сетях IP и наложенных (Overlay) сетях, как описано в [RFC8321] и [RFC8889].

Этот метод применим для потоков «точка-точка» и «точка-много точек». AM создаёт группы (batch) пакетов, меняя значение одного бита (или метки) в заголовке пакета. Эти группы пакетов однозначно распознаются в сети и сравнение счётчиков пакетов позволяет определить потери пакетов. Эта же идея модет применяться для измерения задержки путём выбора специальных (ad hoc) пакетов с битом маркировки для измерения задержки.

Методу AM нужны два счётчика на каждый период маркировки для каждого контролируемого потока. Например, при рассмотрении n точек измерения и m отслеживаемых потоков порядок числа счётчиков для каждого интервала измерений составляет n*m*2 (1 счётчик на цвет).

Поскольку сети предлагают широкий набор данных для измерения производительности (например, счётчики пакетов), традиционные подходы сталкиваются с ограничениями. Узким местом является генерация и экспорт данных, а также объем данных, которые разумно собирать в сети. Кроме того, задачи управления, связанные с определением и настройкой данных для генерации, существенно усложняют развёртывание.

Многоточечная чередующаяся маркировка (Multipoint Alternate-Marking) описанная в [RFC8889], нацелена на решение этой проблемы и повышение гибкости мониторинга производительности при потребности в детальном анализе. Приложение координирует задачи измерения производительности сети для оптимизации мониторинга и может выбрать точность настройки точек измерения в зависимости от потребностей.

Используя AM, можно контролировать многоточечную сеть без углублённого изучения с помощью кластеризации (кластерами названы подсети, являющиеся частью сети и имеющие свойства сети в целом). В случае потери пакетов или слишком большой задержки можно применить специальные фильтры для сбора более детального анализа с использованием иной комбинации кластеров вплоть до измерения на уровне потока, как описано в [RFC8321].

Таким образом, приложение может настроить сквозной мониторинг сети. Если в сети не возникает проблем, приблизительный мониторинг достаточно хорош и не требует значительных сетевых ресурсов. При возникновении проблемы приложение узнает об этом из оценочного мониторинга и настраивает точки измерения более точно для получения дополнительных сведений и локализации связанной с проблемой части сети. После обнаружения и устранения проблем можно вернуться к приблизительному мониторингу.

A.3.2. Динамические сетевые зонды

Аппаратные динамические датчики (Dynamic Network Probe или DNP) [OPSAWG-DNP4IQ] обеспечивают программируемые средства для настройки данных, собираемых приложением из плоскости данных. Явным преимуществом DNP является снижение объёма экспортируемых данных. Полное решение DNP охватывает несколько направлений, включая источники данных, подписку и генерацию данных. Подписка нужна для определения производных данных, которые могут быть составлены и выведены из «сырых» данных. Генерация данных пользуется преимуществами умеренных расчётов в сети для создания желаемых данных.

Хотя DNP могут обеспечить очень высокую гибкость телеметрии в плоскости данных, с ними могут быть связаны некоторые проблемы. Для применения датчиков нужна гибкая плоскость данных с возможностью динамического программирования в процессе работы. Интерфейсы API для этого ещё не разработаны.

A.3.3. Протокол IPFIX

Сетевой трафик можно рассматривать как набор потоков, проходящих через элементы сети. Протокол IPFIX [RFC7011] обеспечивает средства передачи сведений о потоках для администрирования и иных целей. Типичная система с поддержкой IPFIX включает набор измерительных процессов, которые собирают пакеты данных в одной или нескольких точках наблюдения, могут фильтровать их, а затем агрегируют сведения об этих пакетах. После этого экспортёр собирает данные из всех точек наблюдения в домене наблюдения и передаёт эту информацию коллектору по протоколу IPFIX protocol.

A.3.4. In Situ OAM

Классические методы активного и пассивного мониторинга и измерений неточны или потребляют много ресурсов. Предпочтительно напрямую получать данные, связанные с потоками пакета при прохождении пакетов через сеть. Метод генерации данных IOAM [RFC9197] встраивает новый заголовок инструкций в пользовательские пакеты, а инструкции предписывают узлам сети добавлять в пакеты запрошенные данные. Таким образом, в конце пути можно собрать сведения о пакете, полученные в процессе пересылки. Такие данные «из первых рук» неоценимы для многих сетевых приложений OAM. Однако IOAM создаёт некоторые проблемы, влияя на производительность, безопасность, расширяемость и издержки. Кроме того, возникают проблемы с инкапсуляцией в некоторых протоколах, а также сложны реализации в нескольких доменах (cross-domain).

A.3.5. Телеметрия на основе «открыток»

Телеметрия на базе открыток (postcard), воплощенная в IOAM Direct Export (DEX) [IPPM-IOAM-DIRECT-EXPORT] и IOAM Marking [IPPM-POSTCARD-BASED-TELEMETRY], является дополнительным методов для IOAM на основе паспорта [RFC9197]. PBT напрямую экспортирует данные в каждом узле с помощью независимого пакета. За счёт дополнительного расхода пропускной способности и необходимости сопоставления данных PBT обеспечивает несколько уникальных преимуществ, а также помогает идентифицировать место отбрасывания пакета на пути пересылки.

A.3.6. OAM для конкретных плоскостей данных

Требования к OAM отличаются в разных плоскостях данных. В IETF опубликованы документы по методам и моделям OAM (например, [RFC8924] и [RFC5085]), предназначенные для таких плоскостей данных, как MPLS, L2VPN, NVO3 (Network Virtualization over Layer 3), VXLAN, BIER (Bit Index Explicit Replication), SFC (Service Function Chaining), SR (Segment Routing), DETNET (Deterministic Networking). Упомянутые выше методы телеметрии в плоскости данных могут применяться для расширения возможностей OAM в этих плоскостях данных.

A.4. Телеметрия внешних данных и событий

A.4.1. Источники внешних событий

Чтобы информация от внешних детекторов событий, используемая системами управления сетью, была полезна для управления, модель сетевой телеметрии должна обеспечивать таким детекторам (источникам) простоту подключения к средствам управления (приёмникам). Для этого нужна спецификация списка потенциальных внешних источников данных, которые могут быть интересны для управления сетью, и сопоставление источников с соединителями и/или интерфейсами.

Некоторые интересные для управления сетью категории внешних источников перечислены ниже.

- «Умные» объекты и датчики. С консолидацией IoT (Internet of Things) любая сетевая система будет иметь много смарт-объектов, подключённых к её физическому окружению и логическим операционным средам. Большинство таких объектов будет основано на различных датчиках (температура, влажность, давление и пр.) и предоставляемые ими сведения может быть очень полезной для управления сетью, даже если датчики не предназначены специально для этого. Элементы этого типа источников обычно будут предоставлять конкретный протокол для взаимодействия, чаще всего - один из протоколов, связанных с IoT, например CoAP.

- Сетевые службы новостей. Некоторые сетевые службы новостей имеют возможность предоставлять огромный объем информации о происходящих в мире событиях. Некоторые из этих событий могут влиять на сетевые системы, управляемые конкретной моделью, поэтому такая информация модет быть интересная для них. Например, различные отчёты о безопасности, такие как CVE (Common Vulnerabilities and Exposures), от соответствующего агентства могут использоваться управляющим решением для обновления системы при необходимости. Вместо конкретного протокола и формата источники этого типа обычно применяют неформализованный, но структурированный формат. Этот формат может быть частью онтологии и информационной модели платформы телеметрии.

- Анализаторы глобальных событий. Современные анализаторы больших данных предлагают огромные массивы информации и, что ещё интересней, идентификацию событий, обнаруженных путём анализа множества потоков данных из разных источников. В отличие от других типов источников, ориентированных на конкретные события, детекторы этого типа обнаруживают события общего значения. Например, во время спортивного мероприятия какое-то неожиданное движение оказывается захватывающим и множество людей подключается к сайтам, сообщающим о нём. Базовые сети, поддерживающие службу, которая показывает это событие, окажутся под его влиянием, поэтому системе управления следует знать о событии. В отличие от источников иного типа для интеграции этих извещателей нужна новая информационная модель, форматы и протоколы информирования.

В систему могут добавляться типы детекторов, но в общем случае это будет результатом объединения свойств, приведённых выше основных классов.

A.4.2. Соединители и интерфейсы

Для обеспечения интеграции внешних датчиков событий с другими управляющими решениями оба участника процесса должны раскрывать интерфейсы и протоколы, соответствующие их конкретным задачам. Поскольку внешние детекторы событий ориентируются на предоставление сведений своим основным потребителям, которые в общем случае не привязаны к задачам управления сетями, модель должна включать определения требуемых соединителей для обеспечения эффективной связи между детекторами (источниками) и их потребителями в системах управления сетями (получатели.

В некоторых случаях соединение между внешними датчиками событий и системой управления осуществляется в плоскости администрирования. Для этого будут служить специальные соединители, предоставляющие типовые интерфейсы в большинстве других элементов, подключённых к плоскости управления. Например, интерфейсы могут реализовать это с помощью определённой модели данных (YANG) и конкретного протокола телеметрии, такого как NETCONF, YANG-Push, gRPC.

Благодарности

Спасибо Rob Wilton, Greg Mirsky, Randy Presuhn, Joe Clarke, Victor Liu, James Guichard, Uri Blumenthal, Giuseppe Fioccola, Yunan Gu, Parviz Yegani, Young Lee, Qin Wu, Gyan Mishra, Ben Schwartz, Alexey Melnikov, Michael Scharf, Dhruv Dhody, Martin Duke, Roman Danyliw, Warren Kumari, Sheng Jiang, Lars Eggert, Éric Vyncke, Jean-Michel Combes, Erik Kline, Benjamin Kaduk и многим другим, кто предоставил полезные замечания и предложения, улучшившие документ.

Участники работы

В работе над документом участвовали Tianran Zhou, Zhenbin Li, Zhenqiang Li, Daniel King, Adrian Farrel, Alexander Clemm.

Адреса авторов

Haoyu Song
Futurewei
United States of America
Email: haoyu.song@futurewei.com

Fengwei Qin
China Mobile
China
Email: qinfengwei@chinamobile.com

Pedro Martinez-Julia
NICT
Japan
Email: pedro@nict.go.jp

Laurent Ciavaglia
Rakuten Mobile
France
Email: laurent.ciavaglia@rakuten.com

Aijun Wang
China Telecom
China
Email: wangaj3@chinatelecom.cn

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru