

Internet Engineering Task Force (IETF)
Request for Comments: 9940
Category: Informational
ISSN: 2070-1721

N. Davis, Ed.
Ciena
A. Farrel, Ed.
Old Dog Consulting
T. Graf
Swisscom
Q. Wu
C. Yu
Huawei
April 2026

Some Key Terms for Network Fault and Problem Management

Некоторые важные термины для сетевых отказов и решения проблем

Аннотация

Этот документ определяет некоторые термины, имеющие важное значение для понимания сетевых отказов и работы с проблемами в рамках IETF.

Целью документа является внесение ясности в обсуждения и другую работу, связанную с отказами в сетях и решением проблем, в частности, модели данных YANG и протоколы управления, которые информируют и визуализируют сетевые отказы и помогают в решении проблем.

Статус документа

Документ не относится к категории Internet Standards Track и публикуется с информационными целями.

Документ является результатом работы IETF¹ и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG². Не все документы, одобренные IESG, претендуют на статус стандартов (см. раздел 2 в RFC 7841).

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке <https://www.rfc-editor.org/info/rfc9940>.

Авторские права

Авторские права (Copyright (c) 2026) принадлежат IETF Trust и лицам, указанным в качестве авторов документа. Все права защищены.

К документу применимы права и ограничения, указанные в BCP 78 и IETF Trust Legal Provisions и относящиеся к документам IETF (<http://trustee.ietf.org/license-info>), на момент публикации данного документа. Прочтите упомянутые документы внимательно. Фрагменты программного кода, включённые в этот документ, распространяются в соответствии с пересмотренной лицензией BSD (Revised BSD License), как указано в параграфе 4.e документа IETF Trust Legal Provisions, без каких-либо гарантий (как указано в Revised BSD License).

Оглавление

1. Введение.....	1
2. Использование терминов.....	2
3. Терминология.....	2
3.1. Связанные с контекстом термины.....	2
3.2. Основные термины.....	3
3.3. Прочие термины.....	4
4. Рабочие процессы.....	4
5. Вопросы безопасности.....	6
6. Вопросы приватности.....	6
7. Взаимодействие с IANA.....	6
8. Литература.....	6
Благодарности.....	7
Адреса авторов.....	7

1. Введение

Работа больших сетей зависит от эффективности управления сетью. Это требует замкнутого цикла - управление сетью, наблюдение за ней, сетевая аналитика, обеспечение гарантий (надёжности) и возврат на этой основе к управлению. Контроль отказов и решение проблем [RFC6632] являются важной частью управления сетью. Эти действия связаны с обнаружением, информированием, изоляцией, сопоставлением и управлением событиями в сети. Целью документа является сосредоточение внимания на событиях, оказывающих негативное влияние на способность сети пересылать трафик ожидаемым образом, что может сокращать возможности предоставления услуг. Такие события могут также влиять на возможность управлять сетью и её работой. В документе рассматриваются и другие отказы, способные снизить качество или надёжность сетевых услуг. Концепция контроля отказов и проблем распространяется и на действия по определению причин отказов и работы по восстановлению ожидаемого поведения сети.

¹Internet Engineering Task Force - комиссия по решению инженерных задач Internet.

²Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

Ряд работ в рамках IETF направлен на разработку компонентов системы контроля отказов, таких как модели данных YANG и протоколы управления. В таких работах важно использовать единую терминологию, чтобы обеспечить чёткое понимание взаимодействия элементов системы управления и управляющих решений, а также способов устранения отказов и решения проблем.

В этом документе обсуждаются термины, имеющие фундаментальное значение для базового понимания вопросов контроля отказов и решения проблем. Хотя концепции «отказов» (fault) и «проблем» (problem) актуальны на всех уровнях технологий Internet, область применения этого документа охватывает сетевой и нижележащие уровни. Документ посвящён именно контролю отказов и решению проблем в сети. Затронуты также понятие «инцидент» (incident), когда это является следствием одной или нескольких проблем и вызывает нарушение работы сетевых служб.

Отметим, что ряд полезных терминов определён в [RFC3877] и [RFC8632]. Определения в данном документе связаны с приведёнными там определениями, но не зависят от них.

2. Использование терминов

Определённые в документе термины предназначены для согласованного использования в рамках IETF в части вопросов решения проблем и контроля отказов в сети. В тех случаях, когда похожие концепции описаны другими организациями, предпринимались попытки привести описания в соответствие с такими концепциями, но требуется осторожность в тех случаях, когда термины не применяются согласованно разными организациями или относятся к уровням выше сетевого. Если определённые здесь термины будут сочтены полезными другими организациями, они могут свободно пользоваться ими.

Целью документа является определение перечисленных ниже терминов для использования в других документах. Отдельные термины определены для включения в основные определения и они также могут применяться в других документах, хотя это не является основной целью приведённых в документе определений.

- Event - событие
- State - состояние
- Fault - отказ, сбой
- Problem - проблема
- Symptom - симптом
- Cause - причина
- Alert - сигнал тревоги
- Alarm - тревожное оповещение

Предполагается, что при использовании определённых здесь терминов в других документах они будут указываться с заглавной буквы (как здесь), чтобы отличить их от разговорного применения. Также предполагается включение в начальный раздел списка заимствованных из этого документа терминов с цитатами.

3. Терминология

В этом разделе даны определения ключевых терминов:

- параграф 3.1 посвящён терминам, связанным с контекстом систем контроля отказов и решения проблем;
- параграф 3.2 содержит определения основных терминов, которые будут использоваться в документах, описывающих элементы систем контроля отказов и решения проблем;
- параграф 3.3 содержит определения трёх дополнительных терминов, которые могут быть полезны.

3.1. Связанные с контекстом термины

В этом параграфе представлены некоторые термины, помогающие описать контекст остальной части документа. Эти термины можно рассматривать как каскадную последовательность процессов, начиная с сетевой телеметрии и заканчивая наблюдением за сетью. Определения намеренно сделаны сравнительно краткими. В последующих документах эти определения могут быть расширены без потери конкретики. Такую контекстуализацию (при наличии) следует чётко выделять в документах.

Network Telemetry - сетевая телеметрия

Термин определён в [RFC9232] и описывает процесс сбора оперативных параметров сети, классифицируемых в соответствии с сетевой плоскостью (например, уровнями 3, 2 и 1), откуда они были получены. Данные, собранные процессом сетевой телеметрии, не включают сведений об определениях служб (намерений - intent, в соответствии с параграфом 3.1 в [RFC9315]).

Network Monitoring - мониторинг сети

Процесс непрерывной записи параметров, связанных с топологией сети. Мониторинг включает такие аспекты, как картины трафика, работоспособность устройств, показатели производительности и поведение сети в целом. Такой подход различает мониторинг сети и мониторинг ресурсов, который сосредоточен на отдельных ресурсах и компонентах (параграф 3.2).

Network Analytics - сетевая аналитика

Процесс получения аналитической информации из оперативных параметров сети. Аналитикой могут заниматься программные системы или люди, анализирующие оперативные данные и выводящие из них сведения, относящиеся, например, к симптомам.

Network Observability - наблюдение за сетью

Процесс, позволяющий оценивать поведение сети путём анализа наблюдаемых оперативных данных (журнальные файлы, тревожные оповещения, трассировки и т. п.) с целью выявления симптомов поведения сети и выявления аномалий и их причин. Наблюдение начинается со сведений, собранных инструментами мониторинга, которые могут дополняться другими оперативными данными. Ожидаемым результатом наблюдения за сетью является обнаружение и анализ отклонений в наблюдаемом состоянии сети от ожидаемого.

Таким образом, имеется каскад взаимосвязанных процессов:

- телеметрия обеспечивает сбор оперативных данных из сети;

- мониторинг обеспечивает запись и хранение данных сетевой телеметрии;
- аналитика обеспечивает получение новых сведений на основе данных мониторинга;
- наблюдение за сетью позволяет оценивать поведение сети с использованием сетевой аналитики.

3.2. Основные термины

Термины в этом разделе размещены в порядке, помогающем пониманию в процессе чтения. Рисунки и пояснения в разделе 4 могут дополнительно помочь в понимании определяемых здесь терминов.

Resource - ресурс

Элемент сетевой системы.

- Понятие ресурса является рекурсивным, т. е. ресурс может включать набор других ресурсов (например, узел сети включает набор сетевых интерфейсов).

Characteristic - характеристика

Наблюдаемый или измеряемый аспект или поведение, связанное с ресурсом.

- Характеристика может рассматриваться как основанная на фактах (см. Value), а также на контексте и дескрипторах, которые указывают факты и придают им смысл.
- Термин «метрика» (Metric, см. metric в [RFC9417]) служит другим обозначением характеристики и может рассматриваться как аналог термина «переменная» (variable).

Value - значение

Мера характеристики, связанной с ресурсом. Значение может быть представлено категорией (например, высокое, низкое), целым числом (например, показание счётчика или датчика), величиной непрерывной переменной (например, аналоговое измерение) и т. п.

Change - изменение

В контексте мониторинга сети изменением называется смена значения характеристики, связанной с ресурсом. Изменение может занимать некоторый интервал времени.

- Не все изменения значимы (см. Relevance).
- Восприятие изменений зависит от обнаружения, частоты, точности и детализации выборок, а также от точки зрения.
- Возможно, будет полезно уточнить термин как «изменение значения» (Value Change), поскольку английский слово change применяется очень широко.

Event - событие

Смена значения характеристики ресурса в определённый момент времени (короткий интервал).

- В отличие от изменения (Change), которое может занимать некоторое время, событие (Event) происходит в конкретный момент. Событием может быть наблюдение (фиксация) изменений.

Condition - условия, состояние

Интерпретация значений одной или нескольких характеристик ресурса (с точки зрения режима работы или иных аспектов, связанных с назначением или использованием ресурса), например, нехватка памяти. Т. е., это результат функции, применённой к набору переменных.

State - состояние, статус

Конкретные условия на ресурсе в определённый момент времени. Например, маршрутизатор может сообщать объём своей памяти и размер занятой части (значения двух характеристик ресурса), которые могут интерпретироваться как условия на ресурсе и, таким образом, определять состояние маршрутизатора, такое как нехватка памяти.

- Хотя состояние может наблюдаться в определённый момент времени, фактически оно определяется обобщением измерений за некоторый интервал времени, что иногда называют сжатием состояния.
- Может оказаться полезным уточнять этот термин как «состояние ресурса», чтобы отличать от других использований термина state, таких как «состояние протокола» (protocol state).
- Этот термин можно противопоставить «оперативному состоянию» (operational state) из [RFC8342]. Например, состояние канала может быть up/down/degraded, но его оперативное состояние будет включать набор значений характеристик канала.

Detect (hence Detected, Detection) - обнаружение (обнаруженный)

Фиксация наличия чего-либо (State, Change, Event, действия и т. д.).

- Это также означает фиксацию изменения (с точки зрения наблюдателя, например, системы мониторинга).

Relevance - релевантность (взаимосвязь)

Рассмотрение события, состояния или значения (путём применения правил в соответствии с конкретной точкой зрения или намерением, а также в связи с другими событиями, состояниями и значениями) для определения их значимости для системы, контролирующей сеть или управляющей ею. Не все изменения будут релевантными.

- Применимы также термины «релевантные события», «релевантные состояния», «релевантные значения».

Occurrence - произошедшее (событие, состояние и т. п.)

Релевантное событие или конкретное изменение.

- Это может быть совокупность или абстракция множества более мелких событий или изменений.
- Произошедшее можно рассматривать в микро- или макро-масштабе, поскольку понятие ресурса является рекурсивным. Восприятие произошедшего может зависеть от области наблюдения (в соответствии со степенью рекурсии рассматриваемых ресурсов), т. е. понятие происходящего, тоже является рекурсивным.

Fault - отказ, сбой

Нежелательное и ненужное произошедшее (событие или изменение), которое может указывать текущее или будущее нежелательное состояние. Отказ возникает в определённый момент времени и может быть связан с причиной (Cause). Более подробное рассмотрение сетевых отказов приведено в [RFC8632].

- Отметим, что имеются различия между отказом и проблемой в зависимости от контекста. Например, в службе подключения с резервированием отключение канала является проблемой, но с точки зрения управления ресурсами сети это будет отказом. В маршрутизаторе с двумя блоками питания выход из строя резервного источника питания, оставляющий основной источник без защиты, является проблемой.

Problem - проблема

Состояние, которое является нежелательным и может требовать действия по устранению. Проблема не обязательно связана с причиной, а разрешение проблемы не обязательно влияет на объект, в котором проблема возникла.

- Отметим, что с понятием «проблема» связан исторический аспект. Текущее состояние может рабочим, но при этом могут присутствовать непонятные отказы, сам факт наличия которых является проблемой.
- Пока проблема не решена, она может продолжать требовать внимания. Записи о решённых проблемах могут поддерживаться в журнале (log).
- Состояние может рассматриваться как проблема с нескольких точек зрения. Рассмотрим, например, «потерю света» (loss of light), которая может приводить к отказам многих служб. В этом примере новое состояние (восстановление света) может решать проблему с одной точки зрения (службы снова работают), но оставить её нерешённой с другой точки зрения (причина пропадания не была выяснена). Кроме того, в этом примере возможно иное развитие событий, когда проблема была решена (микроизгиб волокна, который был устранён), но при этом остаётся ещё одна проблема - непонятно, почему произошёл изгиб - и она осталась нерешённой.

Cause - причина

События (обнаруженные или нет) вызвавшие возникновение отказа или проблемы.

Incident - инцидент

Используется также термин «сетевой инцидент» (Network Incident). Нежелательное событие или состояние (Occurrence), такое как неожиданное прерывание работы сетевой службы или падение производительности службы ниже целевого уровня. Инцидент ведёт к возникновению одной или нескольких проблем, а проблемы могут вызывать один или несколько инцидентов и влиять на возникшие инциденты. Более подробное обсуждение взаимосвязей сетевых инцидентов, включая клиентские инциденты и контроль инцидентов, приведено в [Net-Incident-Mgmt-YANG].

Symptom - симптом

Наблюдаемое значение, изменение, состояние, событие или условия, служащие индикацией имеющейся или возможной проблемы.

Anomaly - аномалия

Используется также термин «сетевая аномалия» (Network Anomaly). Необычное или неожиданное событие или картина поведения сетевых данных в плоскости пересылки или плоскости управления, отличающиеся от обычного, ожидаемого поведения. Дополнительная информация приведена в [Net-Anomaly-Arch].

Alert - сигнал тревоги

Индикация отказа (сбоя).

Alarm - тревожное оповещение

В соответствии с [RFC8632], тревожное оповещение говорит о нежелательном состоянии ресурса, требующем исправления. С точки зрения управления такое оповещение можно рассматривать как отдельное состояние, переход в которое может приводить к сигналу тревоги (Alert). Получение сигнала тревоги может приводить к постоянной индикации (для оператора), указывающей наличие фактической или возможной проблемы.

3.3. Прочие термины

Полезны могут быть также три приведённых ниже термина, связанных с состояниями.

Intermittent - прерывистое

Состояние, которое не является непрерывным, но повторяется в течение некоего интервала времени.

Transient - временное

Состояние, которое не является непрерывным и происходит однократно в некоем интервале времени.

Recurrent - повторяющееся

Проблема, которую активно решают, но она повторяется

4. Рабочие процессы

Этот раздел предназначен для описания взаимосвязей между терминами, определёнными в параграфе 3.2, в контексте сетевых сбоев и решения проблем. Текст и рисунки являются поясняющими и не имеют нормативного характера.

На рисунке 1 показана связь между ресурсами и характеристиками. Отметим соотношение 1:n между сетевой системой и ресурсами, а также между ресурсами и характеристиками (для простоты это не показано на рисунке).

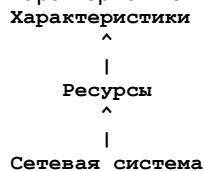


Рисунок 1. Ресурсы и характеристики.

Значение характеристики ресурса может меняться с течением времени. Конкретные изменения значения могут быть отмечены в определённый момент времени (как цифровые изменения), обнаружены (Detected) и сочтены событиями. Это показано в левой части рисунка 2. Средняя часть рисунка 2 показывает, как значение характеристики может меняться со временем. Значение может быть обнаружено в конкретное время или периодически и приводить к возникновению условий, являющихся состояниями (и смене состояний).



Рисунок 2. Характеристики и обновления.

На практике изменение характеристик со временем может быть аналоговым, как показано в правой части рисунка 2. Значение может считываться или сообщаться (обнаруживаться) периодически, что даёт аналоговые значения, которые могут считаться связанными (Relevant) или оцениваться с течением времени, как показано на рисунке 6.

На рисунке 3 показан рабочий процесс для события. Как отмечено выше, событие является изменением значения характеристики в определённый момент. Событие может быть оценено (с учётом правил, с конкретной точки зрения, с учётом намерений и в связи с другими событиями, состояниями и значениями) для определения, является ли это произошедшим (Occurrence) или может указывать изменение состояния. Произошедшее может быть нежелательным (отказ) и может приводить к генерации сигнала тревоги (Alert). Это может быть также свидетельством наличия проблемы и напрямую указывать причину. В некоторых случаях может подаваться сигнал тревоги для оповещения (Alarm) об имеющейся или возможной проблеме.



Рисунок 3. Событие и связанные термины.

На рисунке 4 показан рабочий процесс для состояний. Как показано на рисунке 2, изменение, отмеченное в определённый момент, вызывает состояние. Состояние может считаться значимым (Relevance) в плане правил, с конкретной точки зрения, с учётом намерений и в связи с другими событиями, состояниями и значениями. Релевантное состояние может считаться проблемой или указывать наличие или возможность возникновения проблемы.

Проблемы могут рассматриваться на основе симптомов или сопоставляться напрямую или опосредованно с причинами. Инцидент возникает в результате одной или нескольких проблем. Оповещение о тревоге (Alarm) может быть результатом проблемы, а переход в тревожное состояние может вызывать сигнал тревоги (Alert).



Рисунок 4. Состояние и связанные термины.

На рисунке 5 показано, как можно связать отказы и проблемы для определения причин. Стрелки показывают, как один элемент может порождать другой.

Причина может быть указана или определена по отказам, проблемам и симптомам. Одна причина может указывать на другую, а также может рассматриваться как симптом. При поиске причин может учитываться множество факторов. Инцидент является результатом одной или нескольких проблем.

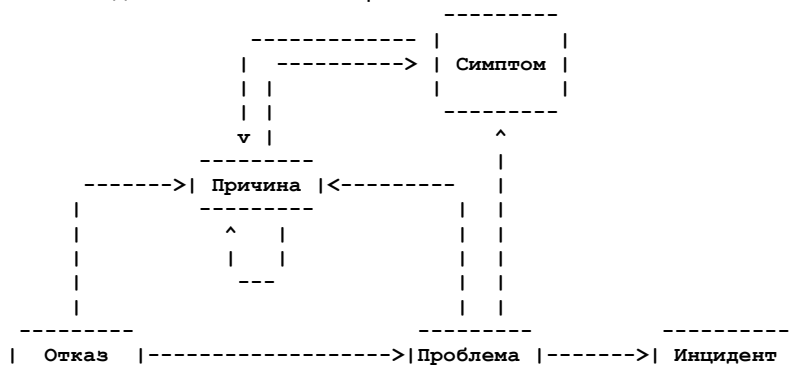


Рисунок 5. Консолидация симптомов и причин.

На рисунке 6 показано, насколько важны пороговые уровни при рассмотрении аналоговых значений и событий. Стрелки на рисунке показывают, как один элемент может порождать или использовать другой. К генерации событий и состояний на основе порогов (а также сигналов тревоги, которые они могут вызвать) следует относиться с осторожностью, чтобы не возникало «раскачки» (flapping), ведущей к неустойчивости состояний, и перегрузки процессов и систем управления. Аналоговые значения, считываемые или получаемые от ресурсов, которые могут пересекать пороги, можно считать

релевантными или оценивать с течением времени. События могут подсчитываться, а счётчики могут пересекать порог или достигать соответствующего (релевантного) значения.

Пороговый процесс может зависеть от реализации и подчиняться определённым правилам. При пересечении порога и выполнении других заданных условий событие может определяться и обрабатываться как любое другое событие.

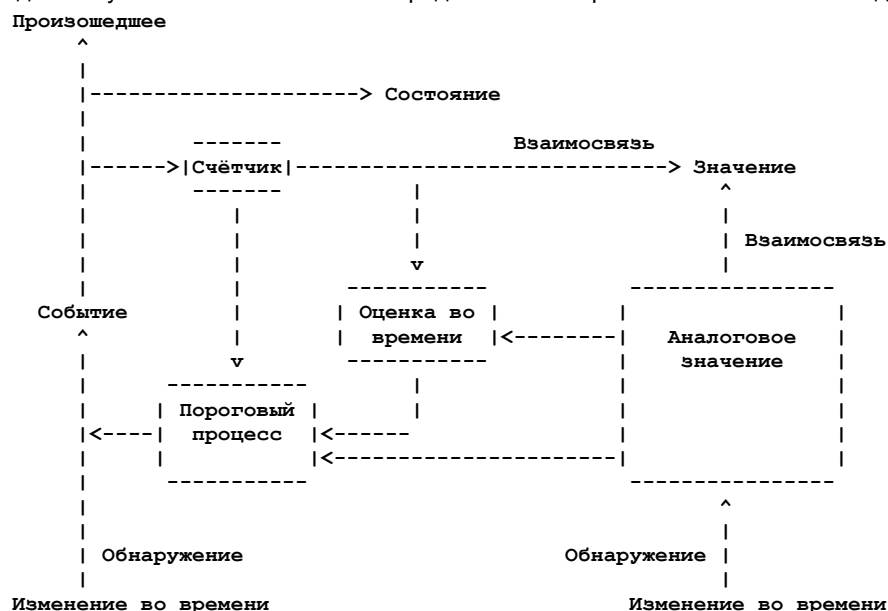


Рисунок 6. Счётчики, пороги и значения.

5. Вопросы безопасности

Этот документ определяет термины и не имеет прямого влияния на безопасность. Однако протокольные решения и модели управления должны учитывать отмеченные ниже аспекты.

- Раскрытие сведений об отказах и проблемах может давать информацию о внутреннем устройстве сети (в частности, о её уязвимостях), которой могут воспользоваться злоумышленники.
- Системы, генерирующие информацию для управления (сообщения, уведомления и т. п.) при возникновении сбоев, могут быть атакованы, в результате чего может существенно возрасти объем данных, которые будут перегружать систему сетевого управления вплоть до лишения способности корректно управлять сетью.
- Ложные сведения об отказах (или маскировка реальных отчётов) могут нарушить работу системы управления.

6. Вопросы приватности

При контроле сетевых отказов и проблем следует сохранять приватность пользователей, не раскрывая их данных и информации о действиях конечных пользователей.

Сетевая телеметрия включает наблюдение за сетевым трафиком и сбор оперативных данных в сети, а мониторинг обеспечивает запись и хранение данных телеметрии. Наблюдаемые и собираемые данные могут включать приватную информацию пользователей. Такие сведения должны быть защищены и доступ к ним должен контролироваться для предотвращения утечки. Может потребоваться особая осторожность при хранении информации, доступ к которой возможен в любое время (включая далёкое будущее).

Кроме того, операторам сетей следует заботиться о сохранении контроля над всей информацией об отказах для защиты своей приватности и деталей управления сетью.

7. Взаимодействие с IANA

Этот документ не требует действий IANA.

8. Литература

- [Net-Anomaly-Arch] Graf, T., Du, W., Francois, P., and A. Huang Feng, "A Framework for a Network Anomaly Detection Architecture", Work in Progress, Internet-Draft, draft-ietf-nmop-network-anomaly-architecture-06, 21 November 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-nmop-network-anomaly-architecture-06>>.
- [Net-Incident-Mgmt-YANG] Hu, T., Contreras, L. M., Wu, Q., Davis, N., and C. Feng, "A YANG Data Model for Network Incident Management", Work in Progress, Internet-Draft, draft-ietf-nmop-network-incident-yang-08, 13 February 2026, <<https://datatracker.ietf.org/doc/html/draft-ietf-nmop-network-incident-yang-08>>.
- [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>>.
- [RFC6632] Ersue, M., Ed. and B. Claise, "An Overview of the IETF Network Management Standards", RFC 6632, DOI 10.17487/RFC6632, June 2012, <<https://www.rfc-editor.org/info/rfc6632>>.
- [RFC8342] Bjorklund, M., Schoenwaelder, J., Shafer, P., Watsen, K., and R. Wilton, "Network Management Datastore Architecture (NMDA)", RFC 8342, DOI 10.17487/RFC8342, March 2018, <<https://www.rfc-editor.org/info/rfc8342>>.

- [RFC8632] Vallin, S. and M. Bjorklund, "A YANG Data Model for Alarm Management", [RFC 8632](#), DOI 10.17487/RFC8632, September 2019, <<https://www.rfc-editor.org/info/rfc8632>>.
- [RFC9232] Song, H., Qin, F., Martinez-Julia, P., Ciavaglia, L., and A. Wang, "Network Telemetry Framework", RFC 9232, DOI 10.17487/RFC9232, May 2022, <<https://www.rfc-editor.org/info/rfc9232>>.
- [RFC9315] Clemm, A., Ciavaglia, L., Granville, L. Z., and J. Tantsura, "Intent-Based Networking - Concepts and Definitions", [RFC 9315](#), DOI 10.17487/RFC9315, October 2022, <<https://www.rfc-editor.org/info/rfc9315>>.
- [RFC9417] Claise, B., Quilbeuf, J., Lopez, D., Voyer, D., and T. Arumugam, "Service Assurance for Intent-Based Networking Architecture", RFC 9417, DOI 10.17487/RFC9417, July 2023, <<https://www.rfc-editor.org/info/rfc9417>>.

Благодарности

Авторы благодарны Med Boucadair, Wanting Du, Joe Clarke, Javier Antich, Benoit Claise, Christopher Janz, Sherif Mostafa, Kristian Larsson, Dirk Von Hugo, Carsten Bormann, Hilarie Orman, Stewart Bryant, Bo Wu, Paul Kyzivat, Jouni Korhonen, Reshad Rahman, Rob Wilton, Mahesh Jethanandani, Tim Bray, Paul Aitken, and Deb Cooley за их полезные замечания.

Особая благодарность команде конференции IETF 120, собравшейся для обсуждения острых вопросов:

Benoit Claise
Watson Ladd
Brad Peters
Bo Wu
Georgios Karagiannis
Olga Havel
Vincenzo Riccobene
Yi Lin
Jie Dong
Aihua Guo
Thomas Graf
Qin Wu
Chaode Yu
Adrian Farrel

Адреса авторов

Nigel Davis (editor)
Ciena
United Kingdom
Email: ndavis@ciena.com

Adrian Farrel (editor)
Old Dog Consulting
United Kingdom
Email: adrian@olddog.co.uk

Thomas Graf
Swisscom
Binzring 17
CH-8045 Zurich
Switzerland
Email: thomas.graf@swisscom.com

Qin Wu
Huawei
101 Software Avenue, Yuhua District
Nanjing
Jiangsu, 210012
China
Email: bill.wu@huawei.com

Chaode Yu
Huawei
Email: yuchaode@huawei.com

Перевод на русский язык

Николай Малых
nmalykh@protokols.ru