

Internet Research Task Force (IRTF)  
Request for Comments: 9315  
Category: Informational  
ISSN: 2070-1721

A. Clemm  
Futurewei  
L. Ciavaglia  
Nokia  
L. Z. Granville  
Federal University of Rio Grande do Sul (UFRGS)  
J. Tantsura  
Microsoft  
October 2022

## Intent-Based Networking - Concepts and Definitions

Сеть на основе намерений - концепции и определения

### Аннотация

Сети на основе намерений (Intent или Intent-Based) берут отрасль штурмом. Однако термины, связанные с такими сетями, часто применяются расплывчато и непоследовательно, во многих случаях перекрываясь и смешиваясь с другими концепциями (например, политика - policy). В этом документе разъяснён термин «намерение» (intent) и дан обзор связанной с ним функциональности. Цель состоит в содействии общему пониманию терминов, концепций и функциональности, которые могли бы послужить основой для дальнейших определений исследовательских и инженерных задач, а также их решения.

Документ является результатом работы группы IRTF Network Management Research Group (NMRG) и отражает согласованное мнение группы, получив множество подробных положительных отзывов от участников группы. Документ публикуется с информационными целями.

### Статус документа

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

Документ является результатом работы IRTF<sup>1</sup>. IRTF публикует результаты относящихся к Internet исследований и разработок. Эти результаты могут оказаться не пригодными для реализации. Данный RFC представляет согласованное мнение исследовательской группы Coding for Efficient Network Communications в рамках IRTF. Документы, одобренные для публикации IRSG, не претендуют на статус Internet Standard (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/rfc9315>.

### Авторские права

Авторские права (Copyright (c) 2022) 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.

## Оглавление

|  |    |
|--|----|
| 1. Введение.....   | 2  |
| 2. Определения и сокращения.....                                   | 3  |
| 3. Концепции.....  | 3  |
| 3.1. Намерения и управление на их основе.....                      | 3  |
| 3.2. Связанные концепции.....                                      | 5  |
| 3.2.1. Модели сервиса.....   | 5  |
| 3.2.2. Политика и управление сетью на её основе.....               | 5  |
| 3.2.3. Различия между намерениями, политикой и моделями служб..... | 6  |
| 4. Принципы.....   | 7  |
| 5. Функциональность IBN.....                                       | 8  |
| 5.1. Реализация намерений.....                                     | 8  |
| 5.1.1. Восприятие намерений и взаимодействие с пользователями..... | 8  |
| 5.1.2. Трансляция намерений.....                                   | 8  |
| 5.1.3. Оркестровка намерений.....                                  | 8  |
| 5.2. Обеспечение намерений.....                                    | 8  |
| 5.2.1. Мониторинг.....   | 9  |
| 5.2.2. Оценка соответствия намерений.....                          | 9  |
| 5.2.3. Действия по обеспечению соответствия.....                   | 9  |
| 5.2.4. Абстракции, агрегирование, отчёты.....                      | 9  |
| 6. Жизненный цикл.....   | 9  |
| 7. Дополнительные соображения.....                                 | 10 |
| 8. Взаимодействие с IANA.....                                      | 10 |
| 9. Вопросы безопасности.....                                       | 10 |
| 10. Литература.....  | 11 |
| Благодарности.....   | 12 |
| Адреса авторов.....  | 12 |

<sup>1</sup>Internet Research Task Force - комиссия по исследовательским задачам Internet.

## 1. Введение

Этот документ является результатом работы исследовательской группы IRTF Network Management (NMRG) и отражает согласованную точку зрения RG, прошедшую рецензирование и получившую поддержку многих участников. Документ публикуется с информационными целями.

В прошлом интерес к управлению и операциям в рамках IETF был сосредоточен на характеристиках отдельных сетей и устройств. В стандартизации акцент обычно был смещён на инструменты управления, которые должны предоставляться сетевым устройствам. Ярким примером служит управление на основе SNMP [RFC3411] и более 200 MIB, заданных IETF за эти годы. Более свежие примеры включают определения моделей данных YANG [RFC7950] для таких аспектов, как настройка интерфейсов, списков управления доступом (Access Control List или ACL) и Syslog.

Есть чёткое понимание и реальность того, что управление сетями путём настройки мириадом «кнопок» (nerd knob) для каждого устройства больше не подходит для современных сетевых сред. Возникают серьёзные проблемы при сохранении согласованности конфигураций устройств не только в сети, но и с потребностями служб и функций, которые они должны обеспечивать. Возникают дополнительные проблемы, связанные с возможностью быстрого приспосабливания сети к потребностям с учётом расширения. В то же время операции должны быть по возможности оптимизированы и автоматизированы не только для снижения операционных расходов, но и для перенастройки сети за доли секунды, а также для гарантированного предоставления ожидаемых функций. Среди прочего, для этого требуется способность воспринимать эксплуатационные данные, выполнять анализ и динамически выполнять действия с учётом контекста и предполагаемых результатов в масштабе времени, близком к реальному.

В соответствии с этим в IETF начали заниматься аспектами сквозного управления, выходящими за рамки отдельных изолированных устройств. Примеры включают задание моделей YANG для топологии сети [RFC8345] или введение моделей служб, применяемых системами оркестровки и контроллерами [RFC8309]. Большой интерес вызвало обсуждение вопросов самоуправления сетей в рабочей группе ANIMA. Такие сети движимы желанием снизить операционные расходы и упростить управление сетью в целом, что вступает в противоречие с необходимостью управлять одним устройством и одной функцией за раз. Хотя самоуправляемые сети предназначены для демонстрации свойств «самоуправления» (self-management), они по-прежнему требуют действий оператора или внешней системы для обеспечения операционных рекомендаций и сведений о целях, задачах и экземплярах служб, которые сеть должна обслуживать.

Эти входные данные и операционные рекомендации обычно называют намерениями (intent), а сеть, позволяющую операторам предоставить свои данные в форме намерений, - сетью на основе намерений (Intent-Based Network или IBN). Сеть, помогающую реализовать намерения, называют основанной на намерениях системой (Intent-Based System или IBS). Такие системы могут по-разному проявлять себя, например, как контроллер, система управления, реализованная в виде приложения, которое работает на сервере или группе серверов, или набор распределённых в сети функций, совместно реализующих основанную на намерениях функциональность.

Однако намерения (цель) состоят не только в обеспечении формы взаимодействия оператора с сетью, включающей абстракции более высокого уровня. Речь идёт также о возможности позволить операторам сосредоточиться на том, как они хотят видеть желаемый результат, оставляя детали его достижения IBN (и IBS). Сосредоточение внимания на результате позволяет операторам повысить эффективность и гибкость в более широком масштабе, в более короткие сроки и с меньшей зависимостью от человеческих действий (и связанных с ними ошибок). Это делает сети IBN идеальным кандидатом для методов искусственного интеллекта, которые могут обеспечить следующий уровень автоматизации сетей [CLEMM20].

Такое представление стало популярным в отрасли и привело к разработке множества решений, предлагающих управление на основе намерений (Intent-Based Management), обещающее сервис-провайдерам целостное управление сетями с высоким уровнем абстракций как системой, состоящей из соединённых компонентов, а не набора независимых устройств (соединённых между собой). Такие предложения включают IBN и IBS (с полным жизненным циклом намерений), контроллеры программно управляемых сетей (Software-Defined Network или SDN), обеспечивающие единую точку управления и администрирования для сети, а также системы управления сетью и системы поддержки операций (Operations Support System или OSS).

Давно признано, что комплексные решения для управления не могут работать лишь на уровне отдельных устройств и конфигураций нижнего уровня. В этом смысле представление намерений не является совсем новым. В прошлом модель ITU-T для управления телекоммуникационной сетью (Telecommunications Management Network или TMN) представляла набор уровней управления, определяющий иерархию управления для сетевых элементов, сети, сетевых служб и бизнеса [M3010]. Операционные цели высокого уровня распространяются в модели сверху вниз. Связанная иерархия абстракций имеет решающее значение для разложения комплексного управления на отдельные области задач. Эта иерархия абстракций сопровождается информационной иерархией, которая на нижнем уровне касалась сведений, относящихся к конкретным устройствам, а на верхних уровнях включала, например, экземпляры сквозного сервиса. Аналогично концепция управления на основе правил (Policy-Based Network Management или PBNM) долгое время расхваливала возможность позволить пользователям<sup>1</sup> управлять сетями путём задания высокоуровневых правил управления, при этом системы управления автоматически «толковали» (rendering) эти правила, т. е. переводили их в конфигурации нижнего уровня и логику управления.

Однако не хватало внесения этих концепций в более актуальный контекст и их обновления с учётом современных технологических тенденций. Этот документ разъясняет концепции, связанные с намерениями, а также содержит обзор основных принципов организации IBN, а также связанные с ними функции. Цель заключается в способствовании общему пониманию, которое может служить основой для формулирования исследовательских и инженерных задач в сфере IBN.

Следует отметить, что формулировка связанных с IBN исследовательских проблем выходит за рамки документа. Однако следует признать, что сети IBN стали важной темой в сообществе исследователей. Согласно IEEE Xplore [IEEEEXPLORE] по состоянию на декабрь 2021 г за 10 лет с 2012 г. было опубликовано 1138 с терминном intent, из которых 411 конкретно посвящены сетям. Только за период с 2020 г. было опубликовано 316 статей о «намерениях» и 153 - о сетях на основе намерений. Кроме того, проводятся семинары, посвящённые этой теме, такие как IEEE

<sup>1</sup>Следует отметить, что в контексте этого документа пользователями называют операторов и администраторов, отвечающих за поддержку и эксплуатацию коммуникационных служб и сетевой инфраструктуры, а не конечных пользователей услуг.

International Workshop on Intent-Based Networking [WIN21], а также специальные выпуски журналов [IEEE-TITS21]. Обзор текущих исследований представлен в [PANG20], где среди наиболее важных исследовательских задач указаны такие вопросы, как трансляция и понимание намерений, интерфейсы и безопасность.

## 2. Определения и сокращения

### ACL

Access Control List - список управления доступом.

### API

Application Programming Interface - интерфейс с прикладными программами.

### IBA

Intent-Based Analytics - основанная на намерениях аналитика. Аналитика, определённая и выведенная из намерений пользователей и служащая для проверки предусмотренного состояния.

### IBN

Intent-Based Network - сеть на базе намерений. Сеть, управляемая с использованием намерений.

### IBS

Intent-Based System - система на базе намерений. Система, поддерживающая функции управления с помощью намерений.

### Intent - намерения

Набор операционных целей (которым следует соответствовать сети) и результатов (которые сети следует обеспечивать), определённый декларативно без указания способов их достижения и реализации.

### Intent-Based Management - управление на базе намерений

Концепция управления на основе концепции намерений.

### PBNM

Policy-Based Network Management - управление сетью на основе правил.

### PDP

Policy Decision Point - точка принятия решений по правилам.

### PEP

Policy Enforcement Point - точка применения правил (политики).

### Policy - правила (политика)

Набор правил, определяющих выбор поведения системы.

### Service Model - модель сервиса

Модель, представляющая услугу, которую сеть предоставляет пользователям.

### SsoT

Single Source of Truth - единая точка доверия. Функциональный блок системы IBN, нормализующий намерения пользователей и служащий единым источником данных для нижележащих уровней.

### Statement of Intent - заявление о намерениях

Спецификация отдельного аспекта или компонента намерений, называемая также заявлением намерений.

### SvoT

Single Version of Truth - единая версия доверия.

### User - пользователь

В контексте этого документа пользователями считаются операторы и/или администраторы, отвечающие за поддержку и эксплуатацию коммуникационных услуг и сетевой инфраструктуры, а не конечные пользователи коммуникационных услуг.

## 3. Концепции

Ниже представлен обзор концепция для намерений и управления на основе намерений (IBN), а также связанных с ними концепций моделей услуг и политики (и PBNM) и описаны их взаимоотношения с намерениями и IBN.

### 3.1. Намерения и управление на их основе

В этом документе намерение определяется как набор операционных целей (которым следует соответствовать сети) и результатов (которые сети следует обеспечивать), заданных декларативно без указания способов достижения и реализации.

Термин intent был впервые введён в контексте самоуправляемых сетей (Autonomic Network), где он был определён как «абстрактная политика высокого уровня, применяемая для работы сети» [RFC7575]. В соответствии с этим определением намерения являются конкретным типом политики, предоставляемым пользователем для обеспечения руководства самоуправляемой сетью, которая в остальном работает без привлечения людей. Однако, чтобы термин «намерения» не рассматривался как синоним политики, нужно чётко указать отличие намерений от иных правил.

Одно из замечаний относится к использованию термина intent во множественном числе. В английском языке слово intent обычно применяется лишь в единственном числе, однако спецификация намерений в целом включает указание отдельных намерений или заявлений о намерениях. В некоторых случаях заявление о намерениях в просторечии называют intents, хотя обычно такое использование не рекомендуется.

Управление на основе намерений (IBN) направлено на создание сетей, которые проще поддерживать и эксплуатировать и которые требуют минимального вмешательства извне. Сети (даже самоуправляемые) не являются ясновидящими и не могут автоматически узнавать, какие операционные цели и экземпляры сетевых служб нужно поддерживать. Иными словами, они не знают намерений провайдера, придающих смысл существованию сети. Все ещё требуется указывать сетям, что собой представляют такие намерения. При этом концепция намерений не ограничивается сетями с самоуправлением, такими как сети с автономной (самоуправляемой) плоскостью управления (Autonomic Control Plane) [RFC8994], а применимы к любым сетям.

Намерения задают цели и результаты декларативно, указывая, что нужно сделать, но не указывая путей достижения. Таким образом, намерения предполагают одновременно несколько разных концепций.

- Абстракция данных. Пользователям не нужно беспокоиться о нижних уровнях конфигурации устройств.

- Функциональная абстракция от конкретной логики поддержки и управления. Пользователям не нужно заботиться даже о способах достижения целей. Указанное является желаемым результатом, при этом IBS автоматически определяет действия (например, с использованием алгоритма или применением набора правил, выведенного из намерений) для достижения результата.

Ниже приведены примеры намерений, для простоты выраженных естественным языком (фактические интерфейсы для передачи намерений могут отличаться).

- Направлять трафик от конечных точек одной географической области в сторону от трафика из другой области, если только получатель не находится в этой второй области (указано, что достичь, но не сказано как).
- Избегать маршрутизации трафика из определённых конечных точек (или связанного с данным клиентом) через оборудование определённого производителя, даже если это ведёт к снижению уровня обслуживания (сказано, что нужно достичь, а не как, с дополнительными рекомендациями о компромиссе между разными целями).
- Максимизировать использование сети, даже если это ведёт к снижению уровня обслуживания (потери, задержки), пока это ухудшение не достигает 20% от исторически среднего значения (желаемый результат с набором ограничений в качестве дополнительных рекомендаций, но без указания способа достижения).
- Обеспечить для услуг постоянную защиту пути на всех путях (желаемый результат с неочевидным способом его достижения).
- Генерировать на месте данные эксплуатации, администрирования и поддержки (Operations, Administration, and Maintenance или OAM) и сетевой телеметрии для последующего автономного анализа при каждом наблюдении значительных флуктуаций задержки на пути (выход за рамки события-условия-действия без задания степени значимости и собираемых данных).
- Направлять трафик в космической сети (Space Information Network) так, чтобы минимизировать зависимость от стратостатов, если предполагаемым получателем не является самолёт (не задан способ достижения, экстраполяция сценариев из [PANG20]).
- Для услуги «умный город» обеспечить использование сигналами светофором выделенных и резервируемых «срезов» (slice), чтобы избежать «общей судьбы» (желаемый результат с набором ограничений и дополнительной рекомендацией без указания способа достижения, экстраполяция сценария из [GHARBAOUI21]).

Ниже приведены примеры, не являющиеся выражением намерений (на естественном языке для простоты).

- Настроить на данном интерфейсе адрес IP (это настройка устройства и манипулирование «кнопками»).
- При превышении порога загрузки интерфейса выдавать сигнал (правило для поддержки автоматизации сети, но простое правило не является намерением).
- Настроить VPN с туннелем между A и B по пути P (это настройка сервиса).
- Запретить трафик к префиксу P1, если он не исходит от префикса P2 (правило доступа или межсетевого экрана, а не намерение).

В сетях (в частности, кажущихся самоуправляемыми) намерения в идеале должны исполняться самой сетью, т. е. транслироваться в зависящие от устройств правила и последовательности действий. В идеале намерения не организуются и не разбиваются централизованной системой (верхним уровнем), а осуществляются устройствами сети с применением комбинации распределённых алгоритмов и абстракций локальных устройств. В этом идеализированном представлении намерение относится к сети в целом и его следует распространять автоматически между всеми устройствами сети, которые сами могут решить, нужно ли им предпринимать какие-либо действия.

Однако такая децентрализация не будет практичной во всех случаях. Например, пользователям может потребоваться единая концептуальная точка взаимодействия с сетью. Обеспечивающая такую точку система выступает как операционный периферийный процессор (front end) для сети, через который пользователи могут направлять запросы и получать обновления о сети. Пользователям этом может казаться единой системой даже при распределённой реализации. Эта система сама взаимодействует с другими системами и управляет ими нужным для реализации намерений способом (исполнение и гарантии). Большинство устройств в сети может не знать о намерениях и заниматься, например, лишь пересылкой пакетов. Многие устройства могут иметь ограничения в части ресурсов обработки и не каждое устройство может быть способно само исполнять намерения. В таких случаях исполнение намерений может обеспечиваться отдельной системой, выполняющей требуемые действия.

Другая причина обеспечения функциональности намерений из концептуально централизованной точки - это ситуации, когда реализация некоторого вида намерений выигрывает от глобальных сведений о сети и её состоянии. Во многих случаях такое глобальное представление может быть непрактичным для поддержки через отдельные устройства, например, из-за большого объёма данных и временных задержек. Для устройств может оказаться непрактичным даже доступ к такому представлению с другой удалённой системы, если таковая имеется.

Все это подразумевает, что во многих случаях та или иная функциональность намерений должна обеспечиваться специализированными функциями и может предоставляться выделенными системами (которые в некоторых случаях могут предоставлять и другие сетевые функции). Например, может потребоваться трансляция определённых намерений в соответствующие действия и алгоритмы для достижения желаемых результатов с помощью таких специализированных функций. Чтобы не возникало критических точек отказа, реализацию и размещение таких функций можно распределить даже при использовании концептуальной централизации.

Независимо от конкретной реализации (централизованной или децентрализованной), сеть IBN управляется через намерения. Это значит, что она способна распознавать и воспринимать намерения оператора или пользователя, настраивая и адаптируя себя для достижения желаемого результата (т. е. состояния или поведения) без необходимости задания им подробных технических деталей. Сеть IBN способна самостоятельно найти пути достижения результата. IBS - это система, позволяющая пользователям управлять сетью через намерения. Такая

система будет точкой взаимодействия с пользователями, реализуя функциональность, требуемую для достижения предусмотренных результатов, и взаимодействуя с сетью по мере необходимости.

Имеются другие определения намерений, такие как [TR523]. Намерения определяются там просто как декларативный интерфейс, обычно предоставляемый контроллером. Это предполагает наличие централизованной функции, преобразующей намерения в правила или инструкции нижнего уровня и организует их в сети. Хотя это и является одним из вариантов реализации, представленное здесь определение имеет более широкий охват и устремления, поскольку оно подчёркивает важность управления сетью путём задания желаемых результатов без указания конкретных шагов по их достижению. API-интерфейс контроллера, который просто обеспечивает абстракцию на уровне сети, более ограничен и не обязательно задаёт намерения. Восприятие и распознавание намерений не обязательно выполняется через API, основанный на вызове функций и простых взаимодействиях запрос-отклик, а может включать иные типы взаимодействия человека с машиной, такие как диалог для разъяснения и уточнения запросов.

## 3.2. Связанные концепции

### 3.2.1. Модели сервиса

Модель сервиса - это модель, представляющая услугу, обеспечиваемую пользователю сетью. В соответствии с [RFC8309] модель сервиса описывает услугу и её параметры независимым от реализации переносимым способом, который можно применять независимо от оборудования и операционной среды, где реализована услуга. Различают две категории - модель обслуживания клиентов (Customer Service Model) описывает экземпляр предоставляемой клиенту услуги, возможно требующей заказа, а модель предоставления услуги (Service Delivery Model) описывает реализацию услуги в имеющейся сетевой инфраструктуре.

Примерами могут служить услуги L3 VPN [RFC8299], Network Slice [NETWORK-SLICE] или локальный доступ в Internet. Модели сервиса представляют экземпляры служб как самостоятельные сущности. Службы имеют свои параметры, действия и жизненные циклы. Обычно экземпляр службы может быть привязан к конкретным пользователям коммуникационных услуг, которым могут быть выставлены счета за предоставляемые услуги.

Создание службы обычно включает несколько аспектов, указанных ниже.

- Пользователь (или северная система) определяет и/или запрашивает создание экземпляра службы.
- Выделяются ресурсы (адреса IP, номера AS, пулы VLAN или VxLAN, интерфейсы, полоса, память).
- Определяется отображение услуг на ресурсы. Зачастую возможно несколько отображений и выбор может зависеть от контекста (например, доступный для соединения конечного пользователя со службой тип доступа).
- Привязки между объектами верхнего и нижнего уровня, которые нужно поддерживать.
- После создания экземпляра нужно проверить рабочее состояние службы и обеспечить предоставление сетью услуг в соответствии с запросами.

Реализация модели сервиса включает систему (такую как контроллер), обеспечивающую логику предоставления. Это включает разбиение высокоуровневых абстракций служб на низкоуровневые абстракции устройств, идентификацию и выделение ресурсов системы, а также организацию отдельных этапов предоставления. Организаций (оркестровка) операций обычно происходит с использованием модели выталкивания (push), где контроллер/менеджер инициирует нужные операции, затем выталкивает конкретные конфигурации на устройства и проверяет, были ли восприняты эти изменения и достигнуты новые рабочие (производные) состояния, а также синхронизировано желаемое (намерение) состояние. Помимо создания новых экземпляров сервиса должно поддерживаться обновление, изменение и вывод служб из эксплуатации. Сами устройства обычно не знают о службе (независимы от неё) или того, что ресурсы и/или конфигурация являются частью службы (концепции) на верхнем уровне.

Созданные экземпляры моделей услуг отображаются на низкоуровневые модели сетей и устройств, например, экземпляры путей или конкретных конфигураций портов. Модель сервиса обычно включает также уровни служб и зависимости от нижележащих сетевых ресурсов, требуемых для предоставления услуги. Это упрощает управление, позволяя следовать зависимостям в действиях по устранению неполадок и анализу влияния, когда события в сети оцениваются с точки зрения воздействия на службы и клиентов. Службы обычно организуются и предоставляются «сверху вниз», что также упрощает отслеживание назначения сетевых ресурсов (композиция), а поиск и устранение неполадок выполняется «снизу вверх» (декомпозиция). Модели сервиса могут быть связаны с другими данными, не относящимися к сети, но обеспечивающими бизнес-контекст. Это включает сведения о клиентах (например, информация для выставления счетов), заказы услуг, каталоги служб, тарифы, договоры на обслуживание и соглашения об уровне обслуживания (Service Level Agreement или SLA), включая договорные соглашения по корректирующим действиям.

[SERVICE-MAPPING-YANG] служит примером модели данных, обеспечивающей отображение моделей обслуживания клиентов (например, L3VPN Service Model) на модели организации трафика (Traffic Engineering или TE, например, TE Tunnel или the Abstraction and Control of Traffic Engineered Networks Virtual Network).

Как и намерения, модели служб обеспечивают высокий уровень абстракции. Модели сервиса часто дополняются отображениями, учитывающими зависимости между услугой и конфигурацией устройств или сетей. В отличие от намерений, модели сервиса не позволяют задать желаемый «результат», которые будет автоматически поддерживаться IBS. Для управления моделями сервиса от сервис-провайдеров или системных интеграторов требуется разработка изолированных алгоритмов и управляющей логики.

### 3.2.2. Политика и управление сетью на её основе

Управление сетью на основе правил (PBNM) - это парадигма управления, разделяющие правила поведения системы и её функциональность. Это обещает снизить расходы на поддержку информационных и коммуникационных систем одновременно повышая гибкость и адаптивность при работе. Сегодня это лежит в основе множества архитектур и парадигм управления, включая основанные на SLA, требованиях бизнеса, самоуправляемые, адаптивные и самоподдерживающиеся [BOUTABA07]. Заинтересованным читателям рекомендуется обратиться к имеющейся литературе, включающей множество ссылок. Здесь представлен лишь краткий обзор.

В основе такого управления лежит концепция правил (политики). Имеется множество определений политики - правила, регулирующие выбор поведения системы [SLOMAN94], набор правил, применяемых для поддержки и управления сменой и поддержанием состояния одного или нескольких объектов [STRASSNER03]. Общим для большинства определений является то, что политика считается «правилом». Обычно определение правила включает событие (которое вызывает правило), набор условий (при выполнении которых происходят фактические действия) и одно или несколько выполняемых действий.

Управление на основе правил можно рассматривать как парадигму императивного управления - политика точно указывает, что, когда и при каких обстоятельствах нужно делать. По сути, управление с использованием политики можно определить как набор простых циклов управления. Это делает его подходящей технологией для реализации автономного поведения со свойствами самоуправления, включая самонастройку, самовосстановление, самооптимизацию и самозащиту. И это возможно, несмотря на то, что управление на основе правил может применять концепцию абстракций (таких как «Боб получает приоритетное обслуживание»), скрывающих от пользователей детали реализации абстракции в конкретном развёртывании.

Политика обычно предполагает некую степень абстракции, чтобы справиться с неоднородностью сетевых устройств. Вместо правил для конкретных устройств, задающих события, условия и действия в терминах зависящих от устройства команд, параметров и моделей данных, политика определяется на более высоком уровне абстракции, включающем каноническую модель систем и устройств, к которым она применяется. Агент политики в контроллере или устройстве последовательно «разбирает» правила, т. е. транслирует каноническую модель в соответствующее устройству представление. Эта концепция позволяет применять одну политику для широкого класса устройств без необходимости создания множества вариантов. Иными словами, определение политики отделено от её реализации и исполнения. Это позволяет расширять операционный масштаб и даёт сетевым операторам и авторам политики возможность использовать абстракции более высокого уровня, нежели специфика устройств, и применять определения высокого уровня в разных сетевых доменах, сетях WAN, центрах обработки данных (ЦОД или DC) облаках общего пользования.

В PBNM обычно применяется выталкивание (push) - правила выталкиваются в устройства, где они разбираются и применяются. Операции выталкивания выполняет менеджер или контроллер, отвечающий за развёртывание политики в сети и отслеживание корректности работы правил. Возможна иная архитектура политики, например, управление на основе правил может включать компонент втягивания (pull) в котором решение о предпринимаемых действиях передаётся точке принятия решений (Policy Decision Point или PDP). PDP может размещаться вне управляемого устройства и обычно имеет глобальную видимость и контекст для принятия решений. Всякий раз при наблюдении устройством события, связанного с политикой, при отсутствии полного определения правила или возможности выбрать действие, устройство обращается к PDP за решением (принимаемым, например, в соответствии с условиями). Затем устройство применяет решение, полученное от PDP, исполняя политику и действуя как точка применения правил (Policy Enforcement Point или PEP). В любом случае архитектура PBNM обычно включает центральный элемент, распространяющий правила по сети или принимающий решения.

Как и намерения, политика обеспечивает высокий уровень абстракции. Реализации политики способны фиксировать динамические аспекты управляемой системы путём задания правил, позволяющих вызывать конкретные действия. В отличие от намерений, определение таких правил (и действий) требуется от пользователя. Поскольку намерения неизвестны, разрешение конфликтов в правилах или между ними требует участия пользователя или некоторой логики, находящейся вне PBNM. В этом смысле политика представляет более низкий уровень абстракции, чем намерения и IBS могут генерировать политику, которая затем развёртывается в PBNM, позволяя той поддерживать сети IBN.

### 3.2.3. Различия между намерениями, политикой и моделями служб

Общим для намерений, политики и модели обслуживания является использование высокого уровня абстракции, который не включает специфику устройств, как правило, выходит за пределы отдельных устройств и упрощает управление сетью для приложений и пользователей-людей по сравнению с управлением на уровне отдельных устройств. Но имеются и различия между этими подходами, указанные ниже.

- Модель обслуживания является моделью данных, применяемой для описания предоставляемых клиентам экземпляров служб. Модель обслуживания зависит от низкоуровневых моделей (модули устройств и сетей) для описания сопоставления службы с базовой сетью и инфраструктурой IT. Создание экземпляра модели обслуживания требует оркестровки со стороны системы - логика организации/управления/предоставления модели обслуживания и способ её отображения на базовые ресурсы не включается в саму модель.
- Политика - это набор правил, обычно моделируемый на основе различных событий/условий/действий, служащих для выражения простых циклов управления, которые можно выполнить на устройствах без вмешательства внешних систем. Политика позволяет пользователям указать, что нужно делать в тех или иных обстоятельствах, но не задаёт желаемый результат.
- Намерения декларативно указывают высокоуровневую цель, которая действует на уровне сети и предоставляемых ею услуг, а не отдельных устройств. Намерения служат для указания результата и высокоуровневых оперативных целей без задания способов достижения результатов и целей, а также без необходимости перечисления конкретных событий, условий и действий. Применяемые алгоритмы или правила могут быть автоматически определены/выведены системой IBS. В контексте самоуправляемых сетей намерения в идеале разбираются и воспроизводятся самой сетью, распространение намерений по сети и требуемая координация между узлами реализуются сетью без необходимости привлечения внешних систем.

Одной из аналогий, позволяющих уловить разницу между системами на основе правил и IBS, являются экспертные системы и обучающиеся системы в сфере искусственного интеллекта. Экспертные системы работают с базами знаний по предоставленным пользователем правилам, подобно системам на базе политики. Они способны автоматически делать выводы на основе правил, заданных пользователем. Обучающиеся системы (популяризированные глубоким изучением и нейросетями) способны обучаться без пользовательского программирования и задания правил. Однако им нужна фаза обучения или тренировки, требующая больших наборов данных. Объяснения предпринимаемых системой действий создают другой набор проблем. По аналогии с IBS пользователи сосредотачиваются на том, что они хотят получить от системы, а не на способах достижения этого.

## 4. Принципы

Ниже указаны основные принципы работы, позволяющие охарактеризовать природу систем, основанных, управляемых, определяемых с помощью намерений.

1. Единый источник (Single Source of Truth или SSoT) и одна версия (Single Version of Truth или SVoT) доверия. SSoT является важной частью IBS, позволяя выполнять несколько важных операций. В качестве SsoT системы служит набор проверенных выражений намерений. SsoT и записи рабочих состояний позволяют сравнивать предполагаемое/желаемое состояние с фактическим/операционным состоянием системы и определять различия между ними. SSoT и различия служат основой для корректирующих действий. Если в IBS имеются средства прогнозирования состояний, можно дополнительно разрабатывать стратегии предсказания, планирования и упреждающих действий в отношении любых тенденций расхождения с целью минимизации их влияния. Помимо предоставления средств для согласования работы системы, SSoT позволяет улучшить отслеживание для проверки, были ли и насколько хорошо выполнены исходные намерения и связанные с ними бизнес-цели для оценки влияния изменений в параметрах намерений, а также влияния и последствий происходящих в системе событий.

Единая версия (или представление - View) доверия выводится из SSoT и может служить для выполнения таких операций, как запросы, опросы или фильтрация измеренных или полученных сопоставлением данных для создания так называемых «представлений» (view). Эти представления могут помогать пользователям IBS. Для создания заявления о намерениях как единого источника доверия система IBS должна следовать чётко заданным и хорошо документированным процессам и моделям. SSoT также называют неизменностью намерений [LENROW15].

2. Одно касание, но не один шаг. В идеальной системе IBS пользователь в той или иной форме выражает намерения, а система выполняет все последующие операции (одно касание). Можно представить и подход «без касания» (zero-touch), если IBS имеет возможности или средства распознавания намерений в любой форме данных. Однако это не должно отвлекать от того, что достижение корректно сформированного и правильного выражения намерений не является одношаговым (one-shot) процессом. Напротив, взаимодействие между пользователем и IBS следует организовывать как итерационный процесс. В зависимости от уровня абстракции выражение намерений исходно может содержать в той или иной степени неявные части, а также неточные или неизвестные параметры и ограничения. Роль IBS заключается в разборе, понимании и уточнении намерений для достижения чётко сформированного и действительного выражения намерений, которое система может исполнять для операций исполнения и подтверждения. Процесс уточнения намерений может включать комбинацию итерационных шагов, вовлекающих пользователя в проверку предложенных уточнений и уточнение некоторых параметров и переменных, которые система не может вывести или узнать самостоятельно. Кроме того, IBS потребуются разрешение конфликтов в намерениях, чтобы помочь пользователю сделать верный выбор среди вариантов, которые могут иметь разные последствия.
3. Автономность и присмотр. Желаемой целью IBS является обеспечения высокого уровня гибкости и свободы для пользователя и сети, например, путём предоставления пользователю возможности выразить намерения своими словами с поддержкой разных форм выражения отдельных намерений и их уточнения для создания корректно сформированных и пригодных для использования выражений. Двойной принцип автономности и присмотра обеспечивает режим работы с требуемым уровнем автономности для выполнения задач и операций без вмешательства пользователя и самостоятельным принятием решений (в рамках сферы ответственности и контроля) в части выполнения задач в соответствии с ожиданиями пользователя с точки зрения производительности и качества. В то же время обеспечивается должный присмотр в соответствии с потребностями пользователя в части отчётности и представления соответствующих результатов.
4. Обучение. IBS - обучающаяся система. В отличие от императивных систем, таких как правила «событие-условие-действие» (Event-Condition-Action), где пользователь заранее задаёт ожидаемое поведение, в IBS пользователь лишь объявляет предполагаемое поведение системы, не указывая способов его достижения. Таким способом происходит передача рассуждений/рационализма от человека (знание предметной области) к системе. Эта передача когнитивных возможностей подразумевает наличие в IBS способов или средств обучения, рассуждения, а также представления знаний и управления ими. Способности IBS к обучению могут применяться для разных задач, таких как оптимизация разбора и уточнения намерений. Способность IBS к постоянному развитию создаёт условия для постоянного обучения и оптимизации. Другие когнитивные возможности, такие как планирование, также могут применяться в IBS для прогнозирования или предсказания будущих состояний системы и откликов на изменения намерений или условий в сети и соответствующей выработки планов по адаптации к этим изменениям при сохранении стабильности и эффективности системы, а также компромисса между стоимостью и надёжностью операций.
5. Раскрытие умений состоит в потребности выражения возможностей, требований и ограничений сети, чтобы можно было составить/разложить намерения и сопоставить ожидания пользователей с возможностями системы.
6. Абстрактность и нацеленность на результат. Пользователям не нужно заботиться о способах реализации намерений и они могут выражать их лишь в терминах желаемого результата. Кроме того, можно указывать концепции с высоким уровнем абстракции, независимые, например, от специфического для производителя разбора намерений.

Описанные принципы, возможно, являются наиболее важными, но список их не полон и следует учитывать также указанные ниже аспекты.

- Намерения нацелены не на отдельные устройства, а обычно на их агрегаты (таких как, группа устройств, соответствующих общим критериям, например, с определённой ролью) или абстракции (такие как типы или экземпляры услуг, топологии).
- Абстракция и связанная с ней виртуализация, не зависящие от деталей реализации.

- Настроенное на человека сетевое взаимодействие. IBN следует «говорить» на языке пользователя, не требуя от него «языка» устройств или сетей.
- Возможность объяснения как важная функция IBN, обнаружение и разрешение с помощью IBN конфликтов намерений, а также согласование желаний пользователя с фактическими возможностями сети.
- Встроенная поддержка, верификация и гарантии доверия.

Все эти принципы и соображения влияют на устройство IBS и поддерживающую архитектуру, поэтому они должны учитываться при задании функциональных и эксплуатационных требований.

## 5. Функциональность IBN

Сети на основе намерений (IBN) включают широкий спектр функций, которые можно условно разделить на 2 категории.

- Реализация намерений (Intent Fulfillment) включает функции и интерфейсы, позволяющие пользователям передать намерения в сеть и выполнить действия, требуемые для исполнения намерений. Это включает алгоритмы определения подходящего направления действий, и функции, которые со временем обучаются оптимизации результатов. Кроме того, сюда входят такие функции, как любая требуемая оркестровка (организация) координированных операций настройки конфигурации в сети и преобразования высокоуровневых абстракций в параметры и элементы управления низкого уровня.
- Обеспечение (гарантия) намерений (Intent Assurance) включает функции и интерфейсы, позволяющие пользователям проверять и отслеживать соответствие сети заданным намерениям. Это нужно для оценки эффективности действий по исполнению намерений, обеспечения обратной связи, позволяющей со временем обучить и настроить эти функции для оптимизации результатов. Кроме того, Intent Assurance требуется для устранения «дрейфа намерений». Намерение не означает транзакцию «задать и забыть» и предполагается, что оно действует в течение некоторого времени (пока явно не указано иное). Дрейф намерений возникает в тех случаях, когда система исходно соответствовала намерениям, но позволяет своему поведению меняться со временем или подвергаться влиянию, пока намерения не перестанут выполняться или эффективность не снизится.

В последующих параграфах приведён более детальный обзор этих функций.

### 5.1. Реализация намерений

Реализация намерений связана с функциями, которые принимают намерение от создавшего его пользователя (обычно, администратор соответствующей организации) для его исполнения в сети.

#### 5.1.1. Восприятие намерений и взаимодействие с пользователями

Первый набор функций связан с восприятием намерений, т. е. их получением через взаимодействие с пользователями. Он представляет функции распознавания намерений из взаимодействия с пользователем, а также функции, позволяющие пользователю уточнить свои намерения и сформулировать их подходящим для IBS способом. Обычно эти функции выходят за рамки API, не основанных на намерениях, хотя некоторые из таких API также могут предоставляться (и требуются для взаимодействия с пользователем без участия человека, т. е. с другой машиной). Во многих случаях включается также набор интуитивно понятных и простых в обращении рабочих процессов, ведущих пользователя на этапе восприятия намерений, гарантируя сбор всех требуемых для моделирования и последовательной трансляции намерений. Они могут поддерживать нетрадиционное взаимодействие человека с машиной, где человек не просто даёт команды, а использует диалог «человек-машина» для разъяснения, указания ветвлений и компромиссов, а также для упрощения корректировок.

Конечная цель состоит в том, чтобы сделать системы IBS как можно более естественными и простыми в использовании, в частности, позволяя человеку, взаимодействующему с IBS способы, не требующие сложного обучения «системным» языкам. В идеале IBS будут скорее учиться пониманию пользователей, нежели наоборот. Для того, чтобы это стало явью, потребуются дополнительные исследования.

#### 5.1.2. Трансляция намерений

Второй набор функций должен преобразовывать намерения пользователя в действия и запросы к сети, значимые для настройки сети и систем обеспечения. Эти функции лежат в основе IBS, устраняя разрыв между взаимодействием с пользователем и управлением и эксплуатацией, которые нужны для организации предоставления и настройки в сети.

Помимо простого разделения абстракции высокого уровня (намерения) на абстракции нижних уровней (политика и конфигурация устройств) функции трансляции намерений (Intent Translation) могут дополняться алгоритмами и функциями, которые обеспечивают оптимизацию, а также способны обучаться и улучшаться со временем для достижения лучших результатов, особенно в случаях наличия разных путей достижения целевых результатов. Например, исполнение намерений может включать расчёт путей и других параметров, которые нужно настроить в сети. Эвристика и алгоритмы для этого могут развиваться для оптимизации результатов, которые могут зависеть от множества меняющихся условий в сети и контекста.

#### 5.1.3. Оркестровка намерений

Третий набор функций связан с фактической настройкой и предоставлением, где требуется оркестровка через сеть, определённая на этапе трансляции намерений.

## 5.2. Обеспечение намерений

Обеспечение намерений (Intent Assurance) связано с функциями, требуемые для гарантии соответствия сети, воспринятым намерениям.





автоматический анализ и проверку намерений на основе наблюдений в пространстве сетевых операций. Наблюдения передаются функции, планирующей представления намерений в сети для внесения при необходимости корректировок в конфигурацию сети. Здесь устраняется дрейф намерений, который может возникать, применяются наблюдения для оценки соответствия сети намерениям и автоматически предлагаются корректировочные действия для устранения несоответствий. Аналогичным способом этот контур позволяет оценить эффективность любых действий, предпринимаемых для постоянного изучения и улучшения путей реализации намерений для достижения желаемых результатов.

- «Внешний» контур управления намерениями распространяется на пространство пользователя. Он включает действия пользователя и корректировку намерений на основе наблюдений и обратной связи от IBS.

Таким образом, намерение проходит жизненный цикл - возникает, может уточняться и изменяться со временем, а в какой-то момент может быть отзвано.

## 7. Дополнительные соображения

С учётом популярности термина «намерения» (intent) возникает соблазн расширить его использование, включив связанные понятия, что ведёт к «размытию намерений» (intent-washing), представляющему эти концепции в новом свете путём простого применения к ним новой терминологии намерений. Типичным примером служит использование для северного интерфейса контроллера SDN термина «интерфейс намерений» (intent interface). Однако в некоторых случаях такой подход имеет смысл не только как маркетинговый ход, но и как способ лучше связать новые концепции с прежними. В этом смысле уместно различать несколько категорий намерений.

### **Operational Intent - эксплуатационные намерения**

Намерения, связанные с эксплуатационными целями оператора. Это соответствует исходному термину intent и концепциям данного документа.

### **Rule Intent - намерения для политики**

Синоним для правил политики, управляющих действиями при возникновении определённых событий.

### **Service Intent - намерения для сервиса**

Синоним модели обслуживания клиентов [RFC8309].

### **Flow Intent - намерения для потока**

Синоним цели уровня обслуживания (Service Level Objective) для данного потока.

Полная классификация концепций и категорий намерений будет приведена в отдельном документе.

## 8. Взаимодействие с IANA

Этот документ не требует действий IANA.

## 9. Вопросы безопасности

В этом документе описаны концепции и даны определения для основанных на намерениях сетей (Intent-Based Networking). Поэтому приведённые ниже соображения безопасности сохраняют высокий уровень, т. е. указаны в виде принципов, рекомендаций или требований. Более подробное рассмотрение будет приведено в документах, задающих архитектуру и функциональность.

Безопасность в IBN имеет несколько аспектов:

- защита самой системы IBS;
- смягчение последствий ошибочных, вредных или скомпрометированных заявлений о намерениях;
- выражение правил или параметров безопасности в заявлениях о намерениях.

Защита IBS нацелена на обеспечения операционной безопасности IBS за счёт внедрения механизмов защиты и применения накопленного опыта. В контексте IBN такие механизмы и методы могут включать проверку намерений, предоставление возможности работать с намерениями лишь проверенным и уполномоченным пользователям, обнаружение фальсифицированных намерений и защиту от них. Такие механизмы могут включать внедрение нескольких уровней намерений. Например, намерения, связанные с защитой сети, следует помещать на «более глубокий» уровень, который при необходимости переопределяет намерения других уровней, а сам не может быть изменён обычными операциями и требует применения защищённых операций. Следует также рассмотреть применение дополнительных механизмов, таких как компоненты разъяснений, описывающие ветвления защиты и компромиссы, которые следует учитывать.

Смягчение последствий ошибочных или скомпрометированных намерений нацелено на обеспечение эксплуатационной безопасности IBS за счёт механизмов проверки и защиты, а также принципов работы. В контексте IBN такие механизмы и принципы могут включать способность автоматически обнаруживать непреднамеренно, враждебное или аномальное поведение, автоматически (и аккуратно) возвращаться к прежнему «безопасному» состоянию, предотвращать или сдерживать усиление ошибок (за счёт комбинации высокого уровня автоматизации и внутренней свободы, неоднозначности или неясной информации, передаваемой в намерениях), наличие динамических уровней присмотра и информирования, предоставляющих пользователям корректные сведения в нужный момент и с подходящим контекстом. Ошибочные и вредоносные намерения могут распространяться по сети и нарушать защиту. Кроме того, скомпрометированные намерения (например, подделанные внутренним злоумышленником) могут саботировать или нарушать работу сетевых ресурсов и делать их уязвимыми для других, более серьёзных атак, например, путём обхода некоторых механизмов защиты.

Выражение правил или связанных с безопасностью параметров намерений включает использование формализма намерений (высокоуровневые декларативные абстракции) или их частей для задания связанных с безопасностью аспектов:

- управление данными;
- уровни конфиденциальности при обмене данными;

- уровни доступности ресурсов системы, защиты на путях пересылки, изоляция в функциях обработки;
- уровни шифрования;
- уполномоченные для выполнения операций.

Разработка и внедрение IBN в рабочие среды, несомненно, приведёт к новым проблемам безопасности. Такие проблемы следует предвидеть во время проектирования и подготовки спецификаций. Однако IBN можно также использовать для повышения уровня безопасности. Например, правила безопасности и приватности можно выразить в более понятной человеку форме и более общим способом, не так зависящим от технологии и менее сложным, что приведёт к снижению ошибок конфигурации на нижних уровнях. Обнаружение угроз и атак также можно упростить и сделать более полным за счёт обнаружения конфликтов на верхних уровнях с меньшей детализацией.

По мере роста уровня понимания технологий IBN потребуется более тщательно анализировать вопросы безопасности.

## 10. Литература

- [BOUTABA07] Boutaba, R. and I. Aib, "Policy-Based Management: A Historical Perspective", Journal of Network and Systems Management (JNSM), Vol. 15, Issue 4, DOI 10.1007/s10922-007-9083-8, November 2007, <<https://doi.org/10.1007/s10922-007-9083-8>>.
- [CLEMM20] Clemm, A., Faten Zhani, M., and R. Boutaba, "Network Management 2030: Operations and Control of Network 2030 Services", Journal of Network and Systems Management (JNSM), Vol. 28, Issue 4, DOI 10.1007/s10922-020-09517-0, October 2020, <<https://doi.org/10.1007/s10922-020-09517-0>>.
- [GHARBAOUI21] Gharbaoui, M., Martini, B., and P. Castoldi, "Implementation of an Intent Layer for SDN-enabled and QoS-Aware Network Slicing", 2021 IEEE 7th International Conference on Network Softwarization (NetSoft), pp. 17-23, DOI 10.1109/NetSoft51509.2021.9492643, June 2021, <<https://doi.org/10.1109/NetSoft51509.2021.9492643>>.
- [IEEE-TITS21] Garg, S., Guizani, M., Liang, Y-C., Granelli, F., Prasad, N., and R. R. V. Prasad, "Guest Editorial Special Issue on Intent-Based Networking for 5G-Envisioned Internet of Connected Vehicles", IEEE Transactions on Intelligent Transportation Systems, Vol. 22, Issue 8, pp. 5009-5017, DOI 10.1109/TITS.2021.3101259, August 2021, <<https://doi.org/10.1109/TITS.2021.3101259>>.
- [IEEEEXPLORE] IEEE, "IEEE Xplore", <<https://ieeexplore.ieee.org/>>.
- [LENROW15] Lenrow, D., "Intent As The Common Interface to Network Resources", Intent Based Network Summit 2015 ONF Boulder: IntentNBI, February 2015.
- [M3010] ITU-T, "Principles for a telecommunications management network", ITU-T Recommendation M.3010, February 2000.
- [NETWORK-SLICE] Farrel, A., Ed., Drake, J., Ed., Rokui, R., Homma, S., Makhijani, K., Contreras, L. M., and J. Tantsura, "Framework for IETF Network Slices", Work in Progress, Internet-Draft, draft-ietf-teas-ietf-network-slices-14, 3 August 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-teas-ietf-network-slices-14>>.
- [PANG20] Pang, L., Yang, C., Chen, D., Song, Y., and M. Guizan, "A Survey on Intent-Driven Networks", IEEE Access, Vol. 8, pp.22862-22873, DOI 10.1109/ACCESS.2020.2969208, January 2020, <<https://doi.org/10.1109/ACCESS.2020.2969208>>.
- [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>>.
- [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>>.
- [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>>.
- [RFC8299] Wu, Q., Ed., Litkowski, S., Tomotaki, L., and K. Ogaki, "YANG Data Model for L3VPN Service Delivery", RFC 8299, DOI 10.17487/RFC8299, January 2018, <<https://www.rfc-editor.org/info/rfc8299>>.
- [RFC8309] Wu, Q., Liu, W., and A. Farrel, "Service Models Explained", RFC 8309, DOI 10.17487/RFC8309, January 2018, <<https://www.rfc-editor.org/info/rfc8309>>.
- [RFC8345] Clemm, A., Medved, J., Varga, R., Bahadur, N., Ananthkrishnan, H., and X. Liu, "A YANG Data Model for Network Topologies", RFC 8345, DOI 10.17487/RFC8345, March 2018, <<https://www.rfc-editor.org/info/rfc8345>>.
- [RFC8994] Eckert, T., Ed., Behringer, M., Ed., and S. Bjarnason, "An Autonomic Control Plane (ACP)", RFC 8994, DOI 10.17487/RFC8994, May 2021, <<https://www.rfc-editor.org/info/rfc8994>>.
- [SERVICE-MAPPING-YANG] Lee, Y., Ed., Dhody, Dhruv., Ed., Fioccola, G., Wu, Q., Ed., Ceccarelli, D., and J. Tantsura, "Traffic Engineering (TE) and Service Mapping YANG Data Model", Work in Progress, Internet-Draft, draft-ietf-teas-te-service-mapping-yang-11, 11 July 2022, <<https://datatracker.ietf.org/doc/html/draft-ietf-teas-te-service-mapping-yang-11>>.
- [SLOMAN94] Sloman, M., "Policy Driven Management for Distributed Systems", Journal of Network and Systems Management (JNSM), Vol. 2, Issue 4, pp. 333-360, December 1994.

- [STRASSNER03] Strassner, J., "Policy-Based Network Management", August 2003.
- [TR523] Open Networking Foundation, "Intent NBI - Definition and Principles", ONF TR-523, October 2016.
- [WIN21] Ciavaglia, L. and E. Renault, "1st International Workshop on Intent-Based Networking", IEEE International Conference on Network Softwarization, June 2021, <<https://netsoft2021.ieee-netsoft.org/program/workshops/win-2021/>>.

## Благодарности

Спасибо членам исследовательской группы IRTF Network Management (NMRG) за полезные дискуссии и отклики. В частности, авторы хотели бы поблагодарить Remi Badonnel, Walter Cerroni, Marinos Charalambides, Luis Contreras, Jerome Francois, Molka Gharbaoui, Olga Havel, Chen Li, William Liu, Barbara Martini, Stephen Mwanje, Jeferson Nobre, Haoyu Song, Peter Szilagyi, Csaba Vulkan за отклики и поддержку. Отдельная благодарность Remi Badonnel, Walter Cerroni, Jerome Francois, Molka Gharbaoui, Barbara Martini, Stephen Mwanje, Peter Szilagyi, Csaba Vulkan, сделавшим ещё один шаг и предоставившим рецензии.

## Адреса авторов

### Alexander Clemm

Futurewei  
2330 Central Expressway  
Santa Clara, CA 95050  
United States of America  
Email: [ludwig@clemm.org](mailto:ludwig@clemm.org)

### Laurent Ciavaglia

Nokia  
Route de Villejust  
91620 Nozay  
France  
Email: [laurent.ciavaglia@nokia.com](mailto:laurent.ciavaglia@nokia.com)

### Lisandro Zambenedetti Granville

Federal University of Rio Grande do Sul (UFRGS)  
Av. Bento Gonçalves  
Porto Alegre-RS  
9500  
Brazil  
Email: [granville@inf.ufrgs.br](mailto:granville@inf.ufrgs.br)

### Jeff Tantsura

Microsoft  
Email: [jefftant.ietf@gmail.com](mailto:jefftant.ietf@gmail.com)

## Перевод на русский язык

Николай Малых

[nmalykh@protokols.ru](mailto:nmalykh@protokols.ru)