Network Working Group
Internet Draft
Intended status: Informational
Expires: November 2022

C. Li
China Telecom
O. Havel
A. Olariu
Huawei Technologies
P. Martinez-Julia
NICT
J. Nobre
UFRGS
D. Lopez
Telefonica, I+D

May 18, 2022

Intent Classification
draft-irtf-nmrg-ibn-intent-classification-08

Abstract

Intent is an abstract, high-level policy used to operate the network. Intent-based management system includes an interface for users to input requests and an engine to translate the intents into the network configuration and manage their life-cycle.

This document discusses mostly the concept of network intents, but other types of intents are also being considered. Specifically, it highlights stakeholder perspectives of intent, methods to classify and encode intent, the associated intent taxonomy, and defines relevant intent terms where necessary. This document provides a foundation for intent related research and facilitates solution development.

This document is a product of the IRTF Network Management Research Group (NMRG).

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any

time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on November 18, 2022.

Table of Contents

1. Introduction

The vision of intent-based networks has attracted a lot of attention, as it promises to simplify the management of networks by human operators. This is done by simply specifying what should happen on the network, without giving any instructions on how to do it. This promise led many researcher-led activities and telecom companies to start researching this new vision, and many Standards Development Organization (SDOs) to propose different intent frameworks.

This draft proposes an intent classification methodology and an intent taxonomy. The scope of these proposals is to ensure a common understanding in the research community in terms of what are the intent users, intent types, or intent solutions, etc. for specific scenarios that are being considered.

The document represents the consensus of the Network Management Research Group (NMRG). It has been reviewed extensively by the Research Group (RG) members who are actively involved in the research and development of the technology covered by this document. It is not an IETF product and is not a standard.

1.1. Research activities

Intent-based networking is an active research topic which spans across different areas that could benefit from an intent classification and taxonomy.

One such area is intent expression and recognition ([Bezahaf21], [Bezahaf19]), NILE [Jacobs18]). The use of a common classification can provide consistency in the understanding of the various forms of intent expressions being proposed and investigated.

Another area where this intent classification could contribute is the orchestration of cognitive autonomous RANs [Banerjee21] where intents are classified based on their content.

The work carried in intent network verification [Tian19] where the authors are proposing new intent language is another candidate where intent classification could be used advantageously.

Furthermore, this draft is proving itself already extremely relevant to the research community as it has been used as the basis for proposing self-generated Intent-based systems [Bezhaf19], for advancing IBN-based VNF placement solutions that rely on defining user intent profiles corresponding to abstract network services [Leivadeas21], for improving existing solutions in provisioning

intent-based networks, and proposing new approaches to service management [Davoli21], or even for defining grammars for users to specify the high-level requirements for blockchain selection in the form of intent [Padovan20]. As well, the draft has been mentioned in surveys addressing the topic of intelligent intent-based autonomous networks [Mehmood21], [Szilagyi21].

This document describes as well an example on how this proposal has been successfully applied in an academic environment [IBN-POC] by researchers in the area of SDN/NFV for defining the scope of their project. The specific problem addressed by researches is how to apply intent concepts at different levels that correspond to different stakeholders.

IEEE Communications Society Technical Committee on Network Operation and Management (IEEE-CNOM), IRTF-NMRG and IFIP WG6.6 have developed a taxonomy for network and service management [IFIP-NSM] that is used by the research community in network management and operations to structure the research area through a well-defined set of keywords and to improve quality of reviews in submissions to journals, conferences and workshops. The proposed intent taxonomy may be contributed as an extension to this taxonomy for intent driven management.

1.2. Standards and open source activities

Several SDOs and open source projects, such as Internet Research Task Force (IRTF)/ Network Management Research Group (NMRG), Open Networking Foundation (ONF) [ONF] / Open Network Operating System (ONOS) [ONOS], European Telecommunications Standards Institute (ETSI)/Experiential Networked Intelligence (ENI), TMF with its Autonomous Networks, have proposed intents for defining a set of network operations to execute in a declarative manner.

More recently, the IRTF NMRG is working on the Intent-based Networking - Concepts and Definitions document, [CLEMM]. This document clarifies the concept of "Intent" and provides an overview of the functionality that is associated with it. The goal is to contribute towards a common and shared understanding of terms, concepts, and functionality that can be used as the foundation to guide further definition of associated research and engineering problems and their solutions.

The present document, together with [CLEMM], aims to become the foundation for future intent-related topic discussions regarding the NMRG.

The SDOs usually came up with their own way of specifying an intent, and with their own understanding of what an intent is. Besides that, each SDO defines a set of terms and level of abstraction, its intended intent users, and the applications and usage scenarios.

However, most intent approaches proposed by SDOs share the same following features:

- It must be declarative in nature, meaning that an intent user specifies the goal on the network without specifying how to achieve that goal.

- It must be vendor agnostic, in the sense that it abstracts the network capabilities, or the network infrastructure from the intent user, and it can be ported across different platforms.

- It must provide an easy-to-use interface, which simplifies the intent users' interaction with the intent system through the usage of familiar terminology or concepts.

It should be able to detect and resolve intent conflicts, which include, for example, static (compile-time) conflicts and dynamic (run-time) conflicts.

1.3. Scope

The focus of this document is on the definition of criteria enabling to categorize intents from the stakeholders' viewpoint. Concepts and definitions related to IBN are provided in [CLEMM].

This document mostly addresses intents in the context of network intents, however other types of intents are not excluded, as presented in section 4.4. and section 6.2. .

It is impossible to fully differentiate intents only by the common characteristics followed by concepts, terms and intentions. This document clarifies what an intent represents for different stakeholders through a classification on various dimensions, such as solutions, intent users, and intent types. This classification ensures common understanding among all participants and is used to determine the scope and priority of individual projects, proof-of-concept (PoCs), research initiatives, or open source projects.

The scope of intent classification in this document includes solutions, intent users and intent types, and the initial

classification table is made according to this scope. The methodology presented can be used to update the classification tables by adding or removing different solutions, intent users, or intent types to cater for future scenarios, applications or domains.

2. Acronyms

AI: Artificial Intelligence

CE: Customer Equipment

CFS: Customer Facing Service

CLI: Command Line Interface

DB: Database

DC: Data Center

ECA: Event-Condition-Action

GBP: Group-Based Policy

GPU: Graphics Processing Unit

IBN: Intent Based Network

NFV: Network Function Virtualization

O&M: Operations & Maintenance

ONF: Open Networking Foundation

ONOS: Open Network Operating System

PNF: Physical Network Function

QoE: Quality of Experience

RFS: Resource Facing Service

SDO: Standards Development Organization

SD-WAN: Software-Defined Wide-Area Network

SLA: Service Level Agreement

SUPA: Simplified Use of Policy Abstractions

VM: Virtual Machine

VNF: Virtual Network Function

3. Definitions

A common and shared understanding of terms and definitions related to IBN is provided in [CLEMM], as follows:

- Intent: A set of operational goals (that a network should meet) and outcomes (that a network is supposed to deliver), defined in a declarative manner without specifying how to achieve or implement them.
- Intent-Based Network: A network that can be managed using intent.
- Policy: A set of rules that governs the choices in behaviour of a system.
- Intent User: A user that defines and issues the intent request to the intent-based management system.

Other definitions relevant to this draft, such as intent scope, intent network scope, intent abstraction, intent abstraction, and intent lifecycle are available in section 5.

4. Abstract Intent Requirements

In order to understand the different intent requirements that would drive intent classification, we first need to understand what intent means for different intent users.

4.1. What is Intent?

The term Intent has become very widely used in the industry for different purposes, sometimes it is not even in agreement with SDO

shared principles mentioned in the Introduction section.[CLEMM] draft brings clarification with relation to what an intent is and how it differentiates from policies and services.

Different stakeholders have different perspective of the network and therefore have different intent requirements. Their intent is sometimes technical, non-technical, abstract or technology specific. Therefore, it is important to start a discussion in the industry and academia communities about what intent is for different solutions and intent users. It is also imperative to try to propose some intent categories/ classifications that could be understood by a wider audience. This would help us define intent interfaces, domain-specific languages, and models.

4.2. Intent Solutions and Intent Users

Intent types are defined by all aspects that are required to profile different requirements to easily distinguish among them. However, in order to facilitate a clustered classification, we can focus on two aspects, the solution and intent user. They can be considered as the main keys to classify intents, as we can easily group requirements by solution and intent user.

On the one hand, different solutions and intent users have different requirements, expectations and priorities for intent-based networking. Therefore, intent users require different intent types, depending on their context, since they participate in different use cases. For instance, some intent users are more technical and require intents that expose more technical information. Other intent users do not have knowledge of the network infrastructure and require intents that shield them from different networking concepts and technologies.

The following are the solutions and intent users that intent-based networking needs to support:

Solutions	Intent Users
Carrier Networks	Network Operator Service Designers/App Developer Service Operators Customers/Subscribers
DC Networks	Cloud Administrator Underlay Network Administrator Application Developers Customer/Tenants
Enterprise Networks	Enterprise Administrator Application Developers End-Users

Table 1 - Intent Solutions and Intent Users

These intent solutions and intent users represent a starting point for the classification and are expendable through the methodology presented in section 6.1. .

- For carrier networks scenario, for example, if a customer/subscriber wants to watch high-definition video, then the intent is to convert the video image to 1080p rate.

- For DC networks scenario, administrators have their own clear network intent such as load balancing. For all traffic flows that need NFV service chaining, restrict the maximum load of any VNF node/container below 50% and the maximum load of any network link below 70%.

- For enterprise networks scenario, when hosting a video conference multiple remote accesses are required. An example of the intent from the network administrator is: for any end-user of this application, the arrival time of hologram objects of all the remote tele-presenters should be synchronised within 50ms to reach the destination viewer for each conversation session.

-

4.3. Benefits of Intents for Different Stakeholders

Current network APIs and CLIs are too complex because they are highly integrated with the low level concepts exposed by networks. Customers, application developers and end-users must not be required to set IP addresses, VLANs, subnets, ports, while operators may still want to have more technical and network visibility. All stakeholders would benefit from the simpler interfaces, like:

- Request gold VPN service between my sites A, B and C
- Provide CE redundancy for the customer sites
- Add access rules to the network service

Operators and administrators manually troubleshoot and fix their networks and services. They instead want to:

- simplify and automate network operations
- simplify definitions of network services
- provide simple customer APIs for value added services (operators)
- be informed if the network or service is not behaving as requested
- enable automatic optimization and correction for selected scenarios
- have systems that learn from historic information and behaviour

Currently, intent users cannot build their own services and policies without becoming technical experts and performing manual maintenance actions. They instead want to be able to:

- build their own network services with their own policies via simple interfaces, without becoming networking experts
- have their network services up and running based on intent and automation only, without any manual actions or maintenance
-

4.4. Intent Types that need to be supported

Next to the intent solutions and intent users, another way to categorize the intent is through the intent types. The following intent types and subtypes need to be supported, in order to address the requirements from different solutions and intent users:

- Customer service intent
  - for customer self-service with SLA
  - for service operator orders
- Network and underlay network service intent
  - for service operator orders
  - for intent driven network configuration, verification, correction and optimization
  - for intent created and provided by the underlay network administrator
- Network and underlay network intent
  - for network configuration
  - for automated lifecycle management of network configurations
  - for network resources (switches, routers, routing, policies, underlay)
- Cloud management intent
  - for DC configuration, VMs, DB servers, APP servers
  - for communication between VMs
- Cloud resource management intent
  - for cloud resource life-cycle management (policy driven self-configuration and auto-scaling and recovery/optimization)
- Strategy intent
  - for security, QoS, application policies, traffic steering, etc.

- for configuring and monitoring policies, alarms generation for non-compliance, auto-recovery
- for design models and policies for network and network service design
- for design workflows, models and policies for operational task intents

- Operational task intents
  - for network migration
  - for device replacements
  - for network software upgrades
  - for automating any other tasks that operators/administrator often perform

It is important to mention there all of the previously mentioned types and subtypes may affect other intents. For example, operational task intent can modify many other intents. The task itself is short-lived, but the modification of other intents has an impact on their life-cycle, so those changes must continue to be continuously monitored and self-corrected/self-optimized.

5. Functional Characteristics and Behaviour

Intent can be used to operate immediately on a target (much like issuing a command), or whenever it is appropriate (e.g., in response to an event). In either case, intent has a number of behaviours that serve to further organize its purpose, as described by the following subsections.

5.1. Abstracting Intent Operation

The modelling of intents can be abstracted using the following three-tuple:

{Context, Capabilities, Constraints}

- Context grounds the intent, and determines if it is relevant or not for the current situation. Thus, context selects intents based on applicability.

- Capabilities describe the functionality that the intent can perform. Capabilities take different forms, depending on the expressivity of the intent as well as the programming paradigm(s) used.

- Constraints define any restrictions on the capabilities to be used for that particular context.

Metadata can be attached via strategy templates to each of the elements of the three-tuple, and may be used to describe how the intent should be used and how it operates, as well as prescribe any operational dependencies that must be taken into account.

Although different intent categories share the same abstracted intent model, each category will have its own specific context, capabilities and constraints.

5.2. Intent User Types

Expanding on the introduction in section 4.2. , intent user types represent the intent users that define and issue the intent request. Depending on the intent solutions, there are specific intent users. Examples of intent users are customers, network operators, service operators, enterprise administrators, cloud administrators, and underlay network administrators, or application developers.

- Customers and end-users do not necessarily know the functional and operational details of the network that they are using. Furthermore, they lack skills to understand such details; in fact, such knowledge is typically not relevant to their job. In addition, the network may not expose these details to its intent users. This class of intent users focuses on the applications that they run, and uses services offered by the network. Hence, they want to specify policies that provide consistent behaviour according to their business needs. They do not have to worry about how the intents are deployed onto the underlying network, and especially, whether the intents need to be translated to different forms to enable network elements to understand them.

- Application developers work in a set of abstractions defined by their application and programming environment(s). For example, many application developers think in terms of objects (e.g., a VPN). While this makes sense to the application developer, most network devices do not have a VPN object per se; rather, the VPN is formed through a set of configuration statements for that device in concert with configuration statements for the other devices that together make up the VPN. Hence, the view of application developers matches the services provided by the network, but may not directly correspond to other views of other intent users.

- Network operators may have the knowledge of the underlying network. However, they may not understand the details of the applications and services of customers.

5.3. Intent Scope

Intents are used to manage the behaviour of the networks they are applied to and all intents are applied within a specific scope, such as:

- Connectivity scope, if the intent creates or modifies a connection.
- Security/privacy scope, if the intent specifies the security characteristics of the network, customers, or end-users.
- Application scope, when the intent specifies the applications to be affected by the intent request.
- QoS scope, when the intent specifies the QoS characteristics of the network.

These intent scopes are expendable through the methodology presented in section 6.1. .

5.4. Intent Network Scope

Regardless on the intent user type, their intent request is affecting the network, or network components, which are representing the intent targets.

Thus, intent network scope, or policy target as known in the area of declarative policy, can represent VNFs or PNFs, physical network elements, campus networks, SD-WAN networks, radio access networks, cloud edge, cloud core, branch, etc.

5.5. Intent Abstraction

Intent can be classified by whether it is necessary to feedback technical network information or non-technical information to the intent user after the intent is executed. As well, intent abstraction covers the level of technical details in the intent itself.

- For non-technical intent users, they do not care how the intent is executed, or the details of the network. As a result, they do not need to know the configuration information of the underlying network. They only focus on whether the intent execution result achieves the goal, and the execution effect such as the quality of completion and the length of execution. In this scenario, we refer to an abstraction without technical feedback.

- For administrators, such as network administrators, they perform intents, such as allocating network resources, selecting transmission paths, handling network failures, etc. They require multiple feedback indicators for network resource conditions, congestion conditions, fault conditions, etc. after execution. In this case, we refer to an abstraction with technical feedback.

As per intent definition provided in [CLEMM], lower-level intents are not considered to qualify as intents. However, we kept this classification to identify any PoCs/Demos/Use Cases that still either require or implement lower level of abstraction for intents.

5.6. Intent Life-cycle

Intents can be classified into transient and persistent intents:

- If the intent is transient, it has no life-cycle management. As soon as the specified operation is successfully carried out, the intent is finished, and can no longer affect the target object.

- If the intent is persistent, it has life-cycle management. Once the intent is successfully activated and deployed, the system will keep all relevant intents active until they are deactivated or removed.

5.7. Autonomous Driving Levels

In different phases of the autonomous driving network [TMF-auto], the intents are different. Depending on the Autonomous Network Level of the overall solution, we may have different intent requirements and

types. For example, at lower level the customer intent is automatically converted to configuration policies only, while at the higher levels the customer intent is covering the full life cycle, it is converted to both configuration and monitoring policies and is self-assured using AI.

A typical example of autonomous driving network level 0 to 5 are listed as below.

- Level 0 - Traditional manual network: O&M personnel manually control the network and obtain network alarms and logs. - No intent

- Level 1 - Partially automated network: Automated scripts are used to automate service provisioning, network deployment, and maintenance. Shallow perception of network status and decision making suggestions of machine; - No intent

- Level 2 - Automated network: Automation of most service provisioning, network deployment, and maintenance of a comprehensive perception of network status and local machine decision making; - simple intent on service provisioning

- Level 3 - Self-optimization network: Deep awareness of network status and automatic network control, meeting requirements of intent users of the network. - Intent based on network status cognition

- Level 4 - Partial autonomous network: In a limited environment, people do not need to participate in decision-making and networks can adjust itself. - Intent based on limited AI

- Level 5 - Autonomous network: In different network environments and network conditions, the network can automatically adapt to and adjust to meet people's intentions. - Intent based on AI

6. Intent Classification

This section proposes an intent classification approach that may help to classify mainstream intent related demos/tools.

The three classifications in this document have been proposed from scratch, following the methodology presented, through three iterations: one for carrier network intent solution, one for DC intent solution, and one for enterprise intent solution. For each intent solution, we identified the specific intent users and intent types. Then, we further identified intent scope, network scope, abstractions, and life-cycle requirements.

These classifications and the generated tables can be easily extended. For example, for the DC intent solution, a new category is identified, i.e. resource scope, and the classification table has been extended accordingly.

In the future, as new scenarios, applications, and domains are emerging, new classifications and taxonomies can be identified, following the proposed methodology.

The intent classifications have been documented to the best of our knowledge at this point in time. Additional classifications will most probably see the light in the future.

The output of the intent classification is the intent taxonomy introduced in the next sections.

Thus, this section first introduces the proposed intent classification methodology, followed by consolidated intent taxonomy for three intent solutions, and then by concrete examples of intent classifications for three different intent solutions (e.g. carrier network, data center, and enterprise) that were derived using the proposed methodology and then can be filled in for PoCs, demos, research projects or future drafts.

6.1. Intent Classification Methodology

This section describes the methodology used to derive the initial classification proposed in the draft. The proposed methodology can be used to create new intent classifications from scratch, by analysing the solution knowledge. As well, the methodology can be used to update existing classification tables by adding or removing different solutions, intent users or intent types in order to cater for future scenarios, applications or domains.

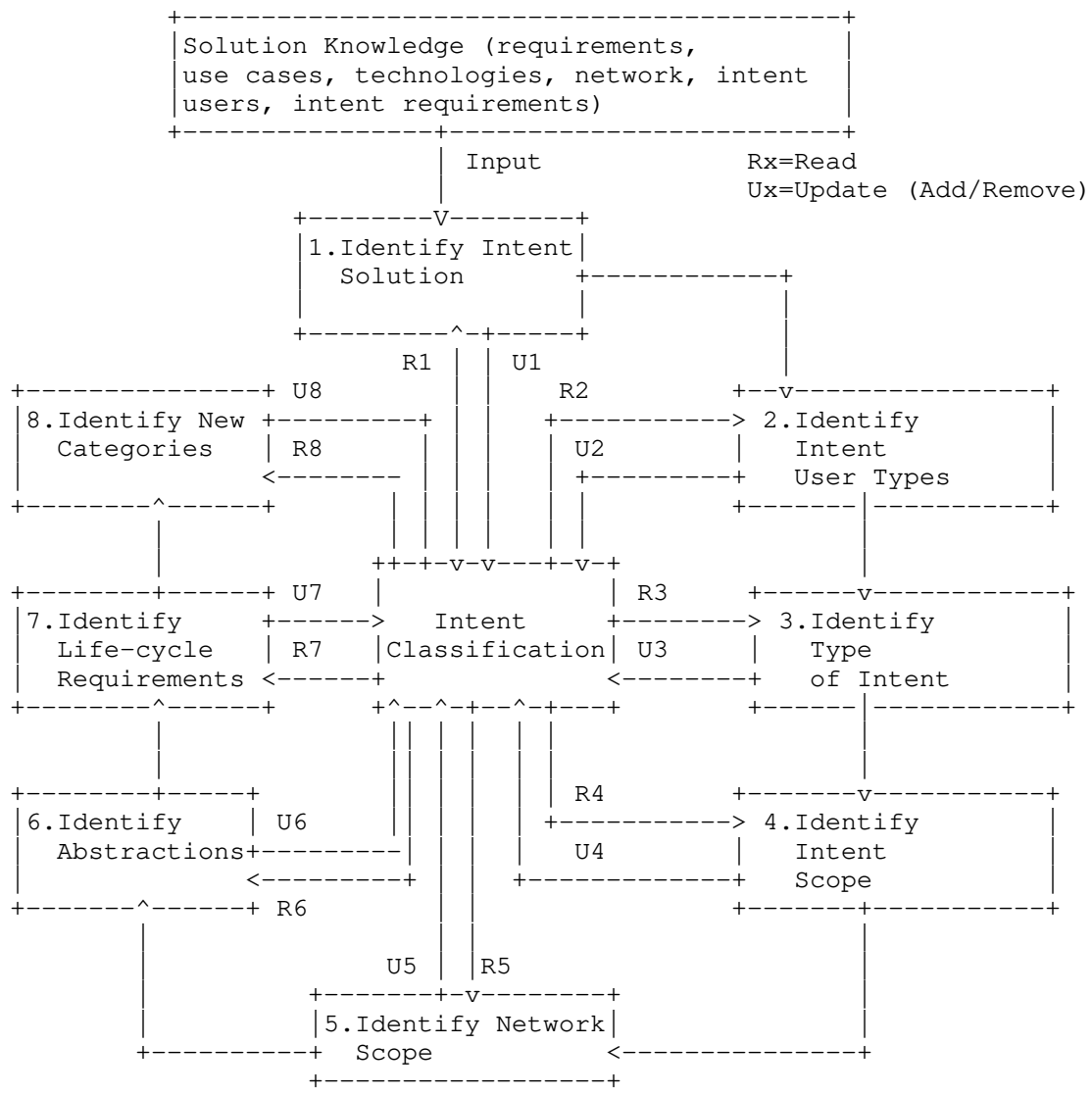

Figure 1 - Intent Classification Methodology

The intent classification workflow starts from the solution knowledge, which can provide information on requirements, use cases, technologies used, network properties, intent users that define and issue the intent request, and requirements. The following, defines the steps to classify an intent:

1. The information provided in the solution knowledge is given as input for identifying the intent solution (e.g. carrier, enterprise, and data center). Intent solutions are reviewed against the existing classification and they can either be used if present or added if not there or removed if not needed, from the classification. (R1-U1).

2. Identify the intent user types (e.g. customer, network operators, service operators, etc.), review existing intent classification and use the intent user type if present, add if it is not there or remove it if not needed (R2-U2).

3. Identify the types of intent (e.g. network intent, customer service intent) and then review existing classification and use/add/remove the intent type (R3-U3).

4. Identify the intent scopes (e.g. connectivity, application) based on the solution knowledge and then review existing classification and use/add/remove the identified intent scope (R4-U4).

5. Identify the network scopes (e.g. campus, radio access) and then review existing classification and either use it or add/remove the identified network scope (R5-U5).

6. Identify the abstractions (e.g. technical, non-technical) and then review existing classification and use/add/remove the abstractions (R6-U6).

7. Identify the life-cycle requirements (e.g. persistent, transient) and then review existing classification and use/add/remove the life-cycle requirements (R7-U7).

8. Identify any new categories and use/add the newly identified categories. New categories can be identified as new domains or applications are emerging, or new areas of concern (e.g. privacy, compliance) might arise, which are not listed in the current methodology.

6.2. Intent Taxonomy

The following taxonomy describes the various intent solutions, intent user types, intent types, intent scopes, network scopes, abstractions and life-cycle and represents the output of the intent classification tables for each of the solutions addressed (i.e. carrier, data center, and enterprise solutions).

The intent scope categories in Figure 2 are shared among the carrier, DC, and enterprise solutions. The abbreviations (Cx) in sections 6.3.2. 6.4.2. are introduced with the scope of fitting as column title in the following tables.

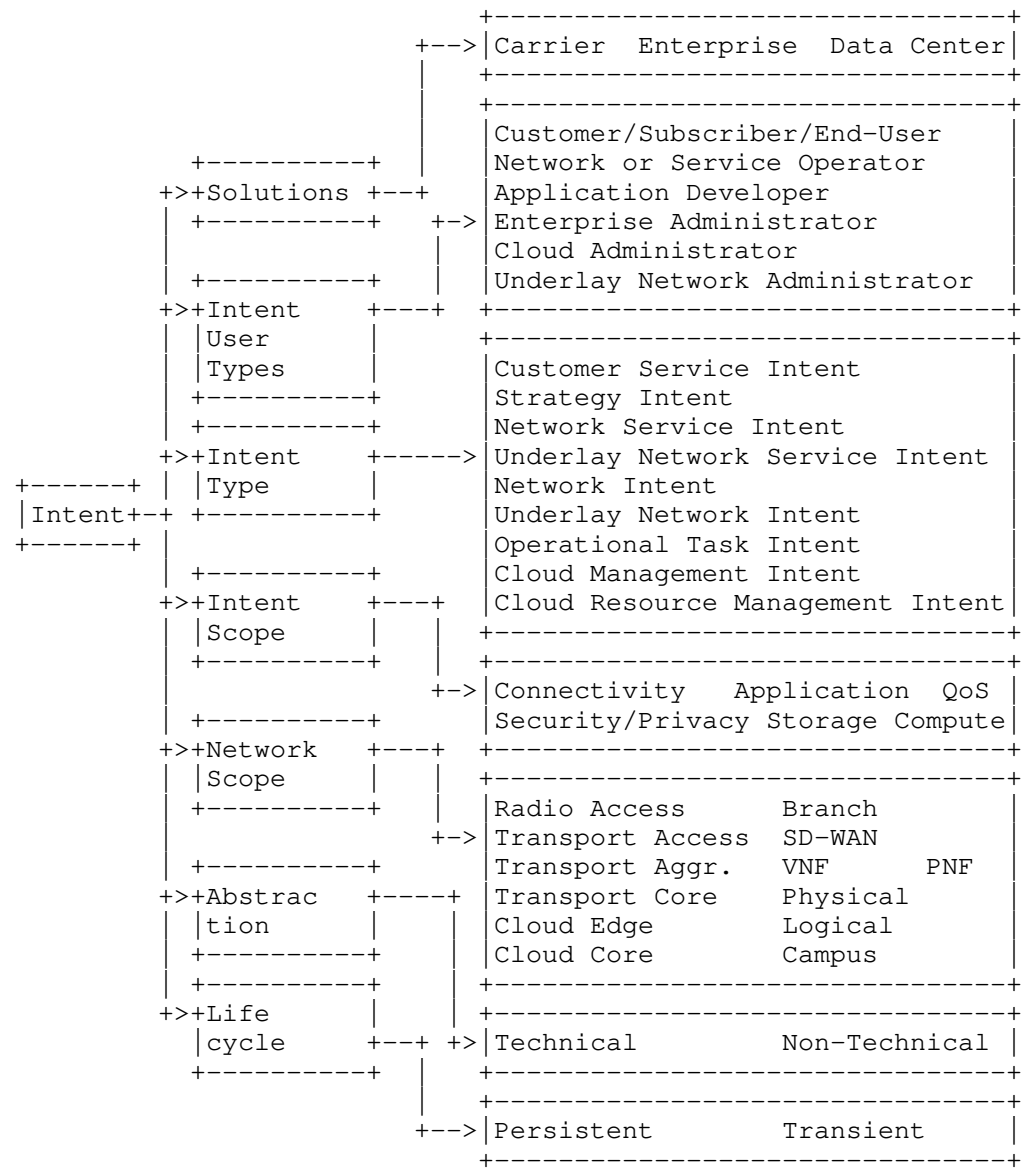

Figure 2 - Intent Taxonomy

6.3. Intent Classification for Carrier Solution

6.3.1. Intent Users and Intent Types

This section addresses step 1, 2, and 3 from Figure 1 and the following table describes the intent users in carrier solutions and intent types with their descriptions for different intent users.

Intent User	Intent Type	Intent Type Description
Customer/ Subscriber	Customer Service Intent	Customer self-service with SLA and value added service Example: Always maintain high quality of service and high bandwidth for gold level subscribers. Operational statement: Measure the network congestion status, give different adaptive parameters to stations of different priority, thus in heavy load situation, make the bandwidth of the high-priority customers guaranteed. At the same time ensure the overall utilization of system, improve the overall throughput of the system.
	Strategy Intent	Customer designs models and policy intents to be used by customer service intents. Example: Request reliable service during peak traffic periods for apps of type video.
Network Operator	Network Service Intent	Service provided by network service operator to the customer (e.g. the service operator) Example: Request network service with delay guarantee for access customer A.
	Network Intent	Network operator requests network-wide (service underlay or other network-wide

		configuration) or network resource configurations (switches, routers, routing, policies). Includes connectivity, routing, QoS, security, application policies, traffic steering policies, configuration policies, monitoring policies, alarm generation for non-compliance, auto-recovery, etc. Example: Request high priority queueing for traffic of class A.
	Operational Task Intent	Network operator requests execution of any automated task other than network service intent and network intent (e.g. network migration, server replacements, device replacements, network software upgrades). Example: Request migration of all services in network N to backup path P.
	Strategy Intent	Network operator designs models, policy intents and workflows to be used by network service Intents, network intents and operational task intents. Workflows can automate any tasks that network operator often performed in addition to network service intents and network intents Example: Ensure the load on any link in the network is not higher than 50%.

Service Operator	Customer Service Intent	Service operator's customer orders, customer service / SLA Example: Provide service S with guaranteed bandwidth for customer A.
	Network Service Intent	Service operator's network orders / network SLA Example: Provide network guarantees in terms of security, low latency and high bandwidth
	Operational Task Intent	Service operator requests execution of any automated task other than customer service intent and network service intent Example: Update service operator portal platforms and their software regularly. Move services from network operator 1 to network operator 2.
	Strategy Intent	Service operator designs models, policy intents and workflows to be used by customer service intents, network service intents and operational task intents. Workflows can automate any tasks that service operator often performed in addition to network service intents and network intents. Example: Request network service guarantee to avoid network congestion during special periods such as black Friday, and Christmas.
Application Developer	Customer Service Intent	Customer service intent API provided to the application developers Example: API to request network to watch HD video 4K/8K.

		Network Service Intent	Network service intent API provided to the application developers Example:API to request network service , monitoring and traffic grooming.
		Network Intent	Network intent API provided to the application developers Example: API to request network resources configuration.
		Operational Task Intent	Operational task intent API provided to the application developers. This is for the trusted internal operator / service providers / customer DevOps Example: API to request server migrations.
		Strategy Intent	Application developer designs models, policy and workflows to be used by customer service intents, network service intents and operational task intents. This is for the trusted internal operator/service provider/ customer DevOps Example: API to design network load balancing strategies during peak times

Table 2 - Intent Classification for Carrier Solution

6.3.2. Intent Categories

This subsection addresses step 4 to 7 from Figure 1, and the following are the proposed categories:

- Intent Scope: C1=Connectivity, C2=Security/Privacy, C3=Application, C4=QoS
- Network Scope:
  - Network Domain: C1=Radio Access, C2=Transport Access, C3=Transport Aggregation, C4=Transport Core, C5=Cloud Edge, C6=Cloud Core)
  - Network Function (NF) Scope: C1=VNFs, C2=PNFs
- Abstraction (ABS): C1=Technical (with technical feedback), C2=Non-technical (without technical feedback) see section 5.2. .
- Life-cycle (L-C): C1=Persistent (full life-cycle), C2=Transient (short lived)

6.3.3. Intent Classification Example

This section depicts an example on how the methodology described in section 6.1. can be used in order to classify intents introduced in the 'A Multi-Level Approach to IBN' PoC demonstration [POC-IBN]. This PoC is led by academics carrying research in the area of SDN/NFV and the specific problem they are addressing is to apply the intent concept at different levels that correspond to different stakeholders. For this research work, they considered two types of intents: slice intents and service chain intents.

In this PoC [POC-IBN], a slice intent expresses a request for a network slice with two types of components: a set of top layer virtual functions, and a set of virtual switches and/or routers of L2/L3 VNFs. A service chain intent expressed a request for a service operated through a chain of service components running in L4-L7 virtual functions.

Following the intent classification methodology described step-by-step in section 6.1. , the following can be derived:

1. The intent solution for both intents is carrier network.

2. The intent user type is network operator for the slice intent, and service operator for the service chain intent.

3. The type of intent, is a network service intent for the slice intent, and a customer service intent for the service chain intent.

4. The intent scopes are connectivity and application.

5. The network scope is VNF, cloud edge, and cloud core.

6. The abstractions are with technical feedback for the slice intent, and without technical feedback for the service chain intent

7. The life-cycle is persistent.

The following table shows how to represent this information in a tabular form. The 'X' in the table refers to the slice intent, and the 'Y' in the table refers to the service chain intent.

Intent User	Intent Type	Intent Scope				NF Scope		Network Scope						ABS		L-C	
		C1	C2	C3	C4	C1	C2	C1	C2	C3	C4	C5	C6	C1	C2	C1	C2
Customer / Sub-scriber	Customer Service Intent																
	Strategy Intent																
Network Operator	Network Service Intent	X		X		X						X		X		X	
	Network Intent																
	Operatio-nal Task Intent																
	Strategy Intent																
Service Operator	Customer Service Intent	Y		Y		Y						Y	Y		Y	Y	
	Network Service Intent																
	Op Task Intent																
	Strategy Intent																

App Developer	Customer Intent																
	Network Service Intent																
	Network Intent																
	Op Task Intent																
	Strategy Intent																

Table 3 - Intent Classification Example for Carrier Solution

6.4. Intent Classification for Data Center Network Solutions

6.4.1. Intent Users and Intent Types

The following table describes the intent users in DC network solutions and intent types with their descriptions for different intent users.

Intent User	Intent Type	Intent Type Description
Customer / Tenants	Customer Service	Customer self-service via tenant portal. Example: Request GPU computing and storage resources to meet 10k video surveillance services.
	Strategy Intent	This includes models and policy intents designed by customers/ tenants to be reused later during instantiation. Example: Request dynamic computing and storage resources of the service in special and daily times.
Cloud Administrator	Cloud Management Intent	Configuration of VMs, DB Servers, app servers, connectivity, communication between VMs. Example: Request connectivity between VMs A,B,and C in network N1.
	Cloud Resource Management Intent	Policy-driven self-configuration and and recovery / optimization Example: Request automatic life -cycle management of VM cloud resources.
	Operational Task Intent	Cloud administrator requests execution of any automated task other than cloud management intents and cloud resource management intents. Example: Request upgrade operating system to version X on all VMs in network N1.

		Operational statement: an intent to update a system might reconfigure the system topology (connect to a service and to peers), exchange data (update the content), and uphold a certain QoE level (allocate sufficient network resources). The network, thus, carries out the necessary configuration to best serve such an intent; e.g. setting up direct connections between terminals, and allocating fair shares of router queues considering other network services.
	Strategy Intent	Cloud administrator designs models, policy intents and workflows to be used by other intents. Automate any tasks that administrator often performs, in addition to life-cycle of cloud management intents and cloud management resource intents. Example: In case of emergency, automatically migrate all cloud resources to DC2.
Underlay Network Administrator	Underlay Network Service Intent	Service created and provided by the underlay network administrator. Example: Request underlay service between DC1 and DC2 with bandwidth B.
	Underlay Network Intent	Underlay network administrator requests some DCN-wide underlay network configuration or network resource configurations. Example: Establish and allocate DHCP address pool.
	Operational Task Intent	Underlay network administrator requests execution of the any automated task other than underlay network service and resource

		intent. Example: Request automatic rapid detection of device failures and pre-alarm correlation.
	Strategy Intent	Underlay network administrator designs models, policy intents & workflows to be used by other intents. Automate any tasks that administrator often performs. Example: For all traffic flows that need NFV service chaining, restrict the maximum load of any VNF node/container below 50% and the maximum load of any network link below 70%.
Application Developer	Cloud Management Intent	Cloud management intent API provided to the application developers. Example: API to request configuration of VMs, or DB Servers.
	Cloud Resource Management Intent	Cloud resource management intent API provided to the application developers. Example: API to request automatic life-cycle management of cloud resources.
	Underlay Network Service Intent	Underlay network service API provided to the application developers. Example: API to request real-time monitoring of device condition.
	Underlay Network Intent	Underlay network resource API provided to the application developers. Example: API to request dynamic management of IPv4 address pool resources.

		Operational Task Intent	Operational task intent API provided to the trusted application developer (internal DevOps). Example: API to request automatic rapid detection of device failures and pre-alarm correlation
		Strategy Intent	Application developer designs models, policy intents and building blocks to be used by other intents. This is for the trusted internal DCN DevOps. Example: API to request load balancing thresholds.

Table 4 - Intent Classification for Data Center Network Solutions

6.4.2. Intent Categories

The following are the proposed categories:

- o Intent Scope: C1=Connectivity, C2=Security/Privacy, C3=Application, C4=QoS C5=Storage C6=Compute
- o Network Scope
  - o Network Domain: DC Network
  - o DCN Network (DCN Net) Scope: C1=Logical, C2=Physical
  - o DCN Resource (DCN Res) Scope: C1=Virtual, C2=Physical
- o Abstraction (ABS): C1=Technical (with technical feedback), C2=Non-technical (without technical feedback), see section 5.2.
- o Life-cycle (L-C): C1=Persistent (full life-cycle), C2=Transient (short lived)

6.4.3. Intent Classification Example

This section depicts an example on how the methodology described in section 6.1. can be used by the research community to classify intents. As mentioned in 6.3.3. a successful use of the classification proposed in this draft is introduced in the 'A Multi-Level Approach to IBN' PoC demonstration [POC-IBN]. The PoC is led by academics carrying research in the area of SDN/NFV and the specific problem they are addressing is to apply the intent concept at different levels that correspond to different stakeholders.

For their research work, they considered two types of intents: slice intents and service chain intents. For the data center solution, only the slice intent is relevant.

As already mentioned in section 6.3.3. , a slice intent expresses a request for a network slice with two types of components: a set of top layer virtual functions, and a set of virtual switches and/or routers of L2/L3 VNFs.

Following the intent classification methodology described step-by-step in section 6.1. , we identify the following:

1. The intent solution is for the data center.

2. The intent user type is the cloud administrator for the slice intent and service chain intent.

3. The type of intent, is a cloud management intent, for the slice intent.

4. The intent scopes are connectivity and application.

5. The network scope is logical, and the resource scope is virtual.

6. The abstractions are with technical feedback for the slice intent.

7. The life-cycle is persistent.

The following table shows how to represent this information in a tabular form, where the 'X' in the table refers to the slice intent.

Intent User	Intent Type	Intent Scope						DCN Res		DCN Net		ABS		L-C	
		C1	C2	C3	C4	C5	C6	C1	C2	C1	C2	C1	C2	C1	C2
Customer /Tenants	Customer Service Intent														
	Strategy Intent														
Cloud Admin	Cloud Management Intent	X		X				X		X		X		X	
	Cloud Resource Management Intent														
	Operational Task Intent														
	Strategy Intent														
Underlay Network Admin	Underlay Network Intent														
	Underlay Network Resource Intent														
	Operational Task Intent														
	Strategy														

	Intent
App Developer	Cloud Management Intent
	Cloud Resource Management Intent
	Underlay Network Intent
	Underlay Network Resource Intent
	Operational Task Intent
	Strategy Intent

Table 5 - Intent Classification Example for Data Center Network Solutions

6.5. Intent Classification for Enterprise Solution

6.5.1. Intent Users and Intent Types

The following table describes the intent users in enterprise solutions and their intent types.

Intent User	Intent Type	Intent Type Description
End-User	Customer Service Intent	Enterprise end-user self-service or applications, enterprise may have multiple types of end-users. Example: Request access to VPN service. Request video conference between end-user A and B.
	Strategy Intent	This includes models and policy intents designed by end-users to be used by end-user intents and their applications. Example: Create a video conference type for a weekly meeting.
Enterprise Administrator (internal or MSP)	Network Service Intent	Service provided by the administrator to the end-users and their applications. Example: For any end-user of application X, the arrival of hologram objects of all the remote tele-presenters should be synchronised within 50ms to reach the destination viewer for each conversation session. Create management VPN connectivity for type of service A. Operational statement: The job of the network layer is to ensure that the delay is between 50-70ms through

		the routing algorithm. At the same time,the node resources need to meet the bandwidth requirements of 4K video conferences.
	Network Intent	Administrator requires network wide configuration (e.g. underlay, campus) or resource configuration (switches, routers, policies). Example: Configure switches in campus network 1 to prioritise traffic of type A. Configure YouTube as business non-relevant.
	Operational Task Intent	Administrator requests execution of any automated task other than network service intents and network intents. Example: Request network security automated tasks such as web filtering and DDOS cloud protection.
	Strategy Intent	Administrator designs models, policy intents and workflows to be used by other intents. Automate any tasks that administrator often performs. Example: In case of emergency, automatically shift all traffic of type A through network N.
Application Developer	End-User Intent	End-user service / application intent API provided to the application developers. Example: API for request to open a VPN service.
	Network Service Intent	Network service API provided to application developers. Example: API for request network

		bandwidth and latency for hosting video conference.
	Network Intent	Network API provided to application developers. Example: API for request of network devices configuration.
	Operational Task Intent	Operational task intent API provided to the trusted application developer (internal DevOps). Example: API for requesting automatic monitoring and interception for network security
	Strategy Intent	Application developer designs models, policy intents and building blocks to be used by other intents. This is for the trusted internal DevOps. Example: API for strategy intent in case of emergencies.

Table 6 - Intent Classification for Enterprise Solution

6.5.2. Intent Categories

The following are the proposed categories:

- Intent Scope: C1=Connectivity, C2=Security/Privacy, C3=Application, C4=QoS
- Network (Net) Scope: C1=Campus, C2=Branch, C3=SD-WAN
- Abstraction (ABS): C1=Technical (with technical feedback), C2=Non-technical (without technical feedback), see section 5.2.
- Life-cycle (L-C): C1=Persistent (full life-cycle), C2=Transient (short lived)

The following is the intent classification table example for enterprise solutions.

Intent User	Intent Type	Intent Scope				Net			ABS		L-C	
		C1	C2	C3	C4	C1	C2	C3	C1	C2	C1	C2
End-User	Customer Service Intent											
	Strategy Intent											
Enterprise Administrator	Network Service Intent											
	Network Intent											
	Operational Task Intent											
	Strategy Intent											
Application Developer	End-User Intent											
	Network Service Intent											
	Network Intent											

	Operational Task Intent											
	Strategy Intent											

Table 7 - Intent Categories for Enterprise Solution

7. Conclusions

This document is aligned with the RG objectives and supports investigations into intent-based networking by proposing an intent categorization methodology and taxonomy. It brings clarification on what an intent represents for different stakeholders through the proposal of an Intent Classification approach, ensuring that a common understanding among all the participants exists. This, together with the proposed intent taxonomy provides a solid foundation for future intent-related topic discussions within NMRG.

The benefits of this intent classification draft in the research community have been demonstrated through a PoC implementation [POC-IBN] in which the draft's concepts at different levels corresponding to different stakeholders have been applied to.

8. Security Considerations

This document identifies the security and privacy as categories of the intent scope. The intents could be solely security intents and privacy intents or security can be embedded in the intents that include also connectivity, application, and QoS scope.

Security and privacy scope, is when the intent specifies the security characteristics of the network, customers, or end-users, and privacy for customers and end-users.

More details of these security intents would be described in future documents that specify architecture, functionality, user intents and models. As well, an analysis of the security considerations of the overall intent-based system is provided in section 10 of [CLEMM].

9. IANA Considerations

This document has no actions for IANA.

10. Contributors

The following people all contributed to creating this document:

Contributed significant text:

Xueyuan Sun, China Telecom
Will (Shucheng) Liu, Huawei

Contributed text in early drafts:
Ying Chen, China Unicom
John Strassner, Huawei
Weiping Xu, Huawei
Richard Meade, Huawei

11. Acknowledgments

This document has benefited from reviews, suggestions, comments and proposed text provided by the following members, listed in alphabetical order: Mehdi Bezahaf, Brian E Carpenter, Laurent Ciavaglia, Benoit Claise, Alexander Clemm, Yehia Elkhatib, Jerome Francois, Pedro Andres Aranda Gutierrez, Daniel King, Branislav Meandzija, Bob Natale, Juergen Schoenwaelder, Xiaolin Song, Jeff Tantsura.

We thank to Barbara Martini, Walter Cerroni, Molka Gharbaoui, Davide Borsatti, for contributing with their 'A multi-level approach to IBN' PoC demonstration a first attempt to adopt the intent classification methodology.

12. Informative References

[Bezahaf21] Bezahaf, M., Davies, E., Rotsos, C. and Race, N., "To All Intents and Purposes: Towards Flexible Intent Expression," 2021 IEEE 7th International Conference on Network Softwarization (NetSoft), 2021.

[Bezhaf19] Bezahaf, M., Hernandez, MP, Bardwell, L., Davies, E., Broadbent, M.,King, D. and Hutchison, D. , "Self-Generated Intent-Based System," 2019 10th International Conference on Networks of the Future (NoF), 2019.

[Jacobs18] Jacobs, A.S., Pfitscher,R.J., Ferreira, R.A., and Granville, L.Z., "Refining Network Intents for Self-Driving Networks", Proceedings of the Afternoon Workshop on Self-Driving Networks (SelfDN 2018), 2018.

[Banerjee21] Banerjee,A., Mwanje. S. and Carle, G., "Contradiction Management in Intent-driven Cognitive Autonomous RAN", 2021.

[Tian19] Tian, B., Zhang, X., Zhai, E., Liu, H. H., Ye, Q., Wang, C., and Zhao, B. Y., "Safely and automatically updating in-network ACL configurations with intent language", SIGCOMM '19, 2019.

[Leivadeas21] Leivadeas, A. and Falkner, M., "VNF Placement Problem: A Multi-Tenant Intent-Based Networking Approach," 24th Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), 2021.

[Davoli21] Davoli, G., "Programmability and Management of Software-defined Network Infrastructures", 2021.

[Padovan20] Padovan, S., "Design and Implementation of a Blockchain Intent Management System", 2020.

[Mehmood21] Mehmood, K., Kralevska, K., and Palma, D., "Intent-driven Autonomous Network and Service Management in Future Networks: A Structured Literature Review", 2021.

[Szilagyi21] Szilagyi, P., "I2BN: Intelligent Intent Based Networks", Journal of ICT Standardization, 2021.

[POC-IBN] Barbara Martini, Walter Cerroni, Molka Gharbaoui, Davide Borsatti, "A multi-level approach to IBN", July 2020, https://www.ietf.org/proceedings/108/slides/slides-108-nmrg-ietf-108-hackathon-report-a-multi-level-approach-to-ibn-02

[IFIP-NSM] IFIP - Network and Service Management Taxonomy, https://www.simpleweb.org/ifip/taxonomy.html

[ONF] ONF, "Intent Definition Principles", 2017, <https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR-523_Intent_Definition_Principles.pdf>.

[ONOS] ONOS, "ONOS Intent Framework", 2017, <https://wiki.onosproject.org/display/ONOS/Intent+Framework/>.

[CLEMM] A. Clemm, L. Ciavaglia, L. Granville, J. Tantsura, "Intent-Based Networking - Concepts and Overview", Work in Progress, draft-irtf-nmrg-ibn-concepts-definitions-05, February 2021, https://tools.ietf.org/html/draft-irtf-nmrg-ibn-concepts-definitions-05

[TMF-auto] Aaron Richard Earl Boasman-Patel,et, A whitepaper of Autonomous Networks: Empowering Digital Transformation For the Telecoms Industry, inform.tmforum.org, 15 May, 2019.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC7575] Behringer, M., Pritikin, M., Bjarnason, S., Clemm, A., Carpenter, B., Jiang, S., and L. Ciavaglia, "Autonomic Networking: Definitions and Design Goals", RFC 7575, June 2015.

[RFC8328] Liu, W., Xie, C., Strassner, J., Karagiannis, G., Klyus, M., Bi, J., Cheng, Y., and D. Zhang, "Policy-Based Management Framework for the Simplified Use of Policy Abstractions (SUPA)", March 2018.

[RFC3198] Westerinen, A., Schnizlein, J., Strassner, J., Scherling, M., Quinn, B., Herzog, S., Huynh, A., Carlson, M., Perry, J., Waldbusser, S., "Terminology for Intent-driven Management", RFC 3198, November 2001.

[RFC6020] Bjorlund, M., "YANG - A Data Modelling Language for Network Configuration Protocol (NETCONF)", RFC 6020, October 2010.

[RFC7285] R. Alimi, R. Penno, Y. Yang, S. Kiesel, S. Previdi, W. Roome, S. Shalunov, R. Woundy "Application-Layer Traffic Optimization (ALTO) Protocol", September 2014.

[ANIMA] Du, Z., "ANIMA Intent Policy and Format", 2017, <https://datatracker.ietf.org/doc/draft-du-anima-an-intent/>.

[SUPA] Strassner, J., "Simplified Use of Policy Abstractions", 2017, <https://datatracker.ietf.org/doc/draft-ietf-supa-generic-policy-info-model/?include_text=1>.

[ANIMA-Prefix] Jiang, S., Du, Z., Carpenter, B., and Q. Sun, "Autonomic IPv6 Edge Prefix Management in Large-scale Networks", draft-ietf-anima-prefix-management-07 (work in progress), December 2017.

Authors' Addresses

Chen Li
China Telecom
No.118 Xizhimennei street, Xicheng District
Beijing 100035
P.R. China
Email: lichen.bri@chinatelecom.cn

Olga Havel
Huawei Technologies
Ireland
Email: olga.havel@huawei.com

Adriana Olariu
Huawei Technologies
Ireland
Email: adriana.olariu@huawei.com

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

Jeferson Campos Nobre
Federal University of Rio Grande do Sul
Porto Alegre
Brazil
Email: jcnobre@inf.ufrgs.br

Diego R. Lopez
Telefonica I+D
Don Ramon de la Cruz, 82
Madrid 28006
Spain
Email: diego.r.lopez@telefonica.com